Invariant Theory

RWTH Aachen, WS 2022
Friedrich-Schiller-Universität Jena, WS 2004
RWTH Aachen, SS 2004
University of Leicester, WS 2003

Jürgen Müller

Contents

0 Introduction

Historical background. Invariant theory dates back to number theoretical considerations, on the representability of integers by binary quadratic forms, begun by LAGRANGE [1773], and later continued by GAUSS [1801] in his famous *Disquisitiones arithmeticae.*

The next landmark is the seminal work of BOOLE [1841], introducing the notion of transformation groups. Since then, invariant theory has developed into a centerpiece of 19^{th} century mathematics, with work done by HESSE, SYLVESTER, CAYLEY, CLEBSCH, GORDAN, LIE, KLEIN, and many more. A basic aim was to develop methods to construct infinitely many invariants of n-ary d-forms, coined 'concomitants' by SYLVESTER. This led CAYLEY to ask whether there are always finitely many 'basic invariants', polynomially generating all invariants. Contrary to the general believe, GORDAN [1868] showed their existence combinatorially for binary forms, earning him the title of 'king of invariant theory'.

The key breakthrough, in particular for the problem of finite generation, was achieved in two famous papers by HILBERT [1890, 1893], which laid the groundwork of modern abstract commutative algebra, and thus of modern algebraic geometry, in their aftermath followed by the work of NOETHER. Actually, while HILBERT was mainly interested in invariants for continuous groups, NOETHER's focus was on finite groups. Still, as the new abstract methods have been nonconstructive in the first place, this led to the famous exclamation of GORDAN, at this time being a dogmatic defender of the view that mathematics must be constructive: *Das ist Theologie und nicht Mathematik! — This is theology and not mathematics!* (Actually, it is reported that GORDAN [1899] has admitted: *I have convinced myself that theology also has its advantages.*)

1 Application: Quadratic forms

(1.1) Action on polynomial algebras. Let K be a field, let $K[\mathcal{X}]$ be the polynomial algebra in the indeterminates $\mathcal{X} := \{X_1, \ldots, X_n\}$, where $n \in \mathbb{N}_0$, and let $K[\mathcal{X}]_1 := \langle \mathcal{X} \rangle_K \leq K[\mathcal{X}]$ be the K-subspace generated by $\mathcal{X}$.

The general linear group $\mathrm{GL}_n(K)$ acts naturally (on the right) K-linearly on the K-vector space K^n. Viewing $K[\mathcal{X}]_1$ as the K-vector space of **linear forms** on K^n, where X_j is the j-th **coordinate function**, for $j \in \{1, \ldots, n\}$, the group $\mathrm{GL}_n(K)$ acts K-linearly by pre-composition on $K[\mathcal{X}]_1$, thus by the universal property of $K[\mathcal{X}]$ giving rise to K-algebra automorphisms of $K[\mathcal{X}]$ as follows:

For $A = [a_{ij}]_{ij} \in \mathrm{GL}_n(K)$ we have $({}^A X_j)(x_1, \ldots, x_n) = X_j([x_1, \ldots, x_n] \cdot A) = \sum_{i=1}^n x_i a_{ij} = (\sum_{i=1}^n a_{ij} X_i)(x_1, \ldots, x_n)$, for $x_1, \ldots, x_n \in K$. In other words we have ${}^A X_j := \sum_{i=1}^n X_i a_{ij} \in K[\mathcal{X}]_1$, that is $A \colon \mathcal{X} \mapsto \mathcal{X} \cdot A$. In terms of the K-basis $\mathcal{X} \subseteq K[\mathcal{X}]_1$, the K-linear map induced by A is given by $A^{\mathrm{tr}} \in K^{n \times n}$. In order to get a (right) action of $\mathrm{GL}_n(K)$ we let $(fA)(\mathcal{X}) := f(\mathcal{X} \cdot A^{-1}) \in K[\mathcal{X}]$, for $f \in K[\mathcal{X}]$; in particular the K-linear map on $K[\mathcal{X}]_1$ induced by A is given by $A^{-\mathrm{tr}} \in K^{n \times n}$, with respect to the K-basis $\mathcal{X} \subseteq K[\mathcal{X}]_1$.

(1.2) Quadratic forms. Let K be a field such that $\mathrm{char}(K) \neq 2$, let $n \in \mathbb{N}$, and let $K[\mathcal{X}]_2 \leq K[\mathcal{X}]$ be the K-subspace generated by the monomials of degree 2; we have $\dim_K(K[\mathcal{X}]_2) = \frac{n(n+1)}{2}$. A polynomial $q := \sum_{1 \leq i \leq j \leq n} q_{ij} X_i X_j \in K[\mathcal{X}]_2$ is called an **n-ary quadratic form** over K.

Then q gives rise to the polynomial map $K^n \to K \colon x = [x_1, \ldots, x_n] \mapsto q(x) = q(x_1, \ldots, x_n)$, which with a slight abuse is also called a quadratic form; thus the map $b \colon K^n \times K^n \to K \colon [x, y] \to \frac{1}{2}(q(x+y) - q(x) - q(y))$ is a symmetric K-bilinear form, and we have $b(x, x) = q(x)$ and the name-giving property $q(\lambda x) = \lambda^2 \cdot q(x)$, for $\lambda \in K$.

Let $K^{n \times n}_{\mathrm{sym}} := \{A \in K^{n \times n}; A^{\mathrm{tr}} = A\} \leq K^{n \times n}$ be the K-subspace of symmetric matrices; we have $\dim_K(K^{n \times n}_{\mathrm{sym}}) = \frac{n(n+1)}{2}$. The quadratic form q is associated with the **Gram matrix** $Q_q := [q'_{ij}]_{ij} \in K^{n \times n}_{\mathrm{sym}}$, where $q'_{ii} = q_{ii}$, and $q'_{ij} = q'_{ji} = \frac{1}{2} \cdot q_{ij}$ for $i < j$. This gives rise to an isomorphism of K-vector spaces $K[\mathcal{X}]_2 \to K^{n \times n}_{\mathrm{sym}} \colon q \mapsto Q_q$, such that conversely $q(\mathcal{X}) = \mathcal{X} \cdot Q_q \cdot \mathcal{X}^{\mathrm{tr}}$.

For $A \in \mathrm{GL}_n(K)$ we get $(qA)(\mathcal{X}) = (\mathcal{X} \cdot A^{-1}) \cdot Q_q \cdot (A^{-\mathrm{tr}} \cdot \mathcal{X}^{\mathrm{tr}})$, thus we have $Q_{qA} = A^{-1} \cdot Q_q \cdot A^{-\mathrm{tr}}$; recall that applying A amounts to applying base change of K^n. Quadratic forms q and q' are called **equivalent** if there is $A \in \mathrm{GL}_n(K)$ such that $q = q'A$, or equivalently $Q_{q'} = A \cdot Q_q \cdot A^{\mathrm{tr}}$.

Then $\mathrm{rk}(q) := \mathrm{rk}(Q_q) \in \{0, \ldots, n\}$ is called the **rank** of q, and $\Delta(q) := \det(Q_q) \in K$ is called the **discriminant** of q [Sylvester, 1852], Thus applying $A \in \mathrm{GL}_n(K)$ yields $\mathrm{rk}(qA) = \mathrm{rk}(q)$ and $\Delta(qA) = \det(A^{-1} \cdot Q_q \cdot A^{-\mathrm{tr}}) = \det(A)^{-2} \cdot \det(Q_q) = \det(A)^{-2} \cdot \Delta(q)$. In particular, the rank is a $\mathrm{GL}_n(K)$-invariant of quadratic forms, while the the discriminant of quadratic forms is invariant with respect to the special linear group $\mathrm{SL}_n(K)$.

(1.3) Complex quadratic forms. a) The classification of quadratic forms up to equivalence is highly dependent on the field K chosen, the simplest case being K algebraically closed. Here, we restrict ourselves to the complex numbers $\mathbb{C}$. Given an n-ary quadratic form $q \in \mathbb{C}[X_1, \ldots, X_n]_2 =: \mathcal{V}$, where $n \in \mathbb{N}$, let $[q] \subseteq \mathcal{V}$ be its equivalence class with respect to the action of $\mathrm{SL}_n(\mathbb{C})$.

Theorem. Any n-ary quadratic form is $\mathrm{SL}_n(\mathbb{C})$-equivalent to precisely one of:
i) $q_{n,\delta} := \delta X_n^2 + \sum_{i=1}^{n-1} X_i^2$, where $\delta \neq 0$; we have $\mathrm{rk}(q_{n,\delta}) = n$ and $\Delta(q_{n,\delta}) = \delta$.
ii) $q_r := \sum_{i=1}^{r} X_i^2$, where $r \in \{0, \ldots, n-1\}$; we have $\mathrm{rk}(q_r) = r$ and $\Delta(q_r) = 0$.

Moreover, all the forms $q_{n,\delta}$ for $\delta \neq 0$ are $\mathrm{GL}_n(\mathbb{C})$-equivalent.

Proof. We show that the Gram matrix Q of any quadratic form q of rank $r := \mathrm{rk}(q)$ is $\mathrm{SL}_n(\mathbb{C})$-diagonalizable (by mimicking the proof of **Sylvester's Theorem of Inertia**):

We may assume that $q \neq 0$. Since $\mathrm{SL}_n(\mathbb{C})$ acts transitively on $\mathbb{C}^n \setminus \{0\}$, we may choose a $\mathbb{C}$-basis of $\mathbb{C}^n$ whose first element, v say, is **non-isotropic**, that is $q(v) \neq 0$. Since any unitriangular matrix belongs to $\mathrm{SL}_n(\mathbb{C})$, by the standard orthogonalization procedure we may complement this by a $\mathbb{C}$-basis of the orthogonal complement $\langle v\rangle_{\mathbb{C}}^{\perp} \leq \mathbb{C}^n$, with respect to the $\mathbb{C}$-bilinear form induced by q. Hence by induction on $n \in \mathbb{N}$ we may assume that $q = \sum_{i=1}^{r} \delta_i X_i^2$, where $\delta_i \neq 0$. (So far the argument works for any field K such that $\mathrm{char}(K) \neq 2$.)

If $r < n$, letting $A := \mathrm{diag}[\epsilon_1, \ldots, \epsilon_r, 1, \ldots, 1, (\prod_{i=1}^{r} \epsilon_i)^{-1}] \in \mathrm{SL}_n(\mathbb{C})$, where $\epsilon_i^2 = \delta_i$ for $i \in \{1, \ldots, r\}$, we get $qA = \sum_{i=1}^{r} \delta_i \epsilon_i^{-2} X_i^2 = q_r$. (The argument given so far, and in the sequel, only uses the fact that $(K^*)^2 = K^*$; for $K = \mathbb{R}$, where $[\mathbb{R}^* \colon (\mathbb{R}^*)^2] = 2$, we recover the **signature** from Sylvester's Theorem.)

If $r = n$, letting $A := \mathrm{diag}[\epsilon_1, \ldots, \epsilon_{n-1}, \epsilon^{-1}] \in \mathrm{SL}_n(\mathbb{C})$, where $\epsilon_i^2 = \delta_i$ for $i \in \{1, \ldots, n-1\}$, and $\epsilon := \prod_{i=1}^{n-1} \epsilon_i$, we get $qA = \delta_n \epsilon^2 X_n^2 + \sum_{i=1}^{n-1} \delta_i \epsilon_i^{-2} X_i^2 = q_{n,\delta_n \epsilon^2}$. Finally, letting $A := \mathrm{diag}[1, \ldots, 1, \epsilon] \in \mathrm{GL}_n(\mathbb{C})$, where $\epsilon^2 = \delta$, we get $q_{n,\delta} A = \delta \epsilon^{-2} X_n^2 + \sum_{i=1}^{n-1} X_i^2 = q_{n,1}$. ♯

b) Apart from the algebraic picture, we also have the complex metric topology at our disposal. (Actually, the arguments to follow remain valid for any algebraically closed field $\mathbb{K}$ such that $\mathrm{char}(\mathbb{K}) \neq 2$, and regular maps with respect to the Zariski topology.)

We may view the discriminant $\Delta \colon \mathcal{V} \to \mathbb{C}$ as a polynomial map, in particular as a continuous map. Its fiber associated with $\delta \in \mathbb{C}$ is the hypersurface $\Delta^{-1}(\delta) \subseteq \mathcal{V}$, which hence is closed. Moreover, since Δ is $\mathrm{SL}_n(\mathbb{C})$-invariant, $\Delta^{-1}(\delta)$ consists of a union of equivalence classes: For $\delta \neq 0$ we have $\Delta^{-1}(\delta) = [q_{n,\delta}]$, while $\Delta^{-1}(0) = \coprod_{r=0}^{n-1} [q_r]$ is a proper union of equivalence classes for $n \geq 2$; note that $[q_0] = \{q_0\}$ is a singleton set.

Thus $[q_{n,\delta}] \subseteq \mathcal{V}$ is closed for $\delta \neq 0$. But for $\delta = 0$ this is different, where for $r \in \{0, \ldots, n-1\}$ the closure of $[q_r] \subseteq \mathcal{V}$ equals $\overline{[q_r]} = \coprod_{s=0}^{r} [q_s] \subseteq \mathcal{V}$:

Since $\mathrm{SL}_n(\mathbb{C})$ acts by homeomorphisms, $\overline{[q_r]}$ is $\mathrm{SL}_n(\mathbb{C})$-invariant as well, hence is a union of equivalence classes. Since $\{M \in \mathbb{C}^{n\times n}; \mathrm{rk}(M) \leq r\} \subseteq \mathbb{C}^{n\times n}$ coincides with the set of all matrices all of whose $((r+1) \times (r+1))$-minors vanish, we conclude that the latter set is closed. Hence $\{M \in \mathbb{C}^{n\times n}_{\mathrm{sym}}; \mathrm{rk}(M) \leq r\} \subseteq \mathbb{C}^{n\times n}_{\mathrm{sym}}$ is closed as well, in other words $\coprod_{s=0}^{r} [q_s]$ is closed, whence $\overline{[q_r]} \subseteq \coprod_{s=0}^{r} [q_s]$.

Conversely, for $r = 0$ we have $\overline{[q_0]} = [q_0]$. For $r \in \{1, \ldots, n-1\}$ and $\epsilon \in \mathbb{C}$ let $q_{r,\epsilon} := \epsilon X_r^2 + \sum_{i=1}^{r-1} X_i^2$. Then we have $q_{r,\epsilon} \in [q_r]$ for $\epsilon \neq 0$, and $\lim_{\epsilon \to 0} q_{r,\epsilon} = q_{r,0} = q_{r-1}$, which entails $[q_{r-1}] \subseteq \overline{[q_r]}$, hence $\overline{[q_{r-1}]} \subseteq \overline{[q_r]}$. By induction this implies $\coprod_{s=0}^{r} [q_s] = [q_r] \,\dot\cup\, \coprod_{s=0}^{r-1} [q_s] = [q_r] \,\dot\cup\, \overline{[q_{r-1}]} \subseteq \overline{[q_r]}$. ♯

From $\Delta^{-1}(0) = \overline{[q_{n-1}]}$ we infer that any $\mathrm{SL}_n(\mathbb{C})$-invariant continuous complex-valued map on $\Delta^{-1}(0)$ is constant, hence the equivalence classes contained in $\Delta^{-1}(0)$ cannot be separated by these maps.

This also entails that any $\mathrm{SL}_n(\mathbb{C})$-invariant continuous complex-valued map F on $\mathcal{V}$ is constant on the fibers of Δ, that is we have $F = \Delta \cdot f$ for some map $f \colon \mathbb{C} \to \mathbb{C}$. Moreover, Δ admits the continuous section $s \colon \mathbb{C} \to \mathcal{V} \colon \delta \mapsto q_{n,\delta}$, where $q_{n,0} := q_{n-1}$, that is we have $s \cdot \Delta = \mathrm{id}_{\mathbb{C}}$. This yields $s \cdot F = s \cdot \Delta \cdot f = f$, entailing that f is continuous, saying that F is a continuous function of Δ. In particular, if F is a polynomial map, we infer that f is a polynomial map as well, saying that F is a polynomial function of Δ.

In terms of invariant algebras, see (3.2), we have thus shown that $\mathbb{C}[\mathcal{V}]^{\mathrm{SL}_n(\mathbb{C})} = \mathbb{C}[\Delta]$, the univariate polynomial algebra generated by Δ. Moreover, by Exercise (18.1), any $\mathrm{GL}_n(\mathbb{C})$-invariant continuous complex-valued map F on $\mathcal{V}$ is constant, implying that $\mathbb{C}[\mathcal{V}]^{\mathrm{GL}_n(\mathbb{C})} = \mathbb{C}$.

(1.4) Binary quadratic forms [Lagrange, 1773; Gauss, 1801]**.** We consider **binary** quadratic forms over a field K such that $\mathrm{char}(K) \neq 2$, that is the case $n = 2$. Letting $\mathcal{V} := K[X, Y]_2$, we consider the K-bases $\{X^2, 2XY, Y^2\} \subseteq \mathcal{V}$ and $\{X^2+Y^2, 2XY, X^2-Y^2\} \subseteq \mathcal{V}$. This yields two identifications of $\mathcal{V}$ with K^3. Letting A, B, C and U, W, V be the associated coordinate functions, respectively, the algebra of polynomial functions on $\mathcal{V}$ is $K[\mathcal{V}] := K[A, B, C] = K[U, W, V]$, where the base change matrix

$$M := \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & -1 \end{bmatrix} \in \mathrm{GL}_3(K)$$

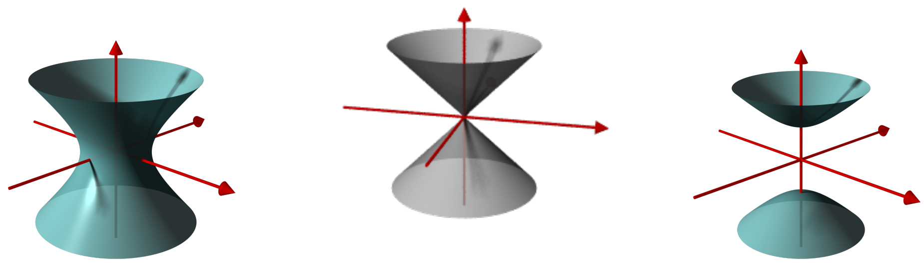
yields $[A, B, C] = [U, W, V] \cdot M = [U + V, W, U - V]$ and $[U, W, V] = [A, B, C] \cdot M^{-1} = [\frac{A+C}{2}, B, \frac{A-C}{2}]$.

Let $q := aX^2 + 2bXY + cY^2 \in \mathcal{V}$, having Gram matrix $Q = \begin{bmatrix} a & b \\ b & c \end{bmatrix} \in K^{2\times 2}_{\mathrm{sym}}$, thus $\Delta(q) = \det(Q) = ac - b^2 \in K$. Hence as polynomial function on $\mathcal{V}$ we have $\Delta = AC - B^2 = (U + V)(U - V) - W^2 = U^2 - V^2 - W^2 \in K[\mathcal{V}]$. For $\delta \in K$ the fiber $\Delta^{-1}(\delta) \subseteq \mathcal{V}$ is, with respect to the above identifications, given as $\{[a, b, c] \in K^3; ac - b^2 = \delta\}$ and $\{[u, w, v] \in K^3; v^2 + w^2 = u^2 - \delta\}$, respectively.

In particular, geometrically for $K = \mathbb{R}$, the Jacobian $[\frac{\partial\Delta}{\partial U}, \frac{\partial\Delta}{\partial W}, \frac{\partial\Delta}{\partial V}] = 2 \cdot [U, -W, -V]$ shows that $\Delta^{-1}(\delta) \subseteq \mathcal{V}$ is smooth for $\delta \neq 0$, while for $\delta = 0$ we get the unique singular point $q_0 \in \Delta^{-1}(0)$. Considering $\Delta^{-1}(\delta)$, we get a **single-shell hyperboloid** for $\delta < 0$, a **double-shell hyperboloid** for $\delta > 0$, and a **cone** for $\delta = 0$; see Table 1, where these are given in the second picture, the u-axis being the vertical one.

In view of Sylvester's Theorem we observe the following: The single-shell hyperboloid for $\delta = -1$ consists of the $\mathrm{SL}_2(\mathbb{R})$-equivalence class containing $q_{2,-1} = X^2 - Y^2$, or likewise $2XY$, which have signature $[1, -1]$; the double-shell hyperboloid for $\delta = 1$ consists of the $\mathrm{SL}_2(\mathbb{R})$-equivalence classes containing $q_{2,1} = X^2 + Y^2$ and $-X^2 - Y^2$, which have signature $[1, 1]$ and $[-1, -1]$, respectively; and in the 'degenerate' case $\delta = 0$, the cone consists of the $\mathrm{SL}_2(\mathbb{R})$-equivalence classes $\{q_0\} = \{0\}$, and the ones containing $q_1 = X^2$ and $q_1 = -X^2$, which have signature $[0, 0]$, as well as $[1, 0]$ and $[-1, 0]$, respectively.

Table 1: Hyperboloids for $\delta < 0$ and $\delta = 0$ and $\delta > 0$.



I Invariant algebras

2 Graded algebras

(2.1) Graded algebras. a) Let K be a field. A (non-commutative) K-algebra R is called **(non-negatively) graded**, if we have $R = \bigoplus_{d \geq 0} R_d$ as K-vector spaces, such that $R_0 \cong K$, and $\dim_K(R_d) \in \mathbb{N}_0$, and $R_d R_{d'} \subseteq R_{d+d'}$ for $d, d' \geq 0$. (In this context the property $\dim_K(R_0) = 1$ is also called **connectedness**.)

For $r = [r_d]_d \in R$, the element $r_d \in R_d$ is called its d-th **homogeneous component**, where since R is a direct sum (rather than a direct product), we have $r_d \neq 0$ for only finitely many d. If $r \neq 0$, the maximum $d \geq 0$ such that $r_d \neq 0$ is called the **degree** $\deg(r) \in \mathbb{N}_0$ of r.

The K-subspace $R_d \leq R$, for $d \in \mathbb{Z}$, is called its d-th **homogeneous component**, where we let $R_d := \{0\}$ for $d < 0$. The **Hilbert(-Poincaré) series** of R is the formal power series $H_R := \sum_{d \geq 0} \dim_K(R_d) \cdot T^d \in \mathbb{Z}[[T]] \subseteq \mathbb{Q}((T))$. For example, the field K is a graded K-algebra with zero homogeneous components of positive degree; thus we have $H_K = 1 \in \mathbb{Z}[T]$.

b) Let R be a graded K-algebra. An R-module M is called **graded**, if $M = \bigoplus_{d \geq d_M} M_d$ as K-vector spaces, for some $d_M \in \mathbb{Z}$, such that $\dim_K(M_d) \in \mathbb{N}_0$, and $M_d R_{d'} \subseteq M_{d+d'}$, for $d \geq d_M$ and $d' \geq 0$. If $d_M \geq 0$ then M is called **non-negatively** graded. For $m = [m_d]_d \in M$, the element $m_d \in M_d$ is called its d-th **homogeneous component**, where we have $m_d \neq 0$ for only finitely many d. If $m \neq 0$, the maximum $d \geq d_M$ such that $m_d \neq 0$ is called the **degree** $\deg(m) \in \mathbb{Z}$ of m.

The K-subspace $M_d \leq M$, for $d \in \mathbb{Z}$, is called the d-th **homogeneous component** of M, where $M_d := \{0\}$ for $d < d_M$. The **Hilbert(-Poincaré) series** of M is the formal Laurent series $H_M := \sum_{d \geq d_M} \dim_K(M_d) \cdot T^d \in \mathbb{Q}((T))$. Moreover, let $M[s] := \bigoplus_{d \in \mathbb{Z}} M_{d+s}$ denote the graded R-module obtained from

M by **shifting** $s \in \mathbb{Z}$ steps to the left; hence for the associated Hilbert series we have $H_{M[s]} = T^{-s} \cdot H_M \in \mathbb{Q}((T))$.

An R-submodule $M' \leq M$ is called **homogeneous**, if whenever $\sum_{d\in\mathbb{Z}} m_d \in M'$ we have $m_d \in M'$ as well, for all $d \in \mathbb{Z}$; in other words, we have $M' = \bigoplus_{d\in\mathbb{Z}} M'_d$, where $M'_d := M' \cap M_d$. Note that M' is homogeneous if and only if M' is as an R-module generated by homogeneous elements. If M' is homogeneous, then both M' and M/M' are graded R-modules as well, the grading being inherited from M; from $(M/M')_d = M_d/(M_d \cap M') = M_d/M'_d$ for $d \in \mathbb{Z}$, we infer that the associated Hilbert series are related by $H_M = H_{M'} + H_{M/M'} \in \mathbb{Q}((T))$.

Let M and M' be graded R-modules. Considering R-module homomorphisms we get the direct product $\mathrm{Hom}_R(M, M') = \prod_{d\in\mathbb{Z}} \prod_{d'\in\mathbb{Z}} \mathrm{Hom}_R(M_d, M'_{d'})$, where $\mathrm{Hom}_R(M, M')_c := \prod_{d\in\mathbb{Z}} \mathrm{Hom}_R(M_d, M'_{d+c})$ is called its c-th **homogeneous component**, for $c \in \mathbb{Z}$. In particular, $\mathrm{Hom}_R(M, M')_0$ consists of the homomorphisms of graded R-modules from M to M'.

c) In particular, the **regular** R-R-bimodule R is graded both as R-module and as left R-module, where $d_R = 0$, and the ideals of R coincide with its R-R-submodules. An ideal $I \trianglelefteq R$ is called **homogeneous** if it is a graded R-submodule of R, that is we have $I = \bigoplus_{d\geq 0} I_d$ where $I_d := I \cap R_d$.

Let $R_+ := \bigoplus_{d>0} R_d \lhd R_R$ be the **irrelevant ideal**; note that it is maximal such that $R/R_+ \cong K$. Since any proper homogeneous ideal of R has zero 0-th component and thus is contained in R_+, we conclude that R_+ is the unique maximal homogeneous ideal of R.

(2.2) Generating sets. a) Let K be a field, let R be a graded K-algebra, and let $M = \bigoplus_{d\geq d_M} M_d$ be a graded R-module. Then $MR_+ \subseteq M_+ := \bigoplus_{d\geq d_M+1} M_d$ is a homogeneous R-submodule; let $\overline{}\colon M \to M/MR_+$ be the natural epimorphism of R-modules, where M/MR_+ are called the **indecomposable** elements of M. Actually, M/MR_+ becomes an R/R_+-module, carrying the grading inherited from M, so that since $R/R_+ \cong R_0 = K$ we may consider M/MR_+ as a graded K-vector space.

Proposition: Graded Nakayama Lemma. Given a set $\mathcal{S} \subseteq M$ of homogeneous elements, then $\mathcal{S}$ generates M as an R-module, if and only if $\overline{\mathcal{S}}$ generates M/MR_+ as a K-vector space.

Proof. We may assume that $\overline{\mathcal{S}}$ generates M/MR_+ as a K-vector space, and let $0 \neq v \in M$ be homogeneous. To show that v belongs to the R-submodule of M generated by $\mathcal{S}$, we proceed by induction on $d := \deg(v) \geq d_M$. Since M_{d_M} embeds into M/MR_+, we are done for $d = d_M$; hence let $d \geq d_M + 1$. Then there are $s_i \in \mathcal{S}$ and $t_j \in M$ homogeneous, as well as $a_i \in K$ and $r_j \in R_+$ homogeneous, such that $v = \sum_{i=1}^k s_i a_i + \sum_{j=1}^l t_j r_j$, where $k, l \in \mathbb{N}_0$, and we may assume that $\deg(s_i) = \deg(t_j r_j) = d$. Hence we have $\deg(t_j) < d$, so that by induction t_j belongs to the R-submodule of M generated by $\mathcal{S}$, so does v. ♯

Thus a homogeneous generating set $\mathcal{S} \subseteq M$ is minimal if and only if $\overline{\mathcal{S}} \subseteq M/MR_+$ is a K-basis. Hence, if R is finitely generated, this entails that a homogeneous generating set of R is minimal if and only if it is of minimal cardinality. Moreover, since M/MR_+ is a graded K-vector space, the cardinality of a minimal homogeneous generating set of M, and the multiset of the degrees of its elements are uniquely defined; in particular we have $M = \{0\}$ if and only if $M/MR_+ = \{0\}$. Let the **embedding number** of M be the above cardinality, and if $M \neq \{0\}$ let the **Noether number** $\beta(M) = \beta_R(M) \in \mathbb{N}_0$ be the maximum of the multiset of degrees; we let $\beta(\{0\}) := 0$ as well, and if M is not finitely generated then M has infinite embedding and Noether numbers.

b) We relate the above observation to K-algebra generating sets of R. (We still do not need to assume that R is commutative, although R typically will be.)

Proposition. Given a set $\mathcal{S} \subseteq R_+$ of homogeneous elements, then $\mathcal{S}$ generates R as a K-algebra, if and only if $\mathcal{S}$ generates $R_+ \trianglelefteq R_R$ as a right ideal.

Proof. Let $\mathcal{S}$ generate R as a K-algebra. Then since any non-empty product of elements of $\mathcal{S}$ belongs to $(\mathcal{S}) \trianglelefteq R_R$, we infer that any element of R_+ belongs to $(\mathcal{S})$ as well. Since we have $(\mathcal{S}) \subseteq R_+$ anyway, this entails equality.

Let conversely $\mathcal{S}$ generate R_+ as a right ideal, and let $0 \neq f \in R$ be homogeneous. To show that f belongs to the K-subalgebra of R generated by $\mathcal{S}$, we proceed by induction on $d := \deg(f) \in \mathbb{N}_0$; the case $d = 0$ being trivial, let $d \geq 1$. There are $s_i \in \mathcal{S}$ and $r_i \in R$ homogeneous, such that $f = \sum_{i=1}^{k} s_i r_i$, for $k \in \mathbb{N}$, and we may assume $\deg(s_i r_i) = d$. Hence we have $\deg(r_i) < d$, so that by induction r_i belongs to the K-subalgebra of R generated by $\mathcal{S}$, so does f. $\sharp$

Thus a homogeneous generating set $\mathcal{S} \subseteq R_+$ of R is minimal if and only if $\overline{\mathcal{S}} \subseteq R_+/(R_+)^2$ is a K-basis, where $\overline{}\colon R_+ \rightarrow R_+/(R_+)^2$ is the natural epimorphism of R-modules, and $R_+/(R_+)^2$ are called the **indecomposable** elements of R. Hence, if R is finitely generated, this entails that a homogeneous generating set of R is minimal if and only if it is of minimal cardinality. Moreover, since $R_+/(R_+)^2$ is a graded K-vector space, the cardinality of a minimal homogeneous generating set of R, and the multiset of the degrees of its elements are uniquely defined. Let the **embedding number** of R be the above cardinality, and if $R \neq K$ let the **Noether number** $\beta(R) \in \mathbb{N}$ be the maximum of the multiset of degrees; let $\beta(K) := 0$, and if R is not finitely generated R has infinite embedding and Noether numbers.

(2.3) Tensor algebras. a) Let K be a field, and let V and W be K-vector spaces. A K-bilinear map $\otimes\colon V \times W \rightarrow T$, where T is a K-vector space, is called a **tensor product** of V and W, if it has the following universal property: For any K-bilinear map $\beta\colon V \times W \rightarrow U$, where U is a K-vector space, there is a unique K-linear map $\overline{\beta}\colon T \rightarrow U$ such that $\beta = \otimes \cdot \overline{\beta}$. Tensor products always exist and are unique up to isomorphism of K-vector spaces, where we write $V \otimes W = V \otimes_K W := T$; see Exercise (19.1).

If V and W are finitely generated, then we have $\dim_K(V \otimes W) = \dim_K(V) \cdot \dim_K(W)$. If $V = \bigoplus_{d \in \mathbb{Z}} V_d$ and $W = \bigoplus_{d \in \mathbb{Z}} W_d$ are graded, then $V \otimes W$ is graded as well such that $d_{V \otimes W} = d_V + d_W$, where $(V \otimes W)_d = \bigoplus_{e \in \mathbb{Z}} (V_e \otimes W_{d-e})$ for $d \in \mathbb{Z}$; hence we have $\dim_K((V \otimes W)_d) = \sum_{e \in \mathbb{Z}} (\dim_K(V_e) \cdot \dim_K(W_{d-e}))$, so that in terms of Hilbert series we have $H_{V \otimes W} = H_V \cdot H_W \in \mathbb{Q}((T))$.

In particular, let R and S be K-algebras. Then $R \otimes S$ becomes a K-algebra, by letting $(f \otimes g)(f' \otimes g') := ff' \otimes gg'$, for $f, f' \in R$ and $g, g' \in S$. If R and S are commutative, then so is $R \otimes S$; if R and S are graded, then so is $R \otimes S$.

b) Let V be a K-vector space such that $n := \dim_K(V) \in \mathbb{N}_0$, let $V^{\otimes d} := V \otimes V \otimes \cdots \otimes V$ be the d-th **tensor power** of V, with $d \in \mathbb{N}$ tensor factors, and let $T(V) := \bigoplus_{d \geq 0} V^{\otimes d}$, where $V^{\otimes 0} := K$. Then $T(V)$ becomes a (non-commutative) graded K-algebra, being called the **tensor algebra** over V, where multiplication is inherited from concatenation of tensor products, which is associative indeed. From $\dim_K(V^{\otimes d}) = n^d$ we infer that the Hilbert series of $T(V)$ is $H_{T(V)} = \sum_{d \geq 0} n^d \cdot T^d = \sum_{d \geq 0} (nT)^d = \frac{1}{1-nT} \in \mathbb{Q}(T) \subseteq \mathbb{Q}((T))$.

The algebra $T(V)$ has the following universal property: Let $\mathcal{B} := \{b_1, \ldots, b_n\} \subseteq V$ be a K-basis, and let $\alpha \colon \mathcal{B} \to R$ be any map, where R is a K-algebra. Then by the universal property of tensor products, α extends to the K-linear multiplication map $\alpha_d \colon V^{\otimes d} \to R \colon b_{i_1} \otimes \cdots \otimes b_{i_d} \mapsto \alpha(b_{i_1}) \cdots \alpha(b_{i_d})$, for $d \in \mathbb{N}$ and $i_1, \ldots, i_d \in \{1, \ldots, n\}$. Hence additionally letting $\alpha_0 \colon K \to R \colon 1_K \mapsto 1_R$, we get a K-linear map $\widehat{\alpha} := \sum_{d \geq 0} \alpha_d \colon T(V) \to R$, which by the definition of the multiplication in $T(V)$ actually is a homomorphism of K-algebras. Since $T(V)$ is generated by $\mathcal{B}$ as a K-algebra, we conclude that $T(V)$ is the **free (non-commutative) K-algebra** with free generating set $\mathcal{B}$.

c) The symmetric group $\mathcal{S}_d$ acts on $V^{\otimes d}$, for $d \in \mathbb{N}_0$ by permuting the tensor factors, that is for $\pi \in \mathcal{S}_d$ we have $\pi \colon v_1 \otimes \cdots \otimes v_d \mapsto v_{1\pi^{-1}} \otimes \cdots \otimes v_{d\pi^{-1}}$, for $v_1, \ldots, v_d \in V$; recall that $\mathcal{S}_0 = \{1\}$ and $V^{\otimes 0} = K$.

The d-th **symmetric power** of V is defined as the quotient K-vector space $S^d(V) := V^{\otimes d}/V^{\otimes d,-}$ of $V^{\otimes d}$ with respect to the K-subspace

$$V^{\otimes d,-} := \langle (v_1 \otimes \cdots \otimes v_d) \cdot (1 - \pi); v_1, \ldots, v_d \in V, \pi \in \mathcal{S}_d \rangle_K \leq V^{\otimes d};$$

note that $V^{\otimes 0,-} = \{0\}$ and $V^{\otimes 1,-} = \{0\}$, so that $S^0(V) \cong K$ and $S^1(V) \cong V$.

Letting $T(V)^-$ be the homogeneous K-subspace $T(V)^- := \bigoplus_{d \geq 0} V^{\otimes d,-} \leq T(V)$, we observe that $T(V)^-$ actually is an ideal of $T(V)$; see Exercise (19.2). Thus $S[V] := T(V)/T(V)^- = \bigoplus_{d \geq 0} S^d(V)$ becomes a graded K-algebra, being called the **symmetric algebra** over V, which by construction is commutative.

In particular, for $n = 0$ we have $V^{\otimes d} = \{0\}$ for $d \in \mathbb{N}$, so that $S[\{0\}] = K$; and for $n = 1$ we have $V^{\otimes d} \cong K$ and $V^{\otimes d,-} = \{0\}$ for $d \geq 0$, so that $S[K] = \bigoplus_{d \geq 0} \langle 1 \otimes \cdots \otimes 1 \rangle_K$, with d tensor factors in the d-th summand.

The algebra $S[V]$ has the following universal property: Let $\mathcal{B} \subseteq V$ be a K-basis, and let $\alpha\colon \mathcal{B} \to R$ be any map, where R is a commutative K-algebra. Then by the universal property of $T(V)$ the map α extends to a homomorphism $\widehat{\alpha}\colon T(V) \to R$ of K-algebras. Since R is commutative, $\widehat{\alpha}$ factors through the quotient map with respect to the ideal $T(V)^{-}$, so that we get a homomorphism $\widehat{\widehat{\alpha}}\colon S[V] \to R$ of K-algebras. Since $S[V]$ is generated by $\mathcal{B}$ as a K-algebra, we conclude that $S[V]$ is the **free commutative K-algebra** with free generating set $\mathcal{B}$, in other words the **polynomial K-algebra** in the indeterminates $\mathcal{B}$.

(2.4) Polynomial algebras. a) Let $R \neq \{0\}$ be a commutative ring, and let $R[X] := \bigoplus_{d\geq 0} X^d \cdot R$ be the free R-module with free generating set $\mathbb{N}_0$. Hence any **polynomial** $f \in R[X]$ can be uniquely written as $f = \sum_{d\geq 0} f_d \cdot X^d$, with **coefficients** $f_d \in R$ such that $f_d \neq 0$ for only finitely many d.

If $f \neq 0$, the maximum $d \geq 0$ such that $f_d \neq 0$ is called the **degree** $\deg(f) \in \mathbb{N}_0$ of f, and $\mathrm{lc}(f) := f_d \in R$ is called its **leading coefficient**; if $\mathrm{lc}(f) = 1$ then f is called **monic**. Then $R[X]$ becomes a commutative R-algebra with respect to the multiplication induced by addition on $\mathbb{N}_0$, by identifying R with $1 \cdot R \subseteq R[X]$.

Then $R[X]$ has the following universal property: Let S be a commutative R-algebra, with structure homomorphism $\alpha\colon R \to S$, and let $x \in S$. Then, by the definition of the multiplication in $R[X]$, there is a unique homomorphism of R-algebras $\widehat{\alpha}\colon R[X] \to S$ extending α, such that $\widehat{\alpha}(X) = x$. Hence $R[X]$ is the univariate **polynomial R-algebra** in the indeterminate X.

In particular, if R is a domain, that is a commutative non-zero ring without zero-divisors, then so is $R[X]$; and if R additionally is factorial, then by the **Lemma of Gauss** so is $R[X]$; see Exercise (19.10).

b) Let $K[\mathcal{X}]$ be the polynomial algebra with indeterminates $\mathcal{X} := \{X_1, \ldots, X_n\}$, where $n \in \mathbb{N}_0$; in particular, for $n = 0$ we have $K[\emptyset] = K$.

Proposition. We have $K[\mathcal{X}] \cong K[X_1] \otimes \cdots \otimes K[X_n]$ as K-algebras.

Proof. Let $R := K[X_1] \otimes \cdots \otimes K[X_n]$. Then by the universal property of $K[\mathcal{X}]$ there is a homomorphism of K-algebras $\alpha\colon K[\mathcal{X}] \to R$ such that $\alpha\colon X_i \mapsto 1 \otimes \cdots \otimes X_i \otimes \cdots \otimes 1$, for $i \in \{1, \ldots, n\}$, where X_i occurs in the i-th tensor factor. Conversely, for $i \in \{1, \ldots, n\}$ there is a homomorphism of K-algebras $\beta_i\colon K[X_i] \to K[\mathcal{X}]$ such that $\beta_i\colon X_i \mapsto X_i$, by the universal property of tensor products giving rise to a homomorphism of K-algebras $\beta := \beta_1 \otimes \cdots \otimes \beta_n\colon R \to K[\mathcal{X}]$ such that $\beta\colon X_1^{a_1} \otimes \cdots \otimes X_n^{a_n} \mapsto \prod_{i=1}^n X_i^{a_i}$, for $a_1, \ldots, a_n \in \mathbb{N}_0$. Finally, we get $\alpha \cdot \beta\colon X_i \mapsto X_i$ and $\beta \cdot \alpha\colon 1 \otimes \cdots \otimes X_i \otimes \cdots \otimes 1 \mapsto 1 \otimes \cdots \otimes X_i \otimes \cdots \otimes 1$. $\sharp$

Hence letting $\mathcal{X}' := \mathcal{X} \setminus \{X_n\}$, for $n \geq 1$, we have $K[\mathcal{X}] \cong K[\mathcal{X}'] \otimes K[X_n] = K[\mathcal{X}'][X_n]$. Thus any polynomial $f \in K[\mathcal{X}]$ can be uniquely written as $f = \sum_{d\geq 0} f_d \cdot X_n^d$, where $f_d \in K[\mathcal{X}']$ such that $f_d \neq 0$ for only finitely many d. Hence by induction on $n \in \mathbb{N}_0$ we infer that $\{\prod_{i=1}^n X_i^{a_i} \in K[\mathcal{X}]; [a_1, \ldots, a_n] \in \mathbb{N}_0^n\}$ is a K-basis of $K[\mathcal{X}]$, and that $K[\mathcal{X}]$ is a factorial domain.

c) Actually, $K[\mathcal{X}]$ carries various gradings: To this end, let $\delta := [d_1, \ldots, d_n] \in \mathbb{N}^n$. Then $K[\mathcal{X}]$ becomes a graded K-algebra by letting $\deg_\delta(\prod_{i=1}^n X_i^{a_i}) := \sum_{i=1}^n d_i a_i \in \mathbb{N}_0$, for $[a_1, \ldots, a_n] \in \mathbb{N}_0^n$. Thus the homogeneous component $K[\mathcal{X}]_d^\delta \leq K[\mathcal{X}]$ is the K-subspace generated by the monomials of degree d with respect to δ, and letting $\deg_{[d_i]}(X_i) := d_i$ we have $K[\mathcal{X}] \cong K[X_1] \otimes \cdots \otimes K[X_n]$ as graded algebras.

The **standard grading** $\deg = \deg_{\mathcal{X}}$ of $K[\mathcal{X}]$ is given by the degrees $[1, \ldots, 1]$, that is by letting $\deg(X_i) := 1$ for $i \in \{1, \ldots, n\}$; note that this is the grading inherited from the symmetric algebra $S[K^n]$.

Given degrees δ, the Hilbert series of $K[X_i]$ with respect to $\deg_{[d_i]}$ is given as $H_{K[X_i]}^{[d_i]} = \sum_{a \geq 0} T^{a d_i} = \frac{1}{1-T^{d_i}} \in \mathbb{Q}(T) \subseteq \mathbb{Q}((T))$. Thus the Hilbert series of $K[\mathcal{X}]$ with respect to $\deg_\delta$ is given as $H_{K[\mathcal{X}]}^\delta = \prod_{i=1}^n \frac{1}{1-T^{d_i}} \in \mathbb{Q}(T)$.

In particular, for the standard grading we get $H_{K[\mathcal{X}]} = \frac{1}{(1-T)^n} = \sum_{d \geq 0} \binom{n+d-1}{d} \cdot T^d \in \mathbb{Q}(T) \subseteq \mathbb{Q}((T))$: Assuming that $n \geq 1$, expanding the left hand side as a power series, the coefficient of T^d is given as the number of possibilities to write d as a sum of n non-negative integers, which of course is the same as the number of monomials of degree d in n indeterminates, and which is well-known to be equal to $\binom{d+(n-1)}{n-1} = \binom{n+d-1}{d}$; see Exercise (19.19).

(2.5) Algebras of polynomial functions. Let K be a field, and let V be a K-vector space having K-basis $\mathcal{B} = \{b_1, \ldots, b_n\} \subseteq V$, where $n := \dim_K(V) \in \mathbb{N}_0$. Moreover, let $V^* := \mathrm{Hom}_K(V, K) \leq \mathrm{Maps}(V, K)$ be the **dual space** of V, that is the K-vector space of **linear forms** on V, and let $\mathcal{X} = \{X_1, \ldots, X_n\} \subseteq V^*$ be the dual K-basis with respect to $\mathcal{B}$, that is $X_j(b_i) = \delta_{ij} \in K$ for $i, j \in \{1, \ldots, n\}$, where δ is the Kronecker function. Then the symmetric algebra $K[V] := S[V^*] = K[\mathcal{X}]$ is called the **algebra of polynomial functions** on V.

Indeed, $\mathrm{Maps}(V, K)$ becomes a commutative K-algebra by pointwise addition and multiplication. Hence by the universal property of $K[\mathcal{X}]$ we get the **evaluation** homomorphism of K-algebras $\epsilon_V \colon K[\mathcal{X}] \to \mathrm{Maps}(V, K)$ given by

$$\epsilon_V \colon \prod_{j=1}^n X_j^{a_j} \mapsto (V \to K \colon \sum_{i=1}^n c_i b_i \mapsto \prod_{j=1}^n c_j^{a_j}), \quad \text{for } [a_1, \ldots, a_n] \in \mathbb{N}_0^n.$$

Proposition. The map ϵ_V is injective if and only if $n = 0$ or K is infinite.

Proof. Since for $n = 0$ we have $K[\emptyset] = K \cong \mathrm{Maps}(\{0\}, K)$, we may assume that $n \geq 1$. Let first $K = \mathbb{F}_q$ be the field with q elements; we may assume that $n = 1$. Then we have $X^q(a) = a = X(a)$, for all $a \in \mathbb{F}_q$, that is $\epsilon_{\mathbb{F}_q}(X^q) = \epsilon_{\mathbb{F}_q}(X)$.

Let K be infinite. We proceed by induction on $n \geq 1$. Let first $n = 1$: Recall that $K[X]$ is factorial, which follows from $K[X]$ being Euclidean with respect

$\deg(\cdot)$. Thus any $0 \neq f \in K[X]$ has only finitely many roots in K, so that there is $x \in K$ such that $f(x) \neq 0$. (Note that here we only need that $\deg(f) < |K|$.)

Let now $n \geq 2$, and let $0 \neq f = \sum_{i=0}^{d} f_i \cdot X_n^i \in K[\mathcal{X}]$, for some $d \in \mathbb{N}_0$, and $f_0, \ldots, f_d \in K[\mathcal{X} \setminus \{X_n\}]$ such that $f_d \neq 0$. Then by induction there are elements $x_1, \ldots, x_{n-1} \in K$ such that $f_d(x_1, \ldots, x_{n-1}) \neq 0$. This entails that $0 \neq f(x_1, \ldots, x_{n-1}, X_n) = \sum_{i=0}^{d} f_i(x_1, \ldots, x_{n-1}) \cdot X_n^i \in K[X_n]$. The latter having only finitely many roots in K, there is $x_n \in K$ such that $f(x_1, \ldots, x_n) \neq 0$. (Note that again we only need that $\deg_{X_n}(f) < |K|$.) $\sharp$

The above argument actually shows that for the finite field $K = \mathbb{F}_q$ the map ϵ_V is injective on $\bigoplus_{d=0}^{q-1} \mathbb{F}_q[\mathcal{X}]_d \leq \mathbb{F}_q[\mathcal{X}]$. In particular, for K arbitrary the map ϵ_V is always injective on $K[\mathcal{X}]_0 \oplus K[\mathcal{X}]_1 \cong K \oplus V^*$, that is the K-vector space of **affine K-linear forms** on V.

3 Invariant algebras

(3.1) Groups. Let K be a field, let V be a K-vector space such that $n := \dim_K(V) \in \mathbb{N}_0$, and let G be a group. Then a group homomorphism $\rho = \rho_V : G \to \mathrm{GL}(V) \cong \mathrm{GL}_n(K)$ is called a **K-representation** of G. The representation ρ is called **faithful** if $\ker(\rho) = \{1\}$; in this case we may identify G with a subgroup of $\mathrm{GL}(V)$.

Hence the K-vector space V becomes a $K[G]$-module, for the **group algebra** $K[G]$ of G over K. The latter is defined as the K-subspace $K[G] := \langle \delta_g ; g \in G \rangle_K \leq \mathrm{Maps}(G, K)$, where $\delta_g : G \to K : x \mapsto \delta_{g,x}$, and becomes a K-algebra by letting $\delta_g \delta_h = \delta_{gh} \in K[G]$ for $g, h \in G$; hence we may identify G with the K-basis $\{\delta_g ; g \in G\} \subseteq K[G]$.

Representations $\rho : G \to \mathrm{GL}_n(K)$ and $\rho' : G \to \mathrm{GL}_n(K)$ are called **equivalent**, if the associated $K[G]$-modules V and V' are isomorphic, that is if there is matrix $A \in \mathrm{GL}_n(K)$ such that $\rho(g) \cdot A = A \cdot \rho'(g) \in \mathrm{GL}_n(K)$, for all $g \in G$.

In particular, for $n = 1$ we have the **trivial** representation $G \to K^* : g \mapsto 1$. Moreover, the dual space V^* of V becomes a $K[G]$-module, being called the **contragredient module** of V, by letting G act by pre-composition, that is for $g \in G$ and $\alpha \in V^*$ we let $\alpha \cdot g \in V^*$ be given by $v \mapsto \alpha(v \cdot g^{-1})$, for $v \in V$.

(3.2) Invariant algebras. a) Let K be a field, and let G be a group. If V and W are $K[G]$-modules, then by the universal property of tensor products $V \otimes W$ becomes a $K[G]$-module again, by **diagonal** G-action given by $(v \otimes w) \cdot g := (v \cdot g) \otimes (w \cdot g)$, for $v \in V$ and $w \in W$, and $g \in G$.

In particular, the tensor power $V^{\otimes d}$ becomes a $K[G]$-module, for $d \in \mathbb{N}$. Moreover, the G-action commutes with the $\mathcal{S}_d$-action, that is $(v_1 \otimes \cdots \otimes v_d) \cdot g \cdot \pi^{-1} = (v_1 g \otimes \cdots \otimes v_d g) \cdot \pi^{-1} = v_{1\pi} g \otimes \cdots \otimes v_{d\pi} g = (v_{1\pi} \otimes \cdots \otimes v_{d\pi}) \cdot g = (v_1 \otimes \cdots \otimes v_d) \cdot \pi \cdot g$, for $v_1, \ldots, v_d \in V$ and $g \in G$, and $\pi \in \mathcal{S}_d$. Hence $V^{\otimes d,-} \leq V^{\otimes d}$ is a $K[G]$-submodule, so that $S^d(V) := V^{\otimes d}/V^{\otimes d,-}$ becomes a $K[G]$-module as well.

Letting G act trivially on $V^{\otimes 0} = K$, the tensor algebra $T(V) = \bigoplus_{d\geq 0} V^{\otimes d}$ and the symmetric algebra $S[V] = \bigoplus_{d\geq 0} S^d(V)$, being direct sums, become $K[G]$-modules as well, whose grading is respected by the G-action. Moreover, since multiplication in $T(V)$ and $S[V]$ are inherited from concatenation of tensor products, G acts by graded K-algebra automorphisms on $T(V)$ and $S[V]$.

b) Hence we are led to the following notion: A graded K-algebra S, on which G acts by graded K-algebra automorphisms, is called **graded G-algebra**. In particular, the symmetric algebra $S[V]$ is a graded G-algebra, which additionally is a finitely generated factorial K-domain; moreover, G acts faithfully on $S[V]$ if and only if S acts faithfully on V.

If S is a graded G-algebra, then the set $S^G = \mathrm{Fix}_S(G) := \{f \in S; f\cdot g = f \text{ for all } g \in G\} \subseteq S$ of **(G-)invariants** is a graded K-subalgebra, being called the associated **invariant algebra**, where $S^G = \bigoplus_{d\geq 0}(S_d)^G$. Moreover, if S is commutative, then so is S^G; and if S is a domain, then so is S^G.

For example, if $N \trianglelefteq G$ is a normal subgroup, then the invariant algebra $S^N \subseteq S$ is acted on by G, where the action factors through the natural epimorphism to G/N; thus S^N becomes a graded G/N-algebra, and we have $S^G = (S^N)^{G/N}$.

For the symmetric algebra we get $S[V]^G = \bigoplus_{d\geq 0}(S^d)^G$, where $(S^d)^G = S[V]^G \cap S^d$; in particular we have $(S^0)^G = S^0(V) = K$ and $S^1(V)^G = \mathrm{Fix}_V(G) := \bigcap_{g\in G} \ker_V(g-1) \leq V$. Note that G enters the picture only through ρ_V, so that we may assume that ρ_V is faithful, in other words $G \leq \mathrm{GL}(V)$.

Example: Quadratic forms. For the action of $\mathrm{SL}_n(\mathbb{C})$ and $\mathrm{GL}_n(\mathbb{C})$ on the $\mathbb{C}$-vector space $\mathcal{V} := \mathbb{C}[X_1,\ldots,X_n]_2$ of n-ary complex quadratic forms, where $n \in \mathbb{N}$, we have seen in (1.3) (using a topological argument), that the invariant algebra $\mathbb{C}[\mathcal{V}]^{\mathrm{SL}_n(\mathbb{C})} = S[\mathcal{V}^*]^{\mathrm{SL}_n(\mathbb{C})} = \mathbb{C}[\Delta]$ is the univariate polynomial algebra generated by the discriminant Δ, and that $\mathbb{C}[\mathcal{V}]^{\mathrm{GL}_n(\mathbb{C})} = S[\mathcal{V}^*]^{\mathrm{GL}_n(\mathbb{C})} = \mathbb{C}$ consists of the constant functions only.

(3.3) Example: Cyclic groups. Let K be a field, let $k \in \mathbb{N}$ such that $\mathrm{char}(K) \nmid k$, and assume that K contains a primitive k-th root of unity ζ_k. We consider various faithful representations of the cyclic group $G := \langle z\rangle \cong C_k$:

a) Let $G \to \mathrm{GL}_1(K) = K^*\colon z \mapsto \zeta_k$. Then G acts on $K[X]$ by $X\cdot z = \zeta_k X$. Hence for $f = \sum_{d\geq 0} a_d X^d \in K[X]$ we have $f\cdot z = \sum_{d\geq 0} \zeta_k^d a_d X^d \in K[X]$, so that by comparing coefficients we observe that $f\cdot z = f$ if and only if $a_d = 0$ whenever $k \nmid d$. Thus we have $K[X]^G = K[X^k]$, which is a univariate polynomial algebra, in degree k, and Hilbert series $H_{K[X]^G} = \frac{1}{1-T^k} \in \mathbb{Q}(T)$.

b) Similarly, let $G \to \mathrm{GL}_2(K)\colon z \mapsto \mathrm{diag}[\zeta_k, 1]$. Then G acts on $S := K[X,Y]$ by $X\cdot z = \zeta_k X$ and $Y \cdot z = Y$. Hence for $d \in \mathbb{N}_0$ and $f = \sum_{i=0}^d a_i X^i Y^{d-i} \in S_d$ we have $f\cdot z = \sum_{i=0}^d \zeta_k^i a_i X^i Y^{d-i} \in S_d$, so that by comparing coefficients we observe that $f \cdot z = f$ if and only if $a_i = 0$ whenever $k \nmid i$. Thus we have

$S^G = K[X^k, Y] \cong K[X^k] \otimes K[Y]$, which is a bivariate polynomial algebra again, but with degrees $[k, 1]$, and Hilbert series $H_{S^G} = \frac{1}{(1-T)(1-T^k)} \in \mathbb{Q}(T)$.

c) Let $G \to \mathrm{GL}_2(K)\colon z \mapsto \mathrm{diag}[\zeta_k, \zeta_k]$. Then we have $K^2 \cong K \oplus K$ as $K[G]$-modules, where the direct summands are both isomorphic to the representation $z \mapsto \zeta_k$ considered above; the associated invariants are called **vector invariants**. Then G acts on $S := K[X, Y]$ by $X \cdot z = \zeta_k X$ and $Y \cdot z = \zeta_k Y$. Hence for $d \in \mathbb{N}_0$ and $f = \sum_{i=0}^{d} a_i X^i Y^{d-i} \in S_d$ we have $f \cdot z = \sum_{i=0}^{d} \zeta_k^d a_i X^i Y^{d-i} \in S_d$, so that by comparing coefficients we observe that $f \cdot z = f$ if and only if $k \mid d$; thus $S^G = \bigoplus_{d \geq 0} S_{kd}$. Since $\dim_K(S_d) = d + 1$, we have $H_{S^G} = \sum_{d \geq 0}(kd + 1)T^{kd} = \frac{\partial}{\partial T}(\sum_{d \geq 0} T^{kd+1}) = \frac{\partial}{\partial T}(T \cdot \sum_{d \geq 0} T^{kd}) = \frac{\partial}{\partial T}(\frac{T}{1-T^k}) = \frac{1+(k-1)T^k}{(1-T^k)^2} \in \mathbb{Q}(T)$.

To elucidate the structure of S^G, let $R := K[X^k, Y^k] \cong K[X^k] \otimes K[Y^k]$ be the bivariate polynomial algebra genenerated by $\{X^k, Y^k\}$, with degrees $[k, k]$; note that the tensor factors are the invariant algebras of the direct summands of the representation $K^2 \cong K \oplus K$ under consideration. We show that $S^G = R \oplus \bigoplus_{i=1}^{k-1}(X^{k-i}Y^i \cdot R)$ as graded R-modules, the latter being the **free graded** R-module generated by $\{1, X^{k-1}Y, \ldots, XY^{k-1}\}$; in particular this entails that as K-algebras we have $S^G = K[X^k, X^{k-1}Y, \ldots, XY^{k-1}, Y^k]$:

Since $S_k \leq S^G$, we have $R \subseteq S^G$ and $\{X^{k-1}Y, \ldots, XY^{k-1}\} \subseteq S^G$, showing that $R + \sum_{i=1}^{k-1}(X^{k-i}Y^i \cdot R) \subseteq S^G$. Conversely, let $f := X^i Y^{kd-i} \in S_{kd}$ be a monomial, where $d \in \mathbb{N}_0$ and $i \in \{0, \ldots, kd\}$. If $k \mid i$, then f is a monomial in $\{X^k, Y^k\}$, thus $f \in R$. If $k \nmid i$, then let $j \in \{1, \ldots, k-1\}$ such that $i \equiv j \pmod{k}$; then we have $X^i Y^{kd-i} = X^j Y^{k-j} \cdot X^{i-j} Y^{k(d-1)-(i-j)}$, where the latter factor is a monomial in $\{X^k, Y^k\}$, thus $f \in X^{k-j}Y^j \cdot R$.

Thus we have $S^G = R + \sum_{i=1}^{k-1}(X^{k-i}Y^i \cdot R)$. It remains to show directness: The free R-module generated by $\{1, X^{k-1}Y, \ldots, XY^{k-1}\}$ has Hilbert series $H_R + \sum_{i=1}^{k-1} H_{X^{k-i}Y^i \cdot R} = \frac{1+(k-1)T^k}{(1-T^k)^2} = H_{S^G} \in \mathbb{Q}(T)$. Thus the natural epimorphism of graded R-modules from the latter free R-module to S^G is injective indeed. $\sharp$

Note that $X^k, X^{k-1}Y, XY^{k-1}, Y^k \in S^G$ are pairwise non-associate irreducible elements, for $k \geq 2$, but fulfill $X^{k-1}Y \cdot XY^{k-1} = X^k \cdot Y^k$, implying that S^G is not factorial, in particular it is not a polynomial algebra.

d) Let $G \to \mathrm{GL}_2(K)\colon z \mapsto \mathrm{diag}[\zeta_k, \zeta_k^{-1}]$. Then we have $X \cdot z = \zeta_k X$ and $Y \cdot z = \zeta_k^{-1} Y$. Hence for $f = \sum_{i,j \geq 0} a_{ij} X^i Y^j \in S$ we have $f \cdot z = \sum_{i,j \geq 0} \zeta_k^{i-j} a_{ij} X^i Y^j \in S$, so that by comparing coefficients we observe that $f \cdot z = f$ if and only if $a_i = 0$ whenever $k \nmid (i - j)$. Thus for a monomial f we have $f \cdot z = f$ if and only if it has the form $f = (XY)^i X^{ak} Y^{bk}$, for $i \in \{0, \ldots, k-1\}$ and $a, b \in \mathbb{N}_0$. Thus we have $S^G = K[XY, X^k, Y^k]$ as graded K-algebras.

Observing that the above monomials are K-linearly independent, letting $R := K[X^k, Y^k]$ we get $S^G = \bigoplus_{i=0}^{k-1}(X^i Y^i \cdot R)$ as graded R-modules. Since R is polynomial with degrees $[k, k]$, we have $H_R = \frac{1}{(1-T^k)^2}$, entailing that $H_{S^G} = (\sum_{i=0}^{k-1} T^{2i}) \cdot H_R = \frac{1-T^{2k}}{(1-T^2)(1-T^k)^2} = \frac{1+T^k}{(1-T^2)(1-T^k)} \in \mathbb{Q}(T)$.

Note that for $k \geq 2$ the elements $XY, (XY)^{k-1}, X^k, Y^k \in S^G$ are pairwise non-associate irreducible, but $XY \cdot (XY)^{k-1} = X^k \cdot Y^k$ shows that S^G is not factorial, thus it is not a polynomial algebra. We elucidate the structure of S^G:

Let $P := K[A, B, C]$ be the polynomial algebra with degrees $[2, k, k]$, and let $I := (A^k - BC) \trianglelefteq P$, where $A^k - BC \in P$ is homogeneous of degree $2k$. Since I is a free P-module generated in degree $2k$, we have $H_{P/I} = H_P - H_I = (1 - T^{2k}) \cdot H_P = \frac{1-T^{2k}}{(1-T^2)(1-T^k)^2} \in \mathbb{Q}(T)$. The epimorphism $P \to S^G$ of graded K-algebras given by $A \mapsto XY$, $B \mapsto X^k$, $C \mapsto Y^k$ factors through P/I, and since $H_{P/I} = H_{S^G}$ we have an isomorphism $P/I \cong S^G$. ♯

(3.4) Example: The cyclic group of order 2. i) Let K be an arbitrary field, and let $G := \langle z \rangle \cong C_2$. We consider the regular representation of G, which with respect to the K-basis $\{1, z\} \subseteq K[G]$ is given as $G \to \mathrm{GL}_2(K)\colon z \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Then G acts on $S := K[X, Y]$ by $X \cdot z = Y$ and $Y \cdot z = X$. Hence for $d \in \mathbb{N}_0$ and $f = \sum_{i=0}^d a_i X^i Y^{d-i} \in S_d$ we have $f \cdot z = \sum_{i=0}^d a_i X^{d-i} Y^i = \sum_{i=0}^d a_{d-i} X^i Y^{d-i} \in S_d$, so that by comparing coefficients we observe that $f \cdot z = f$ if and only if $a_i = a_{d-i}$ for all $i \in \{0, \ldots, d\}$. Thus for d odd and even, respectively, we have

$$S_d^G = \begin{cases} \langle X^d + Y^d, X^{d-1}Y + XY^{d-1}, \ldots, X^{\frac{d+1}{2}} Y^{\frac{d-1}{2}} + X^{\frac{d-1}{2}} Y^{\frac{d+1}{2}} \rangle_K, \\ \langle X^d + Y^d, X^{d-1}Y + XY^{d-1}, \ldots, X^{\frac{d}{2}} Y^{\frac{d}{2}} \rangle_K. \end{cases}$$

In particular we have $\dim_K(S_d^G) = \lfloor \frac{d}{2} \rfloor + 1$. Thus we get $H_{S^G} = 1 + T + 2T^2 + 2T^3 + \cdots = (1 + T) \cdot \sum_{d \geq 0} (d + 1) \cdot T^{2d} \in \mathbb{Z}[[T]]$. Letting $T' := T^2$ we have $\sum_{d \geq 0} (d+1) \cdot T^{2d} = \sum_{d \geq 0} (d + 1) \cdot (T')^d = \frac{\partial}{\partial T'} (\sum_{d \geq 0} (T')^d) = \frac{\partial}{\partial T'} (\frac{1}{1-T'}) = \frac{1}{(1-T')^2} = \frac{1}{(1-T^2)^2}$, hence $H_{S^G} = \frac{1+T}{(1-T^2)^2} = \frac{1}{(1-T)(1-T^2)} \in \mathbb{Q}(T)$.

We show that $S^G = K[X + Y, XY]$: Let R denote the right hand side.

We have $S_1^G = \langle X + Y \rangle_K$ and $S_2^G = \langle X^2 + Y^2, XY \rangle_K$, so that $R \subseteq S^G$. Conversely, we show by induction on $d \geq 1$ that $S_d^G \subseteq R$, where since $S_1^G \subseteq R$ we may assume that $d \geq 2$. Then for $i \in \{1, \ldots, \lfloor \frac{d}{2} \rfloor\}$ we have $X^i Y^{d-i} + X^{d-i} Y^i = (XY)^i (X^{d-2i} + Y^{d-2i})$, where by induction we have $X^{d-2i} + Y^{d-2i} \in S_{d-2i}^G \subseteq R$, from which, since $(XY)^i \in R$ anyway, we conclude that $X^i Y^{d-i} + X^{d-i} Y^i \in R$; note that for $i = \frac{d}{2}$ the latter equals $2(XY)^{\frac{d}{2}}$, but we have $(XY)^{\frac{d}{2}} \in R$ anyway.

Finally, $(X + Y)^d = \sum_{i=0}^d \binom{d}{i} X^i Y^{d-i}$ for d odd and even, respectively, yields

$$(X + Y)^d = \begin{cases} (X^d + Y^d) + \sum_{i=1}^{\frac{d-1}{2}} \binom{d}{i} (X^i Y^{d-i} + X^{d-i} Y^i), \\ (X^d + Y^d) + \binom{d}{\frac{d}{2}} (XY)^{\frac{d}{2}} + \sum_{i=1}^{\frac{d}{2}-1} \binom{d}{i} (X^i Y^{d-i} + X^{d-i} Y^i). \end{cases}$$

Since $(X + Y)^d \in R$ anyway, from what we have seen above we conclude that $X^d + Y^d \in R$ as well, entailing $S_d^G \subseteq R$. ♯

From this we conclude that S^G is a bivariate polynomial algebra with degrees $[1,2]$: Let $R := K[A,B]$ be the polynomial algebra with degrees $[1,2]$; hence $H_R = \frac{1}{(1-T)(1-T^2)} = H_{S^G} \in \mathbb{Q}(T)$. Thus the epimorphism of graded K-algebras $\alpha\colon R \to S^G$ given by $A \mapsto X+Y$ and $B \mapsto XY$ is injective.

ii) If $\mathrm{char}(K) \neq 2$, then the above computation can be simplified considerably, since z has eigenvalues $\{\pm 1\}$, so that z is diagonalizable; note that if $\mathrm{char}(K) = 2$ then z has eigenvalue 1 with multiplicity 1, so that z is not diagonalizable in this case. Hence applying the base change associated with with respect to the eigenvector K-basis $A := \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \in \mathrm{GL}_2(K)$ yields a $K[G]$-isomorphism from the regular representation to the representation $z \mapsto \mathrm{diag}[-1,1]$; see (3.3).

Hence letting $X', Y' \in S$ be the indeterminates associated with the latter K-basis, we have $[X',Y'] = [X,Y] \cdot A^{\mathrm{tr}} = [X-Y, X+Y]$. Thus we have $S^G = K[(X')^2, Y'] = K[(X-Y)^2, X+Y]$, so that from $(X-Y)^2 - (X+Y)^2 = -4XY$ we infer that $S^G = K[X+Y, XY]$.

4 Finite generation

(4.1) Invariant fields. a) Let K be a field, and let S be a graded K-domain; then let $L := \mathrm{Q}(S)$ be its field of fractions. For example, let $S = S[V]$, where V is a finitely generated K-vector space; then $S(V) := \mathrm{Q}(S[V])$ is the associated **field of rational functions**.

If S additionally is a G-algebra, where G is a group, by the universal property of fields of fractions the G-action by K-algebra automorphisms on S extends uniquely to a G-action by field automorphisms on L. Moreover, G acts faithfully on L if and only if G acts faithfully on S.

Hence the associated **invariant field** is given as $L^G = \mathrm{Fix}_L(G) := \{f \in L; f \cdot g = f \text{ for all } g \in G\} \subseteq L$, being a subfield of L such that $S^G = L^G \cap S$. Since $S^G \subseteq S$ is a domain as well, we get a natural embedding of the associated field of fractions $\mathrm{Q}(S^G)$ into $\mathrm{Q}(S) = L$, thus since $\mathrm{Q}(S^G)$ consists of invariant rational functions we have $\mathrm{Q}(S^G) \subseteq L^G$.

b) The question arises whether we might have equality $\mathrm{Q}(S^G) = L^G$. Actually, this is not always the case, not even for $S = S[V]$, where V is a $K[G]$-module, as we will see by way of an example below. Still, under suitable additional hypotheses equality holds (the case of finite groups being dealt with in (4.6)):

To this end, assume that S is factorial; for example, we may have $S = S[V]$. Recall that any element of L can be written as $\frac{f}{g} \in L$ where $f, g \in S$ such that $g \neq 0$, which may be assumed to be coprime. Now assuming that $0 \neq \frac{f}{g} \in L^G$, from $\frac{f}{g} = (\frac{f}{g})^z = \frac{f^z}{g^z}$, for $z \in G$, we infer that $f \cdot g^z = f^z \cdot g$. Since $\gcd(f,g) = S^*$ from this we get $f \mid f^z$, and since $\gcd(f^z, g^z) = \gcd(f,g)^z = S^*$ we also have $f^z \mid f$, thus $f \sim f^z$; and similarly $g \sim g^z$. Hence f and g are **semi-invariants** or **relative invariants**, but not necessarily invariants.

Proposition. Let G have only the trivial one-dimensional K-representation; in other words, the only group homomorphism $G \to K^*$ is given by $z \mapsto 1$, for $z \in G$. Then we have $\mathrm{Q}(S^G) = L^G$.

Proof. Letting $0 \neq \frac{f}{g} \in L^G$, where $0 \neq f, g \in S$ are coprime, we infer that $\langle f \rangle_K \leq S$ and $\langle g \rangle_K \leq S$ are one-dimensional $K[G]$-submodules, hence are trivial $K[G]$-modules. Thus we have $f, g \in S^G$, that is f and g are actually invariants, hence $\frac{f}{g} \in \mathrm{Q}(S^G)$. $\sharp$

(4.2) Example: The multiplicative group. Let K be a field, let $G := \mathrm{GL}_1(K) = K^*$ act on K^2 by $z \mapsto \mathrm{diag}[z, z]$, and let $S := K[X, Y]$ and $L := S(V) = K(X, Y)$; note that $K \subseteq L$ is pure transcendental of transcendence degree $\mathrm{trdeg}_K(L) = 2$. We determine $S^G \subseteq S$ and $L^G \subseteq L$, where G acts by $X \cdot z = zX$ and $Y \cdot z = zY$, distinguishing the cases whether or not K is finite:

a) Let K be infinite. Then G contains an element of arbitrarily large finite order, or of infinite order: Assume that all elements of G have order bounded by some $k \in \mathbb{N}$, then all of them are roots of $\prod_{i=1}^{k}(X^i - 1) \in K[X]$, a contradiction.

We determine $S^G = \bigoplus_{d \geq 0} S_d^G$: Let $0 \neq f \in S_d^G$, for some $d \in \mathbb{N}_0$. Then letting $z \in G$ be an element of infinite order, or of finite order exceeding d, from $f = f^z = z^d f$ we infer that $d = 0$. This implies $S^G = K$, thus $\mathrm{Q}(S^G) = K$.

We proceed to consider L^G: Let $0 \neq \frac{f}{g} \in L^G$, where $0 \neq f, g \in S$ are coprime. Writing $f = \sum_{d \geq 0} f_d$ as sum of its homogeneous components, and letting $z \in G$ be an element of infinite order, or of finite order exceeding $\deg(f)$, then from $f \sim f^z$ we get $\sum_{d \geq 0} c f_d = cf = f^z = \sum_{d \geq 0} z^d f_d \in S$, for some $0 \neq c \in K$. By comparing coefficients we observe that f is homogeneous, of degree $d \in \mathbb{N}_0$ say, so that we have $f = \sum_{i=0}^{d} a_i X^i Y^{d-i} = Y^d \cdot \sum_{i=0}^{d} a_i (\frac{X}{Y})^i \in L$.

Similarly, g is homogeneous, of degree $e \in \mathbb{N}_0$ say, where from $\frac{f}{g} = (\frac{f}{g})^z = \frac{f^z}{g^z} = z^{d-e} \cdot \frac{f}{g} \in L$ we infer that $z^{d-e} = 1$. Thus letting $z \in G$ be an element of infinite order, or of finite order exceeding $\max\{d, e\}$, this entails $d = e$. Hence we have $g = \sum_{i=0}^{d} b_i X^i Y^{d-i} = Y^d \cdot \sum_{i=0}^{d} b_i (\frac{X}{Y})^i \in L$, showing that $\frac{f}{g} = \frac{\sum_{i=0}^{d} a_i (\frac{X}{Y})^i}{\sum_{i=0}^{d} b_i (\frac{X}{Y})^i} \in K(\frac{X}{Y}) \subseteq L$. Conversely, since $(\frac{X}{Y})^z = \frac{X^z}{Y^z} = \frac{zX}{zY} = \frac{X}{Y} \in L$, for all $z \in G$, we have $\frac{X}{Y} \in L^G$. Thus we have $L^G = K(\frac{X}{Y})$; note that $K \subseteq L^G$ and $L^G \subseteq L$ are pure transcendental such that $\mathrm{trdeg}_K(L^G) = 1$ and $\mathrm{trdeg}_{L^G}(L) = 1$.

b) Let $K = \mathbb{F}_q$ be finite. Then, by **Artin's Theorem**, G is cyclic, that is $G \cong C_{q-1}$, so that by (3.3) we have $S^G = K[X^{q-1}, X^{q-2}Y, \ldots, XY^{q-2}, Y^{q-1}]$.

We show that $\mathrm{Q}(S^G) = K(X^{q-1}, \frac{X}{Y})$: From $\frac{X^{q-1}}{X^{q-2}Y} = \frac{X}{Y}$ we get $K(X^{q-1}, \frac{X}{Y}) \subseteq \mathrm{Q}(S^G)$; conversely, from $X^{q-1} \cdot (\frac{Y}{X})^i = X^{q-1-i} Y^i$, for $i \in \{0, \ldots, q-1\}$, we get $\mathrm{Q}(S^G) \subseteq K(X^{q-1}, \frac{X}{Y})$, entailing equality.

We now consider L^G (without using the fact shown in (4.6) below that it already follows from G being finite that we necessarily have $L^G = \mathrm{Q}(S^G)$):

Let $0 \neq \frac{f}{g} \in L^G$, where $0 \neq f, g \in S$ are coprime. Letting $\zeta_{q-1} \in G$ be a primitive $(q-1)$-st root of unity, and writing $f = \sum_{d \geq 0} f_d$, from $f \sim f^{\zeta_{q-1}}$ we get $\sum_{d \geq 0} cf_d = \sum_{d \geq 0} \zeta_{q-1}^d f_d \in S$, for some $0 \neq c \in K$. By comparing coefficients we observe that $f = \sum_{d \geq 0} f_{d(q-1)+j}$, for some $j \in \{0, \ldots, q-2\}$, thus we have $f = \sum_{d \geq 0}(Y^{d(q-1)+j} \cdot \sum_{i=0}^{d(q-1)+j} a_{d,i}(\frac{X}{Y})^i) \in L$.

Similarly, we have $g = \sum_{d \geq 0} g_{d(q-1)+i}$, for some $i \in \{0, \ldots, q-2\}$, where from $\frac{f}{g} = \zeta_{q-1}^{j-i} \cdot \frac{f}{g} \in L$ we infer that $z^{j-i} = 1$, entailing that $i = j$. Hence we have $g = \sum_{d \geq 0}(Y^{d(q-1)+j} \cdot \sum_{i=0}^{d(q-1)+j} b_{d,i}(\frac{X}{Y})^i) \in L$, so that canceling Y^j yields

$$\frac{f}{g} = \frac{\sum_{d \geq 0}(Y^{d(q-1)} \cdot \sum_{i=0}^{d(q-1)+j} a_{d,i}(\frac{X}{Y})^i)}{\sum_{d \geq 0}(Y^{d(q-1)} \cdot \sum_{i=0}^{d(q-1)+j} b_{d,i}(\frac{X}{Y})^i)} \in K(Y^{q-1}, \frac{X}{Y}) = K(X^{q-1}, \frac{X}{Y}).$$

Since $\mathrm{Q}(S^G) \subseteq L^G$ anyway, we conclude that $L^G = \mathrm{Q}(S^G) = K(X^{q-1}, \frac{X}{Y})$. $\sharp$

Note that $K \subseteq L^G$ is pure transcendental such that $\mathrm{trdeg}_K(L^G) = 2$, while $L^G \subseteq L$ is finite. Indeed, since G acts faithfully on L, the field extension $L^G \subseteq L$ is finite Galois with respect to G, hence having degree $[L : L^G] = q-1$. Actually, L is the splitting field of the irreducible polynomial $T^{q-1} - (X^{q-1}) \in (L^G)[T]$, which splits as $\prod_{i=0}^{q-2}(T - \zeta_{q-1}^i X) \in L[T]$, where $\{X, \zeta_{q-1}X, \ldots, \zeta_{q-1}^{q-2}X\} \subseteq L$ is the G-orbit of X.

(4.3) Noetherian algebras. Let R be a commutative ring. An R-module M is called **Noetherian**, if any ascending chain $M_0 \leq M_1 \leq \cdots \leq M_i \leq \cdots \leq M$ of R-submodules **stabilizes**, that is 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 regular R-module R is Noetherian; recall that the R-submodules of R coincide with its ideals. For example, any field K is Noetherian.

We collect a few basic properties; see Exercise (19.4): Letting $N \leq M$ be R-modules, if M is Noetherian then so are N and M/N, and if conversely both N and M/N are Noetherian then so is M. In particular, any finite direct sum of Noetherian R-modules is Noetherian again. Moreover, M is Noetherian if and only if each submodule of M is finitely generated; and if R is Noetherian, then M is Noetherian if and only if M is a finitely generated R-module.

Example. Let K be a field, let $R := K[X_1, X_2, \ldots] := \bigcup_{n \in \mathbb{N}_0} K[X_1, \ldots, X_n]$ be the polynomial algebra in countably infinitely many indeterminates, and for $n \in \mathbb{N}_0$ let $I_n := (X_1, \ldots, X_n) \trianglelefteq R$. Then $\{0\} = I_0 \subset I_1 \subset \cdots \subset I_n \subset \cdots \trianglelefteq R$ is an infinite strictly ascending chain of ideals, hence R is not Noetherian; indeed the ideal $\bigcup_{n \in \mathbb{N}_0} I_n = (X_1, X_2, \ldots) \trianglelefteq R$ is not finitely generated, although the regular R-module $R = (1)$ is finitely generated.

(4.4) Theorem: Hilbert's Basis Theorem [Hilbert, 1890]**.** Let R be a Noetherian ring. Then the polynomial R-algebra $R[X]$ is Noetherian as well.

Proof. We show that any ideal $I \trianglelefteq R[X]$ is finitely generated. To this end let $J_d := \{\mathrm{lc}(f) \in R; 0 \neq f \in I, \deg(f) = d\} \,\dot\cup\, \{0\}$, for $d \in \mathbb{N}_0$. Hence we have $J_d \trianglelefteq R$ and $J_d \subseteq J_{d+1}$. Since R is Noetherian, let $k \in \mathbb{N}_0$ such that $J_d = J_k$ for $d \geq k$. Moreover, since all ideals of R are finitely generated, for $d \in \{0, \ldots, k\}$ let $J_d = (r_{d,1}, \ldots, r_{d,n_d}) \trianglelefteq R$, where $n_d \in \mathbb{N}_0$. Letting $f_{d,i} \in I$ such that $\deg(f_{d,i}) = d$ and $\mathrm{lc}(f_{d,i}) = r_{d,i} \in R$, for $i \in \{1, \ldots, n_d\}$, we show that $I = (f_{d,i}; d \in \{0, \ldots, k\}, i \in \{1, \ldots, n_d\}) \trianglelefteq R[X]$:

Let J denote the right hand side, and let $0 \neq f \in I$ such that $\deg(f) = d \geq 0$. We proceed by induction on $d \in \mathbb{N}_0$: If $d = 0$ then $f \in J_0 \subseteq J$, hence let $d \geq 1$. If $d > k$ then let $c := k$, if $d \leq k$ let $c := d$. Since $J_d = J_c$, there are $c_1, \ldots, c_{n_c} \in R$ such that $f' := f - \sum_{i=1}^{n_c} c_i X^{d-k} f_{k,i} \in I$ has degree $\deg(f') < d$, or we have $f' = 0$. By induction we have $f' \in J$, hence $f \in J$ as well. ♯

In particular, if K is a field, then by induction on $n \in \mathbb{N}_0$ the finitely generated polynomial K-algebra $K[X_1, \ldots, X_n]$ is Noetherian. Moreover, since any finitely generated commutative K-algebra R is a quotient of a finitely generated polynomial K-algebra, we conclude that R is Noetherian.

(4.5) Integral extensions. a) Let R be a commutative ring, and let $R \subseteq S$ be an **extension** of commutative rings, that is S is a commutative ring and we have $1_R = 1_S$. Hence S is an R-algebra, with structure homomorphism being the identity on R. In particular, if K is a field and R is a K-algebra, then S is a K-algebra as well.

An element $s \in S$ is called **integral** over R, if there is $0 \neq f \in R[X]$ monic, such that $f(s) = 0$; note that evaluating f at s refers to the universal property of $R[X]$. The extension $R \subseteq S$ is called **integral**, and S is called **integral** over R, if each element of S is integral over R.

Proposition. An element $s \in S$ is integral over R, if and only if there is an R-subalgebra of S containing s which is finitely generated as an R-module.

Proof. For $s \in S$ let $R \subseteq R[s] := \sum_{i \geq 0} s^i R \subseteq S$ be the smallest R-subalgebra of S containing s. Let now s be integral, and let $f = X^d + \sum_{i=0}^{d-1} f_i X^i \in R[X]$, where $d \geq 1$, such that $f(s) = 0$. Then we have $s^d = -\sum_{i=0}^{d-1} f_i s^i$, so that $R[s] = \sum_{i=0}^{d-1} s^i R$ is generated by $\{1, s, s^2 \ldots s^{d-1}\}$ as an R-module.

Let conversely $R \subseteq R[s] \subseteq T \subseteq S$, where T is an R-subalgebra which is finitely generated by $\{t_1, \ldots, t_k\}$ as an R-module, where $k \in \mathbb{N}$. Then for $j \in \{1, \ldots, k\}$ we have $t_j s = \sum_{i=1}^{k} t_i r_{ij}$, for some $r_{ij} \in R$. Let $A := XE_k - [r_{ij}]_{ij} \in R[X]^{k \times k}$ be the characteristic matrix associated with $[r_{ij}]_{ij} \in R^{k \times k}$, thus $\det(A) \in R[X]$ is monic of degree $k \geq 1$. We show that $\det(A)(s) = \det(A(s)) = 0$, entailing that s is integral over R:

We have $[t_1, \ldots, t_k] \cdot A(s) = [0, \ldots, 0] \in T^k$. Now **Cramer's Rule** says that replacing the i-th row of $A(s)$ by $[t_1, \ldots, t_k] \cdot A(s)$ yields a matrix having determinant $t_i \cdot \det(A(s))$, and since the matrix thus obtained has a zero row we conclude that $t_i \cdot \det(A(s)) = 0$, for all $i \in \{1, \ldots, k\}$. Thus since $1 \in T$ is an R-linear combination of $\{t_1, \ldots, t_k\}$, we infer that $\det(A(s)) = 0$. $\sharp$

Hence $R \subseteq S$ is integral if and only if it is generated as an R-algebra by integral elements. Moreover, the subset $R \subseteq \overline{R}^S := \{s \in S; s \text{ is integral over } R\} \subseteq S$ is a subring of S, being called the **integral closure** or **normalization** of R in S; in particular, if $\overline{R}^S = R$ then R is called **integrally closed** or **normal** in S. Moreover, if R is a K-algebra then $\overline{R}^S$ is a K-algebra as well.

If R is a domain and R is integrally closed in its own field of fractions, then R is called **integrally closed** or **normal**; in particular, if R is factorial then it is integrally closed; see Exercise (19.11).

b) The extension $R \subseteq S$ is called **finite**, if S is a finitely generated integral R-algebra, or equivalently if S is a finitely generated R-module.

Proposition. Let $R \subseteq S$ be an integral extension, such that S is a finitely generated K-algebra. Then R is a finitely generated K-algebra as well, and the extension $R \subseteq S$ is finite.

Proof. Let $\{f_1, \ldots, f_k\} \subseteq S$ be a K-algebra generating set, for some $k \in \mathbb{N}_0$. (Note that for $S = S[V]$ we might choose $k = \dim_K(V)$.) Moreover, let $F_i \in R[X]$ be monic such that $F_i(f_i) = 0 \in S$, for $i \in \{1, \ldots, k\}$, and let $T \subseteq R \subseteq S$ be the K-algebra generated by the coefficients of the polynomials $F_1, \ldots, F_k$.

Since all $f_1, \ldots, f_k \in S$ are integral over T, we conclude that S is integral over T. Since S is a finitely generated K-algebra, it is a finitely generated T-algebra as well, saying that the extension $T \subseteq S$ is finite, that is S is a finitely generated T-module. Thus from $T \subseteq R \subseteq S$ we infer that S is a finitely generated R-module, that is the extension $R \subseteq S$ is finite as well.

Since T is a finitely generated K-algebra, it is Noetherian. Since S is a finitely generated T-module, it is a Noetherian T-module. Thus the T-submodule $R \leq S$ is a Noetherian T-module as well. Hence R is a finitely generated T-module. Since T is a finitely generated K-algebra, R is a finitely generated K-algebra. $\sharp$

(4.6) Theorem: Noether's Finiteness Theorem [Noether, 1916, 1926]**.** Let K be a field, let G be a finite group, and let S be a finitely generated graded G-algebra with faithful G-action.
a) Let S be a domain and let $L := \mathrm{Q}(S)$. Then the field extension $L^G \subseteq L$ is finite Galois with respect to G, and we have $\mathrm{Q}(S^G) = L^G$.
b) The invariant algebra S^G is finitely generated, and the extension $S^G \subseteq S$ is finite. Moreover, if S is an integrally closed domain, then so is S^G.

Proof. a) Let $0 \neq \frac{f}{g} \in L^G$, where $0 \neq f, g \in S$. Letting $g' := \prod_{1 \neq z \in G} g^z \in S$, the **norm** of g is given as $N^G(g) := gg' \in S^G \setminus \{0\}$, and $\frac{fg'}{gg'} = \frac{f}{g} \in L^G$ implies

$fg' \in L^G \cap S = S^G$, entailing $\frac{f}{g} = \frac{fg'}{gg'} \in \mathrm{Q}(S^G)$, showing that $\mathrm{Q}(S^G) = L^G$. Moreover, G acts faithfully on L, hence the field extension $L^G \subseteq L$ is finite Galois with respect to G.

b) For $f \in S$ let $F_f := \prod_{g \in G}(X - f^g) \in S[X]$; hence F_f is monic such that $F_f(f) = 0$. The G-action by K-algebra automorphisms on S can be extended (coefficientwise) to a G-action by K-algebra automorphisms on $S[X]$. Hence we have $(F_f)^h = \prod_{g \in G}(X - f^g)^h = \prod_{g \in G}(X - f^{gh}) = \prod_{g \in G}(X - f^g) = F_f$, for all $h \in G$, thus $F_f \in S^G[X]$, being monic. This shows that the extension $S^G \subseteq S$ is integral. Hence, since S is a finitely generated K-algebra, it follows from (4.5) that the extension $S^G \subseteq S$ is finite and that S^G is finitely generated.

Finally, assume that S is an integrally closed domain, and let $f \in \mathrm{Q}(S^G) = L^G \subseteq L = \mathrm{Q}(S)$ be integral over S^G. Then f is a root of a monic polynomial in $S^G[X] \subseteq S[X]$, thus f is integral over S as well. This implies that $f \in S \cap L^G = S^G$, showing that S^G is integrally closed. $\sharp$

(4.7) Remark: Finite generation. Letting K be a field, note first that there are K-subalgebras of polynomial algebras which are not finitely generated indeed: For example, since $XY^i \notin K[X, XY, \ldots, XY^{i-1}] \subseteq K[X, Y]$, for $i \in \mathbb{N}$, the K-subalgebra of $K[X, Y]$ generated by $\{XY^i; i \in \mathbb{N}_0\}$ is not finitely generated. Actually, this leads to a counterexample to finite generation of invariant algebras in a more general framework, namely for a finitely generated **non-reduced** algebra, that is an algebra having nilpotent elements, which works for certain finite groups; see Exercise (18.20). Moreover, the above proof of finite generation of invariant algebras is purely non-constructive, and does not give the slightest clue how to actually find a finite generating set.

If G is a group, and V is a $K[G]$-module, the invariant algebra $S[V]^G$ is not finitely generated in general: There is a famous counterexample for an infinite group G in dimension 32 over $\mathbb{C}$ by NAGATA [1959]; see Exercise (18.20). This is closely related to **Hilbert's 14-th problem**: If $L \subseteq S(V)$ is a subfield, is $L \cap S[V]$ a finitely generated K-algebra? Since $S(V)^G \cap S[V] = S[V]^G$ for any group G, this counterexample answers this question to the negative as well.

But invariant algebras are finitely generated whenever G is **linearly reductive**; see (5.3). Actually, HILBERT worked on linearly reductive groups, although this notion has only been coined later, whereas NOETHER developed the machinery for finite groups. For example, $\mathrm{SL}_n(\mathbb{C})$ is linearly reductive, for $n \in \mathbb{N}$, so that in particular the invariant algebras $R_{n,d} := S[\mathcal{V}_{n,d}]^{\mathrm{SL}_n(\mathbb{C})}$ for the natural action of $\mathrm{SL}_n(\mathbb{C})$ on the $\mathbb{C}$-vector space $\mathcal{V}_{n,d} := \mathbb{C}[\mathbb{C}^n]_d = S[(\mathbb{C}^n)^*]_d$ of n-ary d-forms, for $d \in \mathbb{N}$, are finitely generated $\mathbb{C}$-algebras.

For binary d-forms, that is $n = 2$, finite generation of the invariant algebra $R_{2,d} := S[\mathcal{V}_{2,d}]^{\mathrm{SL}_2(\mathbb{C})}$ has already been shown combinatorially by GORDAN [1868]. Still, there is only poor knowledge as far as explicit finite generating sets are concerned: We have seen in (1.3) that for quadratic forms the invariant algebra $R_{2,2}$ is a univariate polynomial algebra in the discriminant, which is homogeneous of degree 2. For cubic forms the invariant algebra $R_{2,3}$ also is a univariate polynomial algebra in the discriminant, which is homogeneous of degree 4. For quaternary forms the invariant algebra $R_{2,4}$ is a bivariate polynomial algebra, generated by homogeneous elements of degree $[2, 3]$, while the discriminant has degree 6. Moreover, explicit generators for the invariant algebra $R_{2,d}$ are only known for $d \in \{5, 6, 8\}$, in which cases $R_{2,d}$ no longer is a polynomial algebra [Shioda, 1967].

5 Degree bounds

(5.1) Trace maps. Let G be a group, let $H \leq G$ be a subgroup of index $k := [G\colon H] \in \mathbb{N}$, and let $\mathcal{T} := \{t_1, \ldots, t_k\} \subseteq G$ be a **(right) transversal** of H in G, that is a set of representatives of the right cosets $H\backslash G$ of H in G.

Let K be a field, and let S be a graded G-algebra. Then we have an extension $S^G \subseteq S^H$ of graded K-algebras. The **relative trace map** or **relative transfer map** Tr_H^G with respect to H is defined as the K-linear map $\mathrm{Tr}_H^G\colon S^H \to S^G\colon f \mapsto \sum_{i=1}^k f \cdot t_i$. If G is finite, then $\mathrm{Tr}^G := \mathrm{Tr}_{\{1\}}^G\colon S \to S^G\colon f \mapsto \sum_{g\in G} f \cdot g$ is called the **trace map** or **transfer map**.

The relative trace map is well-defined indeed, and independent of the choice of the transversal: For $f \in S^H$ we have $\mathrm{Tr}_H^G(f) \cdot g = \sum_{i=1}^k (f \cdot t_i g) = \sum_{i=1}^k (f \cdot h_i t_{i\cdot\pi(g)}) = \sum_{i=1}^k (f \cdot t_{i\cdot\pi(g)}) = \sum_{i=1}^k (f \cdot t_i) = \mathrm{Tr}_H^G(f)$, for $g \in G$, where $\pi\colon G \to \mathcal{S}_{H\backslash G} \cong \mathcal{S}_k$ is the permutation action of G on $H\backslash G$, so that $t_i g = h_i t_{i\cdot\pi(g)}$ for some $h_i \in H$; thus we have $\mathrm{Tr}_H^G(f) \in S^G$ indeed, where $\mathrm{Tr}_H^G(S^H) \subseteq S^G$. Moreover, if $\mathcal{T}' := \{t'_1, \ldots, t'_k\} \subseteq G$ also is a transversal of H in G, then we may assume that $t'_i = h_i t_i$, for $i \in \{1, \ldots, k\}$ and some $h_i \in H$, so that we get $\sum_{i=1}^k (f \cdot t'_i) = \sum_{i=1}^k (f \cdot h_i t_i) = \sum_{i=1}^k (f \cdot t_i) = \mathrm{Tr}_H^G(f)$, showing that Tr_H^G is independent of the choice of $\mathcal{T}$.

For any subgroup $H \leq U \leq G$ we have **transitivity** of trace maps, that is $\mathrm{Tr}_H^U \cdot \mathrm{Tr}_U^G = \mathrm{Tr}_H^G$: Letting $\mathcal{T}' \subseteq U$ be a transversal for H in U, and $\mathcal{T}'' \subseteq G$ be a transversal for U in G, we get the transversal $\mathcal{T} := \{t't'' \in G; t' \in \mathcal{T}, t'' \in \mathcal{T}''\}$ for H in G. Then for $f \in S^H$ we have $\mathrm{Tr}_U^G(\mathrm{Tr}_H^U(f)) = \sum_{t''\in\mathcal{T}''} (\mathrm{Tr}_H^U(f) \cdot t'') = \sum_{t''\in\mathcal{T}''} (\sum_{t'\in\mathcal{T}'} (f \cdot t't'')) = \sum_{t\in\mathcal{T}} (f \cdot t) = \mathrm{Tr}_H^G(f)$.

Moreover, $\mathrm{Tr}_H^G\colon S^H \to S^G$ is a homomorphism of graded S^G-modules: For $d \in \mathbb{N}_0$ we have $\mathrm{Tr}_H^G(S_d^H) \leq S_d^G$, and for $f \in S^G$ and $g \in S^H$ we have $\mathrm{Tr}_H^G(gf) = \sum_{i=1}^k (gf)^{t_i} = \sum_{i=1}^k g^{t_i} f^{t_i} = \sum_{i=1}^k g^{t_i} f = (\sum_{i=1}^k g^{t_i}) \cdot f = \mathrm{Tr}_H^G(g) \cdot f$. Thus $S_H^G := \mathrm{Tr}_H^G(S^H) \trianglelefteq S^G$ is a homogeneous ideal, where $S_H^G \subseteq S_U^G \subseteq S_G^G = S^G$.

Proposition. Assume that S is a domain, and that G acts faithfully on S. Then we have $S_H^G \neq \{0\}$.

Proof. We may assume that $H = \{1\}$. Since G acts faithfully on $L := \mathrm{Q}(S)$, the elements of G induce pairwise different field automorphisms of L, which by **Dedekind's Independence Theorem** are L-linearly independent in the L-vector space $\mathrm{End}_K(L)$. Hence the latter are K-linearly independent in the K-vector space $\mathrm{End}_K(S)$; in particular we have $\sum_{g\in G} g \neq 0 \in \mathrm{End}_K(S)$. $\sharp$

If G does not act faithfully on S, then we might have $S_H^G = \{0\}$: For example, let K be such that $\mathrm{char}(K) = 2$, let $G := \langle z\rangle \cong C_2$ act trivially on $V := K$, and let $H := \{1\}$; then we have $S[V]^G = S[V] = K[X]$, and from $\mathrm{Tr}^G(X^d) = X^d + X^d \cdot z = 2X^d = 0$, for $d \in \mathbb{N}_0$, we infer that $S[V]^G_{\{1\}} = \{0\}$.

(5.2) Reynolds operators. Let K be a field, let G be group, let $H \leq G$ be a subgroup of finite index $[G\colon H] \in \mathbb{N}$, and let S be a commutative graded G-algebra. We address the question when we have $S_H^G = S^G$: To this end, letting $\mathcal{T} \subseteq G$ be a transversal for H in G, for $f \in S^G$ we observe that $\mathrm{Tr}_H^G(f) = \mathrm{Tr}_H^G(1 \cdot f) = \mathrm{Tr}_H^G(1) \cdot f = (\sum_{t\in\mathcal{T}}(1 \cdot t)) \cdot f = ([G\colon H] \cdot 1) \cdot f = [G\colon H] \cdot f$, saying that $\mathrm{Tr}_H^G|_{S^G} = [G\colon H] \cdot \mathrm{id}_{S^G}$.

a) If $\mathrm{char}(K) \nmid [G\colon H]$, then the **relative Reynolds operator** with respect to H is defined as $\mathcal{R}_H^G := \frac{1}{[G\colon H]} \cdot \mathrm{Tr}_H^G\colon S^H \to S^G$. Hence $\mathcal{R}_H^G$ restricts to the identity map on S^G, so that $S_H^G = S^G$. Moreover, $\mathcal{R}_H^G(f - \mathcal{R}_H^G(f)) = 0$, for $f \in S^H$, implies that $S^H = S_H^G \oplus \ker(\mathcal{R}_H^G) = S^G \oplus \ker(\mathrm{Tr}_H^G)$ as graded S^G-modules, where $\mathcal{R}_H^G$ is the associated projection.

In particular, if G is finite such that $\mathrm{char}(K) \nmid |G|$, called the **non-modular** case, we have the **Reynolds operator** $\mathcal{R}^G := \mathcal{R}^G_{\{1\}} = \frac{1}{|G|} \cdot \mathrm{Tr}^G\colon S \to S^G$; hence $S = S^G \oplus \ker(\mathcal{R}^G)$ as graded S^G-modules, $\mathcal{R}^G$ being the associated projection.

b) If $\mathrm{char}(K) \mid [G\colon H]$, then Tr_H^G restricts to the zero map on S^G, so that $(\mathrm{Tr}_H^G)^2$ is the zero map. Hence we have $S_H^G \subseteq S^G \subseteq \ker(\mathrm{Tr}_H^G) \subseteq S^H$ as graded S^G-modules, and since $S_0^G = S_0 = K$ we have $S_H^G \subseteq S_+^G \lhd S^G$ and $1 \in \ker(\mathrm{Tr}_H^G)$. Apart from that, only little is known about the trace ideal $S_H^G \lhd S^G$, even for the symmetric algebra $S[V]$ where V is a $K[G]$-module.

Moreover, if S is finitely generated, and G is finite acting faithfully on S, then by Noether's Finiteness Theorem S^G is finitely generated, hence Noetherian, and S is a finitely generated S^G-module, so that $\ker(\mathrm{Tr}_H^G) < S^H$ are finitely generated S^G-modules as well; thus **Carlson's Lemma**, see Exercise (19.18), implies that $\ker(\mathrm{Tr}_H^G)$ is not a direct summand of S^H as graded S^G-modules.

In particular, if G is finite such that $\mathrm{char}(K) \mid |G|$, being called the **modular** case, inasmuch Tr^G restricts to the zero map on $S[V]^G$, we get a fundamentally different behavior of the trace map Tr^G compared to the non-modular case. Again, only little is known about $S^G_{\{1\}}$, even for the symmetric algebra $S[V]$ where V is a $K[G]$-module. (Most notably there is **Feshbach's Theorem** [1981] on $S[V]^G_{\{1\}} \lhd S[V]^G$, whose details we are not able to give here.)

(5.3) Hilbert ideals. a) Let K be a field, let G be group, and let S be a commutative graded G-algebra. The **Hilbert ideal** $\mathcal{I}_G = \mathcal{I}_G(S) \unlhd S$ is the ideal generated by the homogeneous invariants of positive degree, that is $\mathcal{I}_G := S_+^G \cdot S = (S_+ \cap S^G) \cdot S \trianglelefteq S$; hence $\mathcal{I}_G \subseteq S_+$ is a proper homogeneous ideal.

The quotient K-algebra $S_G := S/\mathcal{I}_G$ is called the associated **coinvariant algebra**. Then S_G is a graded G-algebra again, as well as an (S^G/S_+^G)-module, that is a K-vector space. If additionally S is a finitely generated K-algebra, then by Noether's Finiteness Theorem S is a finitely generated S^G-module, so that S_G is a finitely generated K-vector space, and thus is a $K[G]$-module.

If $\operatorname{char}(K) \nmid |G|$, then applying the Reynolds operator $\mathcal{R}^G$, which projects S onto S^G, and S_G onto $(S_G)^G$, we get $(S_G)^G = \mathcal{R}^G(S_G) = \mathcal{R}^G(S/\mathcal{I}_G) = (\mathcal{R}^G(S) + \mathcal{I}_G)/\mathcal{I}_G = (R + \mathcal{I}_G)/\mathcal{I}_G = (R_0 + \mathcal{I}_G)/\mathcal{I}_G = (S_G)_0 \cong K$.

b) Any set of homogeneous invariants of positive degree generating S^G as a K-algebra also generates $\mathcal{I}_G \trianglelefteq S$ as an ideal. Actually, in the non-modular case the converse of this statement holds as well; note that if S is a finitely generated K-algebra, and thus Noetherian, then $\mathcal{I}_G$ indeed is generated by finitely many homogeneous invariants of positive degree:

Theorem: Hilbert's Finiteness Theorem [Hilbert, 1890]**.** Let G be finite such that $\operatorname{char}(K) \nmid |G|$, and let $\mathcal{F} \subseteq S_+^G$ be a set of homogeneous invariants such that $\mathcal{I}_G = (\mathcal{F}) \trianglelefteq S$. Then $\mathcal{F}$ generates S^G as a K-algebra.

Proof. Let $R \subseteq S^G$ be the K-algebra generated by $\mathcal{F}$, and let $h \in S^G$ be homogeneous such that $\deg(h) = d \in \mathbb{N}_0$. We proceed by induction on $d \geq 0$; the case $d = 0$ being trivial, let $d \geq 1$. Since $h \in \mathcal{I}_G$, there are $f_i \in \mathcal{F}$ and $g_i \in S_{d-\deg(f_i)}$ such that $h = \sum_{i=1}^k f_i g_i \in S$, for some $k \in \mathbb{N}_0$. Thus we have $h = \mathcal{R}^G(h) = \sum_{i=1}^k f_i \cdot \mathcal{R}^G(g_i)$. Since $\mathcal{R}^G(g_i) \in S^G$ such that $\deg(\mathcal{R}^G(g_i)) = d - \deg(f_i) < d$, by induction we have $\mathcal{R}^G(g_i) \in R$, so that $h \in R$ as well. $\sharp$

Note that in the above proof only the property of $\mathcal{R}^G \colon S \to S^G$ being a projection of graded S^G-modules is used. In view of this, linear algebraic groups G over an algebraically closed field K, which for any algebraic G-module V possess a **generalized Reynolds operator** $\mathcal{R}^G \colon K[V] = S[V^*] \to S[V^*]^G = K[V]^G$ sharing the above properties, are called **linearly reductive**, see (4.7); thus for these groups the assertion of Hilbert's Finiteness Theorem holds.

(5.4) Noether's degree bound. We proceed to prove a degree bound for generating sets of invariant K-algebras of finite groups G, which holds in the non-modular case. Actually, Noether stated the result in the case $\operatorname{char}(K) = 0$ only, but the proof is valid whenever $(|G|)!$ is invertible in K, thus if $\operatorname{char}(K) > |G|$ as well. We present a recent general proof, thus closing the **Noether gap**.

To this end, let K be a field, let G be a finite group such that $\operatorname{char}(K) \nmid |G|$, and let S be a commutative graded G-algebra.

Proposition: Benson's Lemma [2000]**.** Let $I \trianglelefteq S$ be a G-**stable** ideal, that is $I \cdot g \subseteq I$ for all $g \in G$. Then we have $I^{|G|} \subseteq I^G \cdot S \trianglelefteq S$.

Proof. Let $\{f_g \in I; g \in G\}$. Since $\prod_{g\in G}(gh-1) = 0 \in K[G]$, for $h \in G$, we get $\prod_{g\in G}(f_g \cdot gh - f_g) = f_g \cdot \prod_{g\in G}(gh-1) = 0 \in S$. Expanding the product, using the principle of inclusion-exclusion, and summing over $h \in G$ yields

$$\sum_{M\subseteq G} \Big((-1)^{|G\setminus M|} \cdot \mathrm{Tr}^G(\prod_{g\in M}(f_g \cdot g)) \cdot \prod_{g\in G\setminus M} f_g\Big) = 0.$$

If $M \neq \emptyset$, then we have $\mathrm{Tr}^G(\prod_{g\in M}(f_g \cdot g)) \in I \cap S^G = I^G$, thus the associated summand belongs to $I^G \cdot S \trianglelefteq S$. Hence for $M = \emptyset$ we obtain $\mathrm{Tr}^G(1) \cdot \prod_{g\in G} f_g \in I^G \cdot S$ as well, which since $\mathrm{Tr}^G(1) = |G|$ entails $\prod_{g\in G} f_g \in I^G \cdot S$. ♯

Theorem: Noether's degree bound [Noether, 1916; Fleischmann, 2000; Fogarty, 2001]**.** Let S be generated by homogeneous elements of degree at most $b \in \mathbb{N}$. Then the Hilbert ideal $\mathcal{I}_G \trianglelefteq S$ is generated by homogeneous invariants of positive degree at most $b \cdot |G|$.

Proof. Letting $I := (f \in S_d^G; d \in \{1, \ldots, b \cdot |G|\}) \trianglelefteq S$, we have $I \subseteq \mathcal{I}_G$, and we have to show equality:

Firstly, Benson's Lemma, applied to the G-stable ideal $S_+ \trianglelefteq S$, yields $S_+^{|G|} \subseteq \mathcal{I}_G \trianglelefteq S$. Since any homogeneous generating set of S contains a generating set of the ideal S_+, we conclude that S_+ is generated by homogeneous elements of degree at most b, so that $S_+^{|G|}$ is generated by homogeneous elements of degree at most $b \cdot |G|$. Hence we infer that actually $S_+^{|G|} \subseteq I \subseteq \mathcal{I}_G$.

Now let $f \in (\mathcal{I}_G)_d$, for some $d \geq 1$. If $d \leq b \cdot |G|$ then we may assume that f is of the form $f = gh \in S$, where $g \in S^G$ and $h \in S$ are homogeneous; thus we have $\deg(g) \leq d$, so that $f \in I$. Hence let $d \geq b \cdot |G|$.

Then we may assume hat f is of the form $f = \prod_{i=1}^k f_i \in S$, for some $k \in \mathbb{N}$, where the $f_i \in S_{d_i}$ are homogeneous of degree $d_i \in \{1, \ldots, b\}$, so that we have $b \cdot |G| \leq d = \sum_{i=1}^k d_i \leq kb$; hence $k \geq |G|$, thus $f \in S_+^{|G|} \subseteq I$. (Note that the last part only uses the fact that $f \in S_d$, so that we actually have $S_d \subseteq \mathcal{I}_G$.) ♯

We derive a couple of consequences:

a) If $N \trianglelefteq G$ is normal, then we have the extension $S^G = (S^N)^{G/N} \subseteq S^N \subseteq S$, giving rise to the following relative version of Noether's degree bound:

Let G be arbitrary, let $N \trianglelefteq G$ be of finite index such that $\mathrm{char}(K) \nmid [G\colon N]$, and let S^N be generated by homogeneous N-invariants of degree at most $b \in \mathbb{N}$. Then the **relative Hilbert ideal** $\mathcal{I}_G^N := S_+^G \cdot S^N \trianglelefteq S^N$ is generated by homogeneous G-invariants of positive degree at most $b \cdot [G\colon N]$. Consequently, by Hilbert's Finiteness Theorem applied to G/N, we conclude that S^G is generated by homogeneous invariants of degree at most $b \cdot [G\colon N]$.

b) Let G be finite such that $\mathrm{char}(K) \nmid |G|$ again, and let S be generated by the finite set $\mathcal{F}$ consisting of homogeneous elements of degree at most b. (If $S = S[V]$, where V is a $K[G]$-module, then we may of course take the indeterminates of degree $b = 1$ as homogeneous generators.) Then there is a finite generating set of S^G consisting of homogeneous invariants of degree at most $b \cdot |G|$, thus being contained in the K-subspace $\bigoplus_{d=1}^{b\cdot|G|} S_d^G = \bigoplus_{d=1}^{b\cdot|G|} \mathcal{R}^G(S_d)$.

Hence we may algorithmically find a minimal homogeneous generating set of S^G by evaluating $\mathcal{R}^G$ successively at all monomials in the generators $\mathcal{F}$ of degree $\{1, 2, \ldots, b \cdot |G|\}$, and for a given degree pick suitable indecomposable homogeneous invariants, that is which are not contained in the K-subalgebra generated by the homogeneous invariants of strictly smaller degree.

(5.5) Remark: Degree bounds. Let K be a field, let G be a finite group, and let V be a faithful $K[G]$-module such that $n := \dim_K(V) \in N_0$.

a) In the non-modular case $\mathrm{char}(K) \nmid |G|$, Noether's bound $\beta(S[V]^G) \leq |G|$ is best possible inasmuch no improvement is possible in terms of the group order alone: For the case of cyclic groups we have equality, see (3.3) and (3.4).

But if $\mathrm{char}(K) = 0$ and G is not cyclic, then **Schmid's Theorem** [1991] says that $\beta(S[V]^G) \leq |G| - 1$, and the **Domokos–Hegedűs Theorem** [2000] says that $\beta(S[V]^G) \leq \frac{3}{4} \cdot |G|$ if $|G|$ is even, and $\beta(S[V]^G) \leq \frac{5}{8} \cdot |G|$ if $|G|$ is odd. In practice, Noether's bound and its improvements typically are not at all sharp.

In view of Schmid's Theorem, the relative version of Noether's degree bound can be improved to $\beta(S[V]^G) \leq \beta(S[V]^N) \cdot ([G\colon N] - 1)$ whenever G/N is non-cyclic; note that this in particular holds for if G is a non-cyclic nilpotent group, with respect to the last but one step of its upper central series.

Still, the relative version of Noether's degree bound needs the assumption of $N \trianglelefteq G$ being normal. Actually, as was already mentioned, NOETHER's original proof works more generally for subgroups $H \leq G$, but needs the assumption that $([G\colon H])!$ is invertible in K. Alone, the new elegant technique does not seem to yield this result as well. Hence there still is a **baby Noether gap** left.

b) In the modular case $\mathrm{char}(K) \mid |G|$, Noether's bound does not hold in general, as we will see by an example in (5.7). Similarly, neither Benson's Lemma nor Hilbert's Finiteness Theorem hold in general, as the example in (5.7) also shows. The counterexample mentioned actually is smallest with respect to group order, while one smallest with respect to dimension is given by the regular representation of C_4 in characteristic 2 [BERTIN, 1965]; see (9.8).

Even worse, there cannot be a **global bound** for $\beta(S[V]^G)$ in terms of $|G|$ alone, as is indicated by the example given in (5.7). Indeed, for any field K, it follows from **Richman's lower degree bound** [1996] that if there is a common bound for $\beta(S[V]^G)$, for all $K[G]$-modules V, then we necessarily have $\mathrm{char}(K) \nmid |G|$. Moreover, BRYANT, KEMPER [2005] have shown, that if G is a linear algebraic group having such a common bound for all algebraic G-modules V, then G is necessarily finite (such that $\mathrm{char}(K) \nmid |G|$).

The best, but astronomical general degree bound in terms of $|G|$ and n is given by **Hermann's Theorem** [1926], saying that $\beta(S[V]^G) \leq n(|G|-1) + |G|^{n \cdot 2^{n-1}+1} \cdot n^{2^{n-1}+1}$. Much better results are known under additional assumptions, where supported by substantial computational evidence, the even stronger subsequent conjecture should actually be true:

i) Göbel's degree bound [1995], see (9.6), says that whenever V is a permutation $K[G]$-module, then we have $\beta(S[V]^G) \leq \max\{n, \binom{n}{2}\}$.
ii) Broer's degree bound [1997], see (16.4), says that whenever K is infinite and $S[V]^G$ is Cohen-Macaulay, then $\beta(S[V]^G) \leq \max\{|G|, n(|G|-1)\}$.
iii) Symonds's degree bound [2009] says that whenever K is finite, then again we have $\beta(S[V]^G) \leq \max\{|G|, n(|G|-1)\}$.

Conjecture [Kemper]**.**
a) The Broer-Symonds bound $\beta(S[V]^G) \leq \max\{|G|, n(|G|-1)\}$ always holds.
b) If $S[V]^G$ is Cohen-Macaulay, then Noether's bound $\beta(S[V]^G) \leq |G|$ holds.
c) For the Hilbert ideal, Noether's bound $\beta(\mathcal{I}_G(S[V])) \leq |G|$ always holds.

We remark that Fleischmann [2000] has shown that Noether's bound holds for Hilbert ideals, if V is a **trivial-source** $K[G]$-module, see (6.5), thus in particular if V is a permutation $K[G]$-module.

(5.6) Example: The cyclic group of order 2. Let K be a field, and let $G := \langle z \rangle \cong C_2$ act on K^2 by $z \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. By (3.4), letting $S := K[X,Y]$ we have $S^G = K[X+Y, XY]$, being a polynomial algebra.

Hence the Hilbert ideal is given as $\mathcal{I}_G := (X+Y, XY) = (X+Y, X^2) \trianglelefteq S$. Thus for the coinvariant algebra we have $S_G = S/\mathcal{I}_G \cong K[X]/(X^2)$ as K-algebras, the isomorphism being inherited from the K-algebra homomorphism $S \to K[X] \colon X \mapsto X, Y \mapsto -X$; note that $\dim_K(S_G) = 2$, and actually $S_G \cong K[G]$ as $K[G]$-modules, the isomorphism being inherited from the K-algebra homomorphism $K[X] \to K[G] \colon X \mapsto z+1$.

In particular, Hilbert's Finiteness Theorem holds in any characteristic. From $S_+^2 = (X^2, XY, Y^2) \trianglelefteq S$ we conclude that $S_+^2 \subseteq \mathcal{I}_G \subseteq S_+$, that is Benson's Lemma holds for $I = S_+$ in any characteristic. Similarly, Noether's degree bound holds in any characteristic, and is sharp.

i) If $\mathrm{char}(K) \neq 2$ then we recover the generating set given above as follows: For $d = 1$ we have $\mathrm{Tr}^G(X) = \mathrm{Tr}^G(Y) = X+Y$, so that $S_1^G = \langle X+Y \rangle_K$. For $d = 2$ we have $(X+Y)^2 \in S_2^G$; moreover, we have $\mathrm{Tr}^G(X^2) = \mathrm{Tr}^G(Y^2) = X^2+Y^2$ and $\mathcal{R}^G(XY) = XY$, where from $(X+Y)^2 = (X^2+Y^2) + 2XY$ we infer that $S_2^G = \langle X^2+Y^2, XY \rangle_K = \langle (X+Y)^2, XY \rangle_K$. Hence we have $S^G = K[X+Y, XY]$.

ii) If $\mathrm{char}(K) = 2$, we determine the trace ideal $S_{\{1\}}^G \subseteq S_+^G$: For $d \in \mathbb{N}_0$ odd and even, respectively, we have

$$S_d^G = \begin{cases} \langle X^d + Y^d, X^{d-1}Y + XY^{d-1}, \ldots, X^{\frac{d+1}{2}}Y^{\frac{d-1}{2}} + X^{\frac{d-1}{2}}Y^{\frac{d+1}{2}} \rangle_K, \\ \langle X^d + Y^d, X^{d-1}Y + XY^{d-1}, \ldots, X^{\frac{d}{2}}Y^{\frac{d}{2}} \rangle_K. \end{cases}$$

For $i \in \{0, \ldots, \lfloor \frac{d}{2} \rfloor\}$ we get $\mathrm{Tr}^G(X^iY^{d-i}) = X^iY^{d-i} + X^{d-i}Y^i$, so that we infer $\mathrm{Tr}^G(S_d) = S_d^G$ if d is odd, while $S_d^G/\mathrm{Tr}^G(S_d)$ is one-dimensional if d is even; note that $\mathrm{Tr}^G((XY)^{\frac{d}{2}}) = 2(XY)^{\frac{d}{2}} = 0$. Thus from $\sum_{d\geq 0} T^{2d} = \frac{1}{1-T^2} \in \mathbb{Q}(T)$ we get $H_{S^G_{\{1\}}} = H_{S^G} - \frac{1}{1-T^2} = \frac{1}{(1-T)(1-T^2)} - \frac{1}{1-T^2} = \frac{T}{(1-T)(1-T^2)} \in \mathbb{Q}(T)$.

Since $X + Y = \mathrm{Tr}^G(X)$ we have $(X + Y) \cdot S^G \subseteq S^G_{\{1\}}$, where the principal ideal $(X + Y) \trianglelefteq S^G$ is the free S^G-module generated by $X + Y$, so that $H_{(X+Y)} = T \cdot H_{S^G} = \frac{T}{(1-T)(1-T^2)} = H_{S^G_{\{1\}}} \in \mathbb{Q}(T)$. Thus we infer $S^G_{\{1\}} = (X + Y) \trianglelefteq S^G$.

Finally, letting $R := K[XY] \subseteq S^G$ be the polynomial algebra generated by XY, we have $R \cap S^G_{\{1\}} = \{0\}$ and $H_R = \frac{1}{1-T^2} \in \mathbb{Q}(T)$, from which we infer that $S^G = R \oplus S^G_{\{1\}}$ as graded K-vector spaces, so that $S^G/S^G_{\{1\}} \cong R$ is the univariate polynomial algebra generated in degree 2.

(5.7) Example: Vector invariants. a) Let K be a field, let $G := \langle z \rangle \cong C_2$, and let $V := K^2$ be the permutation $K[G]$-module given by $z \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. We consider the faithful $K[G]$-module $V^{\oplus n} := V \oplus \cdots \oplus V$ for $n \geq 2$; hence $\dim_K(V^{\oplus n}) = 2n$. (We have considered the case $n = 1$ in (5.6).)

Letting $S := K[\mathcal{X}]$, where $\mathcal{X} := \{X_1, Y_1, \ldots, X_n, Y_n\}$, the group G acts on S by $X_i \cdot z = Y_i$ and $Y_i \cdot z = X_i$, for $i \in \{1, \ldots, n\}$. Hence G permutes the K-basis $\mathcal{X}_d \subseteq S_d$ consisting of the monomials of degree $d \in \mathbb{N}_0$, so that writing $\mathcal{X}_d = \coprod_{j=1}^{k_d} \mathcal{X}_{d,j}$ as a disjoint union of G-orbits, where $k_d = |\mathcal{X}_d/G| \in \mathbb{N}$, we conclude that $\{\sum_{f\in\mathcal{X}_{d,j}} f \in S_d; j \in \{1, \ldots, k_d\}\} \subseteq S_d^G$ is a K-basis; see (9.1).

Since z exchanges X_i and Y_i, for all i, we conclude that a monomial f is fixed by z, if and only if X_i and Y_i occur with the same multiplicity in f, for all i, that is f is a monomial in the invariants $q_i := X_iY_i \in S_2^G$. Otherwise, f belongs to an orbit of length 2, yielding an invariant $f \cdot (1 + z) = q \cdot (g \cdot (1 + z))$, where q is a monomial in the q_i, and g is a monomial which is not divisible by any q_i.

Hence, for $d \in \mathbb{N}$ odd, we conclude that z has no fixed points in $\mathcal{X}_d$, so that we have $\dim_K(S_d^G) = \frac{1}{2} \cdot \dim_K(S_d) = \frac{1}{2} \cdot \binom{d+2n-1}{2n-1}$. For $d \in \mathbb{N}_0$ even, we conclude that z has $\binom{\frac{d}{2}+n-1}{n-1}$ fixed points in $\mathcal{X}_d$, hence there are $\frac{1}{2} \cdot (\binom{d+2n-1}{2n-1} - \binom{\frac{d}{2}+n-1}{n-1})$ orbits of length 2, so that $\dim_K(S_d^G) = \frac{1}{2} \cdot (\binom{d+2n-1}{2n-1} + \binom{\frac{d}{2}+n-1}{n-1})$. From this, since $\sum_{d\geq 0} \binom{d+2n-1}{2n-1} \cdot T^d = \frac{1}{(1-T)^{2n}}$ and $\sum_{d\geq 0} \binom{d+n-1}{n-1} \cdot T^{2d} = \frac{1}{(1-T^2)^n}$, we infer that $H_{S^G} = \frac{1}{2} \cdot (\frac{1}{(1-T)^{2n}} + \frac{1}{(1-T^2)^n}) = \frac{1}{2} \cdot \frac{(1+T)^n + (1-T)^n}{(1-T)^n(1-T^2)^n} \in \mathbb{Q}(T)$.

More specifically: For $d = 1$ we have $\dim_K(S_1^G) = \frac{1}{2} \cdot \dim_K(S_1) = n$, where letting $l_i := X_i + Y_i$ be the orbit sums, we get $S_1^G = \langle l_1, \ldots, l_n \rangle_K$. For $d = 3$ we have $\dim_K(S_3^G) = \frac{1}{2} \cdot \dim_K(S_3) = \frac{1}{3}n(n+1)(2n+1)$.

For $d = 2$ we have $\dim_K(S_2) = n(2n+1)$ and $\dim_K(S_2^G) = n(n+1)$. Since z fixes precisely the monomials q_i of degree 2, and letting $p_i := X_i^2 + Y_i^2$, for all i, as well as $r_{ij} := X_iX_j + Y_iY_j$ and $s_{ij} := X_iY_j + X_jY_i$, for $1 \leq i < j \leq n$, be the orbit sums for the orbits of length 2, we get $S_2^G = \langle q_i, p_i, r_{ij}, s_{ij};\ \text{for all } i,j\rangle_K$. Moreover, for the products of two of the l_i we get $l_i^2 = p_i + 2q_i$ and $l_il_j = r_{ij} + s_{ij}$, so that the latter products span a K-subspace of S_2^G of dimension $\frac{1}{2}n(n+1)$, and we get $S_2^G = \langle l_i^2, l_il_j, q_i, r_{ij};\ \text{for all } i,j\rangle_K$.

b) From now on let $\operatorname{char}(K) = 2$.

i) We determine the Hilbert ideal $\mathcal{I}_G$: From $l_i = X_i + Y_i \in \mathcal{I}_G$ and $q_i = X_iY_i \in \mathcal{I}_G$, letting $I := (l_i, q_i; i \in \{1, \ldots, n\}) \trianglelefteq S$, we have $I \subseteq \mathcal{I}_G$. If a monomial $f \in \mathcal{X}_d$, where $d \geq 2$, is fixed by z, then we have $q_i \mid f$ for some i, thus $f \in I$. Otherwise, f belongs to an orbit of length 2, where $f \cdot z$ is obtained from f by exchanging X_i and Y_i, for all i, so that since $X_i \equiv Y_i \pmod{I}$ we get $f \cdot (1+z) \in I$. Thus we conclude that $\mathcal{I}_G = I$; in particular saying that $\mathcal{I}_G$ is generated by homogeneous invariants of positive degree at most 2.

Letting $R_i := K[l_i, q_i]$, which is polynomial with degrees $[1,2]$, we have $R := K[l_i, q_i; i \in \{1, \ldots, n\}] = \bigotimes_{i=1}^n R_i$, so that $H_R = \frac{1}{(1-T)^n(1-T^2)^n} \in \mathbb{Q}(T)$. Hence we have $R \subset S^G$, so that Hilbert's Finiteness Theorem does not hold for any $n \geq 2$. Moreover, from $X_1X_2 \in S_+^2$, but $X_1X_2 \notin \mathcal{I}_G$ we conclude that Benson's Lemma does not hold either for any $n \geq 2$.

Using the homomorphism of K-algebras $S \to K[X_1, \ldots, X_n]$ given by $X_i \mapsto X_i$ and $Y_i \mapsto X_i$, for the coinvariant algebra we get $S_G = S/\mathcal{I}_G = S/I \cong K[X_1, \ldots, X_n]/(X_1^2, \ldots, X_n^2) \cong \bigotimes_{i=1}^n K[X_i]/(X_i^2) \cong (K[X]/(X^2))^{\otimes n}$ as graded K-algebras; in particular we get $\dim_K(S_G) = 2^n$, where actually we have $S_G \cong K[G]^{\otimes n} \cong K[C_2^n]$ as $K[G]$-modules.

ii) We determine the trace ideal $S_{\{1\}}^G \trianglelefteq S^G$: An orbit sum of a monomial belongs to $S_{\{1\}}^G$ if and only if it corresponds to an orbit of length 2. Thus for d odd we have $(S_{\{1\}}^G)_d = S_d^G$, while for d even we get $\dim_K(S_d^G) - \dim_K((S_{\{1\}}^G)_d) = \binom{\frac{d}{2}+n-1}{n-1}$, so that $\dim_K((S_{\{1\}}^G)_d) = \frac{1}{2} \cdot (\binom{d+2n-1}{2n-1} - \binom{\frac{d}{2}+n-1}{n-1})$; in particular, for $d = 2$ we have $(S_{\{1\}}^G)_2 = \langle p_i, r_{ij}, s_{ij};\ \text{for all } i,j\rangle_K = \langle l_i^2, l_il_j, r_{ij};\ \text{for all } i,j\rangle_K$. From this we get $H_{S^G/S_{\{1\}}^G} = \frac{1}{(1-T^2)^n} \in \mathbb{Q}(T)$, and thus $H_{S_{\{1\}}^G} = H_{S^G} - H_{S^G/S_{\{1\}}^G} = \frac{1}{2} \cdot (\frac{1}{(1-T)^{2n}} - \frac{1}{(1-T^2)^n}) = \frac{1}{2} \cdot \frac{(1+T)^n - (1-T)^n}{(1-T)^n(1-T^2)^n} \in \mathbb{Q}(T)$.

Letting $J := (l_1, \ldots, l_n) \trianglelefteq S^G$, we have $J \subseteq S_{\{1\}}^G$. If a monomial f belongs to an orbit of length 2, then the associated orbit sum is given as $f \cdot (1+z) = q \cdot (g \cdot (1+z))$, where q is a monomial in the q_i, and g is a monomial which is not divisible by any q_i. Since $q_i \in S^G$ and $X_i \equiv Y_i \pmod{J}$, for all i, from this we conclude that $f \cdot (1+z) \in J$, so that we infer $S_{\{1\}}^G = J$.

Letting $P := K[q_1, \ldots, q_n] \subseteq S^G$ we observe that $P \cap S_{\{1\}}^G = P \cap J = \{0\}$, and since $H_P = \frac{1}{(1-T^2)^n} \in \mathbb{Q}(T)$ we conclude that $S^G = P \oplus S_{\{1\}}^G$ as graded

K-vector spaces, so that $S^G/S^G_{\{1\}} \cong P$ is polynomial with degrees $[2, \ldots, 2]$.

iii) We finally turn to algebra generation of S^G: Letting $S_i := K[X_i, Y_i]$, we have $S = \bigotimes_{i=1}^n S_i$. Let $H := H_1 \times \cdots \times H_n = \langle z_1 \rangle \times \cdots \times \langle z_n \rangle \cong C_2^n$, where H_i acts on S_i by $X_i \cdot z_i = Y_i$ and $Y_i \cdot z_i = X_i$, and fixes the other tensor factors. Then we have $S_i^{H_i} = K[l_i, q_i] = R_i$, so that $S^H = \bigotimes_{i=1}^n S_i^{H_i} = \bigotimes_{i=1}^n R_i = R$, where $H_R = \frac{1}{(1-T)^n(1-T^2)^n} \in \mathbb{Q}(T)$. Moreover, we have $G \trianglelefteq H$, so that H acts on S^G, and we have $R = S^H = (S^G)^{G/H} \subseteq S^G$,

Let first $n := 2$. Then from $r_{12} = X_1X_2 + Y_1Y_2 \in S^G$ and $r_{12} \cdot z_i = X_1Y_2 + Y_1X_2 = s_{12}$, saying that r_{12} is not fixed by H, we conclude that $R \cap r_{12}R = \{0\}$, which entails $R \oplus r_{12}R \subseteq S^G$. From $H_{R\oplus r_{12}R} = (1+T^2) \cdot H_R = \frac{1+T^2}{(1-T)^2(1-T^2)^2} = H_{S^G}$ we infer that $S^G = R \oplus r_{12}R$ as graded R-modules; in particular we have $S^G = K[l_1, l_2, q_1, q_2, r_{12}]$, so that Noether's degree bound holds in this case.

Now let $n := 3$. Then we have $\dim_K(S_1^G) = 3$, and $\dim_K(S_2^G) = 12$, where the decomposable elements form a K-subspace of dimension 6, and $\dim_K(S_3^G) = 28$. There are $\binom{5}{2} = 10$ products of three of the $l_i \in S_1^G$, and $3 \cdot 6 = 18$ products of one of the $l_i \in S_1^G$ and one of the $q_i, r_{ij} \in S_2^G$, giving rise to 28 elements of S_3^G. But the identity $l_1r_{23} + l_2r_{13} + l_3r_{12} = l_1l_2l_3 + 2 \cdot (X_1X_2X_3 + Y_1Y_2Y_3) \in S_3^G$ entails that these are K-linearly dependent, so that S_3^G is not generated by them as a K-vector space. Hence there is an indecomposable homogeneous invariant of degree 3, so that Noether's degree bound does not hold in this case. (Recall that if $\mathrm{char}(K) \neq 2$ then Noether's degree bound holds, implying that S_3^G is generated as a K-vector space by the above products, in turn saying that the latter are K-linearly independent in this case indeed.)

For $n \geq 3$, Campbell, Hughes, Shank, Wehlau [1997–2010] have shown that $\mathrm{Tr}^G(\prod_{i=1}^n X_i) \in S_n^G$ belongs to a minimal generating set of S^G, in other words is an indecomposable invariant. (Unfortunately, we are not able to present a proof here.) Indeed, for $n = 3$ it turns out that $\{l_i, q_i, r_{ij};\text{ for all } i \neq j\} \cup \{\mathrm{Tr}^G(X_1X_2X_3)\}$ is a minimal homogeneous generating set of S^G, see (17.6).

Note that this implies that Noether's bound does not hold in any of these cases, that there cannot be a bound in terms of $|G|$ alone, and that the Broer-Symonds bound in Kemper's conjecture actually is sharp.

6 Hilbert series

(6.1) Theorem: [Hilbert; Serre]. Let K be a field, let $R := K[f_1, \ldots, f_k]$ be a finitely generated commutative graded K-algebra, where $k \in \mathbb{N}_0$ and the $f_i \in R_{d_i}$ are homogeneous, and let M be a finitely generated graded R-module. Then we have $H_M = \frac{f}{\prod_{i=1}^k (1-T^{d_i})} \in \mathbb{Q}(T)$, where $f \in \mathbb{Z}[T^{\pm 1}]$.

Proof. We proceed by induction on $k \in \mathbb{N}_0$. If $k = 0$, then we have $R = K$, and thus M is a finitely generated K-vector space, entailing $H_M \in \mathbb{Z}[T^{\pm 1}]$.

Hence let $k \geq 1$, and for the R-module endomorphism of M given by multiplication with f_k let $M' := \bigoplus_{d\in\mathbb{Z}} \ker_{M_d}(\cdot f_k)$ and $M'' := \bigoplus_{d\in\mathbb{Z}} \mathrm{cok}_{M_d}(\cdot f_k)$. Then M' and M'', being an R-submodule and a quotient R-module of M, respectively, where R is Noetherian, are finitely finitely generated graded R-modules. Moreover, since $M'f_k = \{0\}$ and $M''f_k = \{0\}$, these are actually finitely generated $K[f_1, \ldots, f_{k-1}]$-modules, so that by induction we have $H_{M'} = \frac{f'}{\prod_{i=1}^{k-1}(1-T^{d_i})} \in \mathbb{Q}(T)$ and $H_{M''} = \frac{f''}{\prod_{i=1}^{k-1}(1-T^{d_i})} \in \mathbb{Q}(T)$, where $f', f'' \in \mathbb{Z}[T^{\pm 1}]$.

We have an exact sequence of graded R-modules $\{0\} \to M' \to M \xrightarrow{\cdot f_k} M[d_k] \to M''[d_k] \to \{0\}$, that is for any $d \in \mathbb{Z}$ we have an exact sequence of K-vector spaces $\{0\} \to M'_d \to M_d \xrightarrow{\cdot f_k} M_{d+d_k} \to M''_{d+d_k} \to \{0\}$, entailing $T^{-d_k}H_{M''} - T^{-d_k}H_M + H_M - H_{M'} = 0$, thus $H_M = \frac{H_{M''} - T^{d_k}H_{M'}}{1-T^{d_k}} \in \mathbb{Q}(T)$ is as asserted. $\sharp$

(6.2) Complexity and degree. a) For $z \in \mathbb{C}$ let $\nu_z \colon \mathbb{C}(T)^* \to \mathbb{Z}$ be the **discrete valuation** of $\mathbb{C}(T)$ at $T = z$, that is writing $0 \neq f \in \mathbb{C}(T)$ as $f = (z-T)^a \cdot \frac{g}{h}$, where $a \in \mathbb{Z}$ and $0 \neq g, h \in \mathbb{C}[T]$ are coprime such that $(z-T) \nmid gh$, we let $\nu_z(f) = a$; we let $\nu_z(0) = \infty$. Then $\mathcal{R}_z := \{f \in \mathbb{C}(T)^*; \nu_z(f) \geq 0\} \,\dot\cup\, \{0\} = \{f \in \mathbb{C}(T); f(z) \text{ well-defined}\} \subseteq \mathbb{C}(T)$ is the associated **valuation ring**, being a local ring with maximal ideal $\wp_z := \{f \in \mathbb{C}(T)^*; \nu_z(f) \geq 1\} \,\dot\cup\, \{0\} = \{f \in \mathbb{C}(T); f(z) \in \mathbb{C}^*\} \trianglelefteq \mathcal{R}_z$. For $f \in \mathbb{C}(T)^*$ we have $\widetilde{f}_z := \frac{f}{(z-T)^{\nu_z(f)}} \in \mathcal{R}_z \setminus \wp_z = \mathcal{R}_z^*$, hence we let $\delta_z(f) := \widetilde{f}_z(z) \in \mathbb{C}^*$; we let $\delta_z(0) := 0$.

Alternatively, from an analytical viewpoint, if a Laurent series $0 \neq f \in \mathbb{C}((T))$ converges in the pointed open unit disc $\{z \in \mathbb{C}; 0 < |z| < 1\} \subseteq \mathbb{C}$, say, then it gives rise to a meromorphic function $f(z)$ on its closure, so that for $|z| \leq 1$ we let $\nu_z(f) \in \mathbb{Z}$ denote the order of z as a root of f; again we may let $\nu_z(0) := \infty$. Moreover, $\widetilde{f}_z := \frac{f}{(z-T)^{\nu_z(f)}}$ is holomorphic at z, having neither a root nor a pole at z, so that we let $\delta_z(f) := \widetilde{f}_z(z) = \lim_{x\to z} \widetilde{f}_z(x) \in \mathbb{C}^*$; again we let $\delta_z(0) := 0$.

b) Now let K be a field, let R be a finitely generated commutative graded K-algebra, and let $M \neq \{0\}$ be a finitely generated graded R-module with Hilbert series $H_M \in \mathbb{Q}(T) \subseteq \mathbb{Q}((T))$. Then the **complexity** of M is defined as $\gamma(M) := -\nu_1(H_M) \in \mathbb{Z}$, that is the order of the pole of H_M at $T-1$; and the **degree** of M is defined as $\delta(M) := \delta_1(H_M) = ((1-T)^{\gamma(M)} \cdot H_M)(1) \in \mathbb{Q}^*$. For completeness we let $\gamma(\{0\}) := -\infty$ and $\delta(\{0\}) := 0$; note that $H_{\{0\}} = 0$. The **complexity** $\gamma(R) := \gamma(R_R) \in \mathbb{Z}$ and the **degree** $\delta(R) := \delta(R_R) \in \mathbb{Q}^*$ of R are defined as the order and the degree of the regular R-module, respectively.

We show that we actually have $\gamma(M) \geq 0$, where $\gamma(M) = 0$ if and only if M is a finitely generated K-vector space: Assume that $\gamma(M) \leq 0$, that is $\nu_1(H_M) \geq 0$. Writing $H_M = \sum_{d\in\mathbb{Z}} \dim_K(M_d) \cdot T^d \in \mathbb{Q}((T))$ we get $H_M(1) = \sum_{d\in\mathbb{Z}} \dim_K(M_d) \in \mathbb{N}$, showing that $\nu_1(H_M) = 0$ and that M is a finitely generated K-vector space. Conversely, if M is a finitely generated K-vector space, then $H_M(1) = \sum_{d\in\mathbb{Z}} \dim_K(M_d) \in \mathbb{N}$ says that $\nu_1(H_M) = 0$. $\sharp$

Note that, viewing Hilbert series as Laurent series, which due to the Hilbert-Serre Theorem converge on the pointed open unit disc, the above definitions coincide with those in the analytical sense. (The terminology of complexity is reminiscent of a similar notion used in representation theory, which is based on the idea of considering the growth behavior of the coefficients of formal power series; for Hilbert series this viewpoint is elucidated in Exercise (19.20).)

Example. For the polynomial algebra $S := K[X_1, \ldots, X_n]$ having degrees $[d_1, \ldots, d_n]$, where $n \in \mathbb{N}_0$, we have $H_S = \prod_{i=1}^n \frac{1}{1-T^{d_i}} \in \mathbb{Q}(T)$, hence we get $\gamma(S) = -\sum_{i=1}^n \nu_1(\frac{1}{1-T^{d_i}}) = \sum_{i=1}^n \nu_1(1-T^{d_i}) = n$, and subsequently $\delta(S) = \delta_1(\prod_{i=1}^n \frac{1-T}{1-T^{d_i}}) = (\prod_{i=1}^n \frac{1}{\sum_{j=0}^{d_i-1} T^j})(1) = \prod_{i=1}^n \frac{1}{d_i}$; in particular for the standard grading we get $\delta(S) = 1$.

(6.3) Degree theorem. Let K be a field, let R be a finitely generated commutative graded K-algebra, and let M be a finitely generated graded R-module.

Proposition. If $M' \leq M$ is a graded R-submodule, or if M' is a graded quotient R-module of M, then we have $\gamma(M') \leq \gamma(M)$. Moreover, if $\gamma(M') = \gamma(M)$ then we have $0 \leq \delta(M') \leq \delta(M)$.

Proof. We may assume that $M' \neq \{0\}$; hence we have $M \neq \{0\}$ as well. For $d \in \mathbb{Z}$ we have $\dim_K(M'_d) \leq \dim_K(M_d)$, hence for $0 < z < 1$ we have $0 \leq H_{M'}(z) \leq H_M(z) \in \mathbb{R}$, entailing $0 \leq \lim_{z\to 1^-}((1-z)^{\gamma(M)} \cdot H_{M'}(z)) \leq \lim_{z\to 1^-}((1-z)^{\gamma(M)} \cdot H_M(z)) = \delta(M) \in \mathbb{Q}^*$, where the latter limit indeed exists. Hence $(1-z)^{\gamma(M)} \cdot H_{M'}(z)$ does not have a pole at $z = 1$, thus $\gamma(M') \leq \gamma(M)$.

If $\gamma(M') = \gamma(M)$ then from the above inequalities we get $0 \leq \delta(M') = \lim_{z\to 1^-}((1-z)^{\gamma(M')} \cdot H_{M'}(z)) = \lim_{z\to 1^-}((1-z)^{\gamma(M)} \cdot H_{M'}(z)) \leq \delta(M)$. ♯

Theorem. Let $R \subseteq S$ be finite, where S is a commutative graded K-algebra.
a) Then we have $\gamma(R) = \gamma(S)$.
b) If S is a domain, then we have $\delta(S) = [\mathrm{Q}(S) \colon \mathrm{Q}(R)] \cdot \delta(R)$.

Proof. a) Since S is a finitely generated R-module, where R is a finitely generated K-algebra, S is a finitely generated K-algebra; thus $\gamma(S) = \gamma(S_S)$ is well-defined. Moreover, $\gamma(S_R)$ is well-defined as well, and thus we have $\gamma(S) = \gamma(S_R)$. Since $R \leq S$ as R-modules, we infer that $\gamma(R) \leq \gamma(S)$. (Thus this holds more generally, as soon as S is finitely generated as a K-algebra.)

The R-module S is a quotient of a free graded R-module $F \cong \bigoplus_{i=1}^k f_i R$, for some $k \in \mathbb{N}$, where the f_i are homogeneous such that $d_i := \deg(f_i) \in \mathbb{N}_0$. Hence we have $\gamma(S) \leq \gamma(F)$. Moreover, from $H_F = (\sum_{i=1}^k T^{d_i}) \cdot H_R$, since $(\sum_{i=1}^k T^{d_i})(1) = k \neq 0$, we conclude that $\gamma(F) = \gamma(R)$, entailing $\gamma(S) \leq \gamma(R)$.

b) We consider the field extension $L := \mathrm{Q}(R) \subseteq \mathrm{Q}(S) =: M$. The minimum polynomial $f \in L[X]$ of any $s \in S$ being irreducible, the L-subalgebra $L[X]/(f) \cong L[s] \subseteq M$ already is a field. Hence we conclude that $M = S \cdot L$. Thus we infer that any homogeneous generating set of S as an R-module generates M as an L-vector space. Hence there is an L-basis $\{f_1, \ldots, f_m\} \subseteq M$ consisting of homogeneous elements of S, where $m := [M \colon L] \in \mathbb{N}$. The f_i being L-linearly independent, we have $U := \bigoplus_{i=1}^m f_i R \subseteq S$ as graded R-modules. Letting $d_i := \deg(f_i) \in \mathbb{N}$, we get $H_U = (\sum_{i=1}^m T^{d_i}) \cdot H_R \in \mathbb{Q}(T)$, where $\sum_{i=1}^m T^{d_i}(1) = m$, so that $\gamma(U) = \gamma(R)$ and $\delta(U) = m \cdot \delta(R)$.

Since any element of a homogeneous generating set of S as an R-module is an L-linear combination of the f_i, choosing a common denominator shows that there is $0 \neq f \in S$ homogeneous such that $S \subseteq U \cdot \frac{1}{f} = \bigoplus_{i=1}^m \frac{f_i}{f} \cdot R$ as graded R-modules. Letting $d := \deg(f) \in \mathbb{N}_0$, we get $H_{U \cdot \frac{1}{f}} = T^{-d} \cdot H_U = (\sum_{i=1}^m T^{d_i - d}) \cdot H_R \in \mathbb{Q}(T)$, where $(\sum_{i=1}^m T^{d_i - d})(1) = m$, so that $\gamma(U \cdot \frac{1}{f}) = \gamma(R)$ and $\delta(U \cdot \frac{1}{f}) = m \cdot \delta(R)$.

Hence in conclusion from $U \leq S \leq U \cdot \frac{1}{f}$ we get $\gamma(R) = \gamma(U) \leq \gamma(S) \leq \gamma(U \cdot \frac{1}{f}) = \gamma(R)$, which entails $\gamma(R) = \gamma(S)$ again, and $m \cdot \delta(R) = \delta(U) \leq \delta(S) \leq \delta(U \cdot \frac{1}{f}) = m \cdot \delta(R)$, so that $\delta(S) = m \cdot \delta(R)$. ♯

Example. If G is a finite group, and V is a $K[G]$-module such that $n := \dim_K(V) \in \mathbb{N}_0$, then the extension $S[V]^G \subseteq S[V]$ is finite, where $S[V] \cong K[X_1, \ldots, X_n]$ as graded K-algebras, with respect to the standard grading on the latter, so that $\gamma(S[V]^G) = \gamma(S[V]) = \gamma(K[X_1, \ldots, X_n]) = n$.

Moreover, if G acts faithfully on V, then $S(V)^G = \mathrm{Q}(S[V]^G) \subseteq \mathrm{Q}(S[V]) = S(V)$ is Galois with respect to G, thus $[S(V) \colon S(V)^G] = |G|$, so that $\delta(S[V]) = 1$ implies that $\delta(S[V]^G) = \frac{1}{|G|}$.

(6.4) Molien's formula. a) Let G be a finite group, let K be a field such that $\mathrm{char}(K) \nmid |G|$, and let V be a $K[G]$-module such that $n := \dim_K(V) \in \mathbb{N}_0$.

Theorem: [Molien, 1897]**.** For the **graded character** of $g \in G$ we have

$$\chi_{S[V]}(g) := \sum_{d \geq 0} \chi_{S[V]_d}(g) \cdot T^d = \frac{1}{\det(E_n - \rho_V(g) \cdot T)} \in K(T),$$

where $\chi_{S[V]_d}(g) \in K$ denotes the trace of the K-linear map $\rho_{S[V]_d}(g)$.

Proof. We may assume that K contains a primitive $|G|$-th root of unity $\zeta_{|G|}$. Then the polynomial $T^{|G|} - 1 \in K[T]$ splits into pairwise non-associate linear factors as $T^{|G|} - 1 = \prod_{i=0}^{|G|-1}(T - \zeta_{|G|}^i) \in K[T]$. Since we have $g^{|G|} = 1 \in G$, the matrix $\rho_{S[V]_d}(g)$ of the action of g with respect to any K-basis of $S[V]_d$ is a root of $T^{|G|} - 1$. Hence $\rho_{S[V]_d}(g)$ is diagonalizable, for any $d \in \mathbb{N}_0$. In particular, we may assume the isomorphism $S[V] \to K[X_1, \ldots, X_n]$ chosen such that the indeterminates correspond to an eigenvector K-basis with respect to $\rho_V(g)$. Letting $\lambda_1, \ldots, \lambda_n \in K$ be the associated eigenvalues, we have $\det(E_n - \rho_V(g) \cdot T) = \prod_{i=1}^n (1 - \lambda_i T) \in K[T] \setminus \{0\}$. We relate this to the graded character:

Considering the K-basis of $S[V]_d$ consisting of the monomials of degree d, which are eigenvectors of $\rho_{S[V]_d}(g)$, we observe that the eigenvalues of $\rho_{S[V]_d}(g)$ are given as $\prod_{i=1}^n \lambda_i^{a_i} \in K$, where $a_1, \ldots, a_n \in \mathbb{N}_0$ such that $\sum_{i=1}^n a_i = d$, thus $\chi_{S[V]}(g) = \sum_{d \geq 0} \chi_{S[V]_d}(g) \cdot T^d = \sum_{d \geq 0} (\sum_{a_1, \ldots, a_n \in \mathbb{N}_0, \sum_{i=1}^n a_i = d} (\prod_{i=1}^n \lambda_i^{a_i}) \cdot T^d) = \sum_{d \geq 0} \sum_{a_1, \ldots, a_n \in \mathbb{N}_0, \sum_{i=1}^n a_i = d} \prod_{i=1}^n (\lambda_i T)^{a_i} = \sum_{a_1, \ldots, a_n \in \mathbb{N}_0} \prod_{i=1}^n (\lambda_i T)^{a_i} = \prod_{i=1}^n (\sum_{j \geq 0} (\lambda_i T)^j) = \prod_{i=1}^n \frac{1}{1 - \lambda_i T} \in K(T)$. ♯

Corollary. If $\mathrm{char}(K) = 0$ then $H_{S[V]^G} = \frac{1}{|G|} \cdot \sum_{g \in G} \frac{1}{\det(E_n - \rho_V(g) \cdot T)} \in \mathbb{Q}(T)$.

Proof. The Reynolds operator $\mathcal{R}^G = \frac{1}{|G|} \cdot \sum_{g \in G} g \in K[G]$ induces a K-linear projection from $S[V]_d$ onto $S[V]_d^G$, for $d \geq 0$. Hence since $\mathrm{char}(K) = 0$ we have $\dim_K(S[V]_d^G) = \chi_{S[V]_d}(\mathcal{R}^G) = \frac{1}{|G|} \cdot \sum_{g \in G} \chi_{S[V]_d}(g)$. Using this we obtain we get $H_{S[V]^G} = \sum_{d \geq 0} \dim_K(S[V]_d^G) \cdot T^d = \frac{1}{|G|} \cdot \sum_{d \geq 0} \sum_{g \in G} \chi_{S[V]_d}(g) \cdot T^d = \frac{1}{|G|} \cdot \sum_{g \in G} \chi_{S[V]}(g) = \frac{1}{|G|} \cdot \sum_{g \in G} \frac{1}{\det(E_n - \rho_V(g) \cdot T)} \in K(T) \cap \mathbb{Q}((T)) = \mathbb{Q}(T)$. ♯

b) We describe a method to evaluate Molien's formula, in terms of ordinary characters of G, letting still $\mathrm{char}(K) = 0$:

For $g \in G$ we have $\det(E_n - \rho_V(g) \cdot T) = \det(-T \cdot (\rho_V(g) - T^{-1} \cdot E_n)) = (-T)^n \cdot \chi_{\rho_V(g)}(T^{-1}) \in K(T)$, where $\chi_{\rho_V(g)} \in K[T]$ is the characteristic polynomial of $\rho_V(g)$; note that $T^n \cdot \chi_{\rho_V(g)}(T^{-1})$ is the **reversed polynomial** of $\chi_{\rho_V(g)}$. Hence we have $\chi_{S[V]}(g) = \frac{1}{(-T)^n \cdot \chi_{\rho_V(g)}(T^{-1})} \in K(T)$.

Assuming that K is large enough, and letting $\lambda_1, \ldots, \lambda_n \in K$ be the eigenvalues of $\rho_V(g)$, we have $\chi_{\rho_V(g)} = \prod_{i=1}^n (T - \lambda_i)$, so that using the elementary symmetric polynomials $e_{n,i} \in K[\mathcal{X}]$, where $\mathcal{X} := \{X_1, \ldots, X_n\}$, and $\deg(e_{n,i}) = i$ for $i \in \{0, \ldots, n\}$, we obtain $\chi_{\rho_V(g)} = \sum_{i=0}^n (-1)^i e_{n,i}(\lambda_1, \ldots, \lambda_n) T^{n-i}$; see (9.3).

By the Newton identities, see Exercise (18.36), the $e_{n,i}$, for $i \in \{1, \ldots, n\}$, can be determined recursively from the **power sums** $p_{n,k} := \sum_{i=1}^n X_i^k \in K[\mathcal{X}]$, for $k \in \{1, \ldots, n\}$. Thus $\chi_{\rho_V(g)}$ can be computed from $p_{n,k}(\lambda_1, \ldots, \lambda_n) \in K$, for $k \in \{1, \ldots, n\}$. Since $\rho_V(g^k)$ has eigenvalues $\lambda_1^k, \ldots, \lambda_n^k \in K$, we conclude that $p_{n,k}(\lambda_1, \ldots, \lambda_n) = \sum_{i=1}^n \lambda_i^k = \chi_V(g^k) \in K$ equals the trace of the K-linear map $\rho_V(g^k)$, where χ_V denotes the character of G afforded by V.

Recalling that any character of G is constant on each conjugacy class of G, we conclude that Molien's formula can be evaluated once the character χ_V is known, together with the power maps $p_k \colon \mathcal{C}l(G) \to \mathcal{C}l(G) \colon g^G \mapsto (g^k)^G$ on the set $\mathcal{C}l(G)$ of conjugacy classes of G, for $k \in \{1, \ldots, n\}$.

(6.5) Lifting modules. Molien's formula, interpreted appropriately, remains valid in the following more general situation, where we use freely some facts from modular representation theory of finite groups:

a) Let G be a finite group, and let F be a finite field such that $p := \mathrm{char}(F) \neq 0$. We may assume that F is a splitting field of $F[G]$, and that if moreover $p \nmid |G|$ then any p-modular representation of G is equivalent to a representation over F. Let $\mathbb{Q} \subseteq K \subseteq \overline{\mathbb{Q}} \subseteq \mathbb{C}$ be an algebraic number field, having a discrete valuation ring $\mathcal{R} \subseteq K$ with maximal ideal $\wp \trianglelefteq \mathcal{R}$ such that $\mathcal{R}/\wp \cong F$, and let $^-\colon \mathcal{R} \to \mathcal{R}/\wp$ be the natural epimorphism. We may assume that K is a splitting field of $K[G]$ as well, in which case $(K, \mathcal{R}, F)$ is called a **splitting p-modular system**.

Let V be a **trivial-source** or **p-permutation** $F[G]$-module such that $n := \dim_F(V) \in \mathbb{N}_0$, that is V is a direct summand of a permutation $F[G]$-module. In particular, this holds true if V is **projective**, that is a direct summand of a free $F[G]$-module, and even more specifically if $p \nmid |G|$ in which case any $F[G]$-module is projective. Then V has a unique **lift** to an $\mathcal{R}$-free trivial-source $\mathcal{R}[G]$-module $\widehat{V}$, that is $\overline{\widehat{V}} := V \otimes_{\mathcal{R}} F \cong V$ as $F[G]$-modules; let $\widehat{V}_K := \widehat{V} \otimes_{\mathcal{R}} K$, which is a semisimple $K[G]$-module. Then we have $\dim_K(\widehat{V}_K) = \mathrm{rk}_{\mathcal{R}}(\widehat{V}) = n$. Note that for the trivial $F[G]$-module we have $\widehat{F} \cong \mathcal{R}$, the trivial $\mathcal{R}[G]$-module.

We now generalize the definitions in (2.1), (2.3), and (3.2) as follows: For $d \in \mathbb{N}$ let $\widehat{V}^{\otimes d}$ be the d-fold tensor power of $\widehat{V}$ over $\mathcal{R}$, which is an $\mathcal{R}$-free trivial-source $\mathcal{R}[G]$-module, such that $\overline{\widehat{V}^{\otimes d}} = (\overline{\widehat{V}})^{\otimes d} = V^{\otimes d}$; let $\widehat{V}^{\otimes 0} := \mathcal{R}$ be the trivial $\mathcal{R}[G]$-module. Using the action of $\mathcal{S}_d$ by permuting the tensor factors, we get the $\mathcal{R}[G]$-submodule $\widehat{V}^{\otimes d,-} \leq \widehat{V}^{\otimes d}$, and the symmetric power $S^d(\widehat{V}) := \widehat{V}^{\otimes d}/\widehat{V}^{\otimes d,-}$, giving rise to the symmetric algebra $S[\widehat{V}] := \bigoplus_{d \geq 0} S[\widehat{V}]_d$, which is a commutative graded $\mathcal{R}$-algebra.

By the right exactness of tensor products, for $d \in \mathbb{N}_0$ we have $(S[\widehat{V}]_d)_K \cong (\widehat{V}^{\otimes d})_K/(\widehat{V}^{\otimes d,-})_K \cong S[\widehat{V}_K]_d$ as $K[G]$-modules, and $\overline{S[\widehat{V}]_d} \cong \overline{\widehat{V}^{\otimes d}}/\overline{\widehat{V}^{\otimes d,-}} \cong S[\overline{\widehat{V}}]_d \cong S[V]_d$ as $F[G]$-modules. Moreover, since $\dim_K(S[\widehat{V}_K]_d) = \binom{n+d-1}{d} = \dim_F(S[V]_d)$, we conclude that $\widehat{V}^{\otimes d,-} \leq \widehat{V}^{\otimes d}$ is $\mathcal{R}$-pure, hence $S[\widehat{V}]_d$ is $\mathcal{R}$-free such that $\dim_F(S[V]_d) = \mathrm{rk}_{\mathcal{R}}(S[\widehat{V}]_d) = \dim_K(S[\widehat{V}_K]_d)$.

Since $S[\widehat{V}] = \bigoplus_{d \geq 0} S[\widehat{V}]_d$ as $\mathcal{R}[G]$-modules, we conclude that G acts on $S[\widehat{V}]$ by automorphisms of graded $\mathcal{R}$-algebras, so that $S[\widehat{V}]$ becomes a graded G-algebra. This gives rise to the invariant algebra $S[\widehat{V}]^G := \bigoplus_{d \geq 0} \mathrm{Fix}_{S[\widehat{V}]_d}(G) \subseteq S[\widehat{V}]$, being a graded $\mathcal{R}$-algebra again, so that $S[\widehat{V}]$ becomes a graded $S[\widehat{V}]^G$-module. Moreover, $S[\widehat{V}]^G_d = \mathrm{Fix}_{S[\widehat{V}]_d}(G) \leq S[\widehat{V}]_d$ is $\mathcal{R}$-torsion free, hence is $\mathcal{R}$-free such that $\mathrm{rk}_{\mathcal{R}}(S[\widehat{V}]^G_d) \leq \mathrm{rk}_{\mathcal{R}}(S[\widehat{V}])$. In particular, the Hilbert series $H_{S[\widehat{V}]^G} := \sum_{d \geq 0} \mathrm{rk}_{\mathcal{R}}(S[\widehat{V}]^G_d) \cdot T^d \in \mathbb{Q}((T))$ is well-defined.

b) We show that $H_{S[V]^G} = H_{S[\widehat{V}]^G} = H_{S[\widehat{V}_K]^G} \in \mathbb{Q}(T)$:

Let W be a permutation $F[G]$-module such that $W = V \oplus U$ as $F[G]$-modules, and let $\widehat{W}$ be the permutation $\mathcal{R}[G]$-module lifting W. Hence we have $\widehat{W} = \widehat{V} \oplus \widehat{U}$ as $\mathcal{R}[G]$-modules, and $\widehat{W}_K = \widehat{V}_K \oplus \widehat{U}_K$ as $K[G]$-modules. Then $S[W]_d$ is a permutation $F[G]$-module, for $d \in \mathbb{N}_0$, where G acts by permuting monomials. Since $S[W]_d = \bigoplus_{i=0}^d (S[V]_i \otimes_F S[U]_{d-i})$ as $F[G]$-modules, we conclude that $S[V]_d$ is a trivial-source $F[G]$-module, where $S[\widehat{W}]_d = \bigoplus_{i=0}^d (S[\widehat{V}]_i \otimes_{\mathcal{R}} S[\widehat{U}]_{d-i})$ as $\mathcal{R}[G]$-modules entails that $S[\widehat{V}]_d$ is the trivial-source lift of $S[V]_d$.

Hence by **liftability of homomorphisms** between trivial-source modules we get $\dim_F(S[V]_d^G) = \dim_F(\mathrm{Hom}_{F[G]}(F, S[V]_d)) = \mathrm{rk}_{\mathcal{R}}(\mathrm{Hom}_{\mathcal{R}[G]}(\mathcal{R}, S[\widehat{V}]_d)) = \mathrm{rk}_{\mathcal{R}}(S[\widehat{V}]_d^G)$, which equals $\dim_K(\mathrm{Hom}_{K[G]}(K, S[\widehat{V}_K]_d)) = \dim_K(S[\widehat{V}_K]_d^G)$. ♯

c) In the non-modular case $p \nmid |G|$ we may alternatively argue as follows:

Since $|G| \in \mathcal{R} \setminus \wp = \mathcal{R}^*$, there is a Reynolds operator $\mathfrak{R}^G := \frac{1}{|G|} \cdot \sum_{g \in G} g \in \mathcal{R}[G]$, which induces a projection of graded $S[\widehat{V}]^G$-modules $S[\widehat{V}] \to S[\widehat{V}]^G$. Interpreting $\mathfrak{R}^G$ as Reynolds operator in $K[G]$ and in $F[G]$, we get $(S[\widehat{V}]_d^G)_K \cong S[\widehat{V}_K]_d^G$ as $K[G]$-modules, and $\overline{S[\widehat{V}]_d^G} \cong (\overline{S[\widehat{V}]_d})^G \cong S[V]_d^G$ as $F[G]$-modules, thus $\dim_K(S[\widehat{V}_K]_d^G) = \mathrm{rk}_{\mathcal{R}}(S[\widehat{V}]_d^G) = \dim_F(S[V]_d^G)$, for $d \in \mathbb{N}_0$.

To evaluate Molien's formula we may assume that K contains a primitive $|G|$-th root of unity $\zeta_{|G|}$. Then we have $\zeta_{|G|} \in \mathcal{R} \setminus \wp$, and thus $\overline{\zeta}_{|G|} \in F$ is a primitive $|G|$-th root of unity as well. Thus the map $\overline{}\colon \mathcal{R} \to F$ induces an isomorphism $\langle \zeta_{|G|} \rangle \to \langle \overline{\zeta}_{|G|} \rangle$ between the cyclic groups of $|G|$-th roots of unity in K and F, respectively; the inverse of the latter map is called the associated **Brauer lift**.

For $g \in G$ we have $\det(E_n - \rho_{\widehat{V}_K}(g) \cdot T) = \prod_{i=1}^n (1 - \lambda_i T) \in K(T)$, where $\lambda_1, \ldots, \lambda_n \in K$ are the eigenvalues of $\rho_{\widehat{V}_K}(g)$, being $|G|$-th roots of unity. Since F contains a primitive $|G|$-th root of unity, we may assume that the F-basis of V is chosen (depending on g) such that g acts diagonally, so that by uniqueness of lifts we may assume that g acts diagonally on $\widehat{V}$ and thus on $\widehat{V}_K$ as well. Hence to determine the eigenvalues of $\rho_{\widehat{V}_K}(g)$ in K, it suffices to determine the eigenvalues of $\rho_V(g)$ in F, and subsequently applying the Brauer lift to them.

(6.6) Example: Dihedral groups. Let K be a field such that $\mathrm{char}(K) \nmid k$, for some $k \in \mathbb{N}$, containing a primitive k-th root of unity ζ_k, let $G = \langle z, s \rangle \cong D_{2k}$ be the dihedral group of order $2k$, where $z^k = s^2 = 1$ and $z^s = z^{-1}$, acting on $V := K^2$ by $z \mapsto \mathrm{diag}[\zeta_k, \zeta_k^{-1}]$ and $s \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, and let $S := K[X, Y]$; note that V is a simple projective $K[G]$-module (in particular if $\mathrm{char}(K) = 2 \nmid k$).

i) Hence in order to determine $H_{S^G} \in \mathbb{Q}(T)$ we may assume that $\mathrm{char}(K) = 0$, and even that $K \subseteq \mathbb{C}$. Then the given representation is equivalent to the complexification of the faithful orthogonal real representation of G coming from the embedding of the regular k-gon into the Euclidean plane, centered at the origin; in this sense the elements of G can be divided into rotations and reflections.

We consider the normal subgroup $H := \langle z \rangle \cong C_k$ of rotations first: In order to apply Molien's formula, we observe that $\det(E_2 - \mathrm{diag}[\zeta_k, \zeta_k^{-1}]^i \cdot T) = (1 - \zeta_k^i T)(1 - \zeta_k^{-i} T) \in K[T]$, for $i \in \{0, \ldots, k-1\}$. From this we get $H_{S^H} = \frac{1}{k} \cdot \sum_{i=0}^{k-1} \frac{1}{(1-\zeta_k^i T)(1-\zeta_k^{-i} T)} = \frac{1}{k} \cdot \sum_{i=0}^{k-1} \frac{1}{1-(\zeta_k^i + \zeta_k^{-i})T + T^2} = \frac{1}{k} \cdot \sum_{i=0}^{k-1} \frac{1}{1 - 2\cos(\frac{i \cdot 2\pi}{k})T + T^2}$.

Unfortunately, number theoretical sums of this type are notoriously hard to evaluate, but fortunately by (3.3) we have $H_{S^H} = \frac{1+T^k}{(1-T^2)(1-T^k)}$. This actually shows the identity $\frac{1}{k} \cdot \sum_{i=0}^{k-1} \frac{1}{1-(\zeta_k^i+\zeta_k^{-i})T+T^2} = \frac{1+T^k}{(1-T^2)(1-T^k)} \in \mathbb{Q}(T)$.

Now we consider $G = H \stackrel{.}{\cup} Hs$, where the coset Hs consists of reflections: From $(z^i s)^2 = 1$ and $\det(\rho_V(z^i s)) = -1$, we infer that $\rho_V(z^i s)$ has eigenvalues ± 1 indeed, so that we get $\det(E_2 - \rho_V(z^i s) \cdot T) = \det(\mathrm{diag}[1-T, 1+T]) = (1-T^2)$, for $i \in \{0, \ldots, k-1\}$. Thus by Molien's formula we obtain $H_{S^G} = \frac{1}{2k} \cdot (\frac{k}{1-T^2} + \sum_{i=0}^{k=1} \frac{1}{(1-\zeta_k^i T)(1-\zeta_k^{-i} T)}) = \frac{1}{2} \cdot (\frac{1}{1-T^2} + \frac{1+T^k}{(1-T^2)(1-T^k)}) = \frac{1}{(1-T^2)(1-T^k)} \in \mathbb{Q}(T)$.

ii) Letting K be arbitrary again such that $\mathrm{char}(K) \nmid k$, in view of $H_{S^G} = \frac{1}{(1-T^2)(1-T^k)}$ we show that S^G is polynomial, with degrees $[2, k]$: Recalling that $S^G = (S^H)^{G/H} = (S^H)^{\langle s \rangle} = \mathrm{Tr}_H^G(S^H) = \mathrm{Tr}^{\langle s \rangle}(S^H)$, from (3.3) we get $f := XY = \frac{1}{2} \cdot \mathrm{Tr}^{\langle s \rangle}(XY) \in S^G$ and $g := X^k + Y^k = \mathrm{Tr}^{\langle s \rangle}(X^k) = \mathrm{Tr}^{\langle s \rangle}(Y^k) \in S^G$.

Moreover, the Jacobian matrix of $\{f, g\}$ is given as

$$J(f,g) = \begin{bmatrix} \frac{\partial f}{\partial X} & \frac{\partial f}{\partial Y} \\ \frac{\partial g}{\partial X} & \frac{\partial g}{\partial Y} \end{bmatrix} = \begin{bmatrix} Y & X \\ kX^{k-1} & kY^{k-1} \end{bmatrix} \in S^{2 \times 2},$$

so that $\det(J(f,g)) = k \cdot (Y^k - X^k) \neq 0 \in S$. Hence by the Jacobian criterion, which will be proven in (7.1) below, we conclude that $\{f, g\}$ is algebraically independent indeed. Thus the Hilbert series of $K[f, g] \subseteq S^G$ is given as $H_{K[f,g]} = \frac{1}{(1-T^2)(1-T^k)} = H_{S^G}$, so that we infer $S^G = K[f, g]$. ♯

7 Polynomial algebras

(7.1) Jacobian criterion. We first collect a few general observations concerning polynomial algebras: Let K be a field, let $S := K[\mathcal{X}]$ be the polynomial algebra in the indeterminates $\mathcal{X} := \{X_1, \ldots, X_n\}$, where $n \in \mathbb{N}_0$, and let $\{f_1, \ldots, f_n\} \subseteq S$. The associated **Jacobian matrix** is defined as $J(f_1, \ldots, f_n) = J_{\mathcal{X}}(f_1, \ldots, f_n) := [\frac{\partial f_i}{\partial X_j}]_{ij} \in S^{n \times n}$, and $\det(J(f_1, \ldots, f_n)) \in S$ is called the associated **Jacobian determinant**.

Proposition: Jacobian criterion. a) If $\det(J(f_1, \ldots, f_n)) \neq 0$, then the set $\{f_1, \ldots, f_n\}$ is algebraically independent.
b) If $\{f_1, \ldots, f_n\}$ is algebraically independent, where $\mathrm{char}(K) = 0$, then we have $\det(J(f_1, \ldots, f_n)) \neq 0$.

Proof. a) If $\mathrm{char}(K) \neq 0$ we may assume additionally that K is perfect, which holds anyway if K is finite, or otherwise by going over to an algebraic closure of K. Now assume to the contrary that there is $0 \neq h \in K[Y_1, \ldots, Y_n]$ such that $h(f_1, \ldots, f_n) = 0$, where we assume h to be chosen of minimal degree.

Then differentiation $\frac{\partial}{\partial X_j}$ with respect to X_j, for $j \in \{1, \ldots, n\}$, using the chain rule yields $\sum_{i=1}^n \frac{\partial h}{\partial Y_i}(f_1, \ldots, f_n) \cdot \frac{\partial f_i}{\partial X_j} = 0$, that is we get the system of linear equations $[\frac{\partial h}{\partial Y_i}(f_1, \ldots, f_n)]_i \cdot J(f_1, \ldots, f_n) = 0 \in \mathrm{Q}(S)^n$.

Assume that we have $\frac{\partial h}{\partial Y_i} = 0 \in K[\mathcal{X}]$, for all $i \in \{1, \ldots, n\}$. Since $\deg(h) > 0$ this implies $\mathrm{char}(K) = p \neq 0$, and since K is perfect we have $h = (h')^p$ for some $0 \neq h' \in K[\mathcal{X}]$. Thus we have $\deg(h') < \deg(h)$, and since $h(f_1, \ldots, f_n) = 0$ we have $h'(f_1, \ldots, f_n) = 0$ as well, contradicting the minimality of h.

Hence there is $i \in \{1, \ldots, n\}$ such that $\frac{\partial h}{\partial Y_i} \neq 0$. Since $\deg(\frac{\partial h}{\partial Y_i}) < \deg(h)$, we have $\frac{\partial h}{\partial Y_i}(f_1, \ldots, f_n) \neq 0$. Thus the above system of linear equations has a non-trivial solution, hence we have $\det(J(f_1, \ldots, f_n)) = 0$, a contradiction.

b) Let $\{f_1, \ldots, f_n\}$ be algebraically independent. Since $\mathrm{trdeg}_K(\mathrm{Q}(S)) = n$, the sets $\{f_1, \ldots, f_n, X_k\}$ are algebraically dependent, for all $k \in \{1, \ldots, n\}$. Let $0 \neq h_k \in K[Y_1, \ldots, Y_n, Y_0]$ be of minimal degree such that $h_k(f_1, \ldots, f_n, X_k) = 0$. Differentiation $\frac{\partial}{\partial X_j}$ with respect to X_j, where $\frac{\partial X_k}{\partial X_j} = \delta_{kj}$, using the chain rule yields $[\frac{\partial h_k}{\partial Y_i}(f_1, \ldots, f_n, X_k)]_{ki} \cdot J(f_1, \ldots, f_n) = -\mathrm{diag}[\frac{\partial h_k}{\partial Y_0}(f_1, \ldots, f_n, X_k)]_k$.

Since $\{f_1, \ldots, f_n\}$ is algebraically independent, the indeterminate Y_0 occurs in h_k, from which since $\mathrm{char}(K) = 0$ we get $\frac{\partial h_k}{\partial Y_0} \neq 0$. Since $\deg(\frac{\partial h_k}{\partial Y_0}) < \deg(h_k)$, we have $\frac{\partial h_k}{\partial Y_0}(f_1, \ldots, f_n, X_k) \neq 0$, so that $\det(\mathrm{diag}[\frac{\partial h_k}{\partial Y_0}(f_1, \ldots, f_n, X_k)]_k) \neq 0$ as well, entailing that $\det(J(f_1, \ldots, f_n)) \neq 0$. ♯

Note that the condition $\mathrm{char}(K) = 0$ in (b) is necessary: If $\mathrm{char}(K) = p \neq 0$, then $\{X^p\} \subseteq K[X]$ is algebraically independent, but we have $\det(J(X^p)) = \det([p \cdot X^{p-1}]) = 0 \in K[X]$.

(7.2) Theorem: [Chevalley, 1967]**.** Let K be a field, let $n \in \mathbb{N}_0$, let $S := K[X_1, \ldots, X_n]$, and let $R \subseteq S$ be a graded K-subalgebra, having a minimal homogeneous generating set $\mathcal{F} := \{f_1, \ldots, f_k\}$, where $k \in \mathbb{N}_0$, and such that the degrees $d_i := \deg(f_i) \in \mathbb{N}$ fulfill $\mathrm{char}(K) \nmid d_i$, for all $i \in \{1, \ldots, n\}$. If S is a finitely generated free graded R-module, that is S has a homogeneous R-basis, then $\mathcal{F}$ is algebraically independent, that is R is polynomial.

Proof. Since S is a finitely generated R-module, the extension $R \subseteq S$ is finite, and hence R necessarily is a finitely generated K-algebra. Moreover, the assumption on $\mathcal{F}$ is equivalent to $\mathcal{F}$ being a minimal generating set of the ideal $R_+ \trianglelefteq R$, and likewise to $\overline{\mathcal{F}} \subseteq R_+/(R_+)^2$ being a K-basis; since the latter property is retained under field extensions we may assume that K is perfect.

Assume to the contrary that there is $0 \neq g \in K[Y_1, \ldots, Y_k]$ such that we have $g(\mathcal{F}) = 0$, where we may assume that g is homogeneous of degree $d := \deg_\delta(g) \in \mathbb{N}$ with respect to the degree vector $\delta := [d_1, \ldots, d_k]$, and g is chosen with d minimal. Let $g_i := \frac{\partial g}{\partial Y_i}(\mathcal{F}) \in R_{d-d_i}$, for $i \in \{1, \ldots, k\}$. Since K is perfect and g is minimal, we infer that there is i such that $g_i \neq 0$. (Recall that we have already used this kind of argument in the proof of (7.1).) Up to reordering we may assume that $(g_1, \ldots, g_k) = (g_1, \ldots, g_l) \trianglelefteq R$, where $l \in \{1, \ldots, k\}$ is minimal; for $t \in \{l+1, \ldots, k\}$ let $g_{ti} \in R_{d_i - d_t}$ such that $g_t = \sum_{i=1}^{l} g_{ti} g_i \in R$.

Let $S = \bigoplus_{s=1}^{r} h_s R$, where $r \in \mathbb{N}$ and the h_s are homogeneous such that $e_s := \deg(h_s) \in \mathbb{N}_0$, and where we may assume that $h_1 := 1$, thus $e_1 = 0$ while $e_s \geq 1$ for $s \geq 2$. Let $\mathcal{R} \colon S \to h_1 R = R$ be the projection of graded R-modules associated with the above direct sum decomposition; note that $\mathcal{R}$ may be considered as the associated **(generalized) Reynolds operator**.

Let $\mathcal{I} := R_+ S = (\mathcal{F}) \trianglelefteq S$ be the **(generalized) Hilbert ideal** of the extension $R \subseteq S$. We show that $\mathcal{F} \subseteq R_+$ is a minimal generating set of $\mathcal{I}$ (mimicking part of the proof of Hilbert's Finiteness Theorem): Let $\mathcal{F}' \subseteq \mathcal{F}$ such that $\mathcal{I} = (\mathcal{F}') \trianglelefteq S$; then we have $R_+ = \mathcal{I} \cap R = \mathcal{R}(\mathcal{I}) = \mathcal{R}(\sum_{f \in \mathcal{F}'} fS) = \sum_{f \in \mathcal{F}'} f\mathcal{R}(S) = \sum_{f \in \mathcal{F}'} fR = (\mathcal{F}') \trianglelefteq R$, hence by minimality we get $\mathcal{F}' = \mathcal{F}$.

Let $f_{ij} := \frac{\partial f_i}{\partial X_j} \in S_{d_i - 1}$, for $i \in \{1, \ldots, k\}$ and $j \in \{1, \ldots, n\}$, and let $f'_{ij} := f_{ij} + \sum_{t=l+1}^{k} g_{ti} f_{tj} \in S_{d_i - 1}$, for $i \in \{1, \ldots, l\}$. Hence there are $f'_{ijs} \in R_{d_i - 1 - e_s}$ such that $f'_{ij} = \sum_{s=1}^{r} f'_{ijs} h_s \in S_{d_i - 1}$. We show that $f'_{ijs} \in R_+$, so that $f'_{ij} \in \mathcal{I}$:

Differentiation yields $\frac{\partial}{\partial X_j}(g(\mathcal{F})) = 0$, so that by the chain rule we get $0 = \sum_{i=1}^{k} \frac{\partial g}{\partial Y_i}(\mathcal{F}) \cdot \frac{\partial f_i}{\partial X_j} = \sum_{i=1}^{k} g_i f_{ij} = \sum_{i=1}^{l} g_i f_{ij} + \sum_{t=l+1}^{k} (\sum_{i=1}^{l} g_{ti} g_i) f_{tj}$, hence $0 = \sum_{i=1}^{l} g_i f_{ij} + \sum_{i=1}^{l} (\sum_{t=l+1}^{k} g_{ti} f_{tj}) g_i = \sum_{i=1}^{l} (f_{ij} + \sum_{t=l+1}^{k} g_{ti} f_{tj}) g_i$, thus $0 = \sum_{i=1}^{l} f'_{ij} g_i = \sum_{i=1}^{l} (\sum_{s=1}^{r} f'_{ijs} h_s) g_i = \sum_{s=1}^{r} (\sum_{i=1}^{l} g_i f'_{ijs}) h_s$. Since the h_s are R-linearly independent, we conclude that $\sum_{i=1}^{l} g_i f'_{ijs} = 0$, for $s \in \{1, \ldots, r\}$. Since the $f'_{ijs} \in R$ are homogeneous, by the minimality of l none of the latter can possibly be a non-zero constant, so that they all belong to R_+. ♯

Since the $f_i \in R$ are homogeneous, the Euler identity says $d_i f_i = \sum_{j=1}^{n} f_{ij} X_j \in S_{d_i}$, so that $\sum_{i=1}^{l} d_i f_i + \sum_{t=l+1}^{k} (\sum_{i=1}^{l} g_{ti}) d_t f_t = \sum_{i=1}^{l} (d_i f_i + \sum_{t=l+1}^{k} g_{ti} d_t f_t) = \sum_{i=1}^{l} (\sum_{j=1}^{n} (f_{ij} + \sum_{t=l+1}^{k} g_{ti} f_{tj}) X_j) = \sum_{i=1}^{l} \sum_{j=1}^{n} f'_{ij} X_j = \sum_{j=1}^{n} \sum_{i=1}^{l} f'_{ij} X_j$. Since $f'_{ij} \in \mathcal{I} = (\mathcal{F}) \trianglelefteq S$ there are $s_{ji} \in S$ (not necessarily homogeneous) such that $\sum_{i=1}^{l} f'_{ij} = \sum_{i=1}^{k} s_{ji} f_i$, thus $\sum_{j=1}^{n} (\sum_{i=1}^{l} f'_{ij}) X_j = \sum_{j=1}^{n} (\sum_{i=1}^{k} s_{ji} f_i) X_j = \sum_{i=1}^{k} (\sum_{j=1}^{n} s_{ji} X_j) f_i \in \mathcal{I} \trianglelefteq S$.

Thus letting $\mathcal{I}_i := (\mathcal{F} \setminus \{f_i\}) \trianglelefteq S$, we conclude that $S/\mathcal{I}_i$ is a graded algebra. Hence for $i \in \{1, \ldots, l\}$ we get $d_i f_i \equiv (\sum_{j=1}^{n} s_{ji} X_j) f_i \pmod{\mathcal{I}_i}$, where the left hand side belongs to $(S/\mathcal{I}_i)_{d_i}$, while the right hand side belongs to $\bigoplus_{e > d_i} (S/\mathcal{I}_i)_e$, from which we infer that $d_i f_i \in \mathcal{I}_i$, which since $d_i \in K^*$ contradicts the minimality of $\mathcal{F}$ as an ideal generating set of $\mathcal{I}$. ♯

Actually, Chevalley's Theorem holds in general, without any assumption on the degree of the generators [Serre, 1967]. (Unfortunately, we are not able to present a proof here.)

Note that from $R = K[f_1, \ldots, f_k]$ being polynomial, and $R \subseteq S$ being finite, we conclude that $k = \gamma(R) = \gamma(S) = n$ anyway. Then the converse of Chevalley's Theorem holds as well: If $R = K[f_1, \ldots, f_n]$ is a polynomial subalgebra of

$S = K[X_1, \ldots, X_n]$ such that $R \subseteq S$ is finite, then S being Cohen-Macaulay, see (15.4), implies that S is a free graded R-module.

From $S = \bigoplus_{s=1}^r h_s R$ we get $H_S = \frac{1}{(1-T)^n} = (\sum_{s=1}^r T^{e_s}) \cdot H_R = (\sum_{s=1}^r T^{e_s}) \cdot \prod_{i=1}^n \frac{1}{1-T^{d_i}} \in \mathbb{Q}(T)$, where $e_s := \deg(h_s) \in \mathbb{N}_0$. Hence $1 = \delta(S) = r \cdot \delta(R) = r \cdot \prod_{i=1}^n \frac{1}{d_i}$ says that S is a free graded R-module of rank $r = \prod_{i=1}^n d_i$. Since $\{h_1, \ldots, h_r\} \subseteq S$ is a minimal homogeneous generating set of S as a graded R-module, we conclude that the **(generalized) Hilbert algebra** S/R_+S is a finitely generated graded K-vector space of K-dimension r, having a homogeneous K-basis with degrees $[e_1, \ldots, e_r]$.

(7.3) Polynomial invariant algebras. We now turn to the question of when invariant algebras are polynomial: Let K be a field, let G be a finite group, let V be a faithful $K[G]$-module such that $n := \dim_K(V) \in \mathbb{N}_0$, and let $S[V]^G = K[f_1, \ldots, f_k]$, where $k \in \mathbb{N}_0$ is chosen minimal, and the f_i are homogeneous such that $\deg(f_i) = d_i \in \mathbb{N}$. Then the Hilbert-Serre Theorem implies that $\gamma(S[V]^G) \leq k$, thus since $\gamma(S[V]^G) = n$ we infer that $k \geq n$.

Proposition. We have $k = n$ if and only if $\{f_1, \ldots, f_k\}$ is algebraically independent, in other words $S[V]^G = K[f_1, \ldots, f_k]$ is a polynomial algebra.

Proof. If $S[V]^G = K[f_1, \ldots, f_k]$ is a polynomial algebra, then we have $k = \gamma(K[f_1, \ldots, f_k]) = \gamma(S[V]^G) = n$. Hence let conversely $k = n$, and assume to the contrary that $\{f_1, \ldots, f_n\}$ is algebraically dependent: Then, by Noether's Finiteness Theorem, for the invariant field we have $S(V)^G = \mathrm{Q}(S[V]^G) = K(f_1, \ldots, f_n)$, so that it has transcendence degree $\mathrm{trdeg}_K(S(V)^G) < n$, while $S(V)$ is a field of rational functions in n indeterminates, so that $\mathrm{trdeg}_K(S(V)) = n$, which since $[S(V) \colon S(V)^G] = |G|$ being finite is a contradiction. $\sharp$

Hence $S[V]^G$ is as a K-algebra generated by a homogeneous set $\{f_1, \ldots, f_n\}$ of cardinality n, if and only if it is a polynomial algebra. In this case, $\{f_1, \ldots, f_n\}$ is a minimal generating set, so that the multiset of degrees $d_1, \ldots, d_n$ is uniquely defined. Moreover, since G acts faithfully, from $\prod_{i=1}^n \frac{1}{d_i} = \delta(K[f_1, \ldots, f_n]) = \delta(S[V]^G) = \frac{1}{|G|}$ we infer that $\prod_{i=1}^n d_i = |G|$.

The f_i are called **basic invariants** or **fundamental invariants**, the d_i are called the associated **(polynomial) degrees**, and the numbers $m_i := d_i - 1 \in \mathbb{N}_0$ are called the associated **exponents**; note that, contrary to the degrees and the exponents, basic invariants are in general not uniquely defined, even not up to reordering and multiplication by scalars.

The degrees can be determined algorithmically from the Hilbert series: From $h := \frac{1}{H_R} = \prod_{i=1}^n (1 - T^{d_i}) \in \mathbb{Q}[T]$, where $d_i \mid |G|$, we infer that h is a product of cyclotomic polynomials Φ_d, where $d \mid |G|$. Hence letting $k \in \mathbb{N}$ run through the divisors of $|G|$, for $d := \frac{|G|}{k}$ we check whether Φ_d divides h, and if so, as long as $1 - T^d$ divides h, we repeat to record d and to replace h by $\frac{h}{1-T^d}$.

Finally, we remark that the converse of the above observation holds as well: If $\{f_1, \ldots, f_n\} \subseteq S[V]^G$ are homogeneous and algebraically independent, such that $\prod_{i=1}^n d_i = |G|$, then it is a (minimal) generating set, so that $S[V]^G$ is polynomial: If $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) > |G|$, then this follows from the Shephard-Todd Theorem, see (8.3); for arbitrary fields K, see (16.2).

Example. i) Let $G := \langle z \rangle \cong C_k$, where $k \in \mathbb{N}$ such that $\mathrm{char}(K) \nmid k$, and let $\zeta_k \in K$ be a primitive k-th root of unity; see (3.3). Letting $G \to K^* \colon z \mapsto \zeta_k$, we have $S[V]^G = K[X]^G = K[X^k] \subseteq K[X] = S[V]$. Similarly, letting $G \to \mathrm{GL}_2(K) \colon z \mapsto \mathrm{diag}[\zeta_k, 1]$, we have $S[V]^G = K[X^k, Y] \subseteq K[X, Y] = S[V]$.

ii) Let K be arbitrary, let $G := \langle z \rangle \cong C_2$, and let $G \to \mathrm{GL}_2(K) \colon z \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Then we have $S[V]^G = K[X + Y, XY] \subseteq K[X, Y] = S[V]$; see (3.4).

iii) Let $G = \langle z, s \rangle \cong D_{2k}$, where $k \in \mathbb{N}$ such that $\mathrm{char}(K) \nmid 2k$, let $\zeta_k \in K$ be a primitive k-th root of unity. Letting $G \to \mathrm{GL}_2(K)$ be given by $z \mapsto \mathrm{diag}[\zeta_k, \zeta_k^{-1}]$ and $s \mapsto \begin{bmatrix} . & 1 \\ 1 & . \end{bmatrix}$, we get $S[V]^G = K[XY, X^k + Y^k] \subseteq K[X, Y] = S[V]$; see (6.6).

8 Pseudoreflection groups

(8.1) Pseudoreflections. a) Let K be a field, let G be a finite group, and let V be a faithful $K[G]$-module such that $n := \dim_K(V) \in \mathbb{N}_0$. An element $s \in G \leq \mathrm{GL}_n(K)$ is called a **pseudoreflection**, if for its fixed point space $\mathrm{Fix}_V(s)$, that is its eigenspace with respect to the eigenvalue 1, we have $\dim_K(\mathrm{Fix}_V(s)) = n - 1$; in this case $\mathrm{Fix}_V(s)$ is called its **reflecting hyperplane**. Let $\mathcal{S}(G) \subseteq G$ be the set of pseudoreflections in G, and let $\sigma(G) := |\mathcal{S}(G)| \in \mathbb{N}_0$ be their number.

A pseudoreflection s which is diagonalizable is called a **homology** or **generalized reflection**; in other words s has an exceptional eigenvalue $\lambda \neq 1$ of multiplicity 1, or equivalently $\mathrm{char}(K) \nmid |s|$. A homology s such that $s^2 = 1$, or equivalently having exceptional eigenvalue -1, is called a **reflection**. A pseudoreflection s which is not diagonalizable is called a **transvection**; in other words s has 1 as its only characteristic root such that its Jordan normal form has a unique block of dimension 2, or equivalently $s^p = 1$ where $\mathrm{char}(K) = p \neq 0$.

b) Given a pseudoreflection s, let $(s - E_n)(V) = \langle t_s \rangle_K \leq V$; hence if s is a homology then t_s is an eigenvector of s with respect to its exceptional eigenvalue, while if s is a transvection then t_s is a distinguished eigenvector of s with respect to its unique eigenvalue 1. Then, in both cases, there is $\delta_s \in \mathrm{Hom}_K(V, K)$ such that $v \cdot s = v + \delta_s(v) t_s$, for all $v \in V$; in particular we have $\ker(\delta_s) = \mathrm{Fix}_V(s)$.

Letting $S := S[V]$, in order to describe the action of s on S, we show that there is a unique **Demazure operator** $\delta_s \in \mathrm{End}_K(S)$ homogeneous of degree -1, extending the map defined above, such that $f \cdot s = f + \delta_s(f) t_s \in S$, for all $f \in S$:

To this end, it suffices to show that $t_s \in V = S_1$ divides $f \cdot (s - 1) \in S$ for all monomials $f := \prod_{i=1}^n X_i^{a_i} \in S = K[X_1, \ldots, X_n]$, where $a_i \in \mathbb{N}_0$; uniqueness then follows from S being a domain: We may assume that $\mathrm{Fix}_V(s) = \langle X_2, \ldots, X_n \rangle_K$ and $a_1 \geq 1$. If s is a homology with exceptional eigenvalue λ, then we may assume that $t_s = X_1$; thus we have $f \cdot (s-1) = (\lambda^{a_1} - 1) \cdot \prod_{i=1}^n X_i^{a_i}$, which is a multiple of X_1. If s is a transvection, then we may assume that $t_s = X_2$ and $X_1 \cdot s = X_1 + X_2$; thus we have $f \cdot (s-1) = ((X_1+X_2)^{a_1} - X_1^{a_1}) \cdot \prod_{i=2}^n X_i^{a_i}$, which is a multiple of X_2. ♯

In particular, we have $\ker(\delta_s) = S^{\langle s \rangle} \subseteq S$. Moreover, δ_s is a **twisted derivation**: For $f, g \in S$, from $(fg)^s = f^s \cdot g^s$ we get $fg + \delta_s(fg)t_s = (f + \delta_s(f)t_s) \cdot (g + \delta_s(g)t_s)$. Hence since S is a domain we get $\delta_s(fg) = f\delta_s(g) + \delta_s(f)g + \delta_s(f)\delta_s(g)t_s = f\delta_s(g) + \delta_s(f)(g + \delta_s(g)t_s) = f \cdot \delta_s(g) + \delta_s(f) \cdot g^s \in S$.

Thus δ_s is a homomorphism of S^G-modules: For $f \in S$ and $g \in S^G$ we have $g^s = g$ and thus $\delta_s(g) = 0$, so that $\delta_s(fg) = f \cdot \delta_s(g) + \delta_s(f) \cdot g^s = \delta_s(f) \cdot g \in S$. In particular, letting $\mathcal{I}_G \trianglelefteq S$ be the Hilbert ideal, which is a homogeneous S^G-submodule, we conclude that δ_s induces a K-endomorphism of the coinvariant algebra $S_G = S/\mathcal{I}_G$, which again is homogeneous of degree -1.

(8.2) Non-modular pseudoreflections. Let G be a finite group, let K be a field such that $\mathrm{char}(K) \nmid |G|$, let V be a faithful $K[G]$-module such that $n := \dim_K(V) \in \mathbb{N}_0$, and let $S := S[V]$.

Theorem. There is $f \in \mathbb{Q}(T)$ such that $\nu_1(f) \geq 0$, and such that we have $H_{S^G} = \frac{1}{|G|} \cdot \frac{1}{(1-T)^n} \cdot \left(1 + \frac{\sigma(G)}{2} \cdot (1-T) + (1-T)^2 \cdot f\right) \in \mathbb{Q}(T)$.

Proof. In view of Molien's formula we may assume that K contains a primitive $|G|$-th root of unity, so that in order to consider the elements $g \in G$ in turn we may further assume that g is a diagonal matrix. Hence g is a pseudoreflection if and only if it has eigenvalue 1 with multiplicity $n-1$, and an exceptional eigenvalue $\lambda \neq 1$ with multiplicity 1. Note that $1 \in G$ is the unique element having eigenvalue 1 with multiplicity n.

Thus we have $\det(E_n - g \cdot T) = (1-T)^n$ if and only if $g = 1$, as well as $\det(E_n - g \cdot T) = (1-T)^{n-1}(1-\lambda T)$ if and only if g is a pseudoreflection with exceptional eigenvalue λ, while otherwise $\nu_1(\det(E_n - g \cdot T)) \leq n-2$. Hence by Molien's formula there are $f \in \mathbb{Q}(T)$ such that $\nu_1(f) \geq 0$, and $\epsilon \in \mathbb{Q}$ such that the Hilbert series of S^G is given as $H_{S^G} = \frac{1}{|G|} \cdot \sum_{g \in G} \frac{1}{\det(E_n - g \cdot T)} = \frac{1}{|G|} \cdot \frac{1}{(1-T)^n} \cdot (1 + \epsilon \cdot (1-T) + (1-T)^2 \cdot f) \in \mathbb{Q}(T)$. It remains to find $\epsilon \in \mathbb{Q}$:

Precisely the summands associated with a pseudoreflection g contribute to ϵ, in which case we have $\frac{(1-T)^{n-1}}{\det(E_n - g \cdot T)} = \frac{1}{1-\lambda T}$, where λ is the exceptional eigenvalue, yielding $(\frac{(1-T)^{n-1}}{\det(E_n - g \cdot T)})(1) = \frac{1}{1-\lambda}$. Since $\frac{1}{1-\lambda} + \frac{1}{1-\frac{1}{\lambda}} = 1$, pairing off mutually inverse pseudoreflections, where for a (self-inverse) reflection we have $\frac{1}{1-\lambda} = \frac{1}{2}$, and summing over all the pseudoreflections $\mathcal{S} = \mathcal{S}(G)$, we get $\epsilon = (\sum_{g \in \mathcal{S}} \frac{(1-T)^{n-1}}{\det(E_n - g \cdot T)})(1) = \frac{|\{g \in \mathcal{S}; g^2 \neq 1\}|}{2} \cdot 1 + |\{g \in \mathcal{S}; g^2 = 1\}| \cdot \frac{1}{2} = \frac{1}{2} \cdot |\mathcal{S}|$. ♯

Note that the above argument also provides an alternative proof of the facts that $\gamma(S^G) = n$ and $\delta(S^G) = \frac{1}{|G|}$, in the case $\mathrm{char}(K) \nmid |G|$.

Theorem. Let $\{f_1, \ldots, f_n\} \subseteq S^G$ be algebraically independent and homogeneous, such that the degrees $d_i := \deg(f_i) \in \mathbb{N}$ fulfill $\prod_{i=1}^n d_i = |G|$. Then we have $\sum_{i=1}^n (d_i - 1) \leq \sigma(G)$, where if $S^G = K[f_1, \ldots, f_n]$ then equality holds.

Proof. Let $R := K[f_1, \ldots, f_n] \subseteq S^G$. Then R is polynomial with degrees $[d_1, \ldots, d_n]$, hence we have $(1-T)^n \cdot H_R = \prod_{i=1}^n \frac{1-T}{1-T^{d_i}} = \prod_{i=1}^n \frac{1}{\sum_{j=0}^{d_i-1} T^j} \in \mathbb{Q}(T)$. Differentiation $\frac{\partial}{\partial T}$ with respect to T, and evaluation at $T = 1$, yields $\frac{\partial}{\partial T}((1-T)^n \cdot H_R)(1) = (-\prod_{i=1}^n \frac{1}{\sum_{j=0}^{d_i-1} T^j} \cdot (\sum_{i=1}^n \frac{\sum_{j=1}^{d_i-1} jT^{j-1}}{\sum_{j=0}^{d_i-1} T^j}))(1) = -\prod_{i=1}^n \frac{1}{d_i} \cdot (\sum_{i=1}^n \frac{\binom{d_i}{2}}{d_i}) = -\frac{1}{2} \cdot \prod_{i=1}^n \frac{1}{d_i} \cdot \sum_{i=1}^n (d_i - 1)$. Thus we have $(1-T)^n \cdot H_R = \frac{1}{|G|} \cdot (1 + \frac{1}{2} \cdot \sum_{i=1}^n (d_i - 1) \cdot (1-T) + (1-T)^2 \cdot g) \in \mathbb{Q}(T)$, where $\nu_1(g) \geq 0$.

From $(1-T)^n \cdot H_{S^G} = \frac{1}{|G|} \cdot (1 + \frac{\sigma(G)}{2} \cdot (1-T) + (1-T)^2 \cdot f) \in \mathbb{Q}(T)$, where $\nu_1(f) \geq 0$, we get $2 \cdot |G| \cdot (1-T)^{n-1} \cdot (H_{S^G} - H_R) = \sigma(G) - \sum_{i=1}^n (d_i - 1) + (1-T) \cdot h \in \mathbb{Q}(T)$, where $\nu_1(h) \geq 0$. Since for $d \in \mathbb{N}_0$ we have $\dim_K(R_d) \leq \dim_K(S_d^G)$, we get $H_R(z) \leq H_{S^G}(z) \in \mathbb{R}$ for $0 < z < 1$, thus we conclude that $\lim_{z \to 1^-}((1-z)^{n-1} \cdot (H_{S^G} - H_R)(z)) \geq 0$, and evaluation at $T = 1$ yields $\sigma(G) \geq \sum_{i=1}^n (d_i - 1)$.

If $R = S^G$, then $H_R = H_{S^G}$ entails $\lim_{z \to 1^-}((1-z)^{n-1} \cdot (H_{S^G} - H_R)(z)) = 0$, thus $\sigma(G) = \sum_{i=1}^n (d_i - 1)$. ♯

(8.3) Non-modular pseudoreflection groups. Let G be a finite group, let K be a field such that $\mathrm{char}(K) \not| \, |G|$, let V be a faithful $K[G]$-module such that $n := \dim_K(V) \in \mathbb{N}_0$, let $S := S[V]$, and let $R := S^G$.

Theorem: [Shephard, Todd, 1954; Chevalley, 1955; Serre, 1967]. Assume that $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) > |G|$. Then the following are equivalent:
i) G is a **pseudoreflection group**, that is $G = \langle \mathcal{S}(G) \rangle$.
ii) S is a (finitely generated) free graded R-module.
iii) R is a polynomial algebra.

Proof. (i)⇒(ii). Let $G = \langle \mathcal{S}(G) \rangle$, where we only assume that $\mathrm{char}(K) \nmid |G|$.

We first consider the coinvariant algebra $S_G := S/(R_+ S)$, being a graded G-algebra again, and being acted on by all Demazure operators. For $s \in \mathcal{S}(G)$, we infer that $\delta_s \in \mathrm{End}_K(S_G)$ is homogeneous of degree -1, and for $v \in S_G$ we have $\delta_s(v) = 0$ if and only if $v \cdot s = v$. Since $G = \langle \mathcal{S}(G) \rangle$, we infer that $\bigcap_{s \in \mathcal{S}(G)} \ker_{S_G}(\delta_s) = (S_G)^G$. Since $(S_G)^G = (S_G)_0 \cong K$, we infer that for any $0 \neq h \in (S_G)_+$ there is $s \in \mathcal{S}(G)$ such that $\delta_s(h) \neq 0$.

Now assume to the contrary that S is not a free graded R-module; recall that by Noether's Finiteness Theorem S is a finitely generated R-module. Thus any minimal homogeneous generating set $\{h_1, \ldots, h_r\}$ of S as an R-module, where $r \in \mathbb{N}$, contains a minimal R-linearly dependent subset of cardinality $l \in \{2, \ldots, r\}$, where we may assume the h_i to be chosen such that l is as small as possible amongst all admissible generating sets. Then we may assume that $\{h_1, \ldots, h_l\}$ is such a smallest R-linearly dependent subset, where for $e_i := \deg(h_i) \in \mathbb{N}_0$ we have $e_1 \leq \cdots \leq e_l$, and necessarily $e_2 \geq 1$.

Hence let $g_1, \ldots, g_l \in R$ be homogeneous such that $\sum_{i=1}^{l} h_i g_i = 0 \in S$. Then there are pseudoreflections $s_1, \ldots, s_e \in \mathcal{S}(G)$, where $e := e_l \geq 1$, such that for the R-module endomorphism $\delta := \delta_{s_1} \cdots \delta_{s_e}$ of S, which is homogeneous of degree $-e$, we have $\delta(h_i) = 0$ whenever $e_i < e$, while $\delta(h_i) \in S_0 = K$ whenever $e_i = e$, and $\delta(h_l) \in K^*$. Hence we get $0 = \delta(\sum_{i=1}^{l} h_i g_i) = \sum_{i=1}^{l} \delta(h_i) g_i \in S$, thus $g_l = -\sum_{i=1}^{l-1} \frac{\delta(h_i)}{\delta(h_l)} \cdot g_i$, so that letting $h_i' := h_i - \frac{\delta(h_i)}{\delta(h_l)} \cdot h_l \in S_{e_i}$, for $i \in \{1, \ldots, l-1\}$, we get $\sum_{i=1}^{l-1} h_i' g_i = \sum_{i=1}^{l-1} (h_i - \frac{\delta(h_i)}{\delta(h_l)} \cdot h_l) g_i = \sum_{i=1}^{l-1} h_i g_i - (\sum_{i=1}^{l-1} \frac{\delta(h_i)}{\delta(h_l)} \cdot g_i) h_l = \sum_{i=1}^{l} h_i g_i = 0$. Since $\{h_1', \ldots, h_{l-1}', h_l, h_{l+1}, \ldots, h_r\}$ also is an admissible generating set, this contradicts the minimality of l. $\sharp$

(ii)⇒(iii). Let S be a free graded R-module, and let $\{f_1, \ldots, f_k\}$ be a minimal homogeneous generating set of R, where $k \in \mathbb{N}_0$ and $d_i := \deg(f_i) \in \mathbb{N}$. To proceed, we only need the fact that $d_i \in K^*$ for all $i \in \{1, \ldots, k\}$; then by Chevalley's Theorem we conclude that $\{f_1, \ldots, f_k\}$ is algebraically independent:

Indeed, by Noether's degree bound (which holds whenever $\mathrm{char}(K) \nmid |G|$) we have $d_i \leq |G|$, so that by the assumption on $\mathrm{char}(K)$ (as made in the statement of the theorem) we have $d_i \in K^*$. $\sharp$

(iii)⇒(i). Let $R = K[f_1, \ldots, f_n]$ be polynomial, where the f_i are homogeneous, and we may assume that the degrees $d_i := \deg(f_i) \in \mathbb{N}$ fulfill $d_1 \leq \cdots \leq d_n$. Moreover, we infer that $\prod_{i=1}^{n} d_i = |G|$.

Let $H := \langle \mathcal{S}(G) \rangle \leq G$ be the subgroup generated by the pseudoreflections in G. Noting that $|H| \leq |G|$, by the implication '(i)⇒(iii)' already shown, we have $R \subseteq S^H = K[g_1, \ldots, g_n] \subseteq S$, where the g_i are algebraically independent and homogeneous, and we may assume that the degrees $e_i := \deg(g_i) \in \mathbb{N}$ fulfill $e_1 \leq \cdots \leq e_n$. Then we actually have $d_i \geq e_i$ for all $i \in \{1, \ldots, n\}$:

Letting the polynomial algebra $K[Y_1, \ldots, Y_n]$ be equipped with the grading with degrees $\delta := [e_1, \ldots, e_n]$, there are $h_i \in K[Y_1, \ldots, Y_n]$ homogeneous such that $\deg_\delta(h_i) = d_i$ and $f_i = h_i(g_1, \ldots, g_n)$. Now assume to the contrary that $d_j < e_j$ for some $j \in \{1, \ldots, n\}$. Then we have $\{h_1, \ldots, h_j\} \subseteq K[Y_1, \ldots, Y_{j-1}]$, so that $\{f_1, \ldots, f_j\} \subseteq K[g_1, \ldots, g_{j-1}]$, thus $\{f_1, \ldots, f_j\}$ cannot possibly be algebraically independent, a contradiction. $\sharp$

Finally, we show that $|H| = |G|$, entailing $G = H = \langle \mathcal{S}(G) \rangle$: By (8.2) we have $\sum_{i=1}^{n} (d_i - 1) \leq \sigma(G) = \sigma(H) = \sum_{i=1}^{n} (e_i - 1)$, so that we conclude that $d_i = e_i$ for all i. Thus we have $H_R = H_{S^H} \in \mathbb{Q}(T)$, in particular implying $|G| = |H|$. $\sharp$

Corollary. Let still $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) > |G|$, and let $\{f_1, \ldots, f_n\} \subseteq R$ be algebraically independent and homogeneous, such that $\prod_{i=1}^n \deg(f_i) = |G|$. Then we have $R = K[f_1, \ldots, f_n]$.

Proof. Proceeding as for the implication '(iii)⇒(i)' above, but for the polynomial K-algebra $P := K[f_1, \ldots, f_n] \subseteq R \subseteq S^H \subseteq S$, where $H := \langle \mathcal{S}(G) \rangle \leq G$, we still infer $H_P = H_{S^H} \in \mathbb{Q}(T)$, so that we have equality $P = R = S^H$. ♯

Originally, Shephard, Todd proved the above theorem in characteristic 0, by first classifying the finite irreducible complex pseudoreflection groups, and subsequently verifying the polynomiality of their invariant algebras in a case-by-case analysis. Later, Chevalley gave a conceptual proof for real reflection groups, which was generalized by Serre to the complex case.

(8.4) Complex pseudoreflection groups. We present the classification of the finite pseudoreflection groups over the field $\mathbb{C}$ [Shephard, Todd, 1954], which extends their classification over the field $\mathbb{R}$ [Coxeter, 1928], and has been generalized to the non-modular case [Clark, Ewing, 1974]:

Let G be a finite group, and let $V \neq \{0\}$ be a faithful $\mathbb{C}[G]$-module such that $G = \langle \mathcal{S}(G) \rangle$ is generated by pseudoreflections. We first reduce ourselves to the (absolutely) irreducible case:

By Maschke's Theorem we have $V = \bigoplus_{i=1}^r V_i$ as $\mathbb{C}[G]$-modules, where the V_i are (absolutely) irreducible. By considering the eigenvalues of the pseudoreflections $s \in \mathcal{S}(G)$ it follows that $\rho_{V_i}(s) \neq \mathrm{id}_{V_i}$ for a unique $i \in \{1, \ldots, r\}$, where $\rho_{V_i}(s)$ is a pseudoreflection again. Hence letting $\mathcal{S}_i := \{s \in \mathcal{S}(G); \rho_{V_i}(s) \neq \mathrm{id}_{V_i}\}$ we get $\mathcal{S}(G) = \coprod_{i=1}^r \mathcal{S}_i$, and letting $G_i := \langle \rho_{V_i}(s); s \in \mathcal{S}_i \rangle \leq G$, we have $G \cong \prod_{i=1}^r G_i$, where G_i acts trivially on $\bigoplus_{j \neq i} V_j$, while V_i is a faithful (absolutely) irreducible $\mathbb{C}[G_i]$-module such that G_i is generated by pseudoreflections. In particular, for the associated invariant algebras we have $S[V]^G \cong \bigotimes_{i=1}^r S[V_i]^{G_i}$, so that $S[V]^G$ is described in terms of the $S[V_i]^{G_i}$; see Exercise (18.5). ♯

Hence we may further assume that V is (absolutely) irreducible, and let χ_V be the associated character of G. We show that χ_V is realizable over its character field $K := \mathbb{Q}(\chi_V)$, that is the algebraic number field generated by the values of χ_V, so that K is the unique minimal realization field:

For $s \in \mathcal{S}(G)$ let $1 \neq \lambda \in K$ be its exceptional eigenvalue, let $H := \langle s \rangle \leq G$, and let $\rho_\lambda \colon H \to K^* \colon s \mapsto \lambda$ be the associated one-dimensional representation. Then by Frobenius reciprocity we have $\dim_{\mathbb{C}}(\mathrm{Hom}_{\mathbb{C}[G]}(\rho_\lambda^G, V)) = \dim_{\mathbb{C}}(\mathrm{Hom}_{\mathbb{C}[H]}(\rho_\lambda, V_H)) = 1$. Since ρ_λ^G is a $K[G]$-module, we conclude that V is realizable as a quotient $K[G]$-module of the latter. (In other words, the Schur index of V over K, which divides $\dim_{\mathbb{C}}(\mathrm{Hom}_{\mathbb{C}[G]}(\rho_\lambda^G, V))$, equals 1.) ♯

Now the classification of the finite (absolutely) irreducible **complex pseudoreflection groups** is given in Table 2, where the classes 1, $2a$, $2b$, and 3 consist of infinite series, while the 34 groups $G_4, \ldots, G_{37}$ are called the **exceptional**

Table 2: Irreducible complex pseudoreflection groups.

G_i	n	$\lvert G_i\rvert$	$d_1, \ldots, d_n$	$\mathbb{Q}(\chi)$	G_i	type
1	n	$(n+1)!$	$2, \ldots, n+1$	$\mathbb{Q}$	$\mathcal{S}_{n+1}$	A_n
$2a$	n	$\frac{m^n}{k} \cdot n!$	$m, \ldots, (n-1)m, \frac{mn}{k}$	$\mathbb{Q}(\zeta_m)$	$G_{m,k,n}$	B_n, D_n $(m=2)$
$2b$	2	$2m$	$2, m$	$\mathbb{Q}(\zeta_m + \zeta_m^{-1})$	D_{2m}	$I_2(m)$
3	1	m	m	$\mathbb{Q}(\zeta_m)$	C_m	

G_i	n	$\lvert G_i\rvert$	$d_1, \ldots, d_n$	$\mathbb{Q}(\chi)$	$G_i/Z(G_i)$	type
4	2	24	$4, 6$	$\mathbb{Q}(\zeta_3)$	$\mathcal{A}_4$	
5	2	72	$6, 12$	$\mathbb{Q}(\zeta_3)$	$\mathcal{A}_4$	
6	2	48	$4, 12$	$\mathbb{Q}(\zeta_{12})$	$\mathcal{A}_4$	
7	2	144	$12, 12$	$\mathbb{Q}(\zeta_{12})$	$\mathcal{A}_4$	
8	2	96	$8, 12$	$\mathbb{Q}(\zeta_4)$	$\mathcal{S}_4$	
9	2	192	$8, 24$	$\mathbb{Q}(\zeta_8)$	$\mathcal{S}_4$	
10	2	288	$12, 24$	$\mathbb{Q}(\zeta_{12})$	$\mathcal{S}_4$	
11	2	576	$24, 24$	$\mathbb{Q}(\zeta_{24})$	$\mathcal{S}_4$	
12	2	48	$6, 8$	$\mathbb{Q}(\sqrt{-2})$	$\mathcal{S}_4$	
13	2	96	$8, 12$	$\mathbb{Q}(\zeta_8)$	$\mathcal{S}_4$	
14	2	144	$6, 24$	$\mathbb{Q}(\zeta_3, \sqrt{-2})$	$\mathcal{S}_4$	
15	2	288	$12, 24$	$\mathbb{Q}(\zeta_{24})$	$\mathcal{S}_4$	
16	2	600	$20, 30$	$\mathbb{Q}(\zeta_5)$	$\mathcal{A}_5$	
17	2	1200	$20, 60$	$\mathbb{Q}(\zeta_{20})$	$\mathcal{A}_5$	
18	2	1800	$30, 60$	$\mathbb{Q}(\zeta_{15})$	$\mathcal{A}_5$	
19	2	3600	$60, 60$	$\mathbb{Q}(\zeta_{60})$	$\mathcal{A}_5$	
20	2	360	$12, 30$	$\mathbb{Q}(\zeta_3, \sqrt{5})$	$\mathcal{A}_5$	
21	2	720	$12, 60$	$\mathbb{Q}(\zeta_{12}, \sqrt{5})$	$\mathcal{A}_5$	
22	2	240	$12, 20$	$\mathbb{Q}(\zeta_4, \sqrt{5})$	$\mathcal{A}_5$	
23	3	120	$2, 6, 10$	$\mathbb{Q}(\sqrt{5})$	$\mathcal{A}_5$	H_3
24	3	336	$4, 6, 14$	$\mathbb{Q}(\sqrt{-7})$	$\mathrm{GL}_3(2)$	
25	3	648	$6, 9, 12$	$\mathbb{Q}(\zeta_3)$	$3^2 \colon \mathrm{SL}_2(3)$	
26	3	1296	$6, 12, 18$	$\mathbb{Q}(\zeta_3)$	$3^2 \colon \mathrm{SL}_2(3)$	
27	3	2160	$6, 12, 30$	$\mathbb{Q}(\zeta_3, \sqrt{5})$	$\mathcal{A}_6$	
28	4	1152	$2, 6, 8, 12$	$\mathbb{Q}$	$2^4 \colon (\mathcal{S}_3 \times \mathcal{S}_3)$	F_4
29	4	7680	$4, 8, 12, 20$	$\mathbb{Q}(\zeta_4)$	$2^4 \colon \mathcal{S}_5$	
30	4	14400	$2, 12, 20, 30$	$\mathbb{Q}(\sqrt{5})$	$(\mathcal{A}_5 \times \mathcal{A}_5) \colon 2$	H_4
31	4	46080	$8, 12, 20, 24$	$\mathbb{Q}(\zeta_4)$	$2^4 \colon \mathcal{S}_6$	
32	4	155520	$12, 18, 24, 30$	$\mathbb{Q}(\zeta_3)$	$\mathrm{PSp}_4(3)$	
33	5	51840	$4, 6, 10, 12, 18$	$\mathbb{Q}(\zeta_3)$	$\mathrm{SO}_5(3)'$	
34	6	39191040	$6, 12, 18, 24, 30, 42$	$\mathbb{Q}(\zeta_3)$	$\mathrm{PSO}_6^-(3)'.2$	
35	6	51840	$2, 5, 6, 8, 9, 12$	$\mathbb{Q}$	$\mathrm{SO}_6^-(2)'$	E_6
36	7	2903040	$2, 6, 8, 10, 12, 14, 18$	$\mathbb{Q}$	$\mathrm{SO}_7(2)$	E_7
37	8	696729600	$2, 8, 12, 14, 18, 20, 24, 30$	$\mathbb{Q}$	$\mathrm{SO}_8^+(2)$	E_8

complex pseudoreflection groups. We give the dimension n of the associated pseudoreflection representation, the group order, the polynomial degrees, and the character fields, where $\zeta_k := \exp(\frac{2\pi\sqrt{-1}}{k}) \in \mathbb{C}$ is a k-th primitive root of unity for $k \in \mathbb{N}$, and we collect some structure information.

The finite **real reflection groups**, also called **Coxeter groups**, are those whose character field is a subfield of $\mathbb{R}$; the real reflection groups having character field $\mathbb{Q}$ are called **crystallographic**. In Table 2 we indicate the **Dynkin type** of the real reflection groups as well. Note that a real reflection group is indeed generated by reflections, but this property does not imply to be a real reflection group, as the example of the group G_{24} shows; see Exercise (18.31).

i) The groups in class 1, being real of Dynkin type A_n for $n \geq 1$, are the symmetric groups $\mathcal{S}_{n+1}$ acting by the **deleted permutation representation**: The group $\mathcal{S}_{n+1} = \langle (1,2), \ldots, (n, n{+}1) \rangle$ is generated by adjacent transpositions, which act by reflections with respect to the natural permutation representation on $W := \mathbb{Q}^{n+1}$; see also (9.2). As $\mathcal{S}_{n+1}$ acts doubly transitively, we have $\dim_{\mathbb{Q}}(\mathrm{End}_{\mathcal{S}_{n+1}}(W)) = 2$. Thus we have $W \cong K \oplus V$, where $\mathrm{Fix}_W(\mathcal{S}_{n+1}) \cong K$ is the trivial representation, and V is an absolutely irreducible faithful $\mathbb{Q}[\mathcal{S}_{n+1}]$-module, with respect to which $\mathcal{S}_{n+1}$ is generated by reflections. Hence we have $V \cong W/\mathrm{Fix}_W(\mathcal{S}_{n+1})$ as $\mathbb{Q}[\mathcal{S}_{n+1}]$-modules. For basic invariants, being derived from the elementary symmetric polynomials in $\mathbb{Q}[W]^{\mathcal{S}_{n+1}}$, see Exercise (18.29).

ii) The groups in class $2a$ encompass the **imprimitive** cases, and are given as follows: For $m \geq 2$, and $k \geq 1$ such that $k \mid m$, and $n \geq 2$, let $T_{m,k,n} := \{\mathrm{diag}[\zeta_m^{a_i}]_i \in \mathrm{GL}_n(\mathbb{C}); a_i \in \mathbb{Z}, k \mid \sum_{i=1}^n a_i\} \leq \mathrm{GL}_n(\mathbb{C})$; note that the condition $k \mid \sum_{i=1}^n a_i$ is equivalent to saying that $(\prod_{i=1}^n \zeta_m^{a_i})^{\frac{m}{k}} = 1$. Letting $\mathcal{S}_n \leq \mathrm{GL}_n(\mathbb{C})$ be the natural permutation representation, we let $G_{m,k,n} := T_{m,k,n} \colon \mathcal{S}_n$, that is the group of all monomial matrices, whose non-zero entries are m-th roots of unity, and whose product is an $(\frac{m}{k})$-th root of unity. (We have to exclude the case $G_{2,2,2}$ which is reducible.)

We show that $G_{m,k,n}$ is a pseudoreflection group indeed: The group $\mathcal{S}_n$ is generated by reflections; the diagonal group $T_{m,k,n}$ is generated by the pseudoreflection $\mathrm{diag}[\zeta_m^k, 1, \ldots, 1]$, together with the $\mathcal{S}_n$-conjugates of $\mathrm{diag}[\zeta_m, \zeta_m^{-1}, 1, \ldots, 1]$, where $\mathrm{diag}[\zeta_m, \zeta_m^{-1}] = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & \zeta_m^{-1} \\ \zeta_m & 0 \end{bmatrix}$ is the product of two reflections.

The group $G_{m,k,n}$ is real if and only if $m = 2$. In this case, $k = 1$ yields Dynkin type B_n, where $G_{2,1,n} \cong 2^n \colon \mathcal{S}_n$ is the group of **signed permutations**; and $k = 2$ yields Dynkin type D_n, where $2^{n-1} \colon \mathcal{S}_n \cong G_{2,2,n} \trianglelefteq G_{2,1,n}$ is the subgroup of index 2 consisting of the elements having an even number of entries -1.

iii) The groups in class $2b$ are real, and isomorphic to the dihedral groups D_{2m} for $m \geq 3$; see (6.6). The group D_{2m} is crystallographic if and only if $m \in \{3, 4, 6\}$; in these cases we get Dynkin types A_2 again, B_2 again, and finally G_2, being equal to $I_2(3)$, $I_2(4)$, and $I_2(6)$, respectively.

The groups in class 3 are the cyclic groups C_m for $m \geq 1$; see (3.3). The group C_m is real if and only if $m \leq 2$; in these cases we get the trivial group and

Dynkin type A_1 again, respectively.

iv) The exceptional groups in dimension $n = 2$, that is the groups $G_i \leq U_2(\mathbb{C})$ for $i \in \{4, \ldots, 22\}$, are centrally amalgamated products of the **binary polyhedral subgroups** $2.\mathcal{A}_4$, $2.\mathcal{S}_4$, and $2.\mathcal{A}_5$ of $\mathrm{SU}_2(\mathbb{C})$ with certain cyclic groups of scalar matrices. Note that counting the pseudoreflections in $G = G_i$ yields the degrees $d_1 \leq d_2$ from the conditions $d_1 d_1 = |G|$ and $d_1 + d_2 = |\sigma(G)| + 2$.

The binary polyhedral subgroups arise from the **polyhedral subgroups** $\mathcal{A}_4$, $\mathcal{S}_4$, and $\mathcal{A}_5$ of $\mathrm{SO}_3(\mathbb{R})$, as preimage with respect to the group homomorphism $\rho\colon \mathrm{SU}_2(\mathbb{C}) \to \mathrm{SO}_3(\mathbb{R})$ which is given as follows:

Let $\mathcal{H} := \{B \in \mathbb{C}^{2\times 2}; \overline{B}^{\mathrm{tr}} = B, \mathrm{Tr}(B) = 0\}$ be the $\mathbb{R}$-vector space of **traceless Hermitian matrices**, where $\overline{}\colon \mathbb{C} \to \mathbb{C}$ denotes complex conjugation. Then $\mathcal{H}$ can be identified with $\mathbb{R}^3$ by writing $B = \begin{bmatrix} a & b+ic \\ b-ic & -a \end{bmatrix} \in \mathcal{H}$, where $a, b, c \in \mathbb{R}$; note that $\det(B) = -(a^2 + b^2 + c^2)$. Moreover, $\mathrm{SU}_2(\mathbb{C}) := \{A \in \mathrm{SL}_2(\mathbb{C}); \overline{A}^{-\mathrm{tr}} = A\}$ acts continuously on $\mathcal{H}$ by $\rho_A\colon \mathcal{H} \to \mathcal{H}\colon B \mapsto \overline{A}^{\mathrm{tr}} BA = A^{-1}BA$.

Hence identifying $\mathcal{H}$ with $\mathbb{R}^3$, and noting that $\det(\rho_A(B)) = \det(B)$, yields a continuous group homomorphism $\rho\colon \mathrm{SU}_2(\mathbb{C}) \to O_3(\mathbb{R})$. Since $\mathrm{SU}_2(\mathbb{C})$ is connected we infer that $\rho(\mathrm{SU}_2(\mathbb{C})) \leq O_3(\mathbb{R})^\circ = \mathrm{SO}_3(\mathbb{R})$. Since $\ker(\rho) = \{\pm E_2\}$, and both $\mathrm{SU}_2(\mathbb{C})$ and $\mathrm{SO}_3(\mathbb{R})$ are 3-dimensional $\mathbb{R}$-manifolds, we conclude that $\rho\colon \mathrm{SU}_2(\mathbb{C}) \to \mathrm{SO}_3(\mathbb{R})$ is surjective, so that actually $\mathrm{PSU}_2(\mathbb{C}) \cong \mathrm{SO}_3(\mathbb{R})$, also being called the **Cayley parametrisation** of $\mathrm{SO}_3(\mathbb{R})$. ♯

The polyhedral subgroups are the rotational symmetry groups of the five **Platonic solids**, that is the regular 3-dimensional polyhedra; these are given in Table 3, where n is the number of edges a face is incident with, k is the number of edges a vertex is incident with, v is the number of vertices, e is the number of edges, and f is the number of faces. Note that there is a duality between the octahedron and the hexahedron, and between the icosahedron and the dodecahedron, while the tetrahedron is self-dual: Connecting the barycenters of the faces one of the mutually dual polyhedra yields the other one; hence polyhedra in duality have the same symmetry group. The polyhedral groups are considered in more detail in Exercise (18.30) as far as the tetrahedron and octahedron are concerned, and in (12.1) as far as the icosahedron is concerned.

(8.5) Remark: Pseudoreflection groups in prime characteristic. Actually, (8.3) remains valid completely in the non-modular case, as does the implication '(iii)⇒(i)' in the modular case [Serre, 1967]; recall that we have already indicated that the equivalence '(ii)⇔(iii)', which essentially is Chevalley's Theorem, holds in general, without any assumption on the characteristic. (Unfortunately, we are not able to present proofs here, which require more machinery from commutative and homological algebra; in particular they are related to the proof of the 'purity of the branch locus' [Auslander, 1962].)

Unfortunately, in the modular case the implication '(i)⇒(ii)' does not hold in

Table 3: Platonic solids.

n	k	v	e	f		
3	3	4	6	4	tetrahedron	$\mathcal{A}_4$
4	3	8	12	6	hexahedron	$\mathcal{S}_4$
3	4	6	12	8	octahedron	$\mathcal{S}_4$
5	3	20	30	12	dodecahedron	$\mathcal{A}_5$
3	5	12	30	20	icosahedron	$\mathcal{A}_5$

general; we present the counterexample given by Nakajima [1979] in Exercise (18.28). Still, the invariant algebra of a pseudoreflection group is factorial [Dress, 1969]. Using the classification of the finite irreducible pseudoreflection groups in prime characteristic [Kantor, 1979; Wagner, 1978, 1980; Zalesskii, Serezkin, 1976, 1981], the classification of polynomial invariant algebras in the irreducible modular case is known [Kemper, Malle, 1997].

9 Permutation groups

(9.1) Permutation groups. Let K be a field, for $n \in \mathbb{N}_0$ let $\mathcal{S}_n$ denote the symmetric group on n letters, let $V := K^n$ be its (faithful) natural permutation module, and let $S := S[V] = K[\mathcal{X}]$, where $\mathcal{X} := \{X_1, \ldots, X_n\}$. Then $\mathcal{S}_n$ permutes $\mathcal{X}$, and thus acts on $K[\mathcal{X}]_d$, for $d \in \mathbb{N}_0$, by permuting its K-basis $\mathcal{X}_d$ consisting of the monomials of degree d.

Let $G \leq \mathcal{S}_n$ be a permutation group. Writing $\mathcal{X}_d = \coprod_{j=1}^{k_d} \mathcal{X}_{d,j}$ as a disjoint union of G-orbits, where $k_d = |\mathcal{X}_d/G| \in \mathbb{N}_0$, let $\mathcal{X}_{d,j}^+ := \sum_{f \in \mathcal{X}_{d,j}} f \in S_d$ be the associated orbit sum; note that $\mathcal{X}_{d,j}^+ = \mathrm{Tr}_{\mathrm{Stab}_G(f)}^G(f)$ for any $f \in \mathcal{X}_{d,j}$.

Then we have $S_d = \bigoplus_{j=1}^{k_d} S_{d,j}$ as $K[G]$-modules, where $S_{d,j} := \langle \mathcal{X}_{d,j} \rangle_K$, and since G acts transitively on $\mathcal{X}_{d,j}$ we infer that $\mathrm{Fix}_{S_{d,j}}(G) = \langle \mathcal{X}_{d,j}^+ \rangle_K$. Hence we conclude that $\dim_K(S_d^G) = k_d = |\mathcal{X}_d/G|$; recall that the Cauchy-Frobenius-Burnside Lemma says that $|\mathcal{X}_d/G| = \frac{1}{|G|} \cdot \sum_{g \in G} |\mathrm{Fix}_{\mathcal{X}_d}(g)|$.

Thus we have $H_{S^G} = \sum_{d \geq 0} |\mathcal{X}_d/G| \cdot T^d = \frac{1}{|G|} \cdot \sum_{d \geq 0} (\sum_{g \in G} |\mathrm{Fix}_{\mathcal{X}_d}(g)|) \cdot T^d = \frac{1}{|G|} \cdot \sum_{g \in G} (\sum_{d \geq 0} |\mathrm{Fix}_{\mathcal{X}_d}(g)| \cdot T^d) = \frac{1}{|G|} \cdot \sum_{g \in G} \chi_S(g) \in \mathbb{Q}(T)$, where $\chi_S(g) = \sum_{d \geq 0} |\mathrm{Fix}_{\mathcal{X}_d}(g)| \cdot T^d \in \mathbb{Q}(T)$ is the associated graded permutation character.

This only depends on the permutation action considered, but is independent of the field K chosen, so that in particular H_{S^G} can be computed by applying Molien's formula to the associated ordinary permutation representation. Indeed, assuming that $\mathrm{char}(K) = 0$ we have $\chi_S(g) = \frac{1}{(-T)^n \cdot \chi_{\rho_V(g)}(T^{-1})}$; and letting $\lambda = [\lambda_1, \ldots, \lambda_l]$ be the cycle type of g, we have $\chi_{\rho_V(g)} = \prod_{i=1}^{l} (T^{\lambda_i} - 1)$, so that we get $\chi_S(g) = \prod_{i=1}^{l} \frac{1}{(1-T^{\lambda_i})}$.

Example: The cyclic group of order p. Let K be a field, let $G := \langle z\rangle \cong C_p$, where p is a prime, and let V be the regular $K[G]$-module, which with respect to the K-basis $\{1, z, \ldots, z^{p-1}\} \subseteq K[G]$ is given by $G \to \mathcal{S}_p\colon z \mapsto (1, \ldots, p)$. Hence $z^i \in G$ has cycle type $[p]$, for $i \in \{1, \ldots, p-1\}$, and $1 \in G$ has cycle type $[1^p]$; this yields $H_{S^G} = \frac{1}{p} \cdot (\frac{p-1}{1-T^p} + \frac{1}{(1-T)^p}) \in \mathbb{Q}(T)$.

Alternatively, more explicitly, for $f \in \mathcal{X}_d$, where $d \in \mathbb{N}_0$, we have $f^z = f$ if and only if all the indeterminates occur with the same multiplicity in f. Hence we have $\mathrm{Fix}_{\mathcal{X}_d}(z) = \emptyset$ whenever $p \nmid d$; thus in this case $\mathcal{X}_d$ consists of G-orbits of length p only, so that $\dim_K(S_d^G) = \frac{1}{p} \cdot \dim_K(S_d) = \binom{p+d-1}{d}$. If $p \mid d$, then $f^z = f$ if and only if $f = (\prod_{i=1}^p X_i)^{\frac{d}{p}}$; thus in this case we have $|\mathrm{Fix}_{\mathcal{X}_d}(z)| = 1$, the other G-orbits having length p, so that $\dim_K(S_d^G) = 1 + \frac{1}{p} \cdot (\dim_K(S_d) - 1) = 1 + \frac{1}{p} \cdot (\binom{p+d-1}{d} - 1)$; thus $H_{S^G} = \frac{p-1}{p} \cdot \sum_{d\geq 0} |\mathrm{Fix}_{\mathcal{X}_d}(z)| \cdot T^d + \frac{1}{p} \cdot \sum_{d \geq 0} |\mathcal{X}_d| \cdot T^d = \frac{p-1}{p} \cdot \sum_{d\geq 0} T^{pd} + \frac{1}{p} \cdot \sum_{d\geq 0} \binom{p+d-1}{d} \cdot T^d = \frac{1}{p} \cdot (\frac{p-1}{1-T^p} + \frac{1}{(1-T)^p})$.

(9.2) Symmetric groups. Let K be a field, and let $V := K^n$ be the natural permutation $K[\mathcal{S}_n]$-module, where $n \in \mathbb{N}_0$.

We determine the pseudoreflections in $\mathcal{S}_n$: For $g \in \mathcal{S}_n$ the K-dimension of its K-space of fixed points coincides with the number of cycles of g. Hence g is a pseudoreflection if and only if it has precisely $n-1$ cycles, in other words if and only if it is a transposition; note that the latter are reflections if and only if $\mathrm{char}(K) \neq 2$. In particular, there are $\binom{n}{2}$ pseudoreflections in $\mathcal{S}_n$, all of which do not belong to $\mathcal{A}_n$.

We have $\mathcal{S}_n = \langle s_1, \ldots, s_{n-1}\rangle$, where $s_i := (i, i+1) \in \mathcal{S}_n$, for $i \in \{1, \ldots, n-1\}$, are the **adjacent transpositions**. Hence $\mathcal{S}_n$ is generated by pseudoreflections, thus the invariant algebra $S[V]^{\mathcal{S}_n}$ is polynomial, whenever $\mathrm{char}(K) \nmid n!$, that is whenever $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) > n$. (Recall that we have only shown this explicitly for $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) > n!$.) Actually, it will turn out below that $K[\mathcal{X}]^{\mathcal{S}_n}$ is polynomial for any field K.

(9.3) Symmetric polynomials. a) Let K be a field, let $\mathcal{X} := \{X_1, \ldots, X_n\}$ where $n \in \mathbb{N}_0$, and let $\mathcal{S}_n$ act naturally on $K[\mathcal{X}]$. The elements of $K[\mathcal{X}]^{\mathcal{S}_n}$ are called **symmetric polynomials**. A distinguished set of symmetric polynomials is given as follows:

We consider the algebra $K[\mathcal{X}, Y]$, for an additional indeterminate Y. Then we have $\prod_{i=1}^n (Y - X_i) = \sum_{i=0}^n (-1)^i e_{n,i}(\mathcal{X}) Y^{n-i} \in K[\mathcal{X}, Y]$, with the **elementary symmetric polynomials** or **Vieta polynomials** $e_{n,i} = e_{n,i}(\mathcal{X}) := \sum_{J \subseteq \{1,\ldots,n\}, |J|=i} (\prod_{j\in J} X_j) \in K[\mathcal{X}]$, for $i \in \{0, \ldots, n\}$. The $e_{n,i}$ are homogeneous such that $\deg(e_{n,i}) = i$, where in particular we have $e_{n,0} = 1$, and $e_{n,1} = \sum_{i=1}^n X_i$, and $e_{n,n} = \prod_{i=1}^n X_i$. Since $\mathcal{S}_n$ permutes (transitively) the subsets of $\{1, \ldots, n\}$ of a fixed cardinality, we conclude that actually $e_{n,i} \in K[\mathcal{X}]^{\mathcal{S}_n}$.

b) We show that $K[\mathcal{X}]^{\mathcal{S}_n} = K[e_{n,1}, \ldots, e_{n,n}]$, implying that it is a polynomial algebra independently of $\mathrm{char}(K)$; for completeness we present an explicit proof of algebraic independence. Hence $\{e_{n,1}, \ldots, e_{n,n}\}$ are basic invariants, and the associated degrees are $[1, \ldots, n]$, entailing $H_{K[\mathcal{X}]^{\mathcal{S}_n}} = \prod_{i=1}^{n} \frac{1}{1-T^i} \in \mathbb{Q}(T)$:

To this end, we consider the auxiliary polynomial algebra $K[\mathcal{Y}]^{\delta}$, where $\mathcal{Y} := \{Y_1, \ldots, Y_n\}$, being equipped with the grading with degrees $\delta := [1, \ldots, n]$; hence we have $\deg_{\delta}(Y_i) = i = \deg(e_{n,i})$. Using this we have:

Theorem. Let $f \in K[\mathcal{X}]_d^{\mathcal{S}_n}$ be homogeneous, where $d \in \mathbb{N}_0$. Then there is a unique $g \in K[\mathcal{Y}]_d^{\delta}$ homogeneous such that $f = g(e_{n,1}, \ldots, e_{n,n}) \in K[\mathcal{X}]$.

Proof. i) In order to show existence, we proceed by induction on $n \in \mathbb{N}_0$; the cases $n \leq 1$ being trivial, let $n \geq 2$. We in turn proceed by induction on $d \in \mathbb{N}_0$; the case $d = 0$ being trivial, let $d \geq 1$. Let $\alpha_n \colon K[\mathcal{X}, Y] \to K[\mathcal{X}', Y]$, where $\mathcal{X}' := \mathcal{X} \setminus \{X_n\}$, be the K-algebra homomorphism given by $Y \mapsto Y$, and $X_i \mapsto X_i$ for $i \in \{1, \ldots, n-1\}$, and $X_n \mapsto 0$.

This yields $\sum_{i=0}^{n} (-1)^i \alpha_n(e_{n,i}) Y^{n-i} = \alpha_n(\sum_{i=0}^{n} (-1)^i e_{n,i} Y^{n-i}) = \alpha_n(\prod_{i=1}^{n} (Y - X_i)) = Y \cdot \prod_{i=1}^{n-1} (Y - X_i) = \sum_{i=0}^{n-1} (-1)^i e_{n-1,i}(\mathcal{X}') Y^{n-i} \in K[\mathcal{X}', Y]$, hence $\alpha_n(e_{n,i}) = e_{n-1,i}$, for $i \in \{0, \ldots, n-1\}$, and $\alpha_n(e_{n,n}) = 0 \cdot \prod_{i=1}^{n-1} X_i = 0$.

We have $\alpha_n(f) = f(X_1, \ldots, X_{n-1}, 0) \in K[\mathcal{X}']_d^{\mathcal{S}_{n-1}}$. By induction there is $g' \in K[\mathcal{Y}']_d^{\delta'}$, where $\mathcal{Y}' := \mathcal{Y} \setminus \{Y_n\}$ and $\delta' := [1, \ldots, n-1]$, such that $\alpha_n(f) = g'(e_{n-1,1}, \ldots, e_{n-1,n-1}) \in K[\mathcal{X}']$. Letting $g := g'(e_{n,1}, \ldots, e_{n,n-1}) \in K[\mathcal{X}]$, we recover $\alpha_n(g) = \alpha_n(g'(e_{n,1}, \ldots, e_{n,n-1})) = g'(e_{n-1,1}, \ldots, e_{n-1,n-1})$, and since the $e_{n,i}$ are homogeneous and $\deg(e_{n,i}) = i$, we conclude that $g \in K[\mathcal{X}]_d$.

Letting $f' := f - g \in K[\mathcal{X}]_d$, from $\alpha_n(f') = 0$ we conclude that $X_n \mid f'$. Since f' is $\mathcal{S}_n$-invariant, and $\mathcal{S}_n$ acts transitively on $\mathcal{X}$, where the $X_i \in K[\mathcal{X}]$ are pairwise non-associate primes, we infer that $e_{n,n} = \prod_{i=1}^{n} X_i \mid f'$, so that $f' = e_{n,n} \cdot f'' \in K[\mathcal{X}]$, for some $f'' \in K[\mathcal{X}]_{d-n}$. Since $K[\mathcal{X}]$ is a domain we conclude that f'' is $\mathcal{S}_n$-invariant as well, so that by induction there is $g'' \in K[\mathcal{Y}]_{d-n}^{\delta}$ such that $f'' = g''(e_{n,1}, \ldots, e_{n,n})$.

Hence in conclusion we have $f = g + e_{n,n} \cdot f'' = g'(e_{n,1}, \ldots, e_{n,n-1}) + e_{n,n} \cdot g''(e_{n,1}, \ldots, e_{n,n}) = (g' + Y_n \cdot g'')(e_{n,1}, \ldots, e_{n,n})$, where $g' + Y_n \cdot g'' \in K[\mathcal{Y}]_d^{\delta}$.

ii) Uniqueness amounts to showing that $\{e_{n,1}, \ldots, e_{n,n}\} \subseteq K[\mathcal{X}]$ is algebraically independent: We proceed by induction on $n \in \mathbb{N}_0$, the cases $n \leq 1$ being trivial, let $n \geq 2$. Assume to the contrary that there is $0 \neq f = \sum_{i \geq 0} f_i(\mathcal{Y}') Y_n^i \in K[\mathcal{Y}]^{\delta}$ homogeneous such that $d := \deg_{\delta}(f) \geq 1$ is minimal, and $f(e_{n,1}, \ldots, e_{n,n}) = 0$. Assume that $f_0 = 0$, then we have $f = Y_n \cdot f' \in K[\mathcal{Y}]$, where $0 \neq f' \in K[\mathcal{Y}]_{d-n}^{\delta}$ and $f'(e_{n,1}, \ldots, e_{n,n}) = 0$, a contradiction. Thus we have $0 \neq f_0 \in F[\mathcal{Y}']$.

From $f(e_{n,1}, \ldots, e_{n,n}) = \sum_{i \geq 0} f_i(e_{n,1}, \ldots, e_{n,n-1}) e_{n,n}^i = 0$, using α_n again, we get $0 = \alpha_n(f(e_{n,1}, \ldots, e_{n,n})) = \sum_{i \geq 0} \alpha_n(f_i(e_{n,1}, \ldots, e_{n,n-1})) \cdot \alpha_n(e_{n,n})^i = f_0(e_{n-1,1}, \ldots, e_{n-1,n-1})$, which by induction contradicts the algebraic independence of $\{e_{n-1,1}, \ldots, e_{n-1,n-1}\}$. $\sharp$

Note that the above proof is constructive, so that given $f \in K[\mathcal{X}]^{\mathcal{S}_n}$ the polynomial $g \in K[\mathcal{Y}]$ such that $f = g(e_{n,1}, \ldots, e_{n,n})$ can be computed algorithmically.

(9.4) Alternating polynomials. a) Let K be a field, let $\mathcal{X} := \{X_1, \ldots, X_n\}$ where $n \in \mathbb{N}_0$, and let $\mathcal{S}_n$ act naturally on $K[\mathcal{X}]$. Let $V_n := [X_j^{i-1}]_{ij} \in K[\mathcal{X}]^{n \times n}$ be the Vandermonde matrix associated with $\mathcal{X}$, and using the Vandermonde formula let $\Delta_n := \det(V_n) = \prod_{1 \le i < j \le n}(X_j - X_i) \in K[\mathcal{X}]$ be the **discriminant** polynomial. Hence Δ_n is homogeneous such that $\deg(\Delta_n) = \binom{n}{2}$, where $\Delta_0 = \Delta_1 = 1$; and for $n \ge 1$ we have $\Delta_n(X_1, \ldots, X_{n-1}, 0) = (-1)^{n-1} e_{n-1,n-1} \Delta_{n-1}$.

Letting $\mathcal{S}_n$ act entrywise on V_n, we observe that $s_j = (j, j+1) \in \mathcal{S}_n$, for $j \in \{1, \ldots, n-1\}$, interchanges columns j and $j+1$ of V_n. Hence we conclude that $\Delta_n \cdot s_j = -\Delta_n$, so that $\Delta_n \cdot g = \mathrm{sgn}(g) \cdot \Delta_n$ for $g \in \mathcal{S}_n$. Thus if $\mathrm{char}(K) \ne 2$ and $n \ge 2$, then we have $\Delta_n \in K[\mathcal{X}]^{\mathcal{A}_n} \setminus K[\mathcal{X}]^{\mathcal{S}_n}$; if $\mathrm{char}(K) = 2$ then we have $\Delta_n \in K[\mathcal{X}]^{\mathcal{S}_n}$. Moreover, we have $\Delta_n^2 \in K[\mathcal{X}]^{\mathcal{S}_n}$, so that Δ_n^2 can be expressed (uniquely) as a polynomial in $\{e_{n,1}, \ldots, e_{n,n}\}$.

Example. We have $\Delta_2 = X_2 - X_1$; thus $\Delta_2^2 = (X_2 - X_1)^2$ and $\Delta_2^2(X_1, 0) = X_1^2 = e_{1,1}^2$, hence letting $g := e_{2,1}^2 = (X_1 + X_2)^2$ we get $\Delta_2^2 - g = (X_2 - X_1)^2 - (X_1 + X_2)^2 = -4X_1X_2 = -4e_{2,2}$, entailing $\Delta_2^2 = e_{2,1}^2 - 4e_{2,2}$.

Moreover, $\Delta_3 = (X_2 - X_1)(X_3 - X_1)(X_3 - X_2) = (X_3^2X_2 + X_2^2X_1 + X_1^2X_3) - (X_3^2X_1 + X_2^2X_3 + X_1^2X_2)$ yields $\Delta_3^2 = (X_2 - X_1)^2(X_3 - X_1)^2(X_3 - X_2)^2$, where $\Delta_3^2 = -4e_{3,1}^3e_{3,3} + e_{3,1}^2e_{3,2}^2 + 18e_{3,1}e_{3,2}e_{3,3} - 4e_{3,2}^3 - 27e_{3,3}^2$.

Finally, $\Delta_4 = (X_2 - X_1)(X_3 - X_1)(X_4 - X_1)(X_3 - X_2)(X_4 - X_2)(X_4 - X_3)$ yields $\Delta_4^2 = -27e_{4,1}^4e_{4,4}^2 + 18e_{4,1}^3e_{4,2}e_{4,2}e_{4,4} - 4e_{4,1}^3e_{4,2}^3 - 4e_{4,1}^2e_{4,2}^3e_{4,4} + e_{4,1}^2e_{4,2}^2e_{4,2}^2 + 144e_{4,1}^2e_{4,2}e_{4,4}^2 - 6e_{4,1}^2e_{4,2}^2e_{4,4} - 80e_{4,1}e_{4,2}^2e_{4,2}e_{4,4} + 18e_{4,1}e_{4,2}e_{4,2}^3 + 16e_{4,2}^4e_{4,4} - 4e_{4,2}^3e_{4,2}^2 - 192e_{4,1}e_{4,2}e_{4,4}^2 - 128e_{4,2}^2e_{4,4}^2 + 144e_{4,2}e_{4,2}^2e_{4,4} - 27e_{4,2}^4 + 256e_{4,4}^3$.

b) We consider the alternating group $\mathcal{A}_n \trianglelefteq \mathcal{S}_n$, where we may assume $n \ge 2$: We have $K[e_{n,1}, \ldots, e_{n,n}] = K[\mathcal{X}]^{\mathcal{S}_n} = (K[\mathcal{X}]^{\mathcal{A}_n})^{\mathcal{S}_n/\mathcal{A}_n} = (K[\mathcal{X}]^{\mathcal{A}_n})^{\langle s \rangle} \subseteq K[\mathcal{X}]^{\mathcal{A}_n}$, where $s \in \mathcal{S}_n$ is any transposition; for example $s = s_{n-1} = (n-1, n)$.

i) Let $\mathrm{char}(K) \ne 2$. Since $s^2 = 1 \in G$, considering the eigenspaces of the action of s on $K[\mathcal{X}]^{\mathcal{A}_n}$, with respect to the eigenvalues 1 and -1, respectively, we get $K[\mathcal{X}]^{\mathcal{A}_n} = (K[\mathcal{X}]^{\mathcal{A}_n})^+ \oplus (K[\mathcal{X}]^{\mathcal{A}_n})^- = K[\mathcal{X}]^{\mathcal{S}_n} \oplus K[\mathcal{X}]^{\mathcal{S}_n}_{\mathrm{sgn}}$ as $K[\mathcal{X}]^{\mathcal{S}_n}$-modules, where the latter summand consists of the semi-invariant **alternating** elements $f \in K[\mathcal{X}]$, that is fulfilling $f^g = \mathrm{sgn}(g) \cdot f$ for all $g \in \mathcal{S}_n$; recall that the trivial and sign representations are the only one-dimensional representations of $\mathcal{S}_n$.

In particular, we have $\Delta_n \in K[\mathcal{X}]^{\mathcal{S}_n}_{\mathrm{sgn}}$, so that $\Delta_n \cdot K[\mathcal{X}]^{\mathcal{S}_n} \subseteq K[\mathcal{X}]^{\mathcal{S}_n}_{\mathrm{sgn}}$. Conversely, we show that $K[\mathcal{X}]^{\mathcal{S}_n}_{\mathrm{sgn}} \subseteq \Delta_n \cdot K[\mathcal{X}]^{\mathcal{S}_n}$:

For $f \in K[\mathcal{X}]^{\mathcal{S}_n}_{\mathrm{sgn}}$ we obtain $f(X_1, \ldots, X_n) = -f(X_1, \ldots, X_{n-1}, X_n)^{s_{n-1}} = -f(X_1, \ldots, X_{n-2}, X_n, X_{n-1})$, so that the K-algebra homomorphism $K[\mathcal{X}] \to K[X_1, \ldots, X_{n-1}]$ given by $X_i \mapsto X_i$ for $i \in \{1, \ldots, n-1\}$, and $X_n \mapsto X_{n-1}$, yields $f(X_1, \ldots, X_{n-1}, X_{n-1}) = -f(X_1, \ldots, X_{n-1}, X_{n-1}) = 0$. Hence we infer that $(X_n - X_{n-1}) \mid f \in K[\mathcal{X}]$. Since f is semi-invariant, and $\mathcal{S}_n$ acts transitively on the subsets of $\{1,\ldots,n\}$ of cardinality 2, where the $(X_j - X_i) \in K[\mathcal{X}]$ are pairwise non-associate primes, we conclude that $\Delta_n = \prod_{1\leq i<j\leq n}(X_j - X_i) \mid f \in K[\mathcal{X}]$. Writing $f = \Delta_n \cdot g$, for some $g \in K[\mathcal{X}]$, since $K[\mathcal{X}]$ is a domain we get $g \in K[\mathcal{X}]^{\mathcal{S}_n}$, showing that $f \in \Delta_n \cdot K[\mathcal{X}]^{\mathcal{S}_n}$. ♯

Hence we have $K[\mathcal{X}]^{\mathcal{A}_n} = K[\mathcal{X}]^{\mathcal{S}_n} \oplus \Delta_n \cdot K[\mathcal{X}]^{\mathcal{S}_n}$, with Hilbert series $H_{K[\mathcal{X}]^{\mathcal{A}_n}} = H_{K[\mathcal{X}]^{\mathcal{S}_n}} + H_{K[\mathcal{X}]^{\mathcal{S}_n}_{\mathrm{sgn}}} = (1+T^{\binom{n}{2}}) \cdot H_{K[\mathcal{X}]^{\mathcal{S}_n}} = (1+T^{\binom{n}{2}}) \cdot \prod_{i=1}^n \frac{1}{1-T^i} \in \mathbb{Q}(T)$.

ii) Let $\mathrm{char}(K) = 2$. We already know that $H_{K[\mathcal{X}]^{\mathcal{A}_n}} = (1+T^{\binom{n}{2}}) \cdot H_{K[\mathcal{X}]^{\mathcal{S}_n}} \in \mathbb{Q}(T)$, where $K[e_{n,1},\ldots,e_{n,n}] = K[\mathcal{X}]^{\mathcal{S}_n} \subseteq K[\mathcal{X}]^{\mathcal{A}_n}$ and $H_{K[\mathcal{X}]^{\mathcal{S}_n}} = \prod_{i=1}^n \frac{1}{1-T^i}$. Thus we are looking for an additional homogeneous $\mathcal{A}_n$-invariant of degree $\binom{n}{2}$:

Let $\Gamma_n := \prod_{1\leq i<j\leq n}(X_j + X_i) \in \mathbb{Q}[\mathcal{X}]^{\mathcal{S}_n}$, and let $\Delta'_n := \frac{1}{2}\cdot(\Delta_n + \Gamma_n) \in \mathbb{Q}[\mathcal{X}]^{\mathcal{A}_n}$ [Bertin, 1970]; then we have $\Delta'_n \cdot s = \frac{1}{2}\cdot(-\Delta_n + \Gamma_n) = \Delta'_n - \Delta_n \in \mathbb{Q}[\mathcal{X}]$. Now $\Delta_n + \Gamma_n$ has integral coefficients, where reduction modulo 2 shows that these are even, so that Δ'_n has integral coefficients as well.

Reduction modulo 2 yields a polynomial $\Delta'_n \in K[\mathcal{X}]^{\mathcal{A}_n}$ (with a slight abuse of notation), so that we have $\Delta'_n \cdot (s+1) = \Delta_n \in K[\mathcal{X}]$, while $\Delta_n \in K[\mathcal{X}]^{\mathcal{S}_n}$. Hence we have $(\Delta'_n \cdot f)^{s+1} = \Delta_n \cdot f$, for $f \in K[\mathcal{X}]^{\mathcal{S}_n}$, implying $(\Delta'_n \cdot K[\mathcal{X}]^{\mathcal{S}_n}) \cap K[\mathcal{X}]^{\mathcal{S}_n} = \{0\}$. This entails that $K[\mathcal{X}]^{\mathcal{S}_n} \oplus \Delta'_n \cdot K[\mathcal{X}]^{\mathcal{S}_n} \subseteq K[\mathcal{X}]^{\mathcal{A}_n}$, where the Hilbert series of the left and right hand sides coincide, so that we have $K[\mathcal{X}]^{\mathcal{A}_n} = K[\mathcal{X}]^{\mathcal{S}_n} \oplus \Delta'_n \cdot K[\mathcal{X}]^{\mathcal{S}_n}$ as $K[\mathcal{X}]^{\mathcal{S}_n}$-modules. ♯

For example, for $n = 2$ we get $\Delta'_2 = \frac{1}{2}\cdot((X_2 - X_1) + (X_2 + X_1)) = X_2$, so that $K[X_1, X_2]^{\mathcal{A}_2} = K[e_{2,1}, e_{2,2}, \Delta'_2] = K[X_1 + X_2, X_1X_2, X_2] = K[X_1, X_2]$. Moreover, for $n = 3$ we get $\Delta'_3 = (X_2X_3^2)^+ + e_{3,3}$, so that we have $K[\mathcal{X}]^{\mathcal{A}_3} = K[e_{3,1}, e_{3,2}, e_{3,3}, (X_2X_3^2)^+] = K[\mathcal{X}]^{\mathcal{S}_3} \oplus (X_2X_3^2)^+ \cdot K[\mathcal{X}]^{\mathcal{S}_3}$.

For $n = 4$ we get $\Delta'_4 = (X_2X_3^2X_4^3)^+ + (X_1X_2X_3X_4^3)^+ + (X_2^2X_3^2X_4^2)^+ + 2\cdot(X_1X_2X_3^2X_4^2)^+$, where the associated orbit lengths are $[12,4,4,6]$, respectively; since the lengths of the associated $\mathcal{S}_4$-orbits are $[24,4,4,6]$, respectively, we conclude that the latter three summands belong to $K[\mathcal{X}]^{\mathcal{S}_4}$, so that we have $K[\mathcal{X}]^{\mathcal{A}_4} = K[e_{4,1},\ldots,e_{4,4}, (X_2X_3^2X_4^3)^+] = K[\mathcal{X}]^{\mathcal{S}_4} \oplus (X_2X_3^2X_4^3)^+ \cdot K[\mathcal{X}]^{\mathcal{S}_4}$.

iii) Note that if $\mathrm{char}(K) \neq 2$ then we have $\Delta'_n \cdot (s-1) = -\Delta_n \in K[\mathcal{X}]$, hence $(\Delta'_n \cdot f)^{s-1} = -\Delta_n \cdot f$, for $f \in K[\mathcal{X}]^{\mathcal{S}_n}$, implying that $(\Delta'_n \cdot K[\mathcal{X}]^{\mathcal{S}_n}) \cap K[\mathcal{X}]^{\mathcal{S}_n} = \{0\}$ in this case as well. Thus, letting K be arbitrary again, in any case we have $K[\mathcal{X}]^{\mathcal{A}_n} = K[\mathcal{X}]^{\mathcal{S}_n} \oplus \Delta'_n \cdot K[\mathcal{X}]^{\mathcal{S}_n}$ as $K[\mathcal{X}]^{\mathcal{S}_n}$-modules.

We conclude that $K[\mathcal{X}]^{\mathcal{A}_n}$ is not a polynomial algebra, for $n \geq 3$: Assume to the contrary it is. We have $\binom{n}{2} > n$ for $n \geq 4$, and $\binom{3}{2} = 3$, so that $K[\mathcal{X}]^{\mathcal{A}_n}_d = K[\mathcal{X}]^{\mathcal{S}_n}_d$ for $d < n$, and for $d = n \geq 4$, while $K[\mathcal{X}]^{\mathcal{A}_3}_3 = K[\mathcal{X}]^{\mathcal{S}_3}_3 \oplus \langle\Delta'_3\rangle_K$. This entails that minimal generating set of $K[\mathcal{X}]^{\mathcal{A}_n}$ can be chosen to contain $\{e_{n,1},\ldots,e_{n.n}\}$, where polynomiality implies that the latter already is a generating set, a contradiction. (Alternatively, since $\mathcal{A}_n$ is not generated by pseudoreflections, in fact does not contain any, by Serre's Theorem $K[\mathcal{X}]^{\mathcal{A}_n}$ cannot possibly be a polynomial algebra, but we have not proven this.)

(9.5) Special partitions. We now turn to arbitrary permutation groups, for which we need a few preparations from the combinatorics of partitions first:

a) Let $\mathcal{P}_d$ be the set of **partitions** of $d \in \mathbb{N}_0$, that is the set of non-increasing sequences $\lambda = [\lambda_1, \lambda_2, \ldots]$, where $\lambda_i \in \mathbb{N}_0$ such that $\sum_{i \geq 1} \lambda_i = d$; then $l = l_\lambda := \max\{i \in \mathbb{N}; \lambda_i \geq 1\}$ is called the **length** of λ,

A partition $\lambda \in \mathcal{P}_d$, where $d \geq 1$, is called **special** or **column 2-regular**, if $\lambda_i - \lambda_{i+1} \leq 1$ for all $i \geq 1$; equivalently we have $\lambda_l = 1$ and $\lambda_i - \lambda_l \leq l - i$, for $i \in \{1, \ldots, l\}$. A special partition λ of length $l = l_\lambda \leq k$ is called k**-special**, for $k \in \mathbb{N}_0$. Then we have $d = \sum_{i=1}^{l} \lambda_i \leq \sum_{i=1}^{l}(l - i + 1) = \sum_{i=1}^{l} i = \binom{l+1}{2}$. Note that we have $l \leq d$ anyway, where for $d = l$ the partition $[1^l]$ is l-special, and for $d = \binom{l+1}{2}$ the **staircase** partition $[l, l-1, \ldots, 1]$ is l-special as well.

If $\lambda \in \mathcal{P}_d$, where $d \geq 1$, is not special, then $s = s_\lambda := \min\{i \in \mathbb{N}; \lambda_i - \lambda_{i+1} \geq 2\}$ is well-defined, and we have $s \in \{1, \ldots, l\}$. Using this, the partition $\overline{\lambda} := [\lambda_1 - 1, \ldots, \lambda_s - 1, \lambda_{s+1}, \ldots, \lambda_l] \in \mathcal{P}_{d-s}$, obtained from λ by decreasing each of its first s parts by 1, is called the **(s-)reduction** of λ; we write $\lambda \to \overline{\lambda}$. Note that λ and $\overline{\lambda}$ have the same length, and that λ can be recovered from $\overline{\lambda}$ together with s. Since $1 \leq \overline{\lambda}_s - \overline{\lambda}_{s+1} < \lambda_s - \lambda_{s+1}$, iterating reduction after finitely many steps ends up with a special partition; see also Table 4.

Let $\lambda \in \mathcal{P}_d$ and $\mu \in \mathcal{P}_e$. Then we have $\lambda \trianglelefteq \mu$ in the **dominance partial order**, if $\sum_{j=1}^{i} \lambda_j \leq \sum_{j=1}^{i} \mu_j$ for all $i \geq 1$; in particular we have $d \leq e$. Note that $\lambda \trianglelefteq \mu \trianglelefteq \lambda$ implies $\lambda = \mu$, so that this indeed defines an anti-symmetric, reflexive, and transitive relation on the set $\mathcal{P} := \coprod_{d \in \mathbb{N}_0} \mathcal{P}_d$ of all partitions, which is **well-founded**, that is it does not have infinite strictly descending chains.

b) We now consider combinations rather than partitions: Let $\alpha = [\alpha_1, \ldots, \alpha_n] \in \mathbb{N}_0^n$, and let $\sigma = \sigma_\alpha \in \mathcal{S}_n$ such that $\alpha^\sigma := [\alpha_{1\sigma^{-1}}, \ldots, \alpha_{n\sigma^{-1}}] \in \mathbb{N}_0^n$ is non-increasing, that is we have $\alpha_{1\sigma^{-1}} \geq \cdots \geq \alpha_{n\sigma^{-1}} \geq 0$; note that α^σ is independent of the ordering of the parts of α, but σ is uniquely defined if and only if α has pairwise distinct parts. We may consider α^σ as a partition of $d = d_\alpha := \sum_{i=1}^{n} \alpha_i$.

Then $\alpha \in \mathbb{N}_0^n$ is called **(k-)special** if $\alpha^\sigma \in \mathcal{P}_d$ is (k-)special; note that being (k-)special is independent of the ordering of the parts of α. If α^σ is not special, and has s-reduction $\overline{\alpha^\sigma} \in \mathcal{P}_{d-s}$, where $s = s_\alpha := s_{\alpha^\sigma}$, then $\overline{\alpha} := (\overline{\alpha^\sigma})^{\sigma^{-1}} \in \mathbb{N}_0^n$, is called the **($s$-)reduction** of α. Note that, since s-reduction affects precisely the s largest entries of α, so that $\overline{\alpha}$ has its s largest entries at the same positions, the reduction of α is well-defined independently of the choice of σ, and α can be recovered from $\overline{\alpha}$ together with s; moreover we have $\overline{\alpha}^g = \overline{\alpha^g}$ for all $g \in \mathcal{S}_n$.

Let $\alpha, \beta \in \mathbb{N}_0^n$. Then we have $\alpha \trianglelefteq \beta$ in the **dominance relation**, if for the associated partitions we have $\alpha^{\sigma_\alpha} \trianglelefteq \beta^{\sigma_\beta}$. The dominance relation again is reflexive and transitive, but neither anti-symmetric nor symmetric. Letting $\alpha \equiv \beta$ if $\alpha \trianglelefteq \beta \trianglelefteq \alpha$, that is $\alpha^{\sigma_\alpha} = \beta^{\sigma_\beta}$, or equivalently β is obtained from α by reordering its parts, we get an equivalence relation; hence the induced **dominance partial order** on the set of equivalence classes is well-founded as well. Note that the property of being (k-)special only depends on equivalence classes.

Table 4: Special partitions for $d \leq 7$.

d	l	special	non-special
1	1	$[1]$	$\leftarrow [n] \quad (n \geq 2)$
2	2	$[1^2]$	$\leftarrow [n^2] \quad (n \geq 2)$
3	2	$[2, 1]$	$\leftarrow [n, 1] \quad (n \geq 3)$
			$\leftarrow [n, n-1] \leftarrow [n+m, n-1] \quad (m \geq 1)$
3	3	$[1^3]$	$\leftarrow [n^3] \quad (n \geq 2)$
4	3	$[2, 1^2]$	$\leftarrow [n, 1^2] \quad (n \geq 3)$
			$\leftarrow [n, (n-1)^2] \leftarrow [n+m, (n-1)^2] \quad (m \geq 1)$
5	3	$[2^2, 1]$	$\leftarrow [n^2, 1] \quad (n \geq 3)$
			$\leftarrow [n^2, n-1] \leftarrow [(n+m)^2, n-1] \quad (m \geq 1)$
6	3	$[3, 2, 1]$	$\leftarrow [n, 2, 1] \quad (n \geq 4)$
			$\leftarrow [n, n-1, 1]$
			$\leftarrow [n, n-1, n-2]$
4	4	$[1^4]$	
5	4	$[2, 1^3]$	$\leftarrow [3, 1^3] \leftarrow [4, 1^3]$
6	4	$[2^2, 1^2]$	
7	4	$[2^3, 1]$	
7	4	$[3, 2, 1^2]$	
5	5	$[1^5]$	
6	5	$[2, 1^4]$	$\leftarrow [3, 1^4]$
7	5	$[2, 1^5]$	
7	5	$[2^2, 1^3]$	
6	6	$[1^6]$	
7	7	$[1^7]$	

(9.6) Permutation groups. Let K be a field, let $\mathcal{X} := \{X_1, \ldots, X_n\}$ where $n \in \mathbb{N}$, let $\mathcal{S}_n$ act naturally on $K[\mathcal{X}]$, and let $G \leq \mathcal{S}_n$ be a permutation group, with respect to which orbits sums on monomials are formed in the sequel. For $\alpha = [\alpha_1, \ldots, \alpha_n] \in \mathbb{N}_0^n$ let $\mathcal{X}^\alpha := \prod_{i=1}^n X_i^{\alpha_i} \in \mathcal{X}_{d_\alpha}$ be the associated monomial, where $d_\alpha := \sum_{i=1}^n \alpha_i \in \mathbb{N}_0$.

Lemma. Let $\alpha, \beta \in \mathbb{N}_0^n$, where $\alpha \neq 0$ is non-special, let $s = s_\alpha \in \{1, \ldots, n\}$.
a) Then the monomial $\mathcal{X}^\beta$ occurs in $(\mathcal{X}^{\overline{\alpha}})^+ \cdot e_{n,s} \in K[\mathcal{X}]$ only if $\beta \trianglelefteq \alpha$.
b) The monomial $\mathcal{X}^\beta$ belongs to the G-orbit of $\mathcal{X}^\alpha$, that is $\mathcal{X}^\beta$ occurs in $(\mathcal{X}^\alpha)^+ \in K[\mathcal{X}]$, if and only if $\beta \equiv \alpha$ and $\mathcal{X}^\beta$ occurs in $(\mathcal{X}^{\overline{\alpha}})^+ \cdot e_{n,s} \in K[\mathcal{X}]$; in this case $\mathcal{X}^\beta$ occurs precisely once in either sum.

Proof. a) Since $\mathcal{X}^\beta$ occurs in $(\mathcal{X}^{\overline{\alpha}})^+ \cdot \sum_{J \subseteq \{1,\ldots,n\}, |J|=s} (\prod_{j \in J} X_j)$, there is $\mathcal{J} = \{j_1, \ldots, j_s\} \subseteq \{1, \ldots, n\}$ of cardinality s, and $g \in G$ such that $\beta = \overline{\alpha}^g + \delta_{\mathcal{J}} \in \mathbb{N}_0^n$, where $\delta_{\mathcal{J}} \in \mathbb{N}_0^n$ is the associated indicator function. Letting $\sigma = \sigma_\alpha \in \mathcal{S}_n$ we get

$\beta^{g^{-1}\sigma} = \overline{\alpha^\sigma} + \delta_{\mathcal{J}^{\sigma^{-1}g}}$. Since the the truth of the assertion $\beta \trianglelefteq \alpha$ only depends on the equivalence classes α and β belong to, we may assume that both $\sigma = 1$ and $g = 1$, so that the parts of α are already sorted non-increasingly, and $\beta = [\beta_1, \ldots, \beta_n]$ is obtained from α by first decreasing the entries $\{1, \ldots, s\}$ by 1, and subsequently increasing the entries $\mathcal{J}$ by 1 again. Thus we have $\beta_i = \alpha_i - 1 + \delta_{i,\mathcal{J}}$ if $i \leq s$, and $\beta_j = \alpha_j + \delta_{j,\mathcal{J}}$ if $j \geq s+1$.

We derive a suitable sorting permutation $\tau = \sigma_\beta \in \mathcal{S}_n$: We have $\alpha_1 \geq \cdots \geq \alpha_s \geq \alpha_{s+1} \geq \cdots \geq \alpha_n$, where $\alpha_s \geq \alpha_{s+1} + 2$. For $i \leq s$ and $j \geq s+1$ we have $\alpha_i \geq \beta_i \geq \alpha_i - 1 \geq \alpha_s - 1 \geq \alpha_{s+1} + 1 \geq \alpha_j + 1 \geq \beta_j \geq \alpha_j$. Thus, whenever $k < l$ such that $\alpha_k > \alpha_l$, distinguishing the cases $l \leq s$, and $s+1 \leq k$, and $k \leq s < s+1 \leq l$, we conclude that $\beta_k \geq \beta_l$. Hence τ can be chosen such that α has constant entries on each τ-orbit, that is $\alpha^\tau = \alpha$, so that we may assume $\tau = 1$, in other words the parts of β are already sorted non-increasingly.

Hence for $i \leq s$ we have $\sum_{k=1}^i \beta_k \leq \sum_{k=1}^i \alpha_k$, where moreover $\sum_{k=1}^s \beta_k = \sum_{k=1}^s \beta_k = \sum_{k=1}^s (\alpha_k - 1) + |\{1, \ldots, s\} \cap \mathcal{J}|$. For $j \geq s+1$ we have $\sum_{k=s+1}^j \beta_k = \sum_{k=s+1}^j \alpha_k + |\{s+1, \ldots, j\} \cap \mathcal{J}|$, thus $\sum_{k=1}^j \beta_k = \sum_{k=1}^s (\alpha_k - 1) + |\{1, \ldots, s\} \cap \mathcal{J}| + \sum_{k=s+1}^j \alpha_k + |\{s+1, \ldots, j\} \cap \mathcal{J}| = (\sum_{k=1}^j \alpha_k) - s + |\{1, \ldots, j\} \cap \mathcal{J}| \leq \sum_{k=1}^j \alpha_k$.

b) If $\mathcal{X}^\beta$ belongs to the G-orbit of $\mathcal{X}^\alpha$, that is $\beta = \alpha^g$ for some $g \in G$, then β is obtained from α by reordering its parts, that is $\beta \equiv \alpha$. Moreover, we have $\overline{\beta} + \delta_{\mathcal{J}} = \beta = \alpha^g = (\overline{\alpha} + \delta_{\mathcal{I}})^g = \overline{\alpha}^g + \delta_{\mathcal{I}}^g = \overline{\alpha^g} + \delta_{\mathcal{I}^{g^{-1}}}$, where $\mathcal{I} \subseteq \{1, \ldots, n\}$ consists of the positions of the s largest entries of α, such that $\overline{\alpha}$ still has its s largest entries at the positions $\mathcal{I}$, and $\mathcal{J} \subseteq \{1, \ldots, n\}$ consists of the s largest entries of β, so that $\overline{\beta}$ still has its s largest entries at the positions $\mathcal{J}$. Hence we conclude that $\overline{\alpha}^g = \overline{\beta}$ and $\mathcal{I} = \mathcal{J}^g$, so that the monomial $\mathcal{X}^\beta$ occurs precisely once, and thus without any cancellation, in the expansion of $(\mathcal{X}^{\overline{\alpha}})^+ \cdot e_{n,s}$.

Conversely, if $\mathcal{X}^\beta$ occurs in $(\mathcal{X}^{\overline{\alpha}})^+ \cdot e_{n,s}$, then β is obtained from α by first decreasing the s largest entries $\mathcal{I}$ of α by 1, so that $\overline{\alpha}$ still has its s largest entries at the positions $\mathcal{I}$, subsequently permuting the entries by some $g \in G$, and finally increasing some s entries $\mathcal{J}$ by 1 again. If $\beta \equiv \alpha$, that is β is a reordering of α, and thus $\overline{\beta}$ is a reordering of $\overline{\alpha}$, then we conclude that $\mathcal{J}$ consists of the s largest entries of β, so that $\overline{\beta}$ still has its s largest entries at the positions $\mathcal{J}$. Thus we infer $\mathcal{J}^g = \mathcal{I}$, so that $\beta = \alpha^g$. ♯

Theorem: Göbel's degree bound [Göbel, 1995]**.** Then the set $\{e_{n,n}\} \,\dot\cup\, \{(\mathcal{X}^\alpha)^+; \alpha \in \mathbb{N}_0^n \text{ } (n-1)\text{-special}\}$ is a homogeneous K-algebra generating set of $K[\mathcal{X}]^G$, consisting of elements of degree at most $\max\{n, \binom{n}{2}\}$.

Proof. Let $R \subseteq K[\mathcal{X}]$ be the K-algebra generated by $\{e_{n,n}\} \,\dot\cup\, \{(\mathcal{X}^\alpha)^+; \alpha \in \mathbb{N}_0^n \text{ } (n-1)\text{-special}\}$; then we have $R \subseteq K[\mathcal{X}]^G$. To show the converse inclusion, let $0 \neq \alpha = [\alpha_1, \ldots, \alpha_n] \in \mathbb{N}_0^n$ be not $(n-1)$-special; we show that $(\mathcal{X}^\alpha)^+ \in R$ by induction on $d = d_\alpha = \sum_{i=1}^n \alpha_i$, and for fixed d on the dominance partial order on the set of equivalence classes on $\mathbb{N}_0^n$:

Let first $\alpha_i \geq 1$ for all $i \in \{1, \ldots, n\}$. This implies that $e_{n,n} = \prod_{i=1}^n X_i \mid \mathcal{X}^\alpha$, thus we have $(\mathcal{X}^\alpha)^+ = e_{n,n} \cdot (\mathcal{X}^\beta)^+ \in K[\mathcal{X}]^G$, where $\beta = [\alpha_1 - 1, \ldots, \alpha_n - 1]$. Since $d_\beta = d - n$ we by induction have $(\mathcal{X}^\beta)^+ \in R$, and since $e_{n,n} \in R$ anyway we infer that $(\mathcal{X}^\alpha)^+ \in R$ as well.

Hence let now α have at most $n-1$ non-zero parts. Since α is not $(n-1)$-special, it cannot be special at all. Thus let $s = s_\alpha \in \{1, \ldots, n-1\}$, and let $f := (\mathcal{X}^\alpha)^+ - (\mathcal{X}^{\overline{\alpha}})^+ \cdot e_{n,s} \in K[\mathcal{X}]^G$. Since G permutes the subsets of $\{1, \ldots, n\}$ of cardinality s, the summands of $e_{n,s} = \sum_{\mathcal{J} \subseteq \{1,\ldots,n\}, |\mathcal{J}|=s} \mathcal{X}^{\delta_\mathcal{J}}$ consist of a union of G-orbits, where since $s \leq n-1$ the indicator functions $\delta_\mathcal{J}$ occurring are $(n-1)$-special, thus we have $e_{n,s} \in R$. Since $d_{\overline{\alpha}} = d - s$ we by induction have $(\mathcal{X}^{\overline{\alpha}})^+ \in R$, so that $(\mathcal{X}^{\overline{\alpha}})^+ \cdot e_{n,s} \in R$ as well.

Finally, for all monomials $\mathcal{X}^\beta$ occurring in f, where $\beta \in \mathbb{N}_0^n$ (such that $d_\beta = d_\alpha$), by the above lemma we have $\beta \trianglelefteq \alpha$ and $\beta \not\equiv \alpha$, that is the equivalence class of β is strictly smaller than the equivalence class of α, with respect to the dominance partial order. Thus by induction we have $f \in R$. $\sharp$

Corollary. $\{(\mathcal{X}^\alpha)^+; \alpha \in \mathbb{N}_0^n\ (n-1)\text{-special}\}$ is a homogeneous generating set of $K[\mathcal{X}]^G$ as $K[\mathcal{X}]^{\mathcal{S}_n}$-module, consisting of elements of degree at most $\max\{n, \binom{n}{2}\}$.

Proof. Letting $R \subseteq K[\mathcal{X}]^G$ be the $K[\mathcal{X}]^{\mathcal{S}_n}$-module generated by $\{(\mathcal{X}^\alpha)^+; \alpha \in \mathbb{N}_0^n\ (n-1)\text{-special}\}$, recalling that $K[\mathcal{X}]^{\mathcal{S}_n} = K[e_{n,1}, \ldots, e_{n,n}]$, and noting that the reduction steps essentially consist of dividing off elementary symmetric polynomials, we may proceed entirely similarly to the above proof, $\sharp$

(9.7) Example: Symmetric and alternating polynomials. Let K be a field, let $\mathcal{X} := \{X_1, \ldots, X_n\}$ where $n \geq 2$, and let $\mathcal{S}_n$ act naturally on $K[\mathcal{X}]$. We apply Göbel's Theorem to the symmetric and alternating groups: The column partition $[1^k]$ and the staircase partition $\lambda_k := [k, k-1, \ldots, 1]$ are $(n-1)$-special, for $k \in \{1, \ldots, n-1\}$.

a) Let $G = \mathcal{S}_n$. Since $\mathcal{S}_n$ acts n-transitively, we only have to consider partitions rather than combinations. We get $(\mathcal{X}^{[1^k]})^+ = (\prod_{i=1}^k X_i)^+ = e_{n,k}$, thus Göbel's generating set encompasses the generating set $\{e_{n,1}, \ldots, e_{n,n}\}$ of $K[\mathcal{X}]^{\mathcal{S}_n}$; in particular, for $n \geq 4$ Göbel's degree bound is not sharp.

But we get additional (actually unnecessary) generators: For example, the staircase partition λ_k yields $\mathcal{X}^{\lambda_k} = \prod_{i=1}^k X_i^{k-i+1}$, having degree $\binom{k+1}{2}$. Since λ_k has pairwise distinct non-zero parts, we have $\mathrm{Stab}_{\mathcal{S}_n}(\mathcal{X}^{\lambda_k}) = \mathcal{S}_{\{k+1,\ldots,n\}} \cong \mathcal{S}_{n-k}$, and hence $(\mathcal{X}^{\lambda_k})^+ = \mathrm{Tr}_{\mathcal{S}_{\{k+1,\ldots,n\}}}^{\mathcal{S}_n}(\mathcal{X}^{\lambda_k})$ is the sum over an orbit of length $[\mathcal{S}_n : \mathcal{S}_{n-k}] = \frac{n!}{(n-k)!} = \prod_{i=0}^{k-1}(n-i)$; for example we recover $(\mathcal{X}^{\lambda_1})^+ = (\mathcal{X}^{[1]})^+ = e_{n,1}$, while $\mathcal{X}^{\lambda_{n-1}}$ gives rise to an $\mathcal{S}_n$-regular orbit.

b) Let $G = \mathcal{A}_n$. Then for any combination μ having multiple parts (including its zero parts) we infer that $\mathrm{Stab}_{\mathcal{S}_n}(\mathcal{X}^\mu)$ is not contained in $\mathcal{A}_n$, so that $[\mathrm{Stab}_{\mathcal{S}_n}(\mathcal{X}^\mu)\colon \mathrm{Stab}_{\mathcal{A}_n}(\mathcal{X}^\mu)] = 2$, and hence $(\mathcal{X}^\mu)^+ = \mathrm{Tr}^{\mathcal{A}_n}_{\mathrm{Stab}_{\mathcal{A}_n}(\mathcal{X}^\mu)}(\mathcal{X}^\mu) = \mathrm{Tr}^{\mathcal{S}_n}_{\mathrm{Stab}_{\mathcal{S}_n}(\mathcal{X}^\mu)}(\mathcal{X}^\mu)$, saying that actually $(\mathcal{X}^\mu)^+ \in K[\mathcal{X}]^{\mathcal{S}_n}$.

The only special partition with n pairwise distinct parts equals $\lambda := \lambda_{n-1} = [n-1, n-2, \ldots, 2, 1, 0]$, giving rise to monomials of degree $\binom{n}{2}$. Since $\mathcal{A}_n$ acts $(n-2)$-transitively, it suffices to consider the combinations λ and $\lambda' := [n-1, n-2, \ldots, 2, 0, 1]$; note that this also holds for $n = 2$. We have $\mathrm{Stab}_{\mathcal{S}_n}(\mathcal{X}^\lambda) = \mathrm{Stab}_{\mathcal{S}_n}(\mathcal{X}^{\lambda'}) = \{1\}$, so that $\mathcal{X}^\lambda$ and $\mathcal{X}^{\lambda'}$ give rise to $\mathcal{A}_n$-regular orbits, which are joined under $\mathcal{S}_n$-action, implying that $(\mathcal{X}^\lambda)^+ + (\mathcal{X}^{\lambda'})^+ \in K[\mathcal{X}]^{\mathcal{S}_n}$.

Hence, using $K[\mathcal{X}]^{\mathcal{S}_n} = K[e_{n,1}, \ldots, e_{n,n}]$, we get the K-algebra generating set $\{e_{n,1}, \ldots, e_{n,n}\} \,\dot\cup\, \{(\mathcal{X}^\lambda)^+\}$ of $K[\mathcal{X}]^{\mathcal{A}_n}$; in particular, Göbel's degree bound is sharp. Since $\mathrm{Stab}_{\mathcal{S}_n}((\mathcal{X}^\lambda)^+) = \mathcal{A}_n$ we infer that $K[\mathcal{X}]^{\mathcal{S}_n} \cap (\mathcal{X}^\lambda)^+ \cdot K[\mathcal{X}]^{\mathcal{S}_n} = \{0\}$, so that $K[\mathcal{X}]^{\mathcal{A}_n} = K[\mathcal{X}]^{\mathcal{S}_n} \oplus (\mathcal{X}^\lambda)^+ \cdot K[\mathcal{X}]^{\mathcal{S}_n}$ as $K[\mathcal{X}]^{\mathcal{S}_n}$-modules; see (9.4).

For example, for $n = 2$ we get $(\mathcal{X}^{[1]})^+ = X_1^+ = X_1$, and for $n = 3$ we get $(\mathcal{X}^{[2,1]})^+ = (X_1^2X_2)^+ = X_1^2X_2 + X_2^2X_3 + X_3^2X_1$.

(9.8) Example: Transitive groups of degree 4**.** Let K be a field, let $\mathcal{X} := \{X_1, \ldots, X_4\}$, and let $\mathcal{S}_4$ act naturally on $K[\mathcal{X}]$. The transitive subgroups of $G \leq \mathcal{S}_4$ are (up to conjugation) given as $\{C_4, V_4, D_8, \mathcal{A}_4, \mathcal{S}_4\}$, with inclusions $C_4 \leq D_8$ and $V_4 \leq D_8 \cap \mathcal{A}_4$. The 3-special partitions λ, which hence fulfill $d_\lambda \leq 6$, are given as $\{[1], [1^2], [1^3], [2,1], [2,1^2], [2^2,1], [3,2,1]\}$; see Table 4. The orbit lengths of the various groups G on monomials associated with the various 3-special combinations are given in Table 5, where since $\mathcal{S}_4$ acts 4-transitively, it suffices to consider partitions λ, rather than combinations, to provide the orbits of $\mathcal{S}_4$, and to describe how the latter split into G-orbits.

Molien's formula yields the associated Hilbert series, and explicit checking up to degree 6 (computing over $\mathbb{Z}$, and omitting the details) yields the following algebra generating sets, consisting of orbit sums associated with suitable 3-special combinations, as well as the R-module structure of the invariant algebras in question, where $R := K[\mathcal{X}]^{\mathcal{S}_4} = K[e_{4,1}, \ldots, e_{4,4}]$ and $H := H_{K[\mathcal{X}]^{\mathcal{S}_4}} = \prod_{i=1}^4 \frac{1}{1-T^i} \in \mathbb{Q}(T)$; note that Göbel's degree bound in general is not sharp:

i) We have $H_{K[\mathcal{X}]^{\mathcal{A}_4}} = (1 + T^6) \cdot H \in \mathbb{Q}(T)$, and by (9.7) we have $K[\mathcal{X}]^{\mathcal{A}_4} = R[(X_1^3X_2^2X_3)^+] = R \oplus (X_1^3X_2^2X_3)^+ \cdot R$.

ii) Let $D_8 := \langle (1,2)(3,4), (1,3) \rangle$. We have $H_{K[\mathcal{X}]^{D_8}} = (1 + T^2 + T^4) \cdot H$, and $K[\mathcal{X}]^{D_8} = R \oplus f \cdot R \oplus f^2 \cdot R$, where $f := (X_1X_3)^+ = X_1X_3 + X_2X_4$, and $\{e_{4,1}, \ldots, e_{4,4}, f\} \subseteq S^{D_8}$ is a minimal homogeneous K-algebra generating set.

iii) Let $V_4 := \langle (1,2)(3,4), (1,3)(2,4) \rangle$. We have $H_{K[\mathcal{X}]^{V_4}} = (1 + 2T^2 + 2T^4 + T^6) \cdot H$, and $K[\mathcal{X}]^{V_4} = \bigoplus_{p \in \mathcal{G}} pR$, where $\mathcal{G} = \{1, g, f, g^2, f^2, g^2f\}$, and $g := (X_1X_2)^+ = X_1X_2 + X_3X_4$, and $f := (X_1X_3)^+ = X_1X_3 + X_2X_4$. Moreover, if $\mathrm{char}(K) \neq 2$ then $\{e_{4,1}, e_{4,2}, e_{4,3}, f, g\}$ is a minimal homogeneous K-algebra generating set, while if $\mathrm{char}(K) = 2$ then we have to take $\{e_{4,1}, \ldots, e_{4,4}, f, g\}$.

iv) Let $C_4 := \langle (1,2,3,4) \rangle$. We have $H_{K[\mathcal{X}]^{C_4}} = (1 + T^2 + T^3 + 2T^4 + T^5) \cdot H$.

Table 5: Transitive groups of degree 4.

λ	d_λ	$\mathrm{Stab}_{\mathcal{S}_4}(\lambda)$	$\mathcal{S}_4$	$\mathcal{A}_4$	D_8	V_4	C_4
$[1]$	1	$\mathcal{S}_3$	4	4	4	4	4
$[1^2]$	2	C_2^2	6	6	$4,2$	$2,2,2$	$4,2$
$[1^3]$	3	$\mathcal{S}_3$	4	4	4	4	4
$[2,1]$	3	C_2	12	12	$8,4$	$4,4,4$	$4,4,4$
$[2,1^2]$	4	C_2	12	12	$8,4$	$4,4,4$	$4,4,4$
$[2^2,1]$	5	C_2	12	12	$8,4$	$4,4,4$	$4,4,4$
$[3,2,1]$	6	$\{1\}$	24	$12,12$	$8,8,8$	$4,4,4,4,4,4$	$4,4,4,4,4,4$
		orbits	7	8	13	20	19

Then for $\mathrm{char}(K) \neq 2$ we get $K[\mathcal{X}]^{C_4} = \bigoplus_{p\in\mathcal{G}} pR$, for $\mathcal{G} = \{1, f, g, f^2, h, fg\}$, and $f := (X_1X_3)^+ = X_1X_3 + X_2X_4$, and $g := (X_1^2X_2)^+ = X_1^2X_2 + X_2^2X_3 + X_3^2X_4 + X_4^2X_1$, and $h := (X_1^2X_2X_3)^+ = X_1^2X_2X_3 + X_2^2X_3X_4 + X_3^2X_4X_1 + X_4^2X_1X_2$. Finally, $\{e_{4,1}, \ldots, e_{4,4}, f, g, h\}$ is a minimal homogeneous K-algebra generating set; hence Noether's degree bound is sharp in this case.

If $\mathrm{char}(K) = 2$, we observe that $z := (X_1^2X_2^2X_3)^+ = X_1^2X_2^2X_3 + X_2^2X_3^2X_4 + X_3^2X_4^2X_1 + X_4^2X_1^2X_2$ is an indecomposable homogeneous invariant of degree 5, hence Noether's degree bound does not hold in this case. We get $K[\mathcal{X}]^{C_4} = \sum_{p\in\mathcal{G}} p \cdot R$, where $\mathcal{G} = \{1, f, g, f^2, h, z, fh\}$; actually, $K[\mathcal{X}]^{C_4}$ is not Cohen-Macaulay, see (17.5), so that $K[\mathcal{X}]^{C_4}$ is not a free graded R-module. Moreover, $\{e_{4,1}, \ldots, e_{4,4}, f, g, h, z\}$ is a minimal homogeneous K-algebra generating set.

10 Application: Galois groups

We indicate how invariant theory helps in the determination of Galois groups.

(10.1) Discriminants. Let K be a field, let $f := X^n + \sum_{i=1}^n a_{n-i}X^{n-i} \in K[X]$ be a monic polynomial of degree $n \in \mathbb{N}$, let $f = \prod_{i=1}^n (X - x_i) \in L[X]$, where $K \subseteq K(x_1, \ldots, x_n) = L$ is a splitting field of f, let $\mathcal{X} := \{X_1, \ldots, X_n\}$, and let $\mathcal{S}_n$ act naturally on $L[\mathcal{X}]$; hence $\mathcal{S}_n$ also acts on $L[\mathcal{X}, X]$ by fixing X.

Using the L-algebra homomorphism $\epsilon_f \colon L[\mathcal{X}, X] \to L[X]$ given by $X \mapsto X$, and $X_i \mapsto x_i$ for $i \in \{1, \ldots, n\}$, for the elementary symmetric polynomials $e_{n,i} \in K[\mathcal{X}]$ we get $\epsilon_f(e_{n,i}) = e_{n,i}(x_1, \ldots, x_n) = (-1)^i a_{n-i} \in K$, for $i \in \{1, \ldots, n\}$. Thus the elementary symmetric polynomials in the roots $\{x_1, \ldots, x_n\}$ of f can be expressed in the coefficients $\{a_0, \ldots, a_{n-1}\}$ of f alone, without knowing the roots, and actually are elements of K, which typically is considerably smaller than the splitting field L. In particular, since $\Delta_n^2 \in K[\mathcal{X}]^{\mathcal{S}_n}$, the **discriminant** of f given as $\Delta(f) := \epsilon_f(\Delta_n^2) = \Delta_n^2(x_1, \ldots, x_n) = \prod_{1\leq i<j\leq n}(x_j - x_i)^2 \in K$ can

be expressed in the coefficients of f alone; indeed we have $\Delta(f) = 0$ if and only if f has a multiple root.

Example. For $n = 2$ and writing $f = X^2 + pX + q = (X - x_1)(X - x_2) \in L[X]$, we get $e_{2,1}(x_1, x_2) = -p$ and $e_{2,2}(x_1, x_2) = q$, so that we recover the well-known discriminant $\Delta(f) = \Delta_2^2(x_1, x_2) = (e_{2,1}^2 - 4e_{2,2})(x_1, x_2) = p^2 - 4q$.

For $n = 3$, if $\mathrm{char}(K) \neq 3$, writing $f = X^3 + cX^2 + aX + b \in K[X]$ and applying the K-algebra automorphism of $K[X]$ given by $X \mapsto X - \frac{c}{3}$, we get $f \mapsto (X - \frac{c}{3})^3 + c(X - \frac{c}{3})^2 + a(X - \frac{c}{3}) + b = X^3 + (-\frac{c^2}{3} + a) \cdot X + (\frac{2c^3}{27} - \frac{ac}{3} + b)$. Thus we may assume that $f = X^3 + aX + b = (X - x_1)(X - x_2)(X - x_3) \in L[X]$ is in **Weierstraß form**; in other words we may assume that $x_1 + x_2 + x_3 = e_{3,1}(x_1, x_2, x_3) = 0$. Hence we get $e_{3,2}(x_1, x_2, x_3) = a$ and $e_{3,3}(x_1, x_2, x_3) = -b$, so that we recover the well-known discriminant $\Delta(f) = \Delta_3^2(x_1, x_2, x_3) = (-4e_{3,2}^3 - 27e_{3,3}^2)(x_1, x_2, x_3) = -4a^3 - 27b^2$.

(10.2) Galois groups. Let K be a field, let $f \in K[X]$ be monic and separable of degree $n \in \mathbb{N}$, that is f has n pairwise distinct roots $\{x_1, \ldots, x_n\}$ in a splitting field $K \subseteq L$, or equivalently $\Delta(f) \in K^*$, or equivalently $\gcd(f, \frac{\partial f}{\partial X}) \in K^*$. Then letting $A := \mathrm{Aut}_K(L)$, by **Artin's Theorem** the field extension $K \subseteq L$ is finite Galois, that is $L^A = K$.

Moreover, let $\mathcal{X} := \{X_1, \ldots, X_n\}$, and let $\mathcal{S}_n$ act naturally on $L[\mathcal{X}]$. Since A acts faithfully on the roots of f, the group A can be identified with a subgroup of $\mathcal{S}_n$, such that $\epsilon_f \colon \mathcal{X} \to \{x_1, \ldots, x_n\}$ is an A-isomorphism; note that $A \leq \mathcal{S}_n$ is transitive if and only if f is irreducible, and that $A \leq \mathcal{S}_n$ is only unique up to $\mathcal{S}_n$-conjugation. In particular, if $F \in K[\mathcal{X}]^A$, then we have $(\epsilon_f(F))^a = \epsilon_f(F^a) = \epsilon_f(F) \in L$, for all $a \in A$, so that actually $\epsilon_f(F) \in L^A = K$.

Let $H \leq G \leq \mathcal{S}_n$, then for $F \in K[\mathcal{X}]^H$ let the associated **(relative) resolvent** polynomial be given as the **relative norm** $\rho_H^G(F) := N_H^G(X - F) = \prod_{g \in H\backslash G}(X - F)^g = \prod_{g \in H\backslash G}(X - F^g) \in K[\mathcal{X}, X]^G = K[\mathcal{X}]^G[X]$, where g runs through a set of representatives for the right cosets of H in G; hence as a polynomial in X the resolvent $\rho_H^G(F)$ is monic of degree $[G \colon H]$.

Proposition: [Stauduhar, 1973]**.** Assume that $A \leq G$, and that the **resolvent** $\rho := \epsilon_f(\rho_H^G(F)) = \prod_{g \in H\backslash G}(X - F^g(x_1, \ldots, x_n)) \in K[X]$ is separable. Then we have $F^g(x_1, \ldots, x_n) \in K$ if and only if $A \leq H^g$. In particular, A is G-conjugate to a subgroup of H if and only if ρ has a root in K.

Proof. Since ρ is separable, its roots $F^g(x_1, \ldots, x_n) \in L$, where $g \in H\backslash G$, are pairwise distinct. Moreover, comparing the action of $a \in A$ on $\{x_1, \ldots, x_n\}$ and on $\mathcal{X}$ we get $F(x_1, \ldots, x_n)^a = F(x_1^a, \ldots, x_n^a) = F(x_{1a}, \ldots, x_{na})$, which equals $F(X_{1a^{-1}}, \ldots, X_{na^{-1}})(x_1, \ldots, x_n) = F^a(X_1, \ldots, X_n)(x_1, \ldots, x_n)$, which in turn equals $F^a(x_1, \ldots, x_n)$; hence we have $F(x_1, \ldots, x_n)^a = F^a(x_1, \ldots, x_n) \in L$. Thus for $g \in G$ we get $F^g(x_1, \ldots, x_n)^a = F^{ga}(x_1, \ldots, x_n) = F^{g^a \cdot g}(x_1, \ldots, x_n)$.

Hence, if ${}^gA \leq H$, then we have $F^g(x_1,\ldots,x_n)^a = F^g(x_1,\ldots,x_n)$ for all $a \in A$, thus $F^g(x_1,\ldots,x_n) \in L^A = K$. Conversely, if $F^g(x_1,\ldots,x_n) \in K$, then for all $a \in A$ we have $F^g(x_1,\ldots,x_n) = F^{{}^g a \cdot g}(x_1,\ldots,x_n)$, thus ${}^g a \in H$. ♯

Corollary. Let $\mathrm{char}(K) \neq 2$ and $n \geq 2$. Then we have $A \leq \mathcal{A}_n$ if and only if the discriminant $\Delta(f) \in K^*$ has a square root in K.

Proof. Since $\Delta_n \cdot g = \mathrm{sgn}(g) \cdot \Delta_n$ for all $g \in \mathcal{S}_n$, we have $\Delta_n \in K[\mathcal{X}]^{\mathcal{A}_n}$, and we get $\rho_{\mathcal{A}_n}^{\mathcal{S}_n}(\Delta_n) = (X - \Delta_n)(X + \Delta_n) = X^2 - \Delta_n^2 \in K[\mathcal{X}]^{\mathcal{S}_n}[X]$, so that $\epsilon_f(\rho_H^G(\Delta_n)) = X^2 - \Delta(f) \in K[X]$, which is separable. Hence the assertion follows. Note that since $\mathcal{A}_n \trianglelefteq \mathcal{S}_n$ is normal we have or have not $A \leq \mathcal{A}_n$ independently of the chosen identification. ♯

A few comments are in order: If $F^g(x_1,\ldots,x_n) \in K$, where $g \in G$, then ${}^gA \leq H$ says that reordering the roots along $[x_1,\ldots,x_n]^{g^{-1}}$ yields an identification of $\mathrm{Aut}_K(L)$ with a subgroup of H, instead of a G-conjugate of H.

Note that for $g \in \mathrm{Stab}_G(F)$ we have $\epsilon_f(F^g) = \epsilon_f(F)$ anyway, so that the separability condition implies that necessarily $\mathrm{Stab}_G(F) = H$. Homogeneous polynomials F having the latter property always exist: Letting $f := \prod_{i=1}^{n-1} X_i^{n-i} \in \mathcal{X}_d$ of degree $d = \binom{n}{2}$, which is associated with the $(n-1)$-special partition $[n-1, n-2, \ldots, 1]$, then we have $\mathrm{Stab}_{\mathcal{S}_n}(f) = \{1\}$, entailing that $F := f^+ = \mathrm{Tr}^H(f) = \sum_{g \in H} f^g \in K[\mathcal{X}]$, belonging to a regular H-orbit, fulfills $\mathrm{Stab}_{\mathcal{S}_n}(F) = H$ (although this choice might not be computationally efficient).

Still, this property does not imply that the separability condition is fulfilled, but this can always be remedied by applying **Tschirnhausen transformations** to the roots of f; recall that the Galois group looked for depends only on L, but not on a specific choice of a polynomial having L as a splitting field.

(10.3) Example: Galois groups in degree 3. Let $f \in \mathbb{Q}[X]$ be monic, separable, and have integral coefficients. Then the roots of f are algebraic integers, and if the check polynomial F has integral coefficients as well, then the roots of the associated resolvent are algebraic integers, too. Thus in this case, since $\mathbb{Z}$ is integrally closed, Stauduhar's criterion amounts to looking for integral roots. If additionally f is irreducible, then $A = \mathrm{Aut}(L)$, where L is a splitting field of f, acts transitively on the roots of f.

Let now f have degree 3. Then f is irreducible if and only if it has no root in $\mathbb{Q}$, or equivalently if it has no root in $\mathbb{Z}$, where any root in $\mathbb{Z}$ divides $f(0)$. In this case A can be identified with a transitive subgroup of $\mathcal{S}_3$, which are $\{\mathcal{A}_3, \mathcal{S}_3\}$. Hence A is determined by a consideration of $\Delta(f)$ alone.

i) Let $f := X^3 + X^2 - 2X - 1$: since $f(\pm 1) = \mp 1$ we infer that f is irreducible. From $e_{3,1} = -1$, and $e_{3,2} = -2$, and $e_{3,3} = 1$ we get $\Delta(f) = 7^2$, thus $G = \mathcal{A}_3$.

ii) Let $f := X^3 + 2$; since f has no root in $\mathbb{Q}$, we conclude that f is irreducible. From $e_{3,1} = 0$, and $e_{3,2} = 0$, and $e_{3,3} = -2$ we get $\Delta(f) = -2^2 \cdot 3^3$, thus $G = \mathcal{S}_3$.

Actually, we may also argue as follows: The polynomial f has a unique root in $\mathbb{R}$, so that it additionally has a pair of complex conjugate roots; thus complex conjugation induces an involutory automorphism of L, so that we have $G = \mathcal{S}_3$.

(10.4) Example: Galois groups in degree 4**.** Let $f \in \mathbb{Q}[X]$ be monic, irreducible, have integral coefficients, and have degree 4. Hence $A = \mathrm{Aut}(L)$, where L is a splitting field of f, can be identified with a transitive subgroup of $\mathcal{S}_4$, which are $\{C_4, V_4, D_8, \mathcal{A}_4, \mathcal{S}_4\}$, with inclusions $C_4 \leq D_8$ and $V_4 \leq D_8 \cap \mathcal{A}_4$. We have the following check polynomials; see (9.8):

i) For $G = D_8$ let $F_D := (X_1X_3)^+ = X_1X_3 + X_2X_4$; then we have $\mathrm{Stab}_{\mathcal{S}_4}(F_D) = D_8$, and its $\mathcal{S}_4$-orbit is $\{F_D, F_D', F_D''\}$, where $F_D' = F_D^{(1,4)} = X_1X_2 + X_3X_4$ and $F_D'' = F_D^{(1,2)} = X_1X_4 + X_2X_3$. Hence we have $\rho_G^{\mathcal{S}_4}(F_D) \in K[\mathcal{X}]^{\mathcal{S}_4}[X]$, where $e_{3,1}(F_D, F_D', F_D'') = e_{4,1}$, and $e_{3,2}(F_D, F_D', F_D'') = e_{4,1}e_{4,3} - 4e_{4,4}$, and $e_{3,3}(F_D, F_D', F_D'') = e_{4,1}^2 e_{4,4} - 4e_{4,2}e_{4,4} + e_{4,3}^2$.

ii) For $G = V_4$ let $F_V := (X_1X_2)^+ = X_1X_2 + X_3X_4 = F_D'$; then we have $\mathrm{Stab}_{\mathcal{A}_4}(F_V) = \mathrm{Stab}_{D_8}(F_V) = V_4$, and its $\mathcal{A}_4$-orbit is $\{F_V, F_V', F_V''\}$, where $F_V' = F_V^{(1,2,3)} = F_D''$ and $F_V'' = F_V^{(1,3,2)} = F_D$. Hence we have $\rho_G^{\mathcal{A}_4}(F_V) = \rho_{D_8}^{\mathcal{S}_4}(F_D)$, and $e_{3,i}(F_V, F_V', F_V'') = e_{3,i}(F_D, F_D', F_D'')$, for $i \in \{1, \ldots, 3\}$.

iii) For $G = C_4$ let $F_C = (X_1^2X_2)^+ = X_1^2X_2 + X_2^2X_3 + X_3^2X_4 + X_4^2X_1$; then we have $\mathrm{Stab}_{D_8}(F_C) = C_4$, and its D_8-orbit is $\{F_C, F_C'\}$, where $F_C' = F_C^{(1,3)} = X_1^2X_4 + X_2^2X_1 + X_3^2X_2 + X_4^2X_3$.

Moreover, let $\widetilde{F}_C := (X_1^2X_2X_3)^+ = X_1^2X_2X_3 + X_2^2X_3X_4 + X_3^2X_4X_1 + X_4^2X_1X_2$; then we have $\mathrm{Stab}_{D_8}(\widetilde{F}_C) = C_4$, and its D_8-orbit is $\{\widetilde{F}_C, \widetilde{F}_C'\}$, where $\widetilde{F}_C' = \widetilde{F}_C^{(1,3)} = X_3^2X_2X_1 + X_2^2X_1X_4 + X_1^2X_4X_3 + X_4^2X_3X_2$. ♯

Here are a few examples, see Table 6: For the various polynomials f we record the discriminant $\Delta(f) = \epsilon_f(\Delta_4^2) \in \mathbb{Z}$, and the factorization of the resolvent $\rho(f) := \epsilon_f(\rho_{D_8}^{\mathcal{S}_4}(F_D)) = \epsilon_f(\rho_{V_4}^{\mathcal{A}_4}(F_V)) \in \mathbb{Q}[X]$.

i) Let $f := X^4 + X + 1$; then reduction modulo 2 shows that f is irreducible. From $\Delta(f)$ and $\rho(f)$ we conclude that $A \not\leq \mathcal{A}_4$ and $A \not\leq D_8$, hence $A = \mathcal{S}_4$.

ii) Let $f := X^4 + 8X + 12$; then reduction modulo 5 shows that f does not split into quadratic factors, since f has no root in $\mathbb{Q}$ implying that f is irreducible. From $\Delta(f)$ and $\rho(f)$ we conclude that $A \leq \mathcal{A}_4$, but $A \not\leq V_4$, hence $A = \mathcal{A}_4$.

iii) Let $f := X^4 + 1$; then we have $f(X-1) = X^4 - 4X^3 + 6X^2 - 4X + 2$, hence by the Eisenstein criterion f is irreducible. From $\Delta(f)$ and $\rho(f)$ we conclude that $A \leq \mathcal{A}_4$ and $A \leq V_4$, hence $A = V_4$. Note that since $V_4 \trianglelefteq \mathcal{A}_4$ is normal the resultant it necessarily splits.

Actually, f is the 8-th cyclotomic polynomial, which is well-known to be irreducible, having splitting field $L = \mathbb{Q}(\zeta_8)$ of degree 4, where $A \cong \mathbb{Z}_8^* \cong V_4$, being generated by $\zeta_8 \mapsto -\zeta_8$ and $\zeta_8 \mapsto \zeta_8^{-1}$.

iv) Let $f := X^4 - 2$; then by the Eisenstein criterion f is irreducible. From

Table 6: Galois groups in degree 4.

f	$\Delta(f)$	$\rho(f)$	A
X^4+X+1	229	X^3-4X-1	$\mathcal{S}_4$
$X^4+8X+12$	$2^{12}\cdot 3^4$	$X^3-48X-64$	$\mathcal{A}_4$
X^4+1	2^8	$X(X+2)(X-2)$	V_4
X^4-2	-2^{11}	$X(X^2+8)$	D_8, C_4
$X^4+X^3+X^2+X+1$	5^3	$(X-1)(X^2+X-1)$	D_8, C_4

$\Delta(f)$ and $\rho(f)$ we conclude that $A \not\leq \mathcal{A}_4$, but A is a subgroup of precisely one of $\{D_8, D_8^{(1,4)}, D_8^{(1,2)}\}$; we have to determine which one, and whether $A \sim C_4$:

The roots of f are $x_i := \zeta_4^i \cdot \sqrt[4]{2} \in \mathbb{C}$, for $i \in \{1,\ldots,4\}$. This yields $\epsilon_f(F_D) = 0$, while $\epsilon_f(F'_D) = -2\zeta_4 \cdot \sqrt{2}$, and $\epsilon_f(F''_D) = 2\zeta_4 \cdot \sqrt{2}$, entailing $A \leq D_8$. Moreover, we get $\epsilon_f(\widetilde{F}_C) = -8\zeta_4$ and $\epsilon_f(\widetilde{F}'_C) = 8\zeta_4$, thus the resultant $(X+8\zeta_4)(X-8\zeta_4) = X^2+64$ is irreducible over $\mathbb{Q}$. Hence we have $A \not\leq C_4$, entailing $A = D_8$. (We get $\epsilon_f(F_C) = 0$ and $\epsilon_f(F'_C) = 0$, which does not help.)

v) Let $f := X^4+X^3+X^2+X+1$; then reduction modulo 2 shows that f is irreducible. From $\Delta(f)$ and $\rho(f)$ we conclude that $A \not\leq \mathcal{A}_4$, but A is a subgroup of precisely one of $\{D_8, D_8^{(1,4)}, D_8^{(1,2)}\}$; we have to determine which one, and whether $A \sim C_4$:

The roots of f are $x_i := \zeta_5^i \in \mathbb{C}$, for $i \in \{1,\ldots,4\}$. This yields $\epsilon_f(F_D) = \zeta_5 + \zeta_5^4$, while $\epsilon_f(F'_D) = \zeta_5^2 + \zeta_5^3$, and $\epsilon_f(F''_D) = 2$. Hence we have $A \leq D_8^{(1,2)}$, and letting $[x_1,\ldots,x_4] = [\zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4]^{(1,2)\cdot(1,2)(3,4)} = [\zeta_5, \zeta_5^2, \zeta_5^4, \zeta_5^3]$ we get $A \leq D_8$.

Moreover, we get $\epsilon_f(F_C) = -1$ and $\epsilon_f(F'_C) = 4$, thus the resultant $(X+1)(X-4)$ is separable, and has a root in $\mathbb{Q}$; since $C_4 \trianglelefteq D_8$ is normal it necessarily splits. Thus we have $A \leq C_4$, entailing $A = C_4$. (We get $\epsilon_f(\widetilde{F}_C) = -1$ and $\epsilon_f(\widetilde{F}'_C) = -1$, which does not help.)

Actually, f is the 5-th cyclotomic polynomial, which is well-known to be irreducible, having splitting field $L = \mathbb{Q}(\zeta_5)$ of degree 4, where $A \cong \mathbb{Z}_5^* \cong C_4$, being generated by $\zeta_5 \mapsto \zeta_5^2$, which is reflected by the adjusted ordering of the roots.

11 Application: Self-dual codes

We indicate how invariant theory helps in coding theory.

(11.1) Weight enumerators. a) Let $\mathbb{F}_q$ be the finite field with q elements, and let $n \in \mathbb{N}$. Letting $v = [x_1,\ldots,x_n] \in \mathbb{F}_q^n$ and $w = [y_1,\ldots,y_n] \in \mathbb{F}_q^n$, then $d(v,w) := |\{i \in \{1,\ldots,n\}; x_i \neq y_i\}| \in \{0,\ldots,n\}$ is called their **Hamming distance**. This defines a discrete **metric** on $\mathbb{F}_q^n$, that is we have **positive definiteness** and **symmetry**, and the **triangle inequality** holds.

Let $0_n := [0, \ldots, 0] \in \mathbb{F}_q^n$, for $v = [x_1, \ldots, x_n] \in \mathbb{F}_q^n$ let $\mathrm{wt}(v) := d(v, 0_n) \in \{0, \ldots, n\}$ be the **Hamming weight** of v, let $\mathrm{supp}(v) := \{i \in \{1, \ldots, n\}; x_i \neq 0\}$ be the **support** of v; hence we have $\mathrm{wt}(v) = |\mathrm{supp}(v)|$. Moreover, we have **translation invariance** $d(v+u, w+u) = d(v, w)$, for all $u, v, w \in \mathbb{F}_q^n$, thus we have $d(v, w) = d(v-w, 0_n) = \mathrm{wt}(v-w)$.

b) An $\mathbb{F}_q$-subspace $\mathcal{C} \leq \mathbb{F}_q^n$ is called a **linear code** of **length** n over $\mathbb{F}_q$; if $q = 2$ or $q = 3$ then $\mathcal{C}$ is called **binary** and **ternary**, respectively. Let $k := \dim_{\mathbb{F}_q}(\mathcal{C}) \in \{0, \ldots, n\}$ be the **dimension** of $\mathcal{C}$; if $k = 0$ then $\mathcal{C}$ is called **trivial**.

If $\mathcal{C}$ is non-trivial then $d(\mathcal{C}) := \min\{d(v, w) \in \mathbb{N}; v \neq w \in \mathcal{C}\} \in \{1, \ldots, n\}$ is called the **minimum distance** of $\mathcal{C}$, and $\mathrm{wt}(\mathcal{C}) := \min\{\mathrm{wt}(v) \in \mathbb{N}; 0_n \neq v \in \mathcal{C}\} \in \{1, \ldots, n\}$ is called the **minimum weight** of $\mathcal{C}$; if $\mathcal{C}$ is trivial we let $d(\mathcal{C}) := \infty$ and $\mathrm{wt}(\mathcal{C}) := \infty$. Then due to translation invariance we have $d := d(\mathcal{C}) = \mathrm{wt}(\mathcal{C})$, and $\mathcal{C}$ is called an $[n, k, d]$**-code** over $\mathbb{F}_q$.

c) For $i \in \mathbb{N}_0$ let $w_i = w_i(\mathcal{C}) := |\{v \in \mathcal{C}; \mathrm{wt}(v) = i\}| \in \mathbb{N}_0$. Hence we have $w_0 \leq 1$, and $w_i = 0$ for $i \in \{1, \ldots, \mathrm{wt}(\mathcal{C}) - 1\}$, and $w_{\mathrm{wt}(\mathcal{C})} \geq 1$, and $w_i = 0$ for $i \geq n+1$, and $\sum_{i=0}^n w_i = |\mathcal{C}| = q^d$. We consider the sequence $[w_0, w_1, \ldots, w_n]$:

Let $\{X, Y\}$ be indeterminates. Then the associated **homogeneous generating function** is given as $W_{\mathcal{C}} := \sum_{i=0}^n w_i X^i Y^{n-i} = \sum_{v \in \mathcal{C}} X^{\mathrm{wt}(v)} Y^{n-\mathrm{wt}(v)} \in \mathbb{Z}[X, Y]$, being called the **(Hamming) weight enumerator** of $\mathcal{C}$. Hence $W_{\mathcal{C}}$ is homogeneous of degree n and has non-negative coefficients. By **dehomogenizing**, that is specializing $X \mapsto X$ and $Y \mapsto 1$, we obtain the **(ordinary) generating function** $W_{\mathcal{C}}(X, 1) = \sum_{i=0}^n w_i X^i = \sum_{v \in \mathcal{C}} X^{\mathrm{wt}(v)} \in \mathbb{Z}[X]$.

For example, for the trivial code $\mathcal{C} := \{0_n\} \leq \mathbb{F}_q^n$ we get $W_{\mathcal{C}} = Y^n$; and for the code $\mathcal{C} := \mathbb{F}_q^n$ by elementary counting we get $w_i = \binom{n}{i}(q-1)^i \in \mathbb{N}_0$, thus $W_{\mathcal{C}} = \sum_{i=0}^n \binom{n}{i}(q-1)^i X^i Y^{n-i} = (Y + (q-1)X)^n$.

(11.2) Duality. Let $\mathbb{F}_q$ be the finite field with q elements, and let $n \in \mathbb{N}$. Let $\langle \cdot, \cdot \rangle \colon \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q \colon [[x_1, \ldots, x_n], [y_1, \ldots, y_n]] \mapsto x \cdot y^{\mathrm{tr}} = \sum_{i=1}^n x_i y_i$ be the **standard** $\mathbb{F}_q$**-bilinear form** on $\mathbb{F}_q^n$; it is symmetric and non-degenerate.

For a code $\mathcal{C} \leq \mathbb{F}_q^n$, the orthogonal space $\mathcal{C}^\perp := \{v \in \mathbb{F}_q^n; \langle v, w \rangle = 0 \in \mathbb{F}_q \text{ for all } w \in \mathcal{C}\} \leq \mathbb{F}_q^n$ with respect to the standard $\mathbb{F}_q$-bilinear form is called the associated **dual code**. Letting $k := \dim_{\mathbb{F}_q}(\mathcal{C}) \in \{0, \ldots, n\}$, we have $\dim_{\mathbb{F}_q}(\mathcal{C}^\perp) = n - k$, and we have $(\mathcal{C}^\perp)^\perp = \mathcal{C}$. If $\mathcal{C} \leq \mathcal{C}^\perp$ then $\mathcal{C}$ is called **weakly self-dual**, and if $\mathcal{C} = \mathcal{C}^\perp$ then $\mathcal{C}$ is called **self-dual**; in the latter case we have $n - k = \dim_{\mathbb{F}_q}(\mathcal{C}^\perp) = \dim_{\mathbb{F}_q}(\mathcal{C}) = k$, thus $n = 2k$ is even.

The weight enumerators $W_{\mathcal{C}}$ and $W_{\mathcal{C}^\perp}$ are related by **MacWilliams's Theorem** [1963], saying that $q^k \cdot W_{\mathcal{C}^\perp} = W_{\mathcal{C}}(Y - X, Y + (q-1)X) \in \mathbb{Z}[X, Y]$. In particular, if $\mathcal{C} = \mathcal{C}^\perp$ is self-dual, then $q^{\frac{n}{2}} \cdot W_{\mathcal{C}} = W_{\mathcal{C}}(Y - X, Y + (q-1)X) \in \mathbb{Z}[X, Y]$.

For example, for $\mathcal{C} := \{0_n\} \leq \mathbb{F}_q^n$ we have $\mathcal{C}^\perp = \mathbb{F}_q^n$, and indeed from $W_{\mathcal{C}} = Y^n$ we recover $W_{\mathbb{F}_q^n} = W_{\mathcal{C}^\perp} = W_{\mathcal{C}}(Y - X, Y + (q-1)X) = (Y + (q-1)X)^n$.

(11.3) Invariants for weight enumerators. Let $\mathbb{F}_q$ be the finite field with q elements, and let $n \in \mathbb{N}$. By MacWilliams's Theorem, phrased in terms of invariant theory, the weight enumerator $W_\mathcal{C}$ of a self-dual code $\mathcal{C} = \mathcal{C}^\perp \leq \mathbb{F}_q^n$ is a non-zero homogeneous invariant of degree n in $S := K[X,Y]$, where $K := \mathbb{Q}(\sqrt{q})$, with respect to the involutory map $s := \frac{1}{\sqrt{q}} \cdot \begin{bmatrix} -1 & 1 \\ q-1 & 1 \end{bmatrix} \in \mathrm{GL}_2(K)$.

Moreover, $W_\mathcal{C}$ has degree $n = 2k$, which is even. To exclude precisely the homogeneous components of S of odd degree, we only allow for invariants with respect to $z := -E_2 \in \mathrm{GL}_2(K)$. Thus we consider the group $G := \langle s, z \rangle \cong V_4$:

Since both s and sz have eigenvalues $\{\pm 1\}$, the group G is a reflection group. Hence the invariant algebra S^G is polynomial generated in degrees $[d_1, d_2]$, where from $d_1 d_2 = |G| = 4$ and $d_1 + d_2 - 2 = \sigma(G) = |\{s, sz\}| = 2$ we get $d_1 = d_2 = 2$. Thus we have $H_{S^G} = \frac{1}{(1-T^2)^2} \in \mathbb{Q}(T)$; in particular, $\dim_K(S_2^G) = 2$ shows that we may choose any pair of K-linearly independent homogeneous invariants of degree 2 as basic invariants.

We have $f := \mathrm{Tr}_{\langle z \rangle}^G(qX^2) = \mathrm{Tr}^{\langle s \rangle}(qX^2) = (q+1)X^2 - 2XY + Y^2 \in S^G$, and $g := \mathrm{Tr}_{\langle z \rangle}^G(qY^2) = \mathrm{Tr}^{\langle s \rangle}(qY^2) = (q-1)^2 X^2 + 2(q-1)XY + (q+1)Y^2 \in S^G$, and $h := \mathrm{Tr}_{\langle z \rangle}^G(-qXY) = \mathrm{Tr}^{\langle s \rangle}(-qXY) = (q-1)X^2 - 2(q-1)XY - Y^2 \in S^G$. Hence letting $f_1 := \frac{1}{2q} \cdot (f+h) = X^2 - XY$, and $f_2 := \frac{1}{q} \cdot (g+h) = (q-1)X^2 + Y^2$, we infer that $\{f_1, f_2\}$ is a set of basic invariants. Thus $W_\mathcal{C} \in S^G = K[f_1, f_2]$ can be written uniquely as a polynomial in $\{X^2 - XY, (q-1)X^2 + Y^2\}$, with coefficients in $K = \mathbb{Q}(\sqrt{q})$; note that, if $q \in \mathbb{Z}$ is not a square, then since $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{q})$ is Galois we conclude that actually $W_\mathcal{C} \in \mathbb{Q}[f_1, f_2]$.

Since $W_\mathcal{C} \in S_n^G$ we have $W_\mathcal{C} = \sum_{j=0}^k a_j f_1^j f_2^{k-j}$, where $a_j \in \mathbb{Q}$. Since $0_n \in \mathcal{C}$ is the only element of weight 0, that is Y^n occurs with coefficient $w_0 = 1$ in $W_\mathcal{C}$, we infer that $a_0 = 1$. Hence $W_\mathcal{C} = Y^n + \sum_{i=1}^n w_i X^i Y^{n-i}$, which is defined by the $n = 2k$ numbers $[w_1, \ldots, w_n]$, only depends on the k numbers $[a_1, \ldots, a_k]$.

In the sequel, we look more closely at the binary and ternary cases, where we refer to computational checks (whose details we spare):

(11.4) Invariants for binary weight enumerators [Gleason, 1970]**.** We consider the case $q = 2$. Let $\mathcal{C} = \mathcal{C}^\perp \leq \mathbb{F}_2^n$, where $n \in \mathbb{N}$, be a self-dual code; then $\mathcal{C}$ is an even-weight code. Let again $s := \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix} \in \mathrm{GL}_2(K)$ and $z := -E_2$, where $K := \mathbb{Q}(\sqrt{2})$; recall that s and sz are reflections.

a) Since $\mathcal{C}$ is an even-weight code, $W_\mathcal{C} \in \mathbb{Q}[X^2 - XY, X^2 + Y^2]$ is invariant with respect to $d := \mathrm{diag}[-1, 1]$. We consider the group $H := \langle s, z, d \rangle \leq \mathrm{GL}_2(K)$:

Since d is a pseudoreflection, H is a real reflection group. It can be checked that $H \cong D_{16}$, and that $\sigma(H) = 8$. Since H does not possess any common eigenvectors, we conclude that H acts (absolutely) irreducibly. Thus H is of type $2b$ in the Shephard-Todd classification, having (non-crystallographic) Dynkin type $I_2(8)$. The invariant algebra S^H is polynomial generated in degrees $[d_1, d_2]$, where from $d_1 d_2 = |H| = 16$, and $d_1 + d_2 - 2 = \sigma(H) = 8$, we conclude that $d_1 = 2$ and $d_2 = 8$. Thus we have $H_{S^H} = \frac{1}{(1-T^2)(1-T^8)} \in \mathbb{Q}(T)$.

We proceed to find basic invariants: We observe that $f_1 := X^2 + Y^2$ actually is H-invariant. Observing that $\mathrm{Stab}_H(Y) = \langle d \rangle \cong C_2$, we get $f_2 := 4 \cdot N^H_{\langle d \rangle}(Y) = X^2Y^2(X^2 - Y^2)^2$. Since $\{f_1^4, f_2\}$ is K-linearly independent, we conclude that $\{f_1, f_2\}$ is a set of basic invariants. Thus $W_\mathcal{C} \in S^H = K[f_1, f_2]$ can be written uniquely as a polynomial in $\{X^2 + Y^2, X^2Y^2(X^2 - Y^2)^2\}$, with coefficients in $K = \mathbb{Q}(\sqrt{2})$; note that since $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ is Galois we infer that $W_\mathcal{C} \in \mathbb{Q}[f_1, f_2]$.

b) We now assume further that $\mathcal{C}$ is **4-divisible**, that is we have $4 \mid \mathrm{wt}(v)$ for all $v \in \mathcal{C}$; then $\mathcal{C}$ is also called a **(doubly-)even self-dual** code. Note that $\mathcal{C}$ is 4-divisible if and only if $\mathcal{C}$ has a 4-divisible $\mathbb{F}_2$-basis; and if $\mathcal{C}$ is cyclic then the latter is the case if and only if the number of monomials occurring in the generating polynomial of $\mathcal{C}$ is divisible by 4.

Hence the weight enumerator $W_\mathcal{C} \in \mathbb{Q}[X^2 + Y^2, X^2Y^2(X^2 - Y^2)^2]$ is even invariant with respect to $d := \mathrm{diag}[\zeta_4, 1]$, where $\zeta_4 \in \mathbb{C}$ is primitive 4-th root of unity. Thus we now consider the group $H := \langle s, z, d \rangle \leq \mathrm{GL}_2(K)$, where $K := \mathbb{Q}(\sqrt{2}, \zeta_4) = \mathbb{Q}(\zeta_8)$, and $\zeta_8 \in \mathbb{C}$ is primitive 8-th root of unity:

Since d is a pseudoreflection, H is a (non-real) complex pseudoreflection group. It can be checked that H has order 192. Since H does not possess any common eigenvectors, we conclude that H acts (absolutely) irreducibly. Moreover, it turns out that $Z(H) = \langle \zeta_8 \cdot E_2 \rangle \cong C_8$; hence the degree of any non-zero homogeneous H-invariant is divisible by 8.

Hence the invariant algebra S^H is polynomial generated in degrees $[d_1, d_2]$, where from $d_1 d_2 = |H| = 192 = 8^2 \cdot 3$, and $8 \mid d_i$, we conclude that $d_1 = 8$ and $d_2 = 24$. (Alternatively, we could check that $\sigma(H) = 30$.) Thus we have $H_{S^H} = \frac{1}{(1-T^8)(1-T^{24})} \in \mathbb{Q}(T)$. Moreover, we infer that H is the group G_9 in the Shephard-Todd classification, being of shape $H \cong 2.(4 \times \mathcal{S}_4)$.

We proceed to find basic invariants, observing that $\mathrm{Stab}_H(Y) = \langle d \rangle \cong C_4$: This yields $f_1 := \frac{1}{10} \cdot \mathrm{Tr}^H_{\langle d \rangle}(Y^8) = X^8 + 14X^4Y^4 + Y^8$. Moreover, we get $2^{16} \cdot N^H_{\langle d \rangle}(Y) = X^8Y^8(X^4 - Y^4)^8$, thus taking square roots we let $f_2 := X^4Y^4(X^4 - Y^4)^4$, which turns out to be H-invariant. Since $\{f_1^3, f_2\}$ is K-linearly independent, we conclude that $\{f_1, f_2\}$ is a set of basic invariants. Thus $W_\mathcal{C} \in S^H = K[f_1, f_2]$ can be written uniquely as a polynomial in $\{X^8 + 14X^4Y^4 + Y^8, X^4Y^4(X^4 - Y^4)^4\}$, with coefficients in $K = \mathbb{Q}(\zeta_8)$; note that since $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_8)$ is Galois we conclude that $W_\mathcal{C} \in \mathbb{Q}[f_1, f_2]$.

Example. Let $\widehat{\mathcal{H}} \leq \mathbb{F}_2^8$ be the **extended Hamming** $[8,4,4]$**-code**, whose generator matrix we may assume to be equal to

$$\left[\begin{array}{ccccccc|c} . & . & . & 1 & 1 & 1 & 1 & . \\ . & 1 & 1 & . & . & 1 & 1 & . \\ 1 & . & 1 & . & 1 & . & 1 & . \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right] \in \mathbb{F}_2^{4\times 8}.$$

Then $\widehat{\mathcal{H}}$ is self-dual and 4-divisible. Hence we necessarily have $W_{\widehat{\mathcal{H}}} = f_1$. (The weight enumerator already follows straightforwardly from 4-divisibility, providing an alternative way to find the basic invariant f_1 in the first place.)

Example. Let $\mathcal{G}_{24} := \widehat{\mathcal{G}}_{23} \leq \mathbb{F}_2^{24}$ be the **extended binary Golay** $[24,12,8]$**-code**, where the **binary Golay** $[23,12,7]$**-code** $\mathcal{G}_{23} \leq \mathbb{F}_2^{23}$ is the cyclic code with generator polynomial $X^{11}+X^9+X^7+X^6+X^5+X+1 \in \mathbb{F}_2[X]$. Then $\mathcal{G}_{24}$ is self-dual and 4-divisible.

Hence we have $W_{\mathcal{G}_{24}} = a\cdot f_1^3 + b\cdot f_2$, where $a,b\in\mathbb{Q}$. Since $0_n \in \mathcal{G}_{24}$ is the only element of weight 0, that is $w_0(\mathcal{G}_{24}) = 1$, and $\mathcal{G}_{24}$ does not possess any elements of weight 4, that is $w_4(\mathcal{G}_{24}) = 0$, we conclude that $a = 1$ and $b = -42$. Hence we have $W_{\mathcal{G}_{24}} = X^{24} + 759X^{16}Y^8 + 2576X^{12}Y^{12} + 759X^8Y^{16} + Y^{24}$. (This is an efficient way to compute the weight enumerator, compared to combinatorial methods. Or, if the latter is already known, this provides an alternative way to find the basic invariant f_2 in the first place.)

(11.5) Invariants for ternary weight enumerators [Gleason, 1970]**.** We consider the case $q = 3$. Let $\mathcal{C} = \mathcal{C}^\perp \leq \mathbb{F}_3^n$, where $n\in\mathbb{N}$, be a self-dual code; then $\mathcal{C}$ necessarily is **3-divisible**, that is we have $3 \mid \mathrm{wt}(v)$ for all $v\in\mathcal{C}$. Let again $s := \frac{1}{\sqrt{3}}\cdot\begin{bmatrix} -1 & 1 \\ 2 & 1\end{bmatrix} \in \mathrm{GL}_2(K)$ and $z := -E_2$, where $K := \mathbb{Q}(\sqrt{3})$; recall that s and sz are reflections.

Hence the weight enumerator $W_{\mathcal{C}} \in \mathbb{Q}[X^2-XY, 2X^2+Y^2]$ is also invariant with respect to $d := \mathrm{diag}[\zeta_3, 1]$, where $\zeta_3\in\mathbb{C}$ is primitive 3-rd root of unity. Thus we consider the group $H := \langle s,z,d\rangle \leq \mathrm{GL}_2(K)$, where $K := \mathbb{Q}(\sqrt{3},\zeta_3) = \mathbb{Q}(\zeta_{12})$, and $\zeta_{12}\in\mathbb{C}$ is primitive 12-th root of unity:

Then H is a (non-real) complex pseudoreflection group. It can be checked (computationally) that H has order 48. Since H does not possess any common eigenvectors, we conclude that H acts (absolutely) irreducibly. Moreover, it turns out that $Z(H) = \langle\zeta_4\cdot E_2\rangle \cong C_4$; hence the degree of any non-zero homogeneous H-invariant is divisible by 4.

Hence the invariant algebra S^H is polynomial generated in degrees $[d_1,d_2]$, where from $d_1d_2 = |H| = 48 = 4^2\cdot 3$, and $4 \mid d_i$, we conclude that $d_1 = 4$ and $d_2 = 12$. (Alternatively, we could check that $\sigma(H) = 14$.) Thus we have $H_{S^H} = \frac{1}{(1-T^4)(1-T^{12})} \in \mathbb{Q}(T)$. Moreover, since H is not metabelian (thus excluding the case $G_{12,6,2}$ in the Shephard-Todd classification), we infer that H is the group G_6 in the Shephard-Todd classification, being of shape $H \cong 2.(2 \times \mathcal{A}_4)$.

We proceed to find basic invariants, observing that $\mathrm{Stab}_H(Y) = \langle d \rangle \cong C_3$ and $\mathrm{Stab}_H(X) = \{1\}$. This yields $f_1 := \frac{3}{16} \cdot \mathrm{Tr}^H_{\langle d \rangle}(Y^4) = 8X^3Y + Y^4 \in S^H$. Moreover, we get $3^{18} \cdot N^H(X) = X^{12}(X^3 - Y^3)^{12}$, thus taking 4-th roots we let $f_2 := X^3(X^3 - Y^3)^3$, which turns out to be H-invariant. Since $\{f_1^3, f_2\}$ is K-linearly independent, we conclude that $\{f_1, f_2\}$ is a set of basic invariants. Thus $W_\mathcal{C} \in S^H = K[f_1, f_2]$ can be written uniquely as a polynomial in $\{8X^3Y + Y^4, X^3(X^3 - Y^3)^3\}$, with coefficients in $K = \mathbb{Q}(\zeta_{12})$; note that since $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_{12})$ is Galois we conclude that $W_\mathcal{C} \in \mathbb{Q}[f_1, f_2]$.

Example. Let $\mathcal{H} \leq \mathbb{F}_3^4$ be the **Hamming** $[4, 2, 3]$**-code** with generator matrix

$$\begin{bmatrix} . & 1 & 1 & 1 \\ 1 & . & 1 & -1 \end{bmatrix} \in \mathbb{F}_3^{2 \times 4}.$$

Then $\mathcal{H}$ is self-dual. Hence we necessarily have $W_\mathcal{H} = f_1$. (The weight enumerator already follows straightforwardly from 3-divisibility, providing an alternative way to find the basic invariant f_1 in the first place.)

Example. Let $\mathcal{G}_{12} := \widehat{\mathcal{G}}_{11} \leq \mathbb{F}_3^{12}$ be the **extended ternary Golay** $[12, 6, 6]$**-code**, where the **ternary Golay** $[11, 6, 5]$**-code** $\mathcal{G}_{11} \leq \mathbb{F}_3^{11}$ is the cyclic code with generator polynomial $X^5 - X^3 + X^2 - X - 1 \in \mathbb{F}_3[X]$. Then $\mathcal{G}_{12}$ is self-dual.

Hence we have $W_{\mathcal{G}_{12}} = a \cdot f_1^3 + b \cdot f_2$, where $a, b \in \mathbb{Q}$. Since $0_n \in \mathcal{G}_{12}$ is the only element of weight 0, that is $w_0(\mathcal{G}_{12}) = 1$, and $\mathcal{G}_{12}$ does not possess any elements of weight 3, that is $w_3(\mathcal{G}_{12}) = 0$, we conclude that $a = 1$ and $b = 24$. Hence we have $W_{\mathcal{G}_{12}} = 24X^{12} + 440X^9Y^3 + 264X^6Y^6 + Y^{12}$. (This again is an efficient way to compute the weight enumerator, compared to combinatorial methods. Or, if the latter is already known, this provides an alternative way to find the basic invariant f_2 in the first place.)

12 Example: The icosahedral group

We present an elaborated classical example, the invariants of the icosahedral group, due to Klein [1884] and Molien [1897]. This in particular shows how geometric features are related to invariant theory. (The other polyhedral groups are considered in Exercise (18.30).)

(12.1) Symmetries of the icosahedron. Let $\mathcal{I} \subseteq \mathbb{R}^3$ be the regular icosahedron, one of the platonic solids, see Table 3. The faces of $\mathcal{I}$ consist of regular triangles, that is $n = 3$, where at each vertex $k = 5$ faces meet. Let f be the number of faces, let e be the number of edges, and let v be the number of vertices. By Euler's Polyhedron Theorem we have $f - e + v = 2$, hence since $2e = nf$ and $kv = nf$, we conclude that $f = 20$, and $e = 30$, and $v = 12$.

Let $G := \{g \in O_3(\mathbb{R}); \mathcal{I} \cdot g = \mathcal{I}\} \leq O_3(\mathbb{R})$ be the the symmetry group of $\mathcal{I}$, being called the **icosahedral group**, where we assume $\mathcal{I}$ to be centered at the origin, and the orthogonal group $O_3(\mathbb{R})$ is the isometry group of Euclidean 3-space. Let $H = G \cap \mathrm{SO}_3(\mathbb{R}) \trianglelefteq G$ be the group of rotational symmetries of $\mathcal{I}$, where $\mathrm{SO}_3(\mathbb{R}) := \{g \in O_3(\mathbb{R}); \det(g) = 1\} \trianglelefteq O_3(\mathbb{R})$.

By regularity of $\mathcal{I}$, the group H acts transitively on its vertices, where the associated point stabilizers have order 5, hence $|H| = 60$. Recalling Euler's Theorem, saying that any rotation of Euclidean 3-space has an axis, the axes of the elements of H are given by the lines joining opposite vertices, and midpoints of opposite edges, and midpoints of opposite faces, respectively. This yields $\frac{v}{2} \cdot (k-1) = 24$ elements of order $k = 5$, and $\frac{e}{2} = 15$ elements of order 2, and $\frac{f}{2} \cdot (n-1) = 20$ elements of order $n = 3$, accounting for all elements of $H \setminus \{1\}$.

We show that $H \cong \mathcal{A}_5$: By regularity we infer that H has a unique conjugacy class of elements of order 2; since the Sylow 2-subgroups are abelian, $N_H(V_4)$ controls 2-fusion, implying that $N_H(V_4) \cong \mathcal{A}_4$. Moreover, H has 10 Sylow 3-subgroups, hence $N_H(C_3) \cong \mathcal{S}_3$, so that there is a unique conjugacy class of elements of order 3; and H has 6 Sylow 5-subgroups, hence $N_H(C_5) \cong D_{10}$, so that there are two conjugacy classes of elements of order 5, of length 12 each. From the lengths of the conjugacy classes we conclude that H is simple, so that the permutation action of H on the cosets of $\mathcal{A}_4$ induces an isomorphism to $\mathcal{A}_5$.

For $s := -E_3 \in O_3(\mathbb{R})$, that is the inversion with respect to the origin, we have $s \in G \setminus H$. Since $s \in Z(O_3(\mathbb{R}))$, we have $G = H \times \langle s \rangle \cong \mathcal{A}_5 \times C_2$, in particular $|G| = 120$; note that s is not a reflection. Since the elements of H are rotations, its elements of order 2 have eigenvalues $\{1, -1, -1\}$, hence are not reflections either. Since H, being simple, is generated by its elements of order 2, we conclude that the set of reflections $\mathcal{S}(G) = \{gs \in G; 1 \neq g \in H, g^2 = 1\} \subseteq G \setminus H$ generates a subgroup of G having $\mathcal{A}_5$ as an epimorphic image, which hence coincides with G. Thus G is a real reflection group. Since the elements of H do not possess any common (real) eigenvector, H acts (absolutely) irreducibly. From this we infer that G is the group G_{23} in the Shephard-Todd classification, having (non-crystallographic) Dynkin type H_3, and having character field $\mathbb{Q}(\sqrt{5})$.

(12.2) Invariants of the icosahedral group. Let $H := \mathcal{A}_5 \leq \mathrm{GL}_3(K)$ and $G := H \times \langle s \rangle \leq \mathrm{GL}_3(K)$, where $s := -E_3$ and $K := \mathbb{Q}(\sqrt{5})$, let $V := K^3$, and let $S := K[\mathcal{X}]$ be the associated polynomial algebra, where $\mathcal{X} := \{X, Y, Z\}$.

Since G is a reflection group, its invariant algebra $S^G = K[f_1, f_2, f_3]$ is polynomial generated in degrees $[d_1, d_2, d_3]$, where $d_1 d_2 d_3 = 120$ and $d_1 + d_2 + d_3 - 3 = \sigma(G) = 15$. Hence we have $d_1 = 2$, and $d_2 = 6$, and $d_3 = 10$, so that $H_{S^G} = \frac{1}{(1-T^2)(1-T^6)(1-T^{10})} \in \mathbb{Q}(T)$. Since H does not contain any reflections, its invariant algebra S^H is not polynomial; we determine the Hilbert series H_{S^H}:

The 15 involutions in H have eigenvalues $\{1, -1, -1\}$; the 20 elements of order 3 have eigenvalues $\{1, \zeta_3, \zeta_3^2\}$, where $\zeta_3 \in \mathbb{C}$ is a primitive 3-rd root of unity; the $12 + 12$ elements of order 5 have eigenvalues $\{1, \zeta_5, \zeta_5^4\}$ and $\{1, \zeta_5^2, \zeta_5^3\}$, respectively, where $\zeta_5 \in \mathbb{C}$ is a primitive 5-th root of unity. Thus Molien's formula entails $H_{S^H} = \frac{1+T^{15}}{(1-T^2)(1-T^6)(1-T^{10})} \in \mathbb{Q}(T)$. Hence we are tempted to look for a homogeneous H-invariant g of degree 15 such that $S^H = K[f_1, f_2, f_3, g]$.

i) Let $\alpha := \zeta_5 + \zeta_5^4 = \frac{1}{2} \cdot (\sqrt{5} - 1) \in \mathbb{R}$ and $\beta := \zeta_5^2 + \zeta_5^3 = -\frac{1}{2} \cdot (\sqrt{5} + 1) \in \mathbb{R}$; hence $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. Being a real reflection group of Dynkin type H_3, choosing the K-basis of V consisting of the fundamental roots associated with the Cartan matrix

$$\Phi := \begin{bmatrix} 2 & \beta & 0 \\ \beta & 2 & -1 \\ 0 & -1 & 2 \end{bmatrix} \in \mathrm{GL}_3(K),$$

we may assume that $G = \langle a, b, c \rangle \leq \mathrm{GL}_3(K)$ is generated by the reflections

$$a := \begin{bmatrix} -1 & 0 & 0 \\ -\beta & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad b := \begin{bmatrix} 1 & -\beta & 0 \\ 0 & -1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \quad c := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & -1 \end{bmatrix},$$

where $(ab)^5 = (ac)^2 = (bc)^3 = 1$. Since G acts transitively on the associated root system, entailing that all roots have the same length, Φ is the Gram matrix of a G-invariant scalar product on V, that is we have $g \cdot \Phi \cdot g^{\mathrm{tr}} = \Phi$ for all $g \in G$. Note that $\det(\Phi) = 2 \cdot (1 - \alpha)$, and that since G acts absolutely irreducibly, Φ is as an G-invariant scalar product uniquely defined up to scalar multiples.

From $g \cdot \Phi \cdot g^{\mathrm{tr}} = \Phi$ we get $g^{-\mathrm{tr}} \cdot \Phi^{-1} \cdot g^{-1} = \Phi^{-1}$, thus $g^{\mathrm{tr}} \cdot \Phi^{-1} \cdot g = \Phi^{-1}$, for all $g \in G$. Let $f := \mathcal{X} \cdot \Phi^{-1} \cdot \mathcal{X}^{\mathrm{tr}} \in S$. Then we have $f^g = (\mathcal{X} \cdot \Phi^{-1} \cdot \mathcal{X}^{\mathrm{tr}})^g = \mathcal{X}^g \cdot \Phi^{-1} \cdot (\mathcal{X}^g)^{\mathrm{tr}} = (\mathcal{X} \cdot g^{\mathrm{tr}}) \cdot \Phi^{-1} \cdot (\mathcal{X} \cdot g^{\mathrm{tr}})^{\mathrm{tr}} = \mathcal{X} \cdot (g^{\mathrm{tr}} \cdot \Phi^{-1} \cdot g) \cdot \mathcal{X}^{\mathrm{tr}} = \mathcal{X} \cdot \Phi^{-1} \cdot \mathcal{X}^{\mathrm{tr}} = f$, so that as first basic invariant we may take

$$f_1 := \det(\Phi) \cdot f = 3X^2 - 4\beta XY - 2\beta XZ + 4Y^2 + 4YZ + (3 + \beta)Z^2.$$

Note that since H acts irreducibly, f_1 cannot possibly be the product of two linear factors, thus f_1 is irreducible in S.

ii) Next, G permutes the $\frac{v}{2} = 6$ lines joining opposite vertices of $\mathcal{I}$ transitively, which are given as the axes of the rotations of order 5 in H. Hence a vector spanning one of these lines is found as an eigenvector of $ab \in H$, with respect to the eigenvalue 1; then the associated G-orbit has length 12. Therefrom we pick the following vectors, up to taking scalar multiples:

$$[\alpha, 0, 1], \quad [-\alpha, 0, 1], \quad [\alpha, 2, 1], \quad [2 + \alpha, 2, 1], \quad [-\beta, 2, \alpha], \quad [-\beta, 2, 3 + \beta].$$

Let $f_2 \in S$ the product of the latter elements, being homogeneous of degree 6. Hence $\langle f_2 \rangle_K$ is a one-dimensional $K[G]$-submodule. Since H is perfect, and $s \in G$ fixes all elements of degree 6 anyway, we conclude that f_2 is G-invariant. Since $\{f_1^3, f_2\}$ is K-linearly independent, we may take f_2 as second basic invariant, where f_2 up to scalar multiples equals

$$X^6 - 4\beta X^5 Y - 2\beta X^5 Z + (-12 - 16\beta) X^4 Y^2$$

$$+(-12-16\beta)X^4YZ+(-17-11\beta)X^4Z^2+(64+32\beta)X^3Y^3+(96+48\beta)X^3Y^2Z$$
$$-8X^3YZ^2+(-20-8\beta)X^3Z^3+(-48-32\beta)X^2Y^4+(-96-64\beta)X^2Y^3Z$$
$$+(8+24\beta)X^2Y^2Z^2+(56+56\beta)X^2YZ^3+(22+19\beta)X^2Z^4-32XY^3Z^2$$
$$-48XY^2Z^3+(-4+12\beta)XYZ^4+(6+6\beta)XZ^5+(16+16\beta)Y^4Z^2$$
$$+(32+32\beta)Y^3Z^3+(-8+4\beta)Y^2Z^4+(-24-12\beta)YZ^5+(-7-4\beta)Z^6.$$

iii) Similarly, G permutes the $\frac{f}{2}=10$ lines joining the midpoints of opposite faces of $\mathcal{I}$ transitively, which are given as the axes of the rotations of order 3 in H. Hence a vector spanning one of these lines is found as an eigenvector of $bc \in H$, with respect to the eigenvalue 1; then the associated G-orbit has length 20. Therefrom we pick the following vectors, up to taking scalar multiples:

$$\begin{array}{lllll} [1,0,1-\alpha], & [1,0,\alpha-1], & [1,2,-\beta], & [1,2,1-\alpha], & [\beta,-2,\alpha], \\ [\beta,-2,\beta-1], & [3\alpha,2,1], & [3+\beta,2,1], & [1+2\alpha,2,-\beta], & [1+2\alpha,2,1-\alpha]. \end{array}$$

Let $f_3 \in S$ the product of the latter elements, being homogeneous of degree 10. Hence $\langle f_3\rangle_K$ is a one-dimensional $K[G]$-submodule. Since H is perfect, and $s \in G$ fixes all elements of degree 10 anyway, we conclude that f_3 is G-invariant. Since $\{f_1^5, f_1^2f_2, f_3\}$ is K-linearly independent, we may take f_3 as third basic invariant, where f_3 up to scalar multiples equals

$$(105-165\beta)X^{10}+(1100-1800\beta)X^9Y+(550-900\beta)X^9Z$$
$$+(5148-8364\beta)X^8Y^2+(5148-8364\beta)X^8YZ+(1098-1839\beta)X^8Z^2$$
$$+(13632-21888\beta)X^7Y^3+(20448-32832\beta)X^7Y^2Z+(8976-14160\beta)X^7YZ^2$$
$$+(1080-1608\beta)X^7Z^3+(21984-35520\beta)X^6Y^4+(43968-71040\beta)X^6Y^3Z$$
$$+(28320-45744\beta)X^6Y^2Z^2+(6336-10224\beta)X^6YZ^3+(354-408\beta)X^6Z^4$$
$$+(22336-36480\beta)X^5Y^5+(55840-91200\beta)X^5Y^4Z+(46720-77376\beta)X^5Y^3Z^2$$
$$+(14240-24864\beta)X^5Y^2Z^3+(224-1896\beta)X^5YZ^4+(-400+156\beta)X^5Z^5$$
$$+(14272-22976\beta)X^4Y^6+(42816-68928\beta)X^4Y^5Z+(43680-70720\beta)X^4Y^4Z^2$$
$$+(16000-26560\beta)X^4Y^3Z^3+(360+480\beta)X^4Y^2Z^4+(-504+2272\beta)X^4YZ^5$$
$$+(-38+294\beta)X^4Z^6+(5120-8192\beta)X^3Y^7+(17920-28672\beta)X^3Y^6Z$$
$$+(21376-31872\beta)X^3Y^5Z^2+(8640-8000\beta)X^3Y^4Z^3+(-1920+7360\beta)X^3Y^3Z^4$$
$$+(-2560+4704\beta)X^3Y^2Z^5+(-560+832\beta)X^3YZ^6+(8+48\beta)X^3Z^7$$
$$+(768-1280\beta)X^2Y^8+(3072-5120\beta)X^2Y^7Z+(2304-4736\beta)X^2Y^6Z^2$$
$$+(-3840+3712\beta)X^2Y^5Z^3+(-6720+8800\beta)X^2Y^4Z^4+(-3456+5440\beta)X^2Y^3Z^5$$
$$+(-688+1200\beta)X^2Y^2Z^6+(-112-48\beta)X^2YZ^7+(-10-27\beta)X^2Z^8$$
$$+(-1024+1024\beta)XY^7Z^2+(-3584+3584\beta)XY^6Z^3+(-4608+4800\beta)XY^5Z^4$$
$$+(-2560+3040\beta)XY^4Z^5+(-448+832\beta)XY^3Z^6+96XY^2Z^7$$
$$+(36-44\beta)XYZ^8+(2-6\beta)XZ^9+256\beta Y^8Z^2+1024\beta Y^7Z^3$$
$$+(-64+1536\beta)Y^6Z^4+(-192+1024\beta)Y^5Z^5+(-192+224\beta)Y^4Z^6$$

$$+(-64-64\beta)Y^3Z^7+(8-36\beta)Y^2Z^8+(8-4\beta)YZ^9+Z^{10}.$$

iv) Finally, G permutes the $\frac{e}{2}=15$ lines joining the midpoints of opposite edges of $\mathcal{I}$ transitively, which are given as the axes of the rotations of order 2 in H. In other words, these are spanned by eigenvectors of the reflections in G, with respect to the eigenvalue -1, where the latter can be chosen to coincide with the positive roots of G. Picking the root $[1,0,0]$, the associated G-orbit has length 30. Therefrom we pick the following roots, up to scalar multiples:

$$\begin{array}{ccccc} [0,0,1], & [0,1,0], & [1,0,0], & [0,1,1], & [1,1,0], \\ [1,1,1], & [\alpha,1,0], & [-\beta,1,0], & [\alpha,1,1], & [-\beta,1,1], \\ [1,1,\alpha], & [1,1,1-\alpha], & [1,-\beta,1], & [1,-\beta,\alpha], & [-\beta,2,1]. \end{array}$$

Let $g\in S$ the product of the latter elements, being homogeneous of degree 15. Hence $\langle g\rangle_K\in S_{15}$ is a one-dimensional $K[G]$-submodule. Since H is perfect, but s negates all elements of degree 15, we conclude that g is G-invariant such that $g\cdot s=-g$, where g up to scalar multiples equals

$$XYZ\cdot\Big(X^{11}Y+X^{11}Z-8\beta X^{10}Y^2-12\beta X^{10}YZ-4\beta X^{10}Z^2+(22-33\beta)X^9Y^3$$

$$+(44-66\beta)X^9Y^2Z+(22-44\beta)X^9YZ^2-11\beta X^9Z^3+(86-108\beta)X^8Y^4$$
$$+(215-270\beta)X^8Y^3Z+(220-220\beta)X^8Y^2Z^2+(115-60\beta)X^8YZ^3+(24-2\beta)X^8Z^4$$
$$+(153-273\beta)X^7Y^5+(459-819\beta)X^7Y^4Z+(480-960\beta)X^7Y^3Z^2$$
$$+(195-555\beta)X^7Y^2Z^3+(27-153\beta)X^7YZ^4+(6-12\beta)X^7Z^5$$
$$+(240-432\beta)X^6Y^6+(840-1512\beta)X^6Y^5Z+(1152-2112\beta)X^6Y^4Z^2$$
$$+(780-1500\beta)X^6Y^3Z^3+(216-600\beta)X^6Y^2Z^4+(-36-156\beta)X^6YZ^5$$
$$+(-24-24\beta)X^6Z^6+(309-456\beta)X^5Y^7+(1236-1824\beta)X^5Y^6Z$$
$$+(2100-2940\beta)X^5Y^5Z^2+(1974-2436\beta)X^5Y^4Z^3+(1176-1050\beta)X^5Y^3Z^4$$
$$+(504-168\beta)X^5Y^2Z^5+(144+24\beta)X^5YZ^6+(15+6\beta)X^5Z^7$$
$$+(238-362\beta)X^4Y^8+(1071-1629\beta)X^4Y^7Z+(1968-3096\beta)X^4Y^6Z^2$$
$$+(1890-3234\beta)X^4Y^5Z^3+(1008-2016\beta)X^4Y^4Z^4+(294-756\beta)X^4Y^3Z^5$$
$$+(72-144\beta)X^4Y^2Z^6+(45+9\beta)X^4YZ^7+(14+8\beta)X^4Z^8$$
$$+(110-209\beta)X^3Y^9+(550-1045\beta)X^3Y^8Z+(1170-2220\beta)X^3Y^7Z^2$$
$$+(1380-2610\beta)X^3Y^6Z^3+(924-1890\beta)X^3Y^5Z^4+(252-924\beta)X^3Y^4Z^5$$
$$+(-120-360\beta)X^3Y^3Z^6+(-150-135\beta)X^3Y^2Z^7+(-60-40\beta)X^3YZ^8$$
$$+(-8-5\beta)X^3Z^9+(44-72\beta)X^2Y^{10}+(242-396\beta)X^2Y^9Z$$
$$+(600-920\beta)X^2Y^8Z^2+(885-1170\beta)X^2Y^7Z^3+(840-888\beta)X^2Y^6Z^4$$
$$+(504-420\beta)X^2Y^5Z^5+(192-120\beta)X^2Y^4Z^6+75X^2Y^3Z^7$$
$$+(40+20\beta)X^2Y^2Z^8+(10+6\beta)X^2YZ^9+(13-13\beta)XY^{11}$$
$$+(78-78\beta)XY^{10}Z+(176-220\beta)XY^9Z^2+(165-385\beta)XY^8Z^3$$
$$+(45-423\beta)XY^7Z^4+(48-240\beta)XY^6Z^5+168XY^5Z^6$$

$$+(171+81\beta)XY^4Z^7+(70+40\beta)XY^3Z^8+(10+6\beta)XY^2Z^9$$
$$-2\beta Y^{12}-13\beta Y^{11}Z+(8-32\beta)Y^{10}Z^2+(44-33\beta)Y^9Z^3$$
$$+(84-10\beta)Y^8Z^4+(48-12\beta)Y^7Z^5+(-48-48\beta)Y^6Z^6$$
$$+(-84-57\beta)Y^5Z^7+(-44-28\beta)Y^4Z^8+(-8-5\beta)Y^3Z^9\Big).$$

Since S^H is the graded direct sum of the eigenspaces of s with respect to the eigenvalues $\{\pm 1\}$, we conclude that $R := S^G \oplus gS^G \subseteq S^H$. Hence from $H_R = (1+T^{15}) \cdot H_{S^G} = H_{S_H} \in \mathbb{Q}(T)$ we conclude that $S^H = S^G \oplus gS^G$, being is a free graded S^G-module of rank 2, generated in degrees $[0, 15]$.

Alternatively, since $\{f_1, f_2, f_3\}$ is algebraically independent, by the Jacobian criterion for the Jacobian determinant we have $h := \det(J(f_1, \ldots, f_3)) \neq 0$. Moreover, since H is perfect we have $\det_V(g) = 1$ for all $g \in H$, but $\det_V(s) = -1$, so that from Exercise (18.8) we infer that $h \in S^H$, being homogeneous of degree $d_1 + d_2 + d_3 - 3 = 15$, but $h \cdot s = -h$. Since $\dim_K(S^H_{15}) = 1$ we conclude that h is associate to g; using the elements given above we find $h = -2^{18} \cdot g$.

(12.3) Modular invariants of the icosahedral group. Let K be a field, such that $T^2 + T - 1 = (T - \alpha)(T - \beta) \in K[T]$ splits. Hence we have $\{\alpha, \beta\} = \{\frac{1}{2} \cdot (-1 \pm \sqrt{5})\}$ if $\mathbb{Q}(\sqrt{5}) \subseteq K \subseteq \mathbb{C}$, which we may assume if $\mathrm{char}(K) = 0$; and modular reduction of the latter algebraic integers yields $\{\alpha, \beta\}$ if $\mathrm{char}(K) \neq 0$.

Keeping the notation of (12.2), let $G = \langle a, b, c\rangle \leq \mathrm{GL}_3(K)$; then G is a reflection group if $\mathrm{char}(K) \neq 2$, while G is generated by transvections if $\mathrm{char}(K) = 2$. Thus G is an epimorphic image of $\mathcal{A}_5 \times C_2$. Since $\mathcal{A}_5$ is simple, we have $G = H \times \langle s \rangle$, where $H \cong \mathcal{A}_5$ and $s = -E_3$, if $\mathrm{char}(K) \neq 2$; while $G = \mathcal{A}_5$, if $\mathrm{char}(K) = 2$. (Recall that by Serre's Theorem, which we have not proven, G possibly but not necessarily has a polynomial invariant algebra.)

a) Let $\mathrm{char}(K) \neq 2$. Then G acts irreducibly on V, where V is unique up to outer automorphisms of G. Let f_1 be as in (12.2)(i), where Φ still is the Gram matrix of a non-degenerate symmetric G-invariant K-bilinear form on V; let f_2 be as in (12.2)(ii), where the G-orbit of a fixed vector of $ab \in H$ still has length 12; let f_3 be as in (12.2)(iii), where the G-orbit of a fixed vector of $bc \in H$ still has length 20; and let g be as in (12.2)(iv), where the G-orbit of the root $[1, 0, 0]$ still has length 30.

i) For the Jacobian determinant of $\{f_1, f_2, f_3\}$ we have $\det(J(f_1, f_2, f_3)) = -2^{18} \cdot g \neq 0$. Hence by the Jacobian criterion $\{f_1, f_2, f_3\}$ is algebraically independent, and since the f_i have degree product $2 \cdot 6 \cdot 10 = 120 = |G|$, by Kemper's Theorem, see (16.2) below, we conclude that $S^G = K[f_1, f_2, f_3]$ is polynomial with basic invariants $\{f_1, f_2, f_3\}$; hence we have $H_{S^G} = \frac{1}{(1-T^2)(1-T^6)(1-T^{10})} \in \mathbb{Q}(T)$.

ii) Taking the determinant representation into account, where $\det_V(H) = \{1\}$ and $\det_V(s) = -1$, we have $S^H = S^G \oplus S^G_{\det}$ as graded S^G-modules. We show that for the set of semi-invariants we have $S^G_{\det} = g \cdot S^G$:

We have $g \in S^G_{\mathrm{det}}$, so that $g \cdot S^G \subseteq S^G_{\mathrm{det}}$. Conversely, let $f \in S^G_{\mathrm{det}}$. Then for the reflection $a \in G$ with respect to the root $[1,0,0]$ we have $f(X,Y,Z) = -f(X,Y,Z)\cdot a = -f(-X,Y-\beta X,Z) \in S$, so that the K-algebra homomorphism $S \to K[Y,Z]$ given by $X \mapsto 0$, and $Y \mapsto Y$, and $Z \mapsto Z$, yields $f(0,Y,Z) = -f(0,Y,Z) = 0$. Hence we infer that $X \mid f \in S$. Since f is semi-invariant, we conclude that g, being the product of a set of representatives of the roots up to scalar multiples, divides f. Writing $f = gf'$, for some $f' \in S$, since S is a domain we get $f' \in S^G$, showing that $f \in g \cdot S^G$. (Note that the preceding argument is strongly reminiscent of the reasoning in (9.4).) $\sharp$

Hence $S^H = S^G \oplus g \cdot S^G$ is a free graded S^G-module generated in degrees $[1, 15]$, so that $H_{S^H} = (1 + T^{15}) \cdot H_{S^G}$. Moreover, $\{f_1, f_2, f_3, g\}$ is a minimal homogeneous K-algebra generating set of S^H.

b) Let $\mathrm{char}(K) = 2$. Then $V \cong [W/K]$ is uniserial as a $K[G]$-module, where G acts trivially on K, and W is irreducible of K-dimension 2; then V is uniquely defined by these properties up to outer automorphisms of G. Moreover, the contragredient $K[G]$-module $V^* \cong [K/W]$ is obtained by 2-modular reduction of the G-action on the weight lattice, instead of the root lattice.

i) We consider the $K[G]$-module V first. Hence we have $\dim_K(S^G_1) = 1$, and we let $f_1 := X + \beta Z \in S^G$. (Actually, the rotation axes of the elements of order 5 and of those of order 3 all coincide with $\langle f_1 \rangle_K$. Moreover, Φ is degenerate, and V is not self-contragredient as a $K[G]$-module.)

Searching explicitly, degree by degree, for indecomposable homogeneous invariants we get $f_2 \in S^G$ of degree 5, which we may choose as

$$X^3Y^2 + X^3YZ + X^3Z^2 + \beta X^2Y^2Z + \beta X^2YZ^2 + \beta X^2Z^3$$

$$+\beta XY^4 + XY^2Z^2 + \alpha XYZ^3 + XZ^4 + \beta Y^4Z + \beta Y^2Z^3 + \beta Z^5.$$

Subsequently we get $f_3 \in S^G$ of degree 12, which we may choose as

$$X^9Y^2Z + X^9YZ^2 + \beta X^8Y^2Z^2 + \beta X^8YZ^3 + \beta X^7Y^4Z + \beta X^7YZ^4 + X^6Y^6$$

$$+X^6Y^5Z + \beta X^6Y^4Z^2 + X^6Y^3Z^3 + X^6Y^2Z^4 + \beta X^6YZ^5 + X^6Z^6$$

$$+\alpha X^5Y^6Z + \alpha X^5Y^5Z^2 + \beta X^5Y^4Z^3 + \alpha X^5Y^3Z^4 + \beta^2 X^5Y^2Z^5 + \beta X^5YZ^6$$

$$+\beta X^4Y^8 + \beta X^4Y^6Z^2 + \beta X^4Y^5Z^3 + \beta X^4Y^4Z^4 + \beta X^4Y^3Z^5 + \beta X^4Y^2Z^6$$

$$+X^4Z^8 + X^3Y^6Z^3 + X^3Y^5Z^4 + \beta X^3Y^4Z^5 + X^3Y^3Z^6 + \alpha X^3YZ^8$$

$$+\alpha X^2Y^{10} + \alpha X^2Y^9Z + \alpha X^2Y^6Z^4 + \alpha X^2Y^5Z^5 + \beta X^2Y^4Z^6 + \beta X^2Y^2Z^8$$

$$+X^2Z^{10} + \beta XY^{10}Z + \beta XY^9Z^2 + \beta XY^8Z^3 + \beta XY^6Z^5 + \beta XY^5Z^6$$

$$+\beta XYZ^{10} + Y^{12} + Y^{10}Z^2 + Y^6Z^6 + Y^2Z^{10} + Z^{12}.$$

For the Jacobian determinant of $\{f_1, f_2, f_3\}$ we get $\det(J(f_1, f_2, f_3)) \neq 0$. Hence by the Jacobian criterion $\{f_1, f_2, f_3\}$ is algebraically independent, and since the f_i have degree product $1 \cdot 5 \cdot 12 = 60 = |G|$, by Kemper's Theorem, see (16.2) below, we conclude that $S^G = K[f_1, f_2, f_3]$ is polynomial with basic invariants $\{f_1, f_2, f_3\}$; hence we have $H_{S^G} = \frac{1}{(1-T)(1-T^5)(1-T^{12})} \in \mathbb{Q}(T)$.

(Picking the root $[1, 0, 0]$, the associated G-orbit has length 15, so that by taking the product of the latter elements we still get a homogeneous invariant g of degree 15; it turns out that $\det(J(f_1, f_2, f_3)) = g$.)

ii) We consider the $K[G]$-module V^*. Hence we have $\dim_K(S_1^G) = 0$, but it turns out that $\dim_K(S_2^G) = 1$, and we let $f_1 := X^2+\beta XY+Y^2+YZ+Z^2 \in S^G$. (Note that f_1 is a degenerate quadratic form associated with Φ.) Proceeding degree by degree as above, we find an indecomposable homogeneous invariant of degree 5, which we may choose as

$$f_2 := X^4Y + XY^4 + \alpha Y^4Z + \alpha YZ^4 = XY(X^3 + Y^3) + \alpha YZ(Y^3 + Z^3) \in S^G.$$

We observe that there is an indecomposable homogeneous invariant of degree 6, which turns out to be accessible as follows: The rotation axes of the elements of order 5 are all G-conjugate, thus choosing an eigenvector of $ab \in G$ with respect to the eigenvalue 1, we obtain a G-orbit of length 6. We pick the following vectors, up to taking scalar multiples:

$$[0, 0, 1], \quad [0, 1, 1], \quad [1, 1, 0], \quad [1, \beta, 0], \quad [\beta, 0, 1], \quad [\beta, 1, 1].$$

Let $f_3 \in S$ the product of the latter elements, being homogeneous of degree 6. Hence $\langle f_3\rangle_K$ is a one-dimensional $K[G]$-submodule. Since G is perfect we conclude that f_3 is G-invariant, and up to scalar multiples equals

$$Z \cdot (X^4Y + X^4Z + \alpha X^2Y^2Z + \alpha X^2Z^3 + XY^4 + XYZ^3 + \beta Y^4Z + \beta Y^2Z^3).$$

For the Jacobian determinant of $\{f_1, f_2, f_3\}$ we get $\det(J(f_1, f_2, f_3)) = \beta \cdot f_2^2 \neq 0$. Hence by the Jacobian criterion $\{f_1, f_2, f_3\}$ is algebraically independent, and since the f_i have degree product $2 \cdot 5 \cdot 6 = 60 = |G|$, by Kemper's Theorem, see (16.2) below, we conclude that $S^G = K[f_1, f_2, f_3]$ is polynomial with basic invariants $\{f_1, f_2, f_3\}$; hence we have $H_{S^G} = \frac{1}{(1-T^2)(1-T^5)(1-T^6)} \in \mathbb{Q}(T)$.

(The rotation axes of the elements of order 3 give rise to a homogeneous invariant of degree 10, being equal to $f_1^2 f_3 + f_2^2$; the transvection $a \in G$ associated with $[0, 1, 0]$ gives rise to a homogeneous invariant of degree 15, being equal to f_2^3.)

II More commutative algebra

13 Dimension theory

(13.1) Krull dimension. Let R be a commutative ring. Then the **height** $\mathrm{ht}(P) \in \mathbb{N}_0 \,\dot\cup\, \{\infty\}$ of a prime ideal $P \trianglelefteq R$ is defined as the maximum length $r \in \mathbb{N}_0$ of a strictly ascending chain $P_0 \subset P_1 \subset \cdots \subset P_r = P$ of prime ideals

$P_i \trianglelefteq R$. The **(Krull) dimension** $\dim(R) \in \mathbb{N}_0 \,\dot{\cup}\, \{\infty\}$ of R is defined as the maximum height of a prime ideal of R, where $\dim(\{0\}) := -\infty$.

The **height** $\operatorname{ht}(I) \in \mathbb{N}_0 \,\dot{\cup}\, \{\infty\}$ of an ideal $I \lhd R$ is defined as the minimum height of a prime divisor of I, that is the prime ideals of R containing I. for completeness we let $\operatorname{ht}(R) = \infty$. The **(Krull) dimension** of an ideal $I \trianglelefteq R$ is defined as $\dim(I) := \dim(R/I)$.

Example. If R is not Noetherian, there are straightforward examples having infinite dimension: Let K be a field, and let $R := K[X_1, X_2, \ldots]$ be the polynomial algebra in countably infinitely many indeterminates. Then letting $P_i := (X_1, \ldots, X_i) \trianglelefteq R$, for $i \in \mathbb{N}_0$, yields an infinite strictly ascending chain $\{0\} = P_0 \subset P_1 \subset \cdots \trianglelefteq R$ of ideals, which since $R/P_i \cong K[X_{i+1}, X_{2+1}, \ldots]$ are all prime ideals. Hence we have $\dim(R) = \infty$.

Similarly, letting $R := K[X_1, \ldots, X_n]$ where $n \in \mathbb{N}_0$, and $P_i := (X_1, \ldots, X_i) \trianglelefteq R$, for $i \in \{0, \ldots, n\}$, yields a strictly ascending chain $\{0\} = P_0 \subset P_1 \subset \cdots \subset P_n \trianglelefteq R$, which since $R/P_i \cong K[X_{i+1}, \ldots, X_n]$ are all prime ideals. Hence we have $\operatorname{ht}(P_i) \geq i$, so that $\operatorname{ht}(P_n) \geq n$ implies that $\dim(R) \geq n$; actually it is surprisingly difficult to prove that $\dim(R) = n$, see Theorem (14.2).

Actually, even a Noetherian K-algebra may have infinite dimension; an example given by Nagata [1962] is given in Exercise (19.16). Despite this, by Krull's Principal Ideal Theorem shown in (13.7) below, whenever R is Noetherian and $I \lhd R$ is a proper ideal we have $\operatorname{ht}(I) < \infty$; and for the above examples we indeed have $\operatorname{ht}(P_i) \leq i$, so that equality holds.

(13.2) Lemma: Prime avoidance. Let R be a commutative ring, and let $P_1, \ldots, P_n \trianglelefteq R$ be prime ideals, for $n \in \mathbb{N}$, and let $I \trianglelefteq R$ be an ideal such that $I \subseteq \bigcup_{i=1}^n P_i$. Then there is $i \in \{1, \ldots, n\}$ such that $I \subseteq P_i$.

Proof. We proceed by induction on $n \in \mathbb{N}$; the case $n = 1$ being trivial, let $n \geq 2$, and assume that there does not exist an i such that $I \subseteq P_i$. Thus by induction we may assume that for all $j \in \{1, \ldots, n\}$ there is $f_j \in I \setminus \bigcup_{i \neq j} P_i$. Hence we have $f_j \in P_j$, thus since $P_n \trianglelefteq R$ is prime we infer that $\prod_{j=1}^{n-1} f_j \in (\bigcap_{i=1}^{n-1} P_i) \setminus P_n$ and $f_n \in P_n \setminus \bigcup_{i=1}^{n-1} P_i$. Thus for $f := f_n + \prod_{j=1}^{n-1} f_j \in I$ we have $f \notin P_n$. Moreover, assume that $f \in \bigcup_{i=1}^{n-1} P_i$, then there is $i \in \{1, \ldots, n-1\}$ such that $f \in P_i$, since $\prod_{j=1}^{n-1} f_j \in P_i$ entailing $f_n \in P_i$, a contradiction. Hence we have $f \notin \bigcup_{i=1}^{n-1} P_i$ as well, so that $f \in I \setminus \bigcup_{i=1}^n P_i$, a contradiction. ♯

(13.3) Localization. a) Let R be a commutative ring. A subset $U \subseteq R$ is called **multiplicatively closed**, if $1 \in U$ and $fg \in U$ whenever $f, g \in U$.

Letting M be an R-module, let $\sim$ denote the equivalence relation on $M \times U$ given by $[m, u] \sim [m', u']$, for $m, m' \in M$ and $u, u' \in U$, if there is $v \in U$ such that $(mu' - m'u)v = 0 \in M$. Then the **localization** of M at U is defined as the set of equivalence classes $M_U := (M \times U)/_\sim$; the equivalence class of $[m, u] \in M \times U$ being denoted by $\frac{m}{u} \in M_U$.

b) We collect a few basic properties of localizations of ideals of R, in particular of prime ideals; see Exercise (19.7): The localization R_U becomes a commutative ring, such that the natural map $\nu = \nu_U : R \to R_U : f \mapsto \frac{f}{1}$ is a homomorphism of rings. For an ideal $J \trianglelefteq R_U$ we have $(\nu^{-1}(J))_U = J$, hence the **contraction** map $\nu^{-1} : \{J \trianglelefteq R_U\} \to \{I \trianglelefteq R\}$ is an inclusion-preserving and intersection-preserving injection, mapping prime ideals to prime ideals. In particular, if R is Noetherian, then R_U is Noetherian as well.

For an ideal $I \trianglelefteq R$ we have $I \subseteq \nu^{-1}(I_U) = \{f \in R; fu \in I \text{ for some } u \in U\} \trianglelefteq R$. Hence for the **extended** ideal I_U we have $I_U \neq R_U$ if and only if $I \cap U = \emptyset$. For a prime ideal $P \trianglelefteq R$ we have $P = \nu^{-1}(P_U)$ if and only if $P \cap U = \emptyset$; in this case $P_U \trianglelefteq R_U$ is a prime ideal as well. Hence extension and contraction are mutually inverse bijections between $\{P \trianglelefteq R \text{ prime}; P \cap U = \emptyset\}$ and $\{Q \trianglelefteq R_U \text{ prime}\}$.

In particular, if $P \trianglelefteq R$ is a prime ideal, then the set $R \setminus P \subseteq R$ is multiplicatively closed, and $R_{R\setminus P}$ is a **local** ring, that is $R_{R\setminus P}$ has a unique maximal ideal, namely $P_{R\setminus P} \trianglelefteq R_{R\setminus P}$. Moreover, the prime ideals of $R_{R\setminus P}$ are given as the extensions $Q_{R\setminus P} \trianglelefteq R_{R\setminus P}$ of the prime ideals $Q \trianglelefteq R$ such that $Q \subseteq P$; in particular we have $\mathrm{ht}(P) = \dim(R_{R\setminus P})$.

(13.4) Radicals. a) Let R be a commutative ring, and let $I \trianglelefteq R$ be an ideal. Then $\sqrt{I} := \{f \in R; f^n \in I \text{ for some } n \in \mathbb{N}\} \trianglelefteq R$ is called the **radical** of I; note that $I \subseteq \sqrt{I}$. In particular, the **nilradical** $\mathrm{nil}(R) := \sqrt{\{0\}} \trianglelefteq R$ is the set of **nilpotent** elements of R; if $\mathrm{nil}(R) = \{0\}$ then R is called **reduced**.

Proposition. We have $\sqrt{I} = \bigcap\{I \subseteq P \trianglelefteq R; P \text{ prime}\}$; where we let the empty intersection being R. In particular, we have $\mathrm{nil}(R) = \bigcap\{P \trianglelefteq R; P \text{ prime}\}$.

Proof. We may assume that $I \neq R$, let $f \in \sqrt{I}$, and let $P \in \mathcal{P} := \{I \subseteq P \trianglelefteq R; P \text{ prime}\}$; then $f^n \in I \subseteq P$ for some $n \in \mathbb{N}$, thus $f \in P$, hence $f \in \bigcap \mathcal{P}$.

Conversely, let $f \notin \sqrt{I}$. Then consider the multiplicatively closed set $U := \{f^n; n \in \mathbb{N}_0\} \subseteq R$, and let $\mathcal{J} := \{I \subseteq J \trianglelefteq R; J \cap U = \emptyset\}$. Since $I \cap U = \emptyset$ we have $I \in \mathcal{J} \neq \emptyset$, and since any chain in $\mathcal{J}$ has a least upper bound in $\mathcal{J}$ by Zorn's Lemma there is a maximal element $J \in \mathcal{J}$.

Since $J \cap U = \emptyset$ we have $J_U \neq R_U$. Since for any proper ideal $\tilde{J} \lhd R_U$ we have $\nu^{-1}(\tilde{J}) \cap U = \emptyset$, and the contraction map is injective, by maximality we conclude that $J_U \trianglelefteq R_U$ is a maximal ideal, thus is a prime ideal. Hence $\nu^{-1}(J_U) \trianglelefteq R$ is a prime ideal as well, and since $J \subseteq \nu^{-1}(J_U)$ by maximality we get $J = \nu^{-1}(J_U) \in \mathcal{P}$. Thus $f \notin J$ implies $f \notin \bigcap \mathcal{P}$. ♯

b) The **Jacobson radical** of R is defined as $\mathrm{rad}(R) := \bigcap\{J \trianglelefteq R; J \text{ maximal}\}$; where we let the empty intersection being R. Recall that for $R \neq \{0\}$ by Zorn's Lemma there is a maximal ideal of R.

In particular, if $f \in R$ such that $f \equiv 1 \pmod{\operatorname{rad}(R)}$, then $f \equiv 1 \pmod{J}$ for any maximal ideal $J \trianglelefteq R$, hence we infer $(f) = R$, that is $f \in R^*$.

Proposition: Nakayama Lemma [Nakayama, Azumaya, Krull]**.** Let $I \trianglelefteq R$ such that $I \subseteq \operatorname{rad}(R)$, let M be a finitely generated R-module, and let $N \leq M$ be an R-submodule. Then we have $M = N$ if and only if $M = N + MI$.

Proof. We may assume that $M = N + MI$, and hence $M = N + MJ$, where $J := \operatorname{rad}(R) \trianglelefteq R$. Then we have $(M/N) \cdot J = (MJ + N)/N = M/N$. Hence it suffices to show that $MJ = M$ implies $M = \{0\}$; then we have $M/N = \{0\}$:

Hence assume that $MJ = M$. Let $\{m_1, \ldots, m_r\} \subseteq M$, for some $r \in \mathbb{N}$, be an R-module generating set. Then there are $a_{ij} \in J$ such that $m_j = \sum_{i=1}^r m_i a_{ij} \in M$. Letting $A := E_r - [a_{ij}]_{ij} \in R^{r \times r}$ we have $[m_1, \ldots, m_r] \cdot A = 0 \in M^r$, implying $[m_1, \ldots, m_r] \cdot \det(A) = [m_1, \ldots, m_r] \cdot A \cdot \operatorname{adj}(A) = 0 \in M^r$. From $\det(A) \equiv 1 \pmod{J}$ we infer that $\det(A) \in R^*$, so that $[m_1, \ldots, m_r] = 0 \in R^r$. ♯

In other words (comparing with the wording of the graded Nakayama Lemma), letting $\overline{}\colon M \to M/MI =: \overline{M}$ be the natural epimorphism of R-modules, then a subset $\mathcal{S} \subseteq M$ generates M, if and only if $\overline{\mathcal{S}} \subseteq \overline{M}$ generates $\overline{M}$, as R-modules.

(13.5) Theorem: [Krull, 1937; Cohen, Seidenberg, 1946]**.** Let $R \subseteq S$ be an integral extension of commutative rings.
a) Let $P \trianglelefteq R$ be a prime ideal, and let $J \trianglelefteq S$ is an ideal such that $J \cap R \subseteq P$. Then there is a prime ideal $Q \trianglelefteq S$ **going up** from J, that is $J \subseteq Q$, and **lying over** P, that is $Q \cap R = P$.
b) Let $Q \neq Q' \trianglelefteq S$ be prime ideals such that $Q \cap R = Q' \cap R$, that is both lying over the same prime ideal of R. Then we have **incomparability** $Q \not\subseteq Q' \not\subseteq Q$.

Proof. a) By going over to the integral extension $R/(J \cap R) \subseteq S/J$ we may assume that $J = \{0\}$, hence we have to show the existence of a prime ideal $Q \trianglelefteq S$ such that $Q \cap R = P$. By going over to the integral extension $R_{R \setminus P} \subseteq S_{R \setminus P}$, and noting that the ideal $Q \trianglelefteq S$ we are looking for fulfills $Q \cap (R \setminus P) = (Q \cap R) \setminus P = \emptyset$, we may assume that R is local with maximal ideal P.

Assume that $PS = S$. Then let $1 = \sum_{i=1}^r p_i s_i \in S$, for some $r \in \mathbb{N}$, where $p_i \in P$ and $s_i \in S$, and let $\{0\} \neq T \subseteq S$ be the R-subalgebra generated by $\{s_1, \ldots, s_r\}$. Hence T is a finitely generated R-algebra, and integral over R, thus it is a finitely generated R-module. We have $PT = T$, where $P = \operatorname{rad}(R)$, hence the Nakayama Lemma implies $T = \{0\}$, a contradiction.

Thus $PS \triangleleft S$ is a proper ideal. Hence by Zorn's Lemma there is a maximal ideal $PS \subseteq Q \triangleleft S$. Since $P \subseteq Q \cap R \triangleleft R$, and $P \trianglelefteq R$ is maximal, we have $P = Q \cap R$.

b) Assume to the contrary that $Q \subseteq Q'$. By going over to the integral extension $R/(Q \cap R) \subseteq S/Q$, we may assume that $Q \cap R = Q' \cap R = \{0\}$. By going over to the integral extension $R \cong (R+Q)/Q \subseteq S/Q$, we may assume that $Q = \{0\}$, so that $R \subseteq S$ is an integral extension of domains and $\{0\} \neq Q' \trianglelefteq S$ is prime.

Let $0 \neq s \in Q'$, and let $f = \sum_{i=0}^{d} f_i X^i \in R[X]$ be monic such that $d \geq 1$ and $f(s) = 0 \in S$. Since S is a domain, we may assume that $f_0 \neq 0 \in R$. Hence we have $f_0 \in (s) \cap R \subseteq Q' \cap R = \{0\}$, a contradiction. $\sharp$

Actually, the above theorem has been proven by KRULL for the case of domains, while COHEN, SEIDENBERG generalized it by allowing for zero-divisors.

Corollary. Let $J \trianglelefteq S$ be an ideal, and let $I := J \cap R \trianglelefteq R$. Then we have $\dim(R/I) = \dim(S/J)$. In particular, we have $\dim(R) = \dim(S)$.

Proof. Let $I \subseteq P_0 \subset \cdots \subset P_r \trianglelefteq R$ be a strictly ascending chain of prime ideals $P_i \trianglelefteq R$, where $r \in \mathbb{N}_0$. By going up and lying over, there is a chain $J \subseteq Q_0 \subseteq \cdots \subseteq Q_r \trianglelefteq S$ of prime ideals $Q_i \trianglelefteq S$, such that $Q_i \cap R = P_i$ for $i \in \{0, \ldots, r\}$. Hence the latter chain is strictly ascending, and we have $\dim(R/I) \leq \dim(S/J)$.

Conversely, let $J \subseteq Q_0 \subset \cdots \subset Q_r \trianglelefteq S$ be a strictly ascending chain of prime ideals $Q_i \trianglelefteq S$, where $r \in \mathbb{N}_0$. Then by incomparability the chain $I = J \cap R \subseteq (Q_0 \cap R) \subseteq \cdots \subseteq (Q_r \cap R) \trianglelefteq R$ of prime ideals $Q_i \cap R \trianglelefteq R$, for $i \in \{0, \ldots, r\}$, is strictly ascending. Hence we have $\dim(R/I) \geq \dim(S/J)$. $\sharp$

(13.6) Ideals associated with a module. We set out to study the relationship between the prime ideals of a (Noetherian) commutative ring, and its action on modules. Actually this is merely the beginning of a long story, related to the notion of **primary decomposition**, which has first been examined by LASKER [1905], but whose modern description is original work by NOETHER [1921].

a) Let R be a commutative ring, and let M be an R-module. Given $m \in M$, we have a natural homomorphism $R \to M \colon f \mapsto mf$ of R-modules, with image $mR \leq M$, and kernel $\mathrm{ann}_R(m) := \{f \in R; mf = 0\} \trianglelefteq R$, being called the associated **annihilator**.

For $\mathcal{S} \subseteq M$ we let $\mathrm{ann}_R(\mathcal{S}) := \bigcap_{m \in \mathcal{S}} \mathrm{ann}_R(m) \trianglelefteq R$, where $\mathrm{ann}_R(\emptyset) := R$. In particular, the **dimension** of M is defined as $\dim(M) := \dim(R/\mathrm{ann}_R(M))$.

b) An element $0 \neq f \in R$ is called a **zero-divisor** on M, if there is $0 \neq m \in M$ such that $f \in \mathrm{ann}_R(m)$. A prime ideal $P \trianglelefteq R$ is called **associated** with M, if there is $0 \neq m \in M$ such that $\mathrm{ann}_R(m) = P$; in particular we have $\mathrm{ann}_R(M) \subseteq P$. Let $\mathrm{ass}_R(M)$ be the set of prime ideals associated with M, whose minimal elements are also called **isolated**; in particular we have $\mathrm{ass}_R(\{0\}) = \emptyset$.

We have $P \in \mathrm{ass}_R(M)$ if and only if $R/P \cong mR \leq M$, for some $0 \neq m \in M$, which holds if and only if R/P is isomorphic to an R-submodule of M. In this case, for any $0 \neq u \in mR$, letting $f \in R \setminus P$ such that $u = mf$, since P is prime we have $\mathrm{ann}_R(u) = \mathrm{ann}_R(mf) = \{g \in R; mfg = 0\} = \{g \in R; fg \in P\} = P$.

Let $I \trianglelefteq R$ be an ideal; we have $\mathrm{ann}_R(R/I) = \mathrm{ann}_R(1 + I) = I$. Then the prime ideals **associated** with I are defined as $\mathrm{ass}(I) := \mathrm{ass}_R(R/I)$. In particular we have $\mathrm{ass}(R) = \mathrm{ass}_R(R/R) = \mathrm{ass}_R(\{0\}) = \emptyset$; and if $P \trianglelefteq R$ is a prime ideal, then we have $\mathrm{ann}_R(f+P) = P$ whenever $f \in R \setminus P$, hence $\mathrm{ass}(P) = \mathrm{ass}_R(R/P) = \{P\}$.

Theorem. Let R be Noetherian, and let $M \neq \{0\}$ be finitely generated.
a) Then $\mathrm{ass}_R(M)$ is a finite non-empty set, whose minimal elements are the minimal prime divisors of $\mathrm{ann}_R(M) \trianglelefteq R$, and $(\bigcup_{P \in \mathrm{ass}_R(M)} P) \setminus \{0\} \subseteq R$ is the set of zero-divisors on M.
b) If R is a graded K-algebra, where K is a field, and M is graded, then $\mathrm{ass}_R(M)$ consists of homogeneous ideals.

Proof. a) i) Let $0 \neq m \in M$ such that $\mathrm{ann}_R(m) \trianglelefteq R$ is maximal amongst the (proper) ideals $\{\mathrm{ann}_R(u) \trianglelefteq R; 0 \neq u \in M\} \trianglelefteq R$, and let $f, g \in R$ such that $fg \in \mathrm{ann}_R(m)$ and $g \notin \mathrm{ann}_R(m)$. Since $\mathrm{ann}_R(m) \subseteq \mathrm{ann}_R(mg)$ we infer $f \in \mathrm{ann}_R(mg) = \mathrm{ann}_R(m)$; thus $\mathrm{ann}_R(m) \trianglelefteq R$ is a prime ideal, hence $\mathrm{ass}_R(M) \neq \emptyset$.

Moreover, by construction $P \setminus \{0\}$ consists of zero-divisors on M, for any $P \in \mathrm{ass}_R(M)$. Conversely, if $f \in \mathrm{ann}_R(u)$ for some $0 \neq u \in M$, then by the above argument there is $0 \neq m \in M$ such that $\mathrm{ann}_R(u) \subseteq \mathrm{ann}_R(m) \trianglelefteq R$ is maximal amongst all annihilators, hence $f \in \mathrm{ann}_R(m) \in \mathrm{ass}_R(M)$.

ii) Next we show that for any R-submodule $N \leq M$ we have $\mathrm{ass}_R(M) \subseteq \mathrm{ass}_R(N) \cup \mathrm{ass}_R(M/N)$: Let $P \in \mathrm{ass}_R(M)$, and let $R/P \cong U \leq M$. If $U \cap N = \{0\}$, then we have $R/P \cong (U+N)/N \leq M/N$, and thus $P \in \mathrm{ass}_R(M/N)$; if $0 \neq m \in U \cap N$, then we have $\mathrm{ann}_R(m) = P \in \mathrm{ass}_R(N)$.

In order to show that $\mathrm{ass}_R(M)$ is finite, we choose $P_1 \in \mathrm{ass}_R(M)$ and let $\{0\} \neq M_1 \leq M$ such that $M_1 \cong R/P_1$, hence we have $\mathrm{ass}_R(M_1) = \{P_1\}$. If $M_1 \leq M$, we choose $P_2 \in \mathrm{ass}_R(M/M_1)$, and let $M_1 < M_2 \leq M$ such that $M_2/M_1 \cong R/P_2$, hence we have $\mathrm{ass}_R(M_2/M_1) = \{P_2\}$. This successively yields a strictly ascending chain $\{0\} = M_0 < M_1 < M_2 < \cdots \leq M$. Since M is Noetherian, we have $M_r = M$ for some $r \in \mathbb{N}$, so that $\mathrm{ass}_R(M) \subseteq \{P_1, \ldots, P_r\}$.

iii) Let $P \trianglelefteq R$ be a prime ideal. First, we show that we have $\mathrm{ann}_R(M)_{R \setminus P} = \mathrm{ann}_{R_{R\setminus P}}(M_{R\setminus P})$: For $f \in \mathrm{ann}_R(M)$ we have $Mf = 0 \in M_{R\setminus P}$, hence we conclude that $\mathrm{ann}_R(M)_{R\setminus P} \subseteq \mathrm{ann}_{R_{R\setminus P}}(M_{R\setminus P})$.

Conversely, let $f \in \nu^{-1}(\mathrm{ann}_{R_{R\setminus P}}(M_{R\setminus P}))$. Then for any $m \in M$ we have $mf \cdot v_m = 0$, for some $v_m \in R \setminus P$. Thus since M is finitely generated there is $v \in R \setminus P$ such that $Mfv = \{0\}$, that is $fv \in \mathrm{ann}_R(M)$, implying that $f \in \mathrm{ann}_R(M)_{R\setminus P}$. Thus we have $\mathrm{ann}_{R_{R\setminus P}}(M_{R\setminus P}) \subseteq \mathrm{ann}_R(M)_{R\setminus P}$ as well. ♯

Next we show that $P \in \mathrm{ass}_R(M)$ if and only if $P_{R\setminus P} \in \mathrm{ass}_{R_{R\setminus P}}(M_{R\setminus P})$: Let $0 \neq m \in M$ such that $P = \mathrm{ann}_R(m)$; hence $\mathrm{ann}_{R_{R\setminus P}}(m) = \{f \in R; mfv = 0 \text{ for some } v \in R \setminus P\}_{R\setminus P} = \bigcup_{v \in R\setminus P}(\mathrm{ann}_R(mv)_{R\setminus P}) = \mathrm{ann}_R(m)_{R\setminus P} = P_{R\setminus P}$.

Conversely, let $0 \neq \frac{m}{u} \in M_{R\setminus P}$ such that $P_{R\setminus P} = \mathrm{ann}_{R_{R\setminus P}}(\frac{m}{u}) = \mathrm{ann}_{R_{R\setminus P}}(m)$, hence we have $\mathrm{ann}_R(m) \subseteq \nu^{-1}(\mathrm{ann}_{R_{R\setminus P}}(m)) = \nu^{-1}(P_{R\setminus P}) = P$, where we may assume that $0 \neq m \in M$ is chosen such that $\mathrm{ann}_R(m)$ is maximal amongst the (proper) ideals $\{\mathrm{ann}_R(mv) \trianglelefteq R; v \in R \setminus P\}$; then for $f \in P$ we have $mf = 0 \in$

$M_{R\setminus P}$, hence $mfv = 0 \in M$ for some $v \in R\setminus P$, thus $f \in \mathrm{ann}_R(mv) = \mathrm{ann}_R(m)$, entailing $P \subseteq \mathrm{ann}_R(m)$, hence $P = \mathrm{ann}_R(m)$. ♯

Finally, we show that all the minimal prime divisors $P \trianglelefteq R$ of $\mathrm{ann}_R(M)$ are actually associated with M: For such a prime ideal we conclude that $P_{R\setminus P} \trianglelefteq R_{R\setminus P}$ is a minimal prime divisor of $\mathrm{ann}_R(M)_{R\setminus P} \trianglelefteq R_{R\setminus P}$, and hence is its unique prime divisor. Since $\mathrm{ann}_R(M)_{R\setminus P} = \mathrm{ann}_{R_{R\setminus P}}(M_{R\setminus P})$, we infer that $M_{R\setminus P} \neq \{0\}$ and that $\mathrm{ass}_{R_{R\setminus P}}(M_{R\setminus P}) = \{P_{R\setminus P}\}$, entailing that $P \in \mathrm{ass}_R(M)$.

b) Let $0 \neq m = \sum_{i=1}^r m_i \in M$, where $r \in \mathbb{N}$ and $m_i \in M_{d_i}$, where $d_i \in \mathbb{Z}$ such that $d_1 < \cdots < d_r$. We show that if $\mathrm{ann}_R(m) \trianglelefteq R$ is a prime ideal, then it is homogeneous: Let $0 \neq f = \sum_{j=1}^s f_j \in \mathrm{ann}_R(m)$, where $s \in \mathbb{N}$ and $f_j \in R_{e_j}$, where $0 \leq e_1 < \cdots < e_s$. We proceed by induction on $r \in \mathbb{N}$: Let $r = 1$; then from $mf = m_1 f = 0$ we get $mf_j = 0$, hence $f_j \in \mathrm{ann}_R(m)$ for all j.

Let $r \geq 2$; we show that $f_1 \in \mathrm{ann}_R(m)$, and then proceed by induction on $s \in \mathbb{N}$: We have $m_1 f_1 = 0$, and thus $\mathrm{ann}_R(m) \subseteq \mathrm{ann}_R(mf_1) = \mathrm{ann}_R(\sum_{i=2}^r m_i f_1)$. If $\mathrm{ann}_R(m) = \mathrm{ann}_R(mf_1)$, then the latter is a prime ideal, hence by induction is homogeneous, so that $f_1 \in \mathrm{ann}_R(m)$; if $\mathrm{ann}_R(m) \neq \mathrm{ann}_R(mf_1)$, then letting $g \in \mathrm{ann}_R(mf_1) \setminus \mathrm{ann}_R(m)$ we get $f_1 g \in \mathrm{ann}_R(m)$, hence $f_1 \in \mathrm{ann}_R(m)$. ♯

Corollary. Let R be Noetherian.
a) Then any ideal $I \trianglelefteq R$ has only finitely many minimal prime divisors.
b) If R is a graded K-algebra, where K is a field, and $I \trianglelefteq R$ is homogeneous, then the minimal prime divisors of I are homogeneous as well.

(13.7) Theorem: Krull's Principal Ideal Theorem [Krull 1928]**.** Let R be a Noetherian commutative ring, let $I := (f_1, \ldots, f_r) \trianglelefteq R$ where $r \in \mathbb{N}$, and let $P \trianglelefteq R$ be a minimal prime divisor of I. Then we have $\mathrm{ht}(P) \leq r$.

Proof. By going over to $R_{R\setminus P}$ we may assume that R is local with maximal ideal P. Let $\overline{}\colon R \to R/I =: \overline{R}$ be the natural epimorphism. Since P is a minimal prime divisor of I, it is the unique one. Hence we have $\mathrm{nil}(\overline{R}) = \overline{P}$, and since P is finitely generated there is $n \in \mathbb{N}$ such that $\overline{P}^n = \{0\}$. Thus we have the chain of R-submodules $\overline{R} \supseteq \overline{P} \supseteq \overline{P}^2 \supseteq \cdots \supseteq \overline{P}^{n-1} \supseteq \overline{P}^n = \{0\}$, whose subquotients are finitely generated R/P-vector spaces. By refining, there is a finite chain of R-submodules whose subquotients are one-dimensional R/P-vector spaces, thus being a finite R-module composition series of $\overline{R}$. Now we proceed by induction on $r \in \mathbb{N}$:

i) Let $r = 1$; we show that for any prime ideal $Q \trianglelefteq R$ such that $Q \subset P$ (if there is any at all) we have $\mathrm{ht}(Q) = 0$; this implies $\mathrm{ht}(P) \leq 1$:

Let $\nu\colon R \to R_{R\setminus Q}$, and for $i \in \mathbb{N}_0$ let the i-th **symbolic power** of Q be the contracted ideal $Q^{(i)} := \nu^{-1}(Q^i_{R\setminus Q}) = \{g \in R; gu \in Q^i \text{ for some } u \in R\setminus Q\} \trianglelefteq R$. Since by the Jordan-Hölder Theorem each finite chain of R-submodules of $\overline{R}$

can be refined to a finite composition series, we conclude that the chain of R-submodules $\overline{R} \supseteq \overline{Q} = \overline{Q^{(1)}} \supseteq \overline{Q^{(2)}} \supseteq \cdots$ stabilizes. Hence letting $m \in \mathbb{N}_0$ such that $\overline{Q^{(m)}} = \overline{Q^{(m+1)}}$, we show that $Q^{(m)} = Q^{(m+1)} + Q^{(m)}I$: Indeed, for $g \in Q^{(m)}$ by assumption there are $g' \in Q^{(m+1)}$ and $h \in R$ such that $g = g' + hf_1$, hence $hf_1 \in Q^{(m)}$; and since $f_1 \in R \setminus Q$ we infer that actually $h \in Q^{(m)}$.

Since $I \subseteq P = \mathrm{rad}(R)$, the Nakayama Lemma implies $Q^{(m)} = Q^{(m+1)}$. This yields $Q^m_{R\setminus Q} = (Q^{(m)})_{R\setminus Q} = (Q^{(m+1)})_{R\setminus Q} = Q^{m+1}_{R\setminus Q} = Q^m_{R\setminus Q} \cdot Q_{R\setminus Q}$. Since $R_{R\setminus Q}$ is local with maximal ideal $\mathrm{rad}(R_{R\setminus Q}) = Q_{R\setminus Q}$, the Nakayama Lemma again implies $Q^m_{R\setminus Q} = \{0\}$. Hence we have $Q_{R\setminus Q} \subseteq \mathrm{nil}(R_{R\setminus Q})$, thus the maximal ideal $Q_{R\setminus Q}$ is the unique prime ideal of $R_{R\setminus Q}$, hence $\mathrm{ht}(Q) = \dim(R_{R\setminus Q}) = 0$.

ii) Now let $r \geq 2$, and let $Q \trianglelefteq R$ be maximal amongst the prime ideals of R being properly contained in P. Hence we have $I \not\subseteq Q$, thus we may assume that $f_r \notin Q$. Hence P is a minimal prime divisor of $J := Q + (f_r) \trianglelefteq R$, thus it is the unique one, hence we have $P/J = \mathrm{nil}(R/J) \trianglelefteq R/J$.

In particular, there are $m_i \in \mathbb{N}$, and $g_i \in Q$, and $h_i \in R$ such that $f_i^{m_i} = g_i + f_r h_i$, for $i \in \{1, \ldots, r-1\}$. We show that $Q \trianglelefteq R$ is minimal prime divisor of $I' := (g_1, \ldots, g_{r-1}) \trianglelefteq R$; then by induction $\mathrm{ht}(Q) \leq r-1$, thus $\mathrm{ht}(P) \leq r$:

Let $J' := I' + (f_r) \trianglelefteq R$. Since $P^n \subseteq I$, and $f_i^{m_i} \in J'$ for $i \in \{1, \ldots, r-1\}$, there is $m \in \mathbb{N}$ such that $P^m \subseteq J'$. Hence $P/J' \subseteq \mathrm{nil}(R/J')$, thus the maximal ideal P/J' is the unique prime ideal of R/J' . Hence $P/I' \trianglelefteq R/I'$ is a minimal prime divisor of J'/I' (actually the unique one), and since $J' = I' + (f_r)$ by part (i) we conclude that $\mathrm{ht}(P/I') \leq 1$. Hence $I' \subseteq Q \subset P$ implies $\mathrm{ht}(Q/I') = 0$. ♯

14 Noether normalization

(14.1) Lemma. Let K be a field, let $R := K[\mathcal{X}] = K[X_1, \ldots, X_n]$ where $n \in \mathbb{N}$, and let $0 \neq f \in R \setminus R^*$. Then there is $\mathcal{Y} := \{Y_1, \ldots, Y_{n-1}\} \subseteq R$ such that $\mathcal{Y} \,\dot{\cup}\, \{f\}$ is algebraically independent and $S := K[\mathcal{Y}, f] \subseteq R$ is finite.

i) We may choose $e \in \mathbb{N}$ such that $Y_i = X_i - (X_n)^{e^i}$, for $i \in \{1, \ldots, n-1\}$.
ii) If K is infinite, then we may choose $a_i \in K$ such that $Y_i = X_i - a_i X_n$.
iii) If f is homogeneous, then we may choose the Y_i homogeneous as well.

Proof. i) Assume that $\mathcal{Y} \,\dot{\cup}\, \{f\} \subseteq R$ such that $S \subseteq R$ is finite. Then $K(\mathcal{Y}, f) \subseteq K(\mathcal{X})$ is a finite field extension, hence algebraic. Thus we conclude that $n = \mathrm{trdeg}_K(K(\mathcal{X})) = \mathrm{trdeg}_K(K(\mathcal{Y}, f))$, hence $\mathcal{Y} \,\dot{\cup}\, \{f\}$ is algebraically independent. Thus it remains to specify $\mathcal{Y} \subseteq R$ suitably such that $S \subseteq R$ is finite:

Let $e \in \mathbb{N}$ be strictly greater than any part of any combination α associated with any monomial $\mathcal{X}^\alpha$ occurring in f. Letting $Y_i := X_i - X_n^{e^i}$, for $i \in \{1, \ldots, n-1\}$, and $\mathcal{Y} := \{Y_1, \ldots, Y_{n-1}\}$, we have $S := K[\mathcal{Y}, f] \subseteq S[X_n] = K[\mathcal{Y}, X_n] = R$, thus R is a finitely generated S algebra; we show that X_n is integral over S:

We have $\mathcal{X}^\alpha = X_n^{\alpha_n} \cdot \prod_{i=1}^{n-1} (Y_i + X_n^{e^i})^{\alpha_i}$, and expanding with respect to X_n we observe that $\mathcal{X}^\alpha$ is monic of degree $d_\alpha = \sum_{i=0}^{n-1} \alpha_i e^i$ with respect to X_n, where $\alpha_0 := \alpha_n$. If $\mathcal{X}^\alpha$ occurs in f, then by the choice of e the above sum coincides with the e-adic representation of d_α. Hence the degrees with respect to X_n of the various monomials occurring in f are pairwise distinct. Thus $f \in K[\mathcal{Y}, X_n]$ has positive degree and is monic, with respect to X_n. Hence $g := f(Y_1 + T^e, \ldots, Y_{n-1} + T^{e^{n-1}}, T) - f \in S[T]$ has positive degree and is monic, with respect to T, such that $g(X_n) = 0$. $\sharp$

ii) Now assume that K is infinite. Let $f = \sum_{j=0}^d f_j \in K[\mathcal{X}]$, where the f_j are homogeneous of degree j, and $d := \deg(f) \geq 1$. Letting $Y_i = X_i - a_i X_n$, for $a_i \in K$ and $i \in \{1, \ldots, n-1\}$, and $\mathcal{Y} := \{Y_1, \ldots, Y_{n-1}\}$, we have $S := K[\mathcal{Y}, f] \subseteq S[X_n] = K[\mathcal{Y}, X_n] = R$, thus R is a finitely generated S algebra; we show that the a_i can be specified suitably such that X_n is integral over S:

Writing $f_j = f(Y_1 + a_1 X_n, \ldots, Y_{n-1} + a_{n-1} X_n, X_n) \in K[\mathcal{Y}, X_n]$, we observe that f_j is homogeneous of degree j, and expanding with respect to X_n shows that f_j has degree j and leading coefficient $f_j(a_1, \ldots, a_{n-1}, 1) \in K$. In particular, since $f_d \neq 0$ and K is infinite, there are $a_1, \ldots, a_{n-1} \in K$ such that $a := f_d(a_1, \ldots, a_{n-1}, 1) \in K^*$; note that for $n = 1$ we have $f_d \in K^*$ anyway. Hence $g := f(Y_1 + a_1 T, \ldots, Y_{n-1} + a_{n-1} T, T) - f \in S[T]$ has degree $d \geq 1$ and leading coefficient $a \in S^*$ with respect to T, such that $g(X_n) = 0$. $\sharp$

iii) Finally, assume that f is homogeneous. If K is infinite, then we have just seen that the Y_i can be chosen homogeneous of degree 1. To deal with the case of finite fields, we let K be arbitrary again:

For $i \in \{1, \ldots, n-1\}$ we successively choose $Y_i \in R_+$ homogeneous such that the ideal $I_i := fR + \sum_{j=1}^{i-1} Y_j R \subseteq R_+$ of R has height $\mathrm{ht}(I_i) = i$:

Since R is a domain, by Krull's Principal Ideal Theorem we have $\mathrm{ht}(I_1) = \mathrm{ht}(fR) = 1$. Now let $P_1, \ldots, P_s \subseteq R_+$ be the (homogeneous) minimal prime divisors of I_i, where $s \in \mathbb{N}$. Assume that $\bigcup_{k=1}^s P_k = R_+$; then by prime avoidance we have $R_+ = P_k$ for some k, hence R_+ is a minimal prime divisor of I_i, and thus by Krull's Principal Ideal Theorem we have $\mathrm{ht}(R_+) \leq i$; since $\mathrm{ht}(R_+) = n$ this is a contradiction.

Thus we may choose $Y_i \in R_+ \setminus \bigcup_{k=1}^s P_k$ homogeneous, so that by Krull's Principal Ideal Theorem again we have $i \leq \mathrm{ht}(I_{i+1}) \leq i+1$. Assume that $\mathrm{ht}(I_{i+1}) = i$; then let $Q \trianglelefteq R$ be a minimal prime divisor of I_{i+1} such that $\mathrm{ht}(Q) = i$; since $I_i \subseteq Q$ and $\mathrm{ht}(I_i) = i$, we conclude that Q is a minimal prime divisor of I_i, hence coincides with P_k for some k, thus $Y_i \notin Q$; since $Y_i \in I_{i+1} \subseteq Q$ this a contradiction. Thus we have $\mathrm{ht}(I_{i+1}) = i + 1$, as desired $\sharp$

Hence we have $\mathrm{ht}(I_n) = n$, and since $\mathrm{ht}(R_+) = n$ we conclude that $R_+ \trianglelefteq R$ is a minimal prime divisor of I_n, and thus is its unique prime divisor. As $R_+ \trianglelefteq R$ is finitely generated, we conclude that $R_+/I_n \trianglelefteq R/I_n$ is nilpotent. Hence R/I_n has a finite filtration consisting of finitely generated R/R_+-modules, since $R/R_+ \cong K$ entailing that R/I_n is a finite-dimensional K-vector space. Since $S = K[\mathcal{Y}, f]$ is a graded K-algebra as well, we have $I_n = (f, \mathcal{Y}) = S_+ R \trianglelefteq R$. Thus R/S_+R being finite-dimensional, by the graded Nakayama Lemma we conclude that R is a finitely generated S-module, hence R is finite over S. $\sharp$

(14.2) Theorem. Let K be a field. Then $\dim(K[X_1, \ldots, X_n]) = n$, for $n \in \mathbb{N}_0$.

Proof. We proceed by induction on n; the case $n = 0$ being trivial, we let $n \geq 1$, and let $R := K[X_1, \ldots, X_n]$. We have already seen that $\dim(R) \geq n$. Hence for any strictly ascending chain of prime ideals $\{0\} = P_0 \subset \cdots \subset P_r \trianglelefteq R$, for $r \in \mathbb{N}_0$, we have to show that $r \leq n$:

For $0 \neq f \in P_1$ let $S := K[f, \mathcal{Y}] \subseteq R$ be as in (14.1). Since $S \subseteq R$ is finite, by incomparability we conclude that $\{0\} = S \cap P_0 \subset S \cap P_1 \subset \cdots \subset S \cap P_r$ is a strictly ascending chain of prime ideals of S, yielding the strictly ascending chain of prime ideals $fS = (S \cap P_1) + fS \subset \cdots \subset (S \cap P_r) + fS \trianglelefteq S/fS \cong K[\mathcal{Y}]$. Since by induction we have $\dim(K[\mathcal{Y}]) = n - 1$, we infer $r - 1 \leq n - 1$. $\sharp$

Corollary. Let $R := K[f_1, \ldots, f_n]$ be a finitely generated commutative K-algebra, for $n \in \mathbb{N}_0$. Then $\dim(R) \leq n$, with equality if and only if $\{f_1, \ldots, f_n\}$ is algebraically independent.

Proof. We have $R \cong K[X_1, \ldots, X_n]/I$, for some ideal $I \trianglelefteq K[X_1, \ldots, X_n]$. This shows that $\dim(R) \leq n$. Moreover, if $I = \{0\}$ then equality holds, while for $I \neq \{0\}$ we have $\mathrm{ht}(I) \geq 1$ so that $\dim(R) < n$. $\sharp$

(14.3) Theorem: Noether's Normalization Theorem [Noether, 1926; Zariski, 1943; Nagata, 1962]**.** Let K be a field, let $R := K[f_1, \ldots, f_r]$, for $r \in \mathbb{N}_0$, be a finitely generated commutative K-algebra, let $n := \dim(R) \in \{0, \ldots, r\}$, and let $\{0\} = I_0 \subset I_1 \subset \cdots \subset I_s$, for $s \in \mathbb{N}_0$, be a strictly ascending chain of ideals $I_k \triangleleft R$ such that $n > n_1 > \cdots > n_s \geq 0$, where $n_k := \dim(R/I_k)$.

Then there is $\mathcal{Y} := \{Y_1, \ldots, Y_n\} \subseteq R$ algebraically independent such that $S := K[\mathcal{Y}] \subseteq R$ is finite and $S \cap I_k = (Y_{n_k+1}, \ldots, Y_n) \trianglelefteq S$, for $0 \in \{1, \ldots, s\}$.

i) If K is infinite, we may choose the Y_i as K-linear combinations of $\{f_1, \ldots, f_r\}$.
ii) If R is graded and the ideals $I_1, \ldots, I_s$ are homogeneous, we may choose the Y_i homogeneous as well.

Proof. We may assume that $R \cong K[X_1, \ldots, X_r]/I$, where $I \subset I_1 \subset \cdots \subset I_s \triangleleft K[X_1, \ldots, X_r]$, hence $\dim(K[X_1, \ldots, X_r]/I) = \dim(R) = n > n_1$. Thus we may assume that $R = K[\mathcal{X}] = K[X_1, \ldots, X_n]$. Moreover, we may assume that $s \geq 1$, and hence that I_s is maximal, so that $n_s = 0$.

Now it is sufficient to find $\mathcal{Y} := \{Y_1, \ldots, Y_n\} \subseteq R$ such that R is finite over $S := K[\mathcal{Y}]$ and $\{Y_{n_k+1}, \ldots, Y_n\} \subseteq I_k$, for $k \in \{1, \ldots, s\}$:

Indeed, since $S \subseteq R$ is finite, we conclude that $K(\mathcal{Y}) \subseteq K(\mathcal{X})$ is an algebraic field extension, hence we have $n = \mathrm{trdeg}(K(\mathcal{X})) = \mathrm{trdeg}(K(\mathcal{Y}))$, thus $\mathcal{Y}$ is algebraically independent. Moreover, we have $\dim(S/(S \cap I_k)) = \dim(R/I_k) =$

$n_k = \dim(K[Y_1, \ldots, Y_{n_k}]) = \dim(S/(Y_{n_k+1}, \ldots, Y_n))$, where $(Y_{n_k+1}, \ldots, Y_n) \trianglelefteq S$ is a prime ideal, hence $(Y_{n_k+1}, \ldots, Y_n) = S \cap I_k$. ♯

To do so, we construct the $Y_i \in R$ successively for $i \in \{n, n-1, \ldots, 1\}$, using auxiliary elements $Y_{i,j} \in R$, for $j \leq i$, where we let $Y_{n,j} := X_j$ for $j \in \{1, \ldots, n\}$. Letting $S_i = K[Y_{i,1}, \ldots, Y_{i,i}, Y_{i+1}, \ldots, Y_n]$ be polynomial such that $S_i \subseteq R$ is finite, and $\{Y_{j+1}, \ldots, Y_n\} \subseteq I_k$ where $j := \max\{n_k, i\}$, for $k \in \{1, \ldots, s\}$, we introduce $Y_i, Y_{i-1,1}, \ldots, Y_{i-1,i-1} \in S_i$, retaining the above conditions, and decrease i. Finally, we let $S := S_0$. We proceed as follows:

Given i, let $k \geq 1$ be minimal such that $n_k < i$. Assume that $K[Y_{i,1}, \ldots, Y_{i,i}] \cap I_k = \{0\}$; since $\{Y_{i+1}, \ldots, Y_n\} \subseteq I_k$, computing modulo $(Y_{i+1}, \ldots, Y_n) \trianglelefteq S_i$ shows that any element of $S_i \cap I_k$ has a representative in $K[Y_{i,1}, \ldots, Y_{i,i}]$; thus we infer $(Y_{i+1}, \ldots, Y_n) = S_i \cap I_k \trianglelefteq S_i$, which since $\dim(S_i/(S_i \cap I_k)) = \dim(R/I_k) = n_k < i = \dim(K[Y_{i,1}, \ldots, Y_{i,i}]) = \dim(S_i/(Y_{i+1}, \ldots, Y_n))$ is a contradiction.

Hence let $0 \neq Y_i \in K[Y_{i,1}, \ldots, Y_{i,i}] \cap I_k$; if I_k and the $Y_{i,j}$ are homogeneous, then Y_i may be chosen homogeneous as well. By (14.1) let $\{Y_{i-1,1}, \ldots, Y_{i-1,i-1}\} \subseteq K[Y_{i,1}, \ldots, Y_{i,i}]$ such that $\{Y_{i-1,1}, \ldots, Y_{i-1,i-1}\} \,\dot{\cup}\, \{Y_i\}$ is algebraically independent such that $K[Y_{i-1,1}, \ldots, Y_{i-1,i-1}, Y_i] \subseteq K[Y_{i,1}, \ldots, Y_{i,i}]$ is finite; if Y_i is homogeneous the $Y_{i-1,j}$ may be chosen homogeneous as well, and if K is infinite the $Y_{i-1,j}$ may be chosen as K-linear combinations of $\{Y_{i,1}, \ldots, Y_{i,i}\}$.

Thus letting $S_{i-1} := K[Y_{i-1,1}, \ldots, Y_{i-1,i-1}, Y_i, Y_{i+1}, \ldots, Y_n]$ we conclude that $S_{i-1} \subseteq S_i$ is finite, and since $S_i \subseteq R$ is finite, we infer that $S_{i-1} \subseteq R$ is finite as well. Moreover, we have $\{Y_i, \ldots, Y_n\} \subseteq I_k$ where $i - 1 = \max\{n_k, i-1\}$. ♯

Actually, in proving the above theorem, Noether dealt with infinite fields only, while Zariski treated arbitrary fields, and the refined version, actually involving only a single ideal, was given by Nagata.

(14.4) Theorem. a) Let K be a field, and let R be a finitely generated commutative graded K-algebra. Then for the complexity of R we have $\gamma(R) = \dim(R)$, and if R is a domain then we have $\dim(R) = \mathrm{trdeg}(\mathrm{Q}(R))$.
b) Let M be a finitely generated graded R-module. Then for the complexity of M we have $\gamma(M) = \gamma(R/\mathrm{ann}_R(M)) = \dim(R/\mathrm{ann}_R(M)) = \dim(M)$.

Proof. a) Let $K[\mathcal{Y}] \cong S \subseteq R$ be a Noether normalization, which is a finite extension. Hence we have $\gamma(R) = \gamma(S)$ and $\dim(R) = \dim(S)$, where $\dim(S) = |\mathcal{Y}| = \gamma(S)$. Moreover, if R is a domain, since $\mathrm{Q}(S) \subseteq \mathrm{Q}(R)$ is algebraic, we have $\dim(R) = \dim(S) = |\mathcal{Y}| = \mathrm{trdeg}(\mathrm{Q}(S)) = \mathrm{trdeg}(\mathrm{Q}(R))$.

b) We may assume that $M \neq \{0\}$. Then note first that $\mathrm{ann}_R(M) \lhd R$ is homogeneous, so that $R/\mathrm{ann}_R(M)$ is a finitely generated commutative graded K-algebra indeed. Now, since M is a quotient of a finitely generated free graded $R/\mathrm{ann}_R(M)$-module, we have $\gamma(M) \leq \gamma(R/\mathrm{ann}_R(M)) = \dim(R/\mathrm{ann}_R(M))$.

Conversely, if $P \trianglelefteq R$ is a (homogeneous) minimal prime divisor of $\mathrm{ann}_R(M)$, we have $P \in \mathrm{ass}_R(M)$. Thus there is an R-submodule $N \leq M$ such that

$R/P \cong N$, entailing that $\dim(R/P) = \gamma(R/P) \leq \gamma(M)$. Hence we conclude that $\dim(R/\mathrm{ann}_R(M)) \leq \gamma(M)$ as well, so that we have equality. $\sharp$

(14.5) Homogeneous systems of parameters. a) Let K be a field, let R be a finitely generated commutative graded K-algebra, and let $\{f_1, \ldots, f_n\} \subseteq R$ be homogeneous of positive degree and algebraically independent, such that $K[f_1, \ldots, f_n] \subseteq R$ is finite. Then $\{f_1, \ldots, f_n\}$ is called a **homogeneous system of parameters**, or **h.s.o.p.** for short, of R.

Note that necessarily $n = \dim(K[f_1, \ldots, f_n] = \dim(R) \in \mathbb{N}_0$, and that by Noether normalization homogeneous system of parameters always exist. But the multiset of the degrees of the elements of a homogeneous system of parameters is in general not uniquely defined:

For example, $\{X_1, \ldots, X_n\} \subseteq K[\mathcal{X}] = K[X_1, \ldots, X_n]$ is a homogeneous system of parameters, but $\{X_1^2, X_2, \ldots, X_n\} \subseteq K[\mathcal{X}]$ is algebraically independent such that $K[\mathcal{X}] = 1 \cdot S \oplus X_1 \cdot S$, where $S := K[X_1^2, X_2, \ldots, X_n]$, saying that $\{X_1^2, X_2, \ldots, X_n\}$ is a homogeneous system of parameters as well.

b) Let G be a finite group, and let V be a $K[G]$-module; then we have $n := \dim(S[V]^G) = \gamma(S[V]^G) = \dim_K(V) \in \mathbb{N}_0$. A homogeneous system of parameters $\mathcal{F} := \{f_1, \ldots, f_n\}$ of $S[V]^G$ is called a set of **primary invariants**; note that since $S[V]^G \subseteq S[V]$ is finite $\mathcal{F} \subseteq S[V]^G$ is a homogeneous system of parameters of $S[V]^G$ if and only if $\mathcal{F}$ is a homogeneous system of parameters of $S[V]$. Moreover, a homogeneous generating set $\{g_1, \ldots, g_m\}$ of $S[V]^G$ as $K[f_1, \ldots, f_n]$-module, for $m \in \mathbb{N}$, is called a set of **secondary invariants**.

i) In particular, if $S[V]^G$ is polynomial, then a set of basic invariants is a set of primary invariants, a set of secondary invariants being given by $\{1\}$.

ii) If V is a permutation $K[G]$-module, then $R := K[e_{n,1}, \ldots, e_{n,n}] \subseteq S[V]^G$, where R is polynomial and $R \subseteq S[V]$ is finite, so that the elementary symmetric polynomials $\{e_{n,1}, \ldots, e_{n,n}\}$ form a set of primary invariants of $S[V]^G$, and by Göbel's Theorem the orbit sums of monomials associated with $(n-1)$-special combinations form a (typically non-minimal) set of secondary invariants.

15 Cohen-Macaulay algebras

(15.1) Regular sequences. a) Let K be a field, let R be a finitely generated commutative graded K-algebra, and let $M \neq \{0\}$ be a finitely generated graded R-module. Then a homogeneous element $0 \neq f \in R_+$ is called **regular** or a **non-zerodivisor** on M, if for the associated multiplication map we have $\ker_M(\cdot f) = \{0\}$. In particular, an element of R being regular on the regular R-module R is called **regular**. Note that, by the graded Nakayama Lemma, for any $f \in R_+$ the multiplication map on $M \neq \{0\}$ is not surjective.

Proposition. We have $\dim(M) - 1 \leq \dim(M/Mf) \leq \dim(M)$, where if f is regular on M then we have $\dim(M/Mf) = \dim(M) - 1$.

Proof. We have $\dim(M) = \gamma(M) \in \mathbb{N}_0$; moreover, since $Mf \neq M$ we have $0 \leq \dim(M/Mf) \leq \dim(M)$. From the exact sequence of graded R-modules $\{0\} \to N := \ker_M(\cdot f) \to M \xrightarrow{\cdot f} M \to \operatorname{cok}_M(\cdot f) = M/Mf \to \{0\}$ we obtain $H_{M/Mf} - H_M + T^{\deg(f)}(H_M - H_N) = 0$, that is $H_M = \frac{H_{M/Mf} - T^{\deg(f)} H_N}{1 - T^{\deg(f)}} \in \mathbb{Q}(T)$; see also the proof of (6.1). Hence we have $\gamma(M) \leq \gamma(M/Mf) + 1$; moreover, if f is regular on M, then $H_N = 0$ yields $\gamma(M) = \gamma(M/Mf) + 1$. ♯

In particular, if $\dim(M) = 0$ there cannot possibly be a regular element on M. Alternatively, this can also be seen as follows: If $\gamma(M) = \dim(M) = 0$, then M is a finitely generated K-vector space, so that any injective K-endomorphism of M is surjective as well, so there is no regular element on M.

b) A homogeneous sequence $[f_1, \ldots, f_k] \subseteq R_+$, where $k \in \mathbb{N}_0$, is called **regular** on M, if f_i is regular on $M/M(f_1, \ldots, f_{i-1}) = M/(\sum_{j=1}^{i-1} Mf_j)$, for all $i \in \{1, \ldots, k\}$; in particular we have $M(f_1, \ldots, f_i) \neq M$ for all $i \in \{0, \ldots, k\}$. The **depth** $\operatorname{depth}(M) \in \mathbb{N}_0 \stackrel{.}{\cup} \{\infty\}$ of M is defined as the maximum length of a regular sequence on M.

Indeed, it follows by induction from the above proposition, and $\operatorname{depth}(M) = 0$ if $\dim(M) = 0$, that the length of any regular sequence on M is bounded above by $\dim(M)$, so that we have $\operatorname{depth}(M) \leq \dim(M) \in \mathbb{N}_0$ as well. In view of this, M is called **Cohen-Macaulay**, if we actually have equality $\operatorname{depth}(M) = \dim(M)$.

In particular, if $\dim(R) = 0$ then we have $\operatorname{depth}(R) = 0$ as well, so that R is Cohen-Macaulay. Moreover, if R is a domain such that $\dim(R) \geq 1$ then $\operatorname{depth}(R) \geq 1$, so that any domain R such that $\dim(R) = 1$ is Cohen-Macaulay.

Example. Let $R = K[X_1, \ldots, X_n]$, for $n \in \mathbb{N}_0$, and let $P_i := (X_1, \ldots, X_i) \trianglelefteq R$, for $i \in \{0, \ldots, n\}$, yielding the strictly ascending chain $\{0\} = P_0 \subset P_1 \subset \cdots \subset P_n \trianglelefteq R$. Since $R/P_{i-1} \cong K[X_i, \ldots, X_n]$ is a domain, we conclude that $0 \neq X_i \in R/P_{i-1}$ is regular, for $i \in \{1, \ldots, n\}$, hence $[X_1, \ldots, X_n] \subseteq R_+$ is a regular sequence of length $n = \dim(R)$, thus R is Cohen-Macaulay.

(15.2) Theorem: [Macaulay, 1916; Cohen, 1946]**.** Let K be a field, let R be a finitely generated commutative graded K-algebra, and let $M \neq \{0\}$ be a finitely generated graded R-module. Then for the depth of M we have $\operatorname{depth}(M) \leq \min\{\dim(R/P) \in \mathbb{N}_0; P \in \operatorname{ass}_R(M)\}$.

Proof. Recall that $\operatorname{ass}_R(M) \neq \emptyset$ indeed. We proceed by induction on $\dim(M) \in \mathbb{N}_0$; since for $\dim(M) = 0$ we have $\operatorname{depth}(M) = 0$, we may assume that $\dim(M) \geq 1$. Let $[f_1, \ldots, f_k] \subseteq R_+$ be a regular sequence on M, for some $k \geq 1$, and abbreviate $f := f_1$. Then by induction we have $k - 1 \leq \operatorname{depth}(M/Mf) \leq \min\{\dim(R/Q) \in \mathbb{N}_0; Q \in \operatorname{ass}_R(M/Mf)\}$. We show that for each $P \in \operatorname{ass}_R(M)$ there is $Q \in \operatorname{ass}_R(M/Mf)$ such that $P \subset Q$; then $k \leq 1 + \min\{\dim(R/Q) \in \mathbb{N}_0; Q \in \operatorname{ass}_R(M/Mf)\} \leq \min\{\dim(R/P) \in \mathbb{N}_0; P \in \operatorname{ass}_R(M)\}$:

Since f is regular on M we have $f \notin P$. Let $N := \{m \in M; mP \leq Mf\} \leq M$, then N is an R-submodule such that $Mf \leq N$. Assume that $Mf = N$; then we consider the R-submodule $U := \{m \in M; P \leq \mathrm{ann}_R(m)\} \leq N = Mf$. Hence for each $u \in U$ there is $m \in M$ such that $u = mf$, thus we get $mfP = uP = \{0\}$, since f is regular on M entailing $mP = \{0\}$, that is $m \in U$. Thus we conclude that $U = Uf$, hence by the graded Nakayama Lemma we have $U = \{0\}$, which since $P \in \mathrm{ass}_R(M)$ is a contradiction.

Hence we have $Mf \neq N$, that is $\{0\} \neq N/Mf \leq M/Mf$, where we have $P \subseteq \mathrm{ann}_R(N/Mf)$, and $f \in \mathrm{ann}_R(M/Mf)$ anyway. We have $\emptyset \neq \mathrm{ass}_R(N/Mf) \subseteq \mathrm{ass}_R(M/Mf)$, and for any $Q \in \mathrm{ass}_R(N/Mf)$ we have $P \subseteq Q$ and $f \in Q \setminus P$. $\sharp$

Since $\mathrm{ass}_R(M)$ encompasses the minimal prime divisors of $\mathrm{ann}_R(M)$, in general we have $\mathrm{depth}(M) \leq \min\{\dim(R/P) \in \mathbb{N}_0; P \in \mathrm{ass}_R(M)\} \leq \max\{\dim(R/P) \in \mathbb{N}_0; P \in \mathrm{ass}_R(M)\} = \dim(R/\mathrm{ann}_R(M)) = \dim(M) \leq \dim(R) \in \mathbb{N}_0$. Hence if M is Cohen-Macaulay then it has the **unmixedness** property $\dim(R/P) = \dim(M)$, for all $P \in \mathrm{ass}_R(M)$; this entails that $\mathrm{ass}_R(M)$ consists precisely of the minimal prime divisors of $\mathrm{ann}_R(M)$, which all have the same dimension.

The unmixedness property was found by Macaulay for polynomial algebras, and by Cohen for regular local rings, which is the reason for the terminology used today. We remark that we only treat a special class of Cohen-Macaulay rings here, inasmuch we only allow for graded algebras and homogeneous regular sequences; these behave kind of similar to local Cohen-Macaulay rings.

(15.3) Cohen-Macaulay modules. Let K be a field, let R be a finitely generated commutative graded K-algebra such that $n := \dim(R) \in \mathbb{N}_0$, and let $M \neq \{0\}$ be a finitely generated graded R-module. We show that in the Cohen-Macaulay case the converse of the assertion in (15.1) also holds:

Proposition. If M is Cohen-Macaulay, then a homogeneous element $0 \neq f \in R_+$ is regular on M, if and only if $\dim(M/Mf) = \dim(M) - 1$.

Proof. We may assume that $0 \neq f \in R_+$ homogeneous is not regular on M, and we have to show that $\dim(M/Mf) = \dim(M)$:

To do so, we first show that $\mathrm{ann}_R(M/Mf) \subseteq \sqrt{\mathrm{ann}_R(M) + (f)}$: To this end, let $g \in \mathrm{ann}_R(M/Mf)$, and letting $\{m_1, \ldots, m_r\} \subseteq M$, for some $r \in \mathbb{N}$, be an R-module generating set, there are $a_{ij} \in (f) \trianglelefteq R$ such that $m_j g = \sum_{i=1}^r m_i a_{ij} \in M$. Letting $A := X \cdot E_r - [a_{ij}]_{ij} \in R[X]^{r \times r}$, we have $\det(A) = X^r + \sum_{k=1}^r a_k X^{r-k} \in R[X]$, where $a_1, \ldots, a_k \in (f)$. Specifying $X \mapsto g$, we have $[m_1, \ldots, m_r] \cdot A(g) = 0$, implying that $[m_1, \ldots, m_r] \cdot \det(A(g)) = [m_1, \ldots, m_r] \cdot A(g) \cdot \mathrm{adj}(A(g)) = 0$. Thus we have $\det(A(g)) \in \mathrm{ann}_R(M)$, implying that $g^r = \det(A(g)) - \sum_{k=1}^r a_k g^{r-k} \in \mathrm{ann}_R(M) + (f)$. (Note that so far we have not used the fact that f is a zero-divisor on M.)

Now, since f is a zero-divisor on M, there is $P \in \mathrm{ass}_R(M)$ such that $f \in P$. Thus we have $\mathrm{ann}_R(M/Mf) \subseteq \sqrt{\mathrm{ann}_R(M) + (f)} \subseteq P$, hence using unmixedness we infer $\dim(M) = \dim(R/P) \leq \dim(M/Mf) \leq \dim(M)$. ♯

(15.4) Cohen-Macaulay algebras. We relate regular sequences to homogeneous sets of parameters, and proceed to the main structure theorem for Cohen-Macaulay algebras, saying that the latter are characterized by having particularly nice Noether normalizations. To this end, let K be a field, and let R be a finitely generated commutative graded K-algebra such that $n := \dim(R) \in \mathbb{N}_0$.

Proposition. Any regular sequence $[f_1, \ldots, f_k] \subseteq R_+$, for $k \in \{0, \ldots, n\}$, can be extended to a homogeneous set of parameters. In particular, a regular sequence of length n is a homogeneous set of parameters.

Proof. Let $\mathcal{F} := \{f_1, \ldots, f_k\}$, and let $^-\colon R \to \overline{R} := R/(\mathcal{F})$ denote the natural epimorphism. By Noether normalization let $\mathcal{G} \subseteq R_+$ homogeneous, such that $\overline{\mathcal{G}} \subseteq \overline{R}_+$ is a homogeneous set of parameters of $\overline{R}$, where by regularity we have $|\mathcal{G}| = \dim(\overline{R}) = n - k$. Moreover, let $\mathcal{H} \subseteq R$ be finite and homogeneous, such that $\overline{\mathcal{H}}$ generates $\overline{R}$ as a $K[\overline{\mathcal{G}}]$-module.

Let $S := K[\mathcal{F}, \mathcal{G}] \subseteq R$. By the graded Nakayama Lemma we conclude that $\overline{\mathcal{H}}$ generates the K-vector space $\overline{R}/(\overline{\mathcal{G}}) \cong R/(\mathcal{F}, \mathcal{G})$. Thus by the graded Nakayama Lemma again we conclude that $\mathcal{H}$ generates R as an S-module. Hence $S \subseteq R$ is finite, thus we have $\dim(S) = \dim(R) = n = k + |\mathcal{G}|$. Since S is as a K-algebra generated by $r + |\mathcal{G}|$ elements, we conclude that S is polynomial. Hence the concatenation of $[f_1, \ldots, f_k]$ with $\mathcal{G}$ is a homogeneous set of parameters of R. ♯

Theorem. The following assertions are equivalent:
i) R is Cohen-Macaulay, that is there is a regular sequence of length n.
ii) Any homogeneous set of parameters is regular (for any ordering).
iii) R is a free graded S-module, for any Noether normalization $S \subseteq R$.
iv) R is a free graded S-module, for some Noether normalization $S \subseteq R$.

Proof. Let $\{f_1, \ldots, f_n\} \subseteq R_+$ be a homogeneous set of parameters of R, let $S := K[f_1, \ldots, f_n] \subseteq R$ be the associated Noether normalization, and let $^-\colon R \to \overline{R} := R/(f_1, \ldots, f_n)$ be the natural epimorphism. Since R is a finitely generated S-module, by the graded Nakayama Lemma we conclude that $\overline{R}$ is a finitely generated K-vector space; thus we have $\dim(\overline{R}) = \gamma(\overline{R}) = 0$.

Moreover, let $\mathcal{G} = \{g_1, \ldots, g_m\} \subseteq R$ homogeneous such that $\overline{\mathcal{G}} \subseteq \overline{R}$ is a K-basis, where $m = \dim_K(\overline{R}) \in \mathbb{N}_0$. Thus $\mathcal{G} \subseteq R$ is a minimal generating set of R as an S-module, where we may assume that $g_1 = 1$. Having this in place we get:

i)⇒ii). Since $\dim(\overline{R}) = 0$ and R is Cohen-Macaulay, $[f_1, \ldots, f_n]$ is regular.

ii)⇒iii). Assume to the contrary that $\mathcal{G}$ is not S-free. Then there are polynomials $h_j \in K[X_1, \ldots, X_n]$, for $j \in \{1, \ldots, m\}$, such that $[h_1, \ldots, h_m] \neq 0$ and $\sum_{j=1}^m g_j h_j(f_1, \ldots, f_n) = 0 \in R$. Let $\alpha \in \mathbb{N}_0$ be maximal such that X_1^α divides all the h_j, and let $h_j = X_1^\alpha \cdot h'_j \in K[X_1, \ldots, X_n]$. Since $f_1 \in R$ is regular, we have $\sum_{j=1}^m g_j h'_j(f_1, \ldots, f_n) = 0 \in R$, entailing $\sum_{j=1}^m g_j h'_j(0, f_2, \ldots, f_n) = 0 \in R/(f_1)$, where by construction $[h'_1(0, X_2, \ldots, X_n), \ldots, h'_m(0, X_2, \ldots, X_n)] \neq 0$.

Hence $\mathcal{G} \subseteq R/(f_1)$ is not $K[f_2, \ldots, f_n]$-free. By iteration this finally yields $\sum_{j=1}^m \lambda_j \overline{g_j} = 0 \in \overline{R}$, where $\lambda_j \in K$ such that $[\lambda_1, \ldots, \lambda_m] \neq 0$; since $\overline{\mathcal{G}}$ is K-linearly independent, this a contradiction.

iii)⇒iv) is trivial.

iv)⇒i). Assume that $R = \bigoplus_{j=1}^m g_j S$ is a free S-module. Since S is a domain, $f_1 \in S = g_1 \cdot S \subseteq R$ is regular, and we have $R/(f_1) = \bigoplus_{j=1}^m (g_j \cdot K[f_2, \ldots, f_n])$. By iteration we conclude that the sequence $[f_1, \ldots, f_n]$ is regular. ♯

(15.5) Hironaka decomposition. a) Let K be a field, let R be a finitely generated commutative graded K-algebra such that $n := \dim(R) \in \mathbb{N}_0$, let $\mathcal{F} := \{f_1, \ldots, f_n\} \subseteq R$ be a homogeneous set of parameters, let $S := K[\mathcal{F}] \subseteq R$, let $\{g_1, \ldots, g_m\} \subseteq R$, where $m \in \mathbb{N}$, be a minimal homogeneous generating set of R as a graded S-module, and let $d_i := \deg(f_i) \in \mathbb{N}$ and $e_j := \deg(g_j) \in \mathbb{N}_0$.

Let R be Cohen-Macaulay. Then we have the associated **Hironaka decomposition** $R = \bigoplus_{j=1}^m g_j S$ as a free graded S-module. Hence the Hilbert series of R is given as $H_R = (\sum_{j=1}^m T^{e_j}) \cdot H_S = (\sum_{j=1}^m T^{e_j}) \cdot \prod_{i=1}^n \frac{1}{1-T^{d_i}} \in \mathbb{Q}(T)$. Since $\gamma(R) = \gamma(S) = n$ we have $\delta(R) = m \cdot \delta(S) = m \cdot \prod_{i=1}^n \frac{1}{d_i} \in \mathbb{Q}$; and if R is a domain then by the degree theorem we have $[\mathrm{Q}(R) \colon \mathrm{Q}(S)] = \frac{\delta(R)}{\delta(S)} = m$.

b) If a Noether normalization S of R is given, since S is polynomial the associated degrees are uniquely defined and can be read off from H_S, see (7.3). Then the cardinality m of a minimal homogeneous generating set of R as an S-module, and the associated degrees, can be read off from H_R. Alone, the degrees of the elements of a homogeneous set of parameters are not uniquely defined; thus a certain amount of educated guesswork is needed to find a Noether normalization in practice, where H_R typically yields hints where to look.

We have the following method to check whether we have actually found a Noether normalization of R: The homogeneous sets of parameters coincide with the regular sequences of length n, where the latter can be built up successively, checking the regularity condition in each step. Indeed, a homogeneous sequence $[f_1, \ldots, f_k] \subseteq R_+$, for some $k \in \{0, \ldots, n\}$, is regular, and thus can be further extended regularly for $k < n$, if and only if $\dim(R/(f_1, \ldots, f_k)) = n - k$; recall that $\dim(R/(f_1, \ldots, f_k)) \geq n - k$ anyway. In particular, a homogeneous sequence $[f_1, \ldots, f_n] \subseteq R_+$ is regular if and only if $\gamma(R/(f_1, \ldots, f_n)) = \dim(R/(f_1, \ldots, f_n)) = 0$, that is $R/(f_1, \ldots, f_n)$ is a finitely generated graded K-vector space. In this case, by the graded Nakayama Lemma, a homogeneous set $\mathcal{G} := \{g_1, \ldots, g_m\}$, for some $m \in \mathbb{N}$, is a minimal homogeneous generating set of R as an S-module, if and only if $\overline{\mathcal{G}} \subseteq \overline{R} = R/(f_1, \ldots, f_n)$ is a K-basis.

(15.6) Cohen-Macaulay invariant algebras. We proceed to show how the notion of Cohen-Macaulayness relates to invariant algebras. Let K be a field.

Proposition. Let R be a finitely generated commutative graded K-algebra, and let M be a finitely generated graded R-module which is a homogeneous direct summand of a finitely generated free graded R-module (that is M is **projective graded**). Then M is a free graded R-module.

Proof. Let $\{m_1, \ldots, m_r\} \subseteq M$ be a minimal homogeneous generating set of M, where $r \in \mathbb{N}_0$ and $d_i := \deg(m_i) \in \mathbb{Z}$, and let $F = \bigoplus_{i=1}^r f_i R$ be the free graded R-module generated in degrees d_i, so that there is an epimorphism of graded R-modules $\varphi\colon F \to M\colon f_i \mapsto m_i$. We show that φ is an isomorphism:

By assumption there is a free graded R-module $F' = \bigoplus_{j=1}^s f'_j R$, where $s \in \mathbb{N}_0$, such that there is an epimorphism of graded R-modules $\pi\colon F \to M$ together with a splitting $\iota\colon M \to F$, that is $\iota\pi = \mathrm{id}_M$. For $j \in \{1, \ldots, s\}$ choose $h_j \in F$ homogeneous such that $\varphi(h_j) = \pi(f'_j)$, and let $\psi\colon F' \to F$ be the homomorphism of graded R-modules given by $f'_j \mapsto h_j$. Then we have $(\psi\varphi)(f'_j) = \pi(f'_j)$, thus $\psi\varphi = \pi$. Hence we have $\iota\psi \cdot \varphi = \iota\pi = \mathrm{id}_M$, saying that $\iota\psi\colon M \to F$ is a splitting of φ, so that $F = (\iota\psi)(M) \oplus \ker(\varphi)$.

Since F is Noetherian, $\ker(\varphi)$ is a finitely generated graded R-module. Moreover, for $\sum_{i=1}^r f_i g_i \in \ker(\varphi)$, where the $g_i \in R$ are homogeneous, applying φ we get $\sum_{i=1}^r m_i g_i = 0 \in M$. Since by the graded Nakayama Lemma we infer that $\{m_1, \ldots, m_r\} \subseteq M/MR_+$ is K-linearly independent, we conclude that $g_i \in R_+$ for all i. Thus we have $\ker(\varphi) \leq FR_+ = (\iota\psi)(M)R_+ \oplus \ker(\varphi)R_+$, so that $\ker(\varphi) = \ker(\varphi)R_+$, by the graded Nakayama Lemma entailing $\ker(\varphi) = \{0\}$. $\sharp$

Theorem: [Hochster, Eagon, 1971; Campbell, Hughes, Pollack, 1991]**.** Let G be a finite group, let $H \leq G$ be a subgroup such that $\mathrm{char}(K) \nmid [G\colon H]$, and let V be a $K[G]$-module. If $S[V]^H$ is Cohen-Macaulay, then so is $S[V]^G$.

Proof. Let $S := S[V]$, and let $\{f_1, \ldots, f_n\} \subseteq S^G$ be a set of primary invariants, where $n := \dim_K(V) \in \mathbb{N}_0$. Hence we have $R := K[f_1, \ldots, f_n] \subseteq S^G \subseteq S^H \subseteq S$. Both extensions $R \subseteq S^G \subseteq S$ are finite, hence S is a finitely generated R-module. Since R is Noetherian, the R-submodule $S^H \leq S$ is finitely generated as well, hence $\{f_1, \ldots, f_n\} \subseteq S^H$ is a set of primary invariants of S^H as well. Now we have to alternative ways to proceed:

i) More abstractly, since S^H is Cohen-Macaulay, S^H is a free graded R-module. The relative Reynolds operator $\mathcal{R}_H^G\colon S^H \to S^G$ is a projection of graded R-modules. Hence S^G is a direct summand of S^H, thus is a free graded R-module, entailing that S^G is Cohen-Macaulay.

ii) Alternatively, more concretely, we show that the sequence $[f_1, \ldots, f_n] \subseteq S^G$ is regular, using the fact that, since S^H is Cohen-Macaulay, the sequence $[f_1, \ldots, f_n] \subseteq S^H$ is regular: Let $k \in \{1, \ldots, n\}$, and let $I_{k-1} := (f_1, \ldots, f_{k-1}) = \sum_{i=1}^{k-1} f_i \cdot S^G \trianglelefteq S^G$. Then we have $f_k \notin I_{k-1} \cdot S^H \trianglelefteq S^H$, so that $f_k \notin I_{k-1}$.

Moreover, let $g_k \in S^G$ such that $f_k g_k = 0 \in S^G/I_{k-1}$, that is $f_k g_k \in I_{k-1} \subseteq I_{k-1} \cdot S^H$. By regularity in S^H we conclude that $g_k \in I_{k-1} \cdot S^H$, that is there are

$h_1, \ldots, h_{k-1} \in S^H$ such that $g_k = \sum_{i=1}^{k-1} f_i h_i$. Applying the relative Reynolds operator $\mathcal{R}_H^G \colon S^H \to S^G$ yields $g_k = \mathcal{R}_H^G(g_k) = \sum_{i=1}^{k-1} f_i \cdot \mathcal{R}_H^G(h_i) \in I_{k-1}$, that is $g_k = 0 \in S^G/I_{k-1}$. This shows that $f_k \in S^G/I_{k-1}$ is regular. ♯

Corollary. **i)** If $\mathrm{char}(K) \nmid |G|$, then $S[V]^G$ is Cohen-Macaulay.
ii) If $p := \mathrm{char}(K) \mid |G|$, and H is a Sylow p-subgroup of G such that $S[V]^H$ is Cohen-Macaulay, then so is $S[V]^G$.

The absolute version of the previous theorem is due to Hochster, Eagon, while the relative version is due to Campbell, Hughes, Pollack.

(15.7) Remark: Depth of invariant algebras. Compared to the non-modular case, in the modular case the picture is much more complicated. We give a few indications: To this end, let G be a finite group, let K be a field such that $\mathrm{char}(K) \mid |G|$, and let V be a faithful $K[G]$-module.

a) The depth of $S[V]^G$ is at least $\min\{3, \dim_K(V)\}$ [Campbell, Hughes, Kemper, Shank, Wehlau, 2000]. In particular, if $\dim_K(V) \leq 3$ then $S[V]^G$ is Cohen-Macaulay [Smith, 1996].

Moreover, the depth of $S[V]^G$ is at least $\min\{\dim_K(\mathrm{Fix}_V(G)) + 2, \dim_K(V)\}$ [Ellingsrud, Skjelbred, 1980]. If $\dim_K(\mathrm{Fix}_V(G)) \geq \dim_K(V) - 1$, then $S[V]^G$ is even polynomial [Landweber, Stong, 1984].

b) Let V be the regular $K[G]$-module. Then $S[V]^G$ is Cohen-Macaulay if and only if $G \in \{C_2, C_3, V_4\}$ [Kemper, 1999]; for the 'if' direction see (3.4), and (9.7), and (17.4) below, respectively. (For the example $G = C_4$, see (17.5).)

c) Let G be a p-group. (Here we expect the most complicated phenomena.)

i) If G is cyclic, then the depth of $S[V]^G$ is equal to $\min\{\dim_K(\mathrm{Fix}_V(G)) + 2, \dim_K(V)\}$ [Ellingsrud, Skjelbred, 1980].

In particular, if V is the regular $K[G]$-module, then the depth of $S[V^{\oplus n}]^G$, where $n \in \mathbb{N}$, is $\min\{n+2, n \cdot |G|\}$; thus $S[V^{\oplus n}]^G$ is Cohen-Macaulay if and only if $n \cdot (|G| - 1) \leq 2$, that is $G = C_2$ and $n \leq 2$, or $G = C_3$ and $n = 1$. (Again, for the smallest counterexample $G = C_4$, see (17.5).)

ii) An element $1 \neq s \in G$ is called a **bireflection**, if we have $\dim_K(\mathrm{Fix}_V(s)) \geq \dim_K(V) - 2$. Then $S[V]^G$ is Cohen-Macaulay only if G is generated by bireflections [Kemper, 1999]. (The converse does not hold.)

In particular, if G then $S[V^{\oplus n}]^G$ is not Cohen-Macaulay whenever $n \geq 3$ [Campbell, Geramita, Hughes, Shank, Wehlau, 1999]. (This is another incarnation of the philosophy that vector invariants tend to be badly behaved.)

16 Cohen-Macaulay invariant algebras

(16.1) Cohen-Macaulayness of invariant algebras. Let K be a field, let G be a finite group, let V be a faithful $K[G]$-module such that $n := \dim_K(V) \in \mathbb{N}_0$, let $\mathcal{F} := \{f_1, \ldots, f_n\} \subseteq S^G \subseteq S := S[V]$ be a set of primary invariants such that $d_i := \deg(f_i) \in \mathbb{N}$, and let $d := \prod_{i=1}^n d_i \in \mathbb{N}$ be their degree product. Then $\mathcal{F}$ is called **optimal** if its degree product d is minimal.

Theorem. a) Let $m \in \mathbb{N}$ be the cardinality of a minimal set of secondary invariants associated with $\mathcal{F}$. Then we have $|G| \mid d$ and $m \cdot |G| \geq d$, where equality $m \cdot |G| = d$ holds if and only if the invariant algebra S^G is Cohen-Macaulay. Moreover, we have $m = 1$ if and only if $d = |G|$.
b) For the coinvariant algebra we have $\dim_K(S_G) \geq |G|$, where we have equality $\dim_K(S_G) = |G|$ if and only if S is a free graded S^G-module.

Proof. a) Both extensions $R := K[\mathcal{F}] \subseteq S^G \subseteq S$ are finite, hence $\mathcal{F}$ is a homogeneous set of parameters of S; thus we have $\gamma(R) = \gamma(S^G) = \gamma(S) = n$, and $\delta(R) = \frac{1}{d}$, and $\delta(S^G) = \frac{1}{|G|}$, and $\delta(S) = 1$. From the field extensions $\mathrm{Q}(R) \subseteq S(V)^G \subseteq S(V)$, by the degree theorem we get $\frac{\delta(S)}{\delta(R)} = [S(V) \colon \mathrm{Q}(R)] = [S(V) \colon S(V)^G] \cdot [S(V)^G \colon \mathrm{Q}(R)] = \frac{\delta(S)}{\delta(S^G)} \cdot \frac{\delta(S^G)}{\delta(R)} \in \mathbb{Z}$, entailing $d = |G| \cdot \frac{\delta(S^G)}{\delta(R)} \in \mathbb{Z}$.

Let $\mathcal{G} := \{g_1, \ldots, g_m\} \subseteq S^G$ be a set of secondary invariants such that $e_j := \deg(g_j) \in \mathbb{N}_0$. Now the minimum polynomial of any $f \in S$ is irreducible over $\mathrm{Q}(R)$, hence the $\mathrm{Q}(R)$-subalgebra $\mathrm{Q}(R)[f] \subseteq S(V)$ already is a field, entailing that $S(V)^G = S^G \cdot \mathrm{Q}(R)$; see also the proof of (6.3). Thus $\mathcal{G}$ generates $S(V)^G$ as a $\mathrm{Q}(R)$-vector space, hence $m = |\mathcal{G}| \geq [S(V)^G \colon \mathrm{Q}(R)] = \frac{\delta(S^G)}{\delta(R)} = \frac{d}{|G|}$. Moreover, we have $m \cdot |G| = d$ if and only if $\mathcal{G}$ is $\mathrm{Q}(R)$-linearly independent, that is $\mathcal{G}$ is R-linearly independent, in other words S^G is a free graded R-module.

Finally, we have already shown that $m = 1$ implies $d = |G|$; hence let $d = |G|$. Then we have $[S(V)^G \colon \mathrm{Q}(R)] = \frac{\delta(S^G)}{\delta(R)} = 1$, thus $S(V)^G = \mathrm{Q}(R)$, hence we get $R \subseteq S^G \subseteq S(V)^G = \mathrm{Q}(R)$. Since R is factorial, thus is integrally closed, see Exercise (19.11), from $R \subseteq S^G$ being integral we get $R = S^G$, that is $m = 1$.

b) Let $\mathcal{H} := \{h_1, \ldots, h_r\}$ be a minimal homogeneous generating set of S as a graded S^G-module, for $r \in \mathbb{N}$, such that $c_s := \deg(h_s) \in \mathbb{N}_0$. By the graded Nakayama Lemma we conclude that $S_G = S/\mathcal{I}_G = S/(S^G_+ \cdot S)$ is a graded K-vector space of K-dimension r. As we have seen above, we have $S(V) = S \cdot S(V)^G$, thus $\mathcal{H}$ generates $S(V)$ as an $S(V)^G$-vector space, hence we have $r = |\mathcal{H}| \geq [S(V) \colon S(V)^G] = |G|$. Moreover, we have $r = |G|$ if and only if $\mathcal{H}$ is $S(V)^G$-linearly independent, that is $\mathcal{H}$ is S^G-linearly independent, in other words S is a free graded S^G-module. $\sharp$

i) In particular, if $m = 1$ then S^G is polynomial; conversely, if S^G is polynomial then choosing $\mathcal{F}$ as a set of basic invariants entails $m = 1$.

If S^G is polynomial, then S being Cohen-Macaulay entails that S is a free graded S^G-module. Conversely, by Chevalley's Theorem (which we have proven in (7.2) for the case $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) > |G|$, but which actually holds in general), it follows from S being a free graded S^G-module that S^G is polynomial.

ii) If S^G is not polynomial, but $\mathcal{F}$ can be chosen such that $d = 2\cdot|G|$ and $m = 2$, then S^G is Cohen-Macaulay. Choosing $g \in S^G \setminus K[\mathcal{F}]$ homogeneous of minimal degree $e := \deg(g) \in \mathbb{N}$, we get $S^G = K[\mathcal{F}] \oplus g \cdot K[\mathcal{F}]$ as graded $K[\mathcal{F}]$-modules.

Letting $P := K[X_1, \ldots, X_n, X]$ with degrees $[d_1, \ldots, d_n, e]$, since g is integral over $K[\mathcal{F}]$, there are $F, F' \in K[X_1, \ldots, X_n]$ homogeneous such that $\deg(F) = e$ and $\deg(F') = 2e$, and $(X^2+FX+F')(f_1, f_2, g) = g^2+F(f_1, f_2)g+F'(f_1, f_2) = 0$. Thus we have $S^G \cong P/(X^2 + FX + F')$ as graded K-algebras, via $X_i \mapsto f_i$ and $X \mapsto g$; hence S^G is a **hypersurface**.

(16.2) Polynomial invariant algebras. a) Let K be a field, let G be a finite group, let V be a faithful $K[G]$-module such that $n := \dim_K(V) \in \mathbb{N}_0$, let $\mathcal{F} := \{f_1, \ldots, f_n\} \subseteq S^G \subseteq S := S[V]$ be algebraically independent and homogeneous, such that $d_i := \deg(f_i) \in \mathbb{N}$, and let $d := \prod_{i=1}^n d_i$. In order to ensure polynomiality, we show that the (strong) finiteness assumption on $K[\mathcal{F}] \subseteq S^G$ can actually be replaced by an (apparently weaker) degree assumption on $\mathcal{F}$:

Theorem: [Kemper, 1996]**.** Assume that $d = |G|$. Then we have $S^G = K[\mathcal{F}]$, that is S^G is polynomial having $\mathcal{F}$ as a set of basic invariants.

Proof. Let $S = K[\mathcal{X}]$, where $\mathcal{X} = \{X_1, \ldots, X_n\}$, and where we may assume that $n \geq 1$, let $\mathcal{Y} := \{Y_1, \ldots, Y_n\}$ be indeterminates, and let L be an algebraic closure of $K(\mathcal{Y})$. Hence we have a field isomorphism $K(\mathcal{Y}) \to K(\mathcal{F})\colon Y_i \mapsto f_i$. Since $\operatorname{trdeg}(K(\mathcal{F})) = \operatorname{trdeg}(K(\mathcal{X})) = n$, the field extension $K(\mathcal{F}) \subseteq K(\mathcal{X})$ is algebraic; hence there are $x_1, \ldots, x_n \in L$ such that $K(\mathcal{Y}, x_1, \ldots, x_n) \to K(\mathcal{X})\colon Y_i \mapsto f_i, x_i \mapsto X_i$ is a field isomorphism. Let $g_i(\mathcal{Y}, T) \in K(\mathcal{Y})[T]$ be the minimum polynomial of x_i over $K(\mathcal{Y})$; hence $g_i(\mathcal{F}, X_i) = 0 \in K(\mathcal{X})$. Moreover, since $K(\mathcal{F}) \subseteq K(\mathcal{X})^G$, letting G act trivially on $K(\mathcal{Y})$, there an action of G by field automorphisms on $K(\mathcal{Y}, x_1, \ldots, x_n)$ such that the identification $K(\mathcal{Y}, x_1, \ldots, x_n) \to K(\mathcal{X})$ is an isomorphism of G-sets.

Letting $\mathcal{Z} := \{Z_1, \ldots, Z_n\}$ be indeterminates, we consider the system of equations $f_i(\mathcal{Z}) - Y_i = 0 \in L[\mathcal{Z}]$. Its solutions are precisely the identifications of $K(\mathcal{X})$ with a subfield of L, being compatible with the fixed identification $K(\mathcal{F}) \to K(\mathcal{Y})$; hence in particular $[x_1, \ldots, x_n] \in L^n$ is amongst the solutions. Given any solution $[z_1, \ldots, z_n] \in L^n$, we conclude that $\{z_1, \ldots, z_n\} \subseteq L$ is algebraically independent, and we get $g_i(\mathcal{Y}, z_i) = g_i(\mathcal{F}(z_1, \ldots, z_n), z_i) = g_i(\mathcal{F}(\mathcal{Z}), Z_i)(z_1, \ldots, z_n) = 0$. Hence there are at most $\deg_T(g_i)$ possibilities for z_i, so that the above system of equations has at most $\prod_{i=1}^n \deg_T(g_i)$ solutions. Moreover, for $[x_1, \ldots, x_n]^g \in L^n$, where $g \in G$, we have $f_i(x_1^g, \ldots, x_n^g) - Y_i = (f_i(x_1, \ldots, x_n) - Y_i)^g = 0$. Since $\mathcal{X} \subseteq V$ is a K-basis, and G acts faithfully, we conclude that $[X_1, \ldots, X_n]$ gives rise to a regular G-orbit. Hence $\{[x_1, \ldots, x_n]^g \in L^n; g \in G\}$ provides $|G|$ solutions.

We consider the homogenized system of equations $f_i(\mathcal{Z})-Y_iZ_0^{d_i} = 0 \in L[\mathcal{Z}, Z_0]$, and let $\mathcal{V} \subseteq \mathcal{P} := \mathbf{P}^n(L)$ be the associated projective variety. Being the intersection of hypersurfaces of degree d_i, by **Bézout's Theorem** $\mathcal{V}$ has at most

$\prod_{i=1}^n d_i = d = |G|$ irreducible components, with respect to the Zariski topology. Since the above system has at least $|G|$ isolated solutions in the affine open subset $\mathcal{A} := \{[z_1 \colon \cdots \colon z_n \colon z_0] \in \mathcal{P}; z_i \in L, z_0 \neq 0\} \subseteq \mathcal{P}$, we conclude that these are all solutions, thus $\mathcal{V} = \{[x_1 \colon \cdots \colon x_n \colon 1] \in \mathcal{P}; g \in G\} \subseteq \mathcal{A}$ such that $|\mathcal{V}| = |G|$.

Moreover, there are no solutions in the closed subset $\mathcal{P} \setminus \mathcal{A} = \{[z_1 \colon \ldots \colon z_n \colon 0] \in \mathcal{P}; [z_1, \ldots, z_n] \neq 0\} \subseteq \mathcal{P}$, saying that the system of equations $f_i(\mathcal{Z}) = 0 \in L[\mathcal{Z}]$ has only the solution $0 \in L^n$. Thus by **Hilbert's Nullstellensatz** [1893] we conclude that $L[\mathcal{Z}]_+ \trianglelefteq L[\mathcal{Z}]$ is the only maximal ideal dividing $(\mathcal{F}(\mathcal{Z}))$, thus is its only prime divisor, so that $\sqrt{\mathcal{F}(\mathcal{Z})} = L[\mathcal{Z}]_+$. This implies that $\sqrt{\mathcal{F}} = K[\mathcal{X}]_+$, hence $\dim(K[\mathcal{X}]/(\mathcal{F})) = 0$, thus $\mathcal{F} \subseteq K[\mathcal{X}]$ is regular, hence is a homogeneous set of parameters. Finally, we conclude $m = \frac{d}{|G|} = 1$, that is $K[\mathcal{X}]^G = K[\mathcal{F}]$. $\sharp$

Since the degrees of a set of basic invariants are uniquely defined, this yields the following straightforward algorithm to check for polynomiality: We run the standard algorithm to collect indecomposable homogeneous invariants, and look for an n-set of them having degree product $|G|$. If such a set does not exist, by exceeding n or $|G|$, we conclude that S^G is not polynomial; if such a set exists then we decide polynomiality of S^G by checking for algebraic independence of the set found, by using the Jacobian criterion. For example, this approach yields for the pseudoreflection representation of $G = \mathcal{A}_5$ in characteristic 2, see (12.3).

b) Let now S^G be polynomial. Then the coinvariant algebra S_G, which is a finite-dimensional graded K-algebra anyway, not only has K-dimension $|G|$, but its structure as a $K[G]$-module can be explicitly determined:

Theorem: [Chevalley, 1955]. Let $S^G = K[\mathcal{F}]$ be polynomial. Then the Hilbert series of the coinvariant algebra is $H_{S_G} = \prod_{i=1}^n (\sum_{j=0}^{d_i-1} T^j) \in \mathbb{Z}[T]$, and if $\mathrm{char}(K) \nmid |G|$ then the $K[G]$-module S_G is equivalent to the regular module.

Proof. Letting $R := S^G$, the algebra S is a free graded R-module, of rank $r := \dim_K(S_G) = |G|$. More precisely, let $\mathcal{H} := \{h_1, \ldots, h_r\}$ be a minimal homogeneous generating set of S as a graded R-module. Then we have $S = \bigoplus_{s=1}^r h_s R$ as graded R-modules, and $R_+ S = \bigoplus_{s=1}^r h_s R_+ \subseteq S$, so that $S_G = S/R_+S$ has homogeneous K-basis $\overline{\mathcal{H}} := \{\overline{h_1}, \ldots, \overline{h_r}\}$, where $\overline{} \colon S \to S_G$ is the natural epimorphism. Hence we have $S \cong S_G \otimes R$ as graded R-modules, the isomorphism being given by $h_s \mapsto \overline{h_s} \otimes 1$. Moreover, since G acts trivially on R, and naturally on S_G and S, we conclude that the above isomorphism is an isomorphism of graded G-algebras.

Hence for the associated Hilbert series we have $\frac{1}{(1-T)^n} = H_S = H_{S_G} \cdot H_R = H_{S_G} \cdot \prod_{i=1}^n \frac{1}{1-T^{d_i}} \in \mathbb{Q}(T)$, entailing $H_{S_G} = \prod_{i=1}^n \frac{1-T^{d_i}}{1-T} = \prod_{i=1}^n (\sum_{j=0}^{d_i-1} T^j) \in \mathbb{Q}(T)$,

For $g \in G$ let $A(g) := [a_{ij}(g)]_{ij} \in R^{r \times r}$ be the representing matrix of its action on S with respect to the R-basis $\mathcal{H}$; note that the matrix entries are homogeneous such that $a_{ij}(g) = 0$ or $\deg(a_{ij}(g)) = \deg(h_j) - \deg(h_i) \in \mathbb{N}_0$, in particular we have $a_{ii}(g) \in R_0 = K$. Noting that $\overline{} \colon S \to S_G$ restricts to the natural epimorphism $R \to R/R_+ = K$, we infer that $\overline{A(g)} \in K^{r\times r}$ is the representing matrix of the action of g on S_G with respect to the K-basis $\overline{\mathcal{H}}$.

Since $\mathcal{H}$ is an $S(V)^G$-basis of $S(V)$, see (16.1), we conclude that $A(g)$ also is a representing matrix of the action of g on $S(V)$. Now the field extension $S(V)^G \subseteq S(V)$ is Galois with respect to G, so that by the **normal basis theorem** $S(V)$ carries the regular G-permutation action. Hence for the associated matrix traces we get $\chi_{S_G}(g) = \sum_{s=1}^r \overline{a_{ss}(g)} = \sum_{s=1}^r a_{ss}(g) = \chi_{S(V)}(g) = |G| \cdot \delta_{1,g} \in K$, saying that S_G affords the regular character. Since $\mathrm{char}(K) \nmid |G|$, from this we conclude that S_G carries the regular representation. ♯

In particular, we have $\deg(H_{S_G}) = \sum_{i=1}^n (d_i - 1)$. Recall that if $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) > |G|$ then G is a pseudoreflection group having precisely $\sigma(G) = \sum_{i=1}^n (d_i - 1)$ pseudoreflections. (Again, this actually holds whenever $\mathrm{char}(K) \nmid |G|$, but we have not shown this.) From the viewpoint of representation theory, this shows that the group algebra $K[G]$ of a pseudoreflection group G also carries the structure of a commutative graded K-algebra, with degrees $\{0, \ldots, \sigma(G)\}$, unraveling hidden combinatorial information about G (to say the least).

Note that, although H_{S_G} is unchanged, the characteristic dependent result above cannot possibly hold whenever $\mathrm{char}(K) \mid |G|$: In this case the unique one-dimensional trivial $K[G]$-submodule of the regular module is not a direct summand, while we have $S_G = K \oplus (S_G)_+$ as $K[G]$-modules.

(16.3) Finding primary invariants. Let K be a field, let G be a finite group, let V be a faithful $K[G]$-module such that $n := \dim_K(V) \in \mathbb{N}_0$.

Since $S^G \subseteq S := S[V]$ is finite, a subset $\{f_1, \ldots, f_n\} \subseteq S^G \subseteq S$ is a homogeneous set of parameters of S^G if and only if it is a homogeneous set of parameters of S; see (15.4). Since the polynomial algebra S is Cohen-Macaulay, this is equivalent to $[f_1, \ldots, f_n]$ being a regular sequence in S. (Although this does not imply that it is a regular sequence in S^G.) Letting $(f_1, \ldots, f_n) \trianglelefteq S$ be the associated (generalized Hilbert) ideal of S, this in turn is equivalent to $\dim(S/(f_1, \ldots, f_n)) = 0$, which by the graded Nakayama Lemma amounts to $S/(f_1, \ldots, f_n)$ being a finitely generated graded K-vector space.

This paves the way to the following generic method to finding primary invariants, which typically are far from being optimal:

Theorem: [Dade, 1996]. Let $\{X_1, \ldots, X_n\} \subseteq V$ be a **Dade K-basis**, that is

$$X_i \notin \bigcup_{g_1, \ldots, g_{i-1} \in G} \langle X_1 \cdot g_1, \ldots, X_{i-1} \cdot g_{i-1} \rangle_K,$$

for $i \in \{1, \ldots, n\}$, and let $f_i := \prod_{f \in X_i^G} f \in S^G$ be the associated orbit product. Then $\{f_1, \ldots, f_n\} \subseteq S^G$ is a set of primary invariants, such that $\deg(f_i) \mid |G|$.

Proof. We indeed have $f_i \in S^G$ such that $\deg(f_i) = |f_i^G| = \frac{|G|}{|\mathrm{Stab}_G(f_i)|}$. Letting $I := (f_1, \ldots, f_n) \trianglelefteq S$, we proceed to show that $\dim(S/I) = 0$:

Let $K \subseteq \overline{K}$ be an algebraic closure of K, let $\overline{V} := V \otimes \overline{K}$, let $\overline{S} = S[\overline{V}] = S \otimes \overline{K}$, and let $\overline{I} := I \otimes \overline{K} = (f_1, \ldots, f_n) \trianglelefteq \overline{S}$. Now let $l \in \overline{V}^*$ be a $\overline{K}$-linear form on $\overline{V}$ such that $l(f_i) = 0$, for all $i \in \{1, \ldots, n\}$. Then we have $l(X_i \cdot g_i) = 0$, for some $g_i \in G$. Since the set $\{X_1 \cdot g_1, \ldots, X_n \cdot g_n\} \subseteq V$ is a K-basis, and thus is a $\overline{K}$-basis of $\overline{V}$, this implies $l = 0$.

Thus by **Hilbert's Nullstellensatz**, saying that the maximal ideals of $\overline{S}$ are in correspondence with the elements of $\overline{V}^*$, we infer that $\overline{S}_+ \trianglelefteq \overline{S}$ is the only maximal ideal dividing $\overline{I}$, thus is the only prime divisor of $\overline{I}$, hence we have $\sqrt{\overline{I}} = \overline{S}_+ \trianglelefteq \overline{S}$. This entails that $\sqrt{I} = S_+ \trianglelefteq S$, which is a maximal ideal, hence is the only prime divisor of I. Thus we have $\dim(S/I) = \dim(S/S_+) = 0$. ♯

Corollary: Dade's degree bound. Let K be infinite. Then there is a set of primary invariants of degree at most $|G|$.

Proof. We show that V is not the union of finitely many proper K-subspaces; thus there is a Dade K-basis of V, hence an associated set of primary invariants:

We proceed by induction on $n \in \mathbb{N}$; the cases $n \leq 1$ being trivial, let $n \geq 2$, and assume that $V = \bigcup_{i=1}^r V_i$, for some $r \in \mathbb{N}$ and maximal K-subspaces $V_i \leq V$. Since K is infinite, there are infinitely many maximal K-subspaces $V' \leq V$. Choosing $V' \neq V_i$ for all i, we get $V = V \cap (\bigcup_{i=1}^r V_i) = \bigcup_{i=1}^r (V \cap V_i)$, where $V \cap V_i \leq V$ are maximal K-subspaces, which by induction is a contradiction. ♯

The assumption on the field cannot generally be dispensed of: If K is finite, V need not have a Dade K-basis, as for example the pseudoreflection representation of $G = \mathcal{A}_5$ over the (splitting) field $K = \mathbb{F}_4$ (having a polynomial invariant algebra) shows; see (12.3).

(16.4) Broer's degree bound. Let K be a field, let G be a finite group, let V be a faithful $K[G]$-module such that $n := \dim_K(V) \in \mathbb{N}_0$, let $\{f_1, \ldots, f_n\}$ be a set of primary invariants such that $d_i := \deg(f_i) \in \mathbb{N}$, and let $\{g_1, \ldots, g_m\}$ be a minimal set of secondary invariants such that $e_j := \deg(g_j) \in \mathbb{N}_0$, for $m \in \mathbb{N}$.

Theorem: [Broer, 1997]**.** If $S[V]^G$ is Cohen-Macaulay, then for the degrees of the secondary invariants we have $e_j \leq \sum_{i=1}^n (d_i - 1)$, for all $j \in \{1, \ldots, m\}$.

Proof. Let $R := K[f_1, \ldots, f_n] \subseteq S^G \subseteq S := S[V]$, since $R \subseteq S$ is finite let $\{h_1, \ldots, h_r\} \subseteq S$, where $r \in \mathbb{N}$, be a minimal homogeneous generating set of S an an R-module, such that $c_k := \deg(h_k)$, where $h_1 = 1$ and where we assume that $0 = c_1 \leq \cdots \leq c_r$. Since S is Cohen-Macaulay we have $S = \bigoplus_{k=1}^r h_k R$ as graded R-modules, hence we have $H_S = \frac{1}{(1-T)^n} = (\sum_{k=1}^r T^{c_k}) \cdot \prod_{i=1}^n \frac{1}{1-T^{d_i}} \in \mathbb{Q}(T)$. Thus we have $\sum_{k=1}^r T^{c_k} = \prod_{i=1}^n \frac{1-T^{d_i}}{1-T}$, hence $c_r = \sum_{i=1}^n (d_i - 1)$.

The elements of $\mathrm{Hom}_R(S,R)$ are determined by the image of $\{h_1,\ldots,h_r\}$, thus $\mathrm{Hom}_R(S,R)_d = \{0\}$ for $d < -c_r$. Similarly, by assumption we have $S^G = \bigoplus_{j=1}^m g_j R$ as graded R-modules, where we may assume that $0 = e_1 \leq \cdots \leq e_m$; hence we have $\mathrm{Hom}_R(S^G,R)_{-e_m} \neq \{0\}$. We have to show that $e_m \leq c_r$:

Since G acts faithfully, the trace map $\mathrm{Tr}^G \colon S \to S^G$ is a non-zero homomorphism of graded S^G-modules, that is $0 \neq \mathrm{Tr}^G \in \mathrm{Hom}_{S^G}(S,S^G)_0$. Extending yields the non-zero $S(V)^G$-linear map $\mathrm{Tr}^G \colon S(V) \to S(V)^G$, which hence is surjective. Since the field extension $Q(R) \subseteq S(V)$ is generated by S, there are $f \in S$ and $0 \neq h \in R$ such that $\mathrm{Tr}^G(\frac{f}{h}) = 1$. Since $R \subseteq S^G$, this entails $\mathrm{Tr}^G(f) = h \in R$.

Let $0 \neq \varphi \in \mathrm{Hom}_R(S^G,R)_{-e_m}$, and let $g \in S^G$ such that $\varphi(g) \neq 0$. Hence we have $\varphi(\mathrm{Tr}^G(fg)) = \varphi(\mathrm{Tr}^G(f)g) = \varphi(hg) = \varphi(g)h \neq 0 \in R$. Thus we conclude that $0 \neq (\mathrm{Tr}^G \cdot \varphi) \in \mathrm{Hom}_R(S,R)_{-e_m}$, entailing that $-e_m \geq -c_r$. ♯

Corollary: Broer's degree bound. Let K be infinite. Then, if $S[V]^G$ is Cohen-Macaulay, there is homogeneous generating set of $S[V]^G$ as a K-algebra consisting of elements of degree at most $\max\{|G|, n(|G|-1)\}$.

Proof. By Dade's degree bound we have $d_i \leq |G|$ for all $i \in \{1,\ldots,n\}$, hence we have $e_j \leq n(|G|-1)$ for all $j \in \{1,\ldots,m\}$, ♯

17 Examples: Some small groups

(17.1) Example: Cyclic groups. Let K be a field, let $k \in \mathbb{N}$ such that $\mathrm{char}(K) \nmid k$, and assume that K contains a primitive k-th root of unity ζ_k, let $G := \langle z \rangle \cong C_k$, and let $S := K[X,Y]$; see (3.3).

i) We consider $G \to \mathrm{GL}_2(K) \colon z \mapsto \mathrm{diag}[\zeta_k,\zeta_k]$. Then $R := K[X^k,Y^k] \subseteq S^G$ is a Noether normalization, where $S^G = R \oplus \bigoplus_{i=1}^{k-1}(X^{k-i}Y^i \cdot R)$ as graded R-modules, hence $H_{S^G} = \frac{1+(k-1)T^k}{(1-T^k)^2} \in \mathbb{Q}(T)$. Thus $\{X^k,Y^k\}$ is a set of primary invariants, and $\{1, X^{k-1}Y, \ldots, XY^{k-1}\}$ is a minimal set of secondary invariants.

Indeed, the primary invariants have degree product $d = k^2$, and there are $m = k$ secondary invariants. Since there are no homogeneous invariants of positive degree smaller than k, the degree product $d = k^2$ is as small as possible, so that $\{X^k,Y^k\}$ is an optimal set of primary invariants.

ii) We consider $G \to \mathrm{GL}_2(K) \colon z \mapsto \mathrm{diag}[\zeta_k,\zeta_k^{-1}]$. Then $R := K[X^k,Y^k] \subseteq S^G = K[XY,X^k,Y^k]$ is a Noether normalization, and $S^G = \bigoplus_{i=0}^{k-1}(X^iY^i \cdot R)$ as graded R-modules, hence $H_{S^G} = (\sum_{i=0}^{k-1} T^{2i}) \cdot \frac{1}{(1-T^k)^2} = \frac{1+T^k}{(1-T^2)(1-T^k)} \in \mathbb{Q}(T)$. Thus $\{X^k,Y^k\}$ is a set of primary invariants, and $\{1, XY, \ldots, X^{k-1}Y^{k-1}\}$ is an associated minimal set of secondary invariants; we have $d = k^2$ and $m = k$. Alone, this set of primary invariants is not in general optimal:

Let $G \leq H := \langle z,s \rangle \cong D_{2k}$, where $s \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in \mathrm{GL}_2(K)$; see (6.6). Then we have $S^H = K[XY, X^k+Y^k]$, which is polynomial with degrees $[2,k]$. (Note that to show equality, by Kemper's Theorem it suffices to verify that $\{XY, X^k+Y^k\}$ is algebraically independent.) Thus $Q := S^H \subseteq S^G$ is a Noether normalization, where $d = 2k$ and $m = 2$. Hence H_{S^G} implies that there is an associated minimal set of secondary invariants of degrees $[0,k]$. Since $Y^k \in S^G$ is indecomposable, we conclude that $S^G = Q \oplus (Y^k \cdot Q)$ as graded Q-modules.

Hence $\{XY, X^k+Y^k\}$ is a set of primary invariants, with associated minimal set $\{1, Y^k\}$ of secondary invariants. Since S^G is not polynomial, this set of primary invariants is optimal for all $k \geq 2$, while the former one is so only for $k \leq 2$. $\sharp$

(17.2) Example: Symmetric and alternating groups. a) Let K be a field, let $S := K[\mathcal{X}] = K[X_1, \ldots, X_n]$ where $n \geq 1$, and let $\mathcal{F} := \{e_{n,1}, \ldots, e_{n,n}\}$. Then $R := S^{\mathcal{S}_n} = K[\mathcal{F}] \subseteq S$ is a Noether normalization, thus $\mathcal{F}$ is a **universal** set of primary invariants of $K[\mathcal{X}]^G$, for any subgroup $G \leq \mathcal{S}_n$.

If $\mathrm{char}(K) \not| \, |G|$, then, since $\sum_{i=1}^{n}(\deg(e_{n,i}) - 1) = \sum_{i=0}^{n-1} i = \binom{n}{2}$, Broer's Theorem entails that S^G has a homogeneous K-algebra generating set consisting of elements of degree at most $\max\{n, \binom{n}{2}\}$. This coincides with Göbel's degree bound; but note that the latter holds for arbitrary permutation groups, while their invariant algebras are in general not Cohen-Macaulay.

b) For $n \geq 2$ we have $S^{\mathcal{A}_n} = R \oplus (\mathcal{X}^\lambda)^+ \cdot R$, where $\lambda = [n-1, n-2, \ldots, 2, 1, 0]$; see (9.7). Thus $\{1, (\mathcal{X}^\lambda)^+\}$ is an associated minimal set of secondary invariants; we have $d = \prod_{i=1}^{n} i = n! = 2 \cdot |\mathcal{A}_n|$ and $m = 2$. This shows that $S^{\mathcal{A}_n}$ is Cohen-Macaulay for any field K. Moreover, since $S^{\mathcal{A}_n}$ is not polynomial for $n \geq 3$, we conclude that in this case $\mathcal{F}$ is an optimal set of primary invariants; recall that for $n = 2$ we have $S^{\mathcal{A}_2} = S$. Note that if $\mathrm{char}(K) \neq 2$, then we have $S^{\mathcal{A}_n} = R \oplus \Delta_n \cdot R$ as well, where Δ_n is the discriminant polynomial, so that $\{1, \Delta_n\}$ also is an associated minimal set of secondary invariants. $\sharp$

In the sequel we consider the transitive permutation groups of degree $n = 4$ again; see (9.8): In order to do so, let $S := K[X_1, \ldots, X_4]$, and let $R := K[e_{4,1}, \ldots, e_{4,4}]$. (We again need computational checks, whose details we spare.)

(17.3) Example: The dihedral group of order 8**.** We consider $G := D_8 = \langle (1,2)(3,4), (1,3) \rangle \leq \mathcal{S}_4$. Let $f := (X_1X_3)^+$ and $g := (X_1X_2)^+$; note that $e_{4,2} = f + g$. Then we have $S^G = \bigoplus_{i=0}^{2}(f^i \cdot R)$. We have $d = 24$ and $m = 3$, hence S^G is Cohen-Macaulay for any field K; and $\{e_{4,1}, \ldots, e_{4,4}, f\}$ is a minimal K-algebra generating set, with degrees $[1,2,3,4,2]$, thus S^G is not polynomial.

We have $H_{S^G} = \frac{1+T^2+T^4}{(1-T)(1-T^2)(1-T^3)(1-T^4)} = \frac{1+T^3}{(1-T)(1-T^2)^2(1-T^4)} \in \mathbb{Q}(T)$, which indicates that there might be primary invariants of degree $[1,2,2,4]$, and associated secondary invariants of degree $[1,3]$; then $d = 16$ and $m = 2$, so that the putative primary invariants are optimal:

Let $f_1 := e_{4,1} = X_1^+$, and $f_2 := f$, and $f_3 := g$, and $f_4 := e_{4,4} = X_1X_2X_3X_4$, and $g_2 := e_{4,3} = (X_1X_2X_3)^+$. Letting $R' := K[f_1, \ldots, f_4]$, we check that

$S^G = R' \oplus g_2R'$. Hence $R' \subseteq S^G$ is finite, so that $\{e_{4,1}, f, g, e_{4,4}\}$ is a set of primary invariants, with associated minimal set of secondary invariants $\{1, e_{4,3}\}$; moreover, $\{e_{4,1}, f, g, e_{4,3}, e_{4,4}\}$ is a minimal K-algebra generating set.

(17.4) Example: The Klein 4-group. We consider the regular representation of $G := V_4 = \langle (1,2)(3,4), (1,3)(2,4) \rangle \leq \mathcal{S}_4$. Let $f := (X_1X_3)^+$, and $g := (X_1X_2)^+$, and $h := (X_1X_4)^+$; note that $e_{4,2} = f + g + h$. Then we have $S^G = \bigoplus_{p \in \mathcal{G}} pR$, where $\mathcal{G} := \{1, g, f, g^2, f^2, g^2f\}$. Thus we have $d = 24$ and $m = 6$, hence S^G is Cohen-Macaulay for any field K.

Moreover, if $\mathrm{char}(K) \neq 2$ then $\{e_{4,1}, e_{4,2}, e_{4,3}, f, g\}$ is a minimal K-algebra generating set, having degrees $[1,2,3,2,2]$; but if $\mathrm{char}(K) = 2$ then actually $\{e_{4,1}, \ldots, e_{4,4}, f, g\}$ is a minimal K-algebra generating set, having degrees $[1,2,3,4,2,2]$. Hence, in both cases, S^G is not polynomial.

We get $H_{S^G} = \frac{1+2T^2+2T^4+T^6}{(1-T)(1-T^2)(1-T^3)(1-T^4)} = \frac{1+T^3}{(1-T)(1-T^2)^3} = \frac{1+T^2+T^4}{(1-T)(1-T^2)^2(1-T^3)} = \frac{1+T^2+T^3+T^5}{(1-T)(1-T^2)^2(1-T^4)} \in \mathbb{Q}(T)$, which indicates that there might be primary invariants of degree $[1,2,2,2]$, and associated secondary invariants of degree $[1,3]$; or primary invariants of degree $[1,2,2,3]$, and secondary ones of degree $[1,2,4]$; or primary invariants of degree $[1,2,2,4]$, and secondary ones of degree $[1,2,3,5]$.

i) Let $\mathrm{char}(K) \neq 2$, let $f_1 := e_{4,1} = X_1^+$, and $f_2 := f$, and $f_3 := g$, and $f_4 := h$, and $g_2 := e_{4,3} = (X_1X_2X_3)^+$, and let $R' := K[f_1, \ldots, f_4]$. Then we check that $S^G = R' \oplus g_2R'$. Hence $R' \subseteq S^G$ is finite, so that $\{e_{4,1}, f, g, h\}$ is a set of primary invariants, with associated minimal set of secondary invariants $\{1, e_{4,3}\}$; we have $d = 8$ and $m = 2$, so that the primary invariants are optimal. From this we get the minimal K-algebra generating set $\{e_{4,1}, f, g, h, e_{4,3}\}$.

ii) Let $\mathrm{char}(K) = 2$. Since S^G is not generated in degrees at most 3, there cannot possibly be primary invariants of degree $[1,2,2,2]$, excluding the case $m = 2$. Next we check that there cannot possibly be primary invariants of degree $[1,2,2,3]$, excluding the case $m = 3$:

By considering the homogeneous components of $S_+^G/(S_+^G)^2$ of degree at most 4 we observe that $\{e_{4,1}, f, g, h, e_{4,3}, e_{4,4}\}$ are indecomposable invariants. Hence assuming to the contrary that there are primary invariants of degree $[1,2,2,3]$, we conclude that S^G is generated by $\{1, e_{4,4}\}$ as an R'-module, where $R' := K[e_{4,1}, f, g, h, e_{4,3}] \subseteq S^G$ (which is not polynomial). But we observe that $e_{4,4}^2$ is not contained in the right hand side, a contradiction. $\sharp$

Hence let $f_1 := e_{4,1}$, and $f_2 := e_{4,2}$, and $f_3 := f$, and $f_4 := e_{4,4} = X_1X_2X_3X_4$, as well as $g_2 := g$, and $g_3 := e_{4,3}$, and $g_4 = z := (X_1^2X_2^2X_3)^+$, and let $R' := K[f_1, \ldots, f_4]$. Then we check that $S^G = R' \oplus \bigoplus_{i=2}^4 g_iR'$. Hence $R' \subseteq S^G$ is finite, so that $\{e_{4,1}, e_{4,2}, f, e_{4,4}\}$ is a set of primary invariants, with associated minimal set of secondary invariants $\{1, g, e_{4,3}, z\}$; we have $d = 16$ and $m = 4$, so that the primary invariants are optimal. This yields the minimal K-algebra generating set $\{e_{4,1}, e_{4,2}, f, g, e_{4,3}, e_{4,4}\}$. (The latter sets are suitable for $\mathrm{char}(K) \neq 2$ as well, but they are neither optimal nor minimal.)

(17.5) Example: The cyclic group of order 4**.** We consider the regular representation of $G := C_4 = \langle (1,2,3,4) \rangle \leq \mathcal{S}_4$. Let $f := (X_1X_3)^+$, and $f' := (X_1X_2)^+$, and $g := (X_1^2X_2)^+$, and $h := (X_1^2X_2X_3)^+$; note that $e_{4,2} = f + f'$.

a) Let $\mathrm{char}(K) \neq 2$. Then $S^G = \bigoplus_{p \in \mathcal{G}} pR$, where $\mathcal{G} := \{1, f, g, f^2, h, fg\}$. We have $d = 24$ and $m = 6$, where S^G is Cohen-Macaulay by the Hochster-Eagon Theorem. Moreover, $\{e_{4,1}, \ldots, e_{4,4}, f, g, h\}$ is a minimal K-algebra generating set, having degrees $[1, 2, 3, 4, 2, 3, 4]$, hence S^G is not polynomial.

We have $H_{S^G} = \frac{1+T^2+T^3+2T^4+T^5}{(1-T)(1-T^2)(1-T^3)(1-T^4)} = \frac{1+2T^3+T^4}{(1-T)(1-T^2)^2(1-T^4)} \in \mathbb{Q}(T)$, which indicates that there might be primary invariants of degree $[1, 2, 2, 4]$, and associated secondary invariants of degree $[1, 3, 3, 4]$; then $d = 16$ and $m = 4$, and since H_{S^G} contradicts $m \in \{2, 3\}$, the putative primary invariants are optimal:

Let $f_1 := e_{4,1} = X_1^+$, and $f_2 := f$, and $f_3 := f'$, and $f_4 := e_{4,4} = X_1X_2X_3X_4$, and $g_2 := e_{4,3} = (X_1X_2X_3)^+$, and $g_3 := g$, and $g_4 := h$, and let $R' := K[f_1, \ldots, f_4]$. Then we check that $S^G = R' \oplus \bigoplus_{i=2}^4 g_iR'$. Hence $R' \subseteq S^G$ is finite, so that $\{e_{4,1}, f, f', e_{4,4}\}$ is a set of primary invariants, with associated minimal set of secondary invariants $\{1, e_{4,3}, g, h\}$, and $\{e_{4,1}, f, f', e_{4,3}, g, e_{4,4}, h\}$ is a minimal K-algebra generating set.

b) i) Let $\mathrm{char}(K) = 2$ and $z := (X_1^2X_2^2X_3)^+$. We get $S^G = \sum_{p \in \mathcal{G}} pR$, where $\mathcal{G} := \{1, f, g, f^2, h, z, fh\}$ is a minimal set of secondary invariants. Hence $d = 24$ and $m = 7$, thus S^G is not Cohen-Macaulay. Moreover, $\{e_{4,1}, \ldots, e_{4,4}, f, g, h, z\}$ is a minimal K-algebra generating set, having degrees $[1, 2, 3, 4, 2, 3, 4, 5]$.

We show that there are primary invariants of degree $[1, 2, 2, 4]$; since by the Hilbert-Serre Theorem H_{S^G} contradicts the existence of primary invariants of degree $[1, 2, 2, 2]$ or $[1, 2, 2, 3]$, the putative primary invariants are optimal:

Let again $f_1 := e_{4,1}$, and $f_2 := f$, and $f_3 := f'$, and $f_4 := e_{4,4}$, and $g_2 := e_{4,3}$, and $g_3 := g$, and $g_4 := h$, and $g_4 := z$, and let $R' := K[f_1, \ldots, f_4]$. Then we check that $S^G = R' + \sum_{i=2}^5 g_iR'$. Hence $R' \subseteq S^G$ is finite, so that $\{e_{4,1}, f, f', e_{4,4}\}$ is a set of primary invariants, with associated minimal set of secondary invariants $\{1, e_{4,3}, g, h, z\}$; thus we have $d = 16$ and $m = 5$, also indicating that S^G is not Cohen-Macaulay. Moreover, $\{e_{4,1}, f, f', e_{4,3}, g, e_{4,4}, h, z\}$ is a minimal K-algebra generating set.

Note that, being an invariant algebra of a finite p-group in defining characteristic, S^{C_4} is factorial; see Exercise (18.6). Hence this disproves **Samuel's conjecture**, saying that a factorial finitely generated graded K-algebra should be Cohen-Macaulay [Bertin, 1965].

ii) We show that actually $\mathrm{depth}(S^G) = 3$, by showing that the sequences $[e_{4,1}, e_{4,4}, f]$ and $[e_{4,1}, e_{4,4}, f']$ are regular in S^G:

First, since S is a domain we have $e_{4,1}S \cap S^G = e_{4,1}S^G$, and since $e_{4,1} \in S$ is irreducible and S is factorial, we conclude that $e_{4,1}S \trianglelefteq S$ and thus $e_{4,1}S^G \trianglelefteq S^G$ are prime, so that $S^G/e_{4,1}S^G =: \overline{S^G} = \overline{S}^G \subseteq \overline{S} := S/e_{4,1}S$ are domains, where $\overline{S}$ is a polynomial graded G-algebra again. Next we show that $e_{4,4}\overline{S^G} \trianglelefteq \overline{S^G}$ is prime as well: Since $X_i \in \overline{S}$ is irreducible, hence $X_i\overline{S} \trianglelefteq \overline{S}$ is prime, it suffices to show that $X_i\overline{S} \cap \overline{S}^G = e_{4,4}\overline{S}^G$, where $e_{4,4}\overline{S}^G \subseteq X_i\overline{S}$ anyway; hence letting conversely $a \in X_i\overline{S} \cap \overline{S}^G$, then since G acts transitively on $\{X_1, \ldots, X_4\}$, where the latter are pairwise coprime, we conclude that $a \in \bigcap_{i=1}^n X_i\overline{S} = \prod_{i=1}^4 X_i\overline{S} = e_{4,4}\overline{S}$, hence $a \in e_{4,4}\overline{S} \cap \overline{S}^G = e_{4,4}\overline{S}^G$. Finally, since $\overline{S}^G/e_{4,4}\overline{S}^G$ is a domain, both $f, f' \in \overline{S}^G/e_{4,4}\overline{S}^G$ are regular. $\sharp$

Since S^G is not Cohen-Macaulay, the sequence $[e_{4,1}, e_{4,4}, f, f']$ cannot possibly be regular in S^G. We check this explicitly:

We observe that $e_{4,2} \cdot e_{4,3} = 2z + f \cdot (2e_{4,3} + g) + e_{4,1} \cdot (2e_{4,4} - h) \in \mathbb{Z}[X_1, \ldots, X_4]$, which reduces to the relation $e_{4,2} \cdot e_{4,3} = f \cdot g + e_{4,1} \cdot h \in S$, in degree 5, thus we have $f' \cdot e_{4,3} = f \cdot (e_{4,3} + g) + e_{4,1} \cdot h \in S^G$. This shows that $f \in S^G/(e_{4,1}S^G + e_{4,4}S^G + fS^G)$ is a zero-divisor.

Note that this is related to the fact that, compared to the non-modular case, an additional homogeneous generator of degree 5 is necessary; and that it even shows that $f' \in S^G/(e_{4,1}S^G + fS^G)$ is a zero-divisor. $\sharp$

(17.6) Example: Vector invariants. Let K be a field such that $\mathrm{char}(K) = 2$, let $G := \langle z \rangle \cong C_2$, and let $V := K^2$ be the permutation $K[G]$-module given by $z \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. We consider the faithful $K[G]$-module $V^{\oplus n}$ for $n \geq 2$; see (5.7):

For $i \in \{1, \ldots, n\}$ let $S_i := K[X_i, Y_i] \cong K[V]$, let $S := \bigotimes_{i=1}^n S_i \cong K[V^{\oplus n}]$, let $H := H_1 \times \cdots \times H_n = \langle z_1 \rangle \times \cdots \times \langle z_n \rangle \cong C_2^n$, let $R_i := K[l_i, q_i] = S_i^{H_i}$, where $l_i := X_i + Y_i$ and $q_i := X_iY_i$, and let $R := \bigotimes_{i=1}^n R_i = \bigotimes_{i=1}^n S_i^{H_i} = S^H \subseteq S^G$.

Then R is polynomial, where $H_R = \frac{1}{(1-T)^n(1-T^2)^n} \in \mathbb{Q}(T)$, and we have $H_{S^G} = \frac{1}{2} \cdot ((1+T)^n + (1-T)^n) \cdot H_R \in \mathbb{Q}(T)$. Moreover, since $R \subseteq S$ is finite, we conclude that $R \subseteq S^G$ is finite as well, saying that R is a Noether normalization of S^G, and that $\{l_1, \ldots, l_n, q_1, \ldots, q_n\}$ is a set of primary invariants. Since $K[e_{2n,1}, \ldots, e_{2n,2n}] = S^{\mathcal{S}_{2n}} \subseteq R \subseteq S^G$, from Göbel's degree bound we infer that S^G has a set of secondary invariants with respect to R consisting of orbit sums associated with $(2n-1)$-special combinations, thus having degree at most $\beta := n(2n-1)$; note that $l_i := X_i^+$ and $q_i := (X_iY_i)^+$ are orbit sums associated with the special partitions $[1]$ and $[1, 1]$, respectively.

i) Let first $n := 2$; hence $\beta = 6$. Then we have $H_{S^G} = \frac{1+T^2}{(1-T)^2(1-T^2)^2} \in \mathbb{Q}(T)$, and we recover $r_{12} := (X_1X_2)^+ = X_1X_2 + Y_1Y_2 \in S^G \setminus S^H$, being associated with the special partition $[1, 1]$. Comparing Hilbert series shows that $S^G = R \oplus r_{12}R$, being Cohen-Macaulay, having $\{1, r_{12}\}$ as a minimal set of secondary invariants.

ii) Now let $n := 3$; hence $\beta = 15$ (so that we revert to computations whose details we spare). Then $H_{S^G} = \frac{1+3T^2}{(1-T)^3(1-T^2)^3} \in \mathbb{Q}(T)$, and we recover $r_{ij} := (X_iX_j)^+$ for $i \neq j$, being associated with the special partition $[1, 1]$. We observe that $\{r_{12}, r_{13}, r_{23}\}$ is a K-linearly independent set of indecomposable invariants.

From this, it already follows that S^G is not Cohen-Macaulay: Assume to the contrary that S^G is Cohen-Macaulay. Then S^G is a free graded R-module of rank 4, with minimal set of secondary invariants of degrees $[1, 2, 2, 2]$; hence we conclude that $\{1, r_{12}, r_{13}, r_{23}\}$ is R-linearly independent, which by the identity $l_1 r_{23} + l_2 r_{13} + l_3 r_{12} = l_1 l_2 l_3$ is a contradiction.

Alternatively, Cohen-Macaulayness implies that $[l_1, l_2, l_3] \subseteq S^G$ is a regular sequence; but $l_1 r_{23} + l_2 r_{13} + l_3 r_{12} = l_1 l_2 l_3$ shows that $l_3 r_{12} \in (l_1, l_2) \trianglelefteq S^G$, while since r_{12} is indecomposable we have $r_{12} \notin (l_1, l_2)_2 = \langle l_1^2, l_1 l_2, l_1 l_3, l_2^2, l_2 l_3 \rangle_K$, so that $0 \neq l_3 \in S^G/(l_1, l_2)$ is a zero-divisor, a contradiction. $\sharp$

It remains to find a complete set of secondary invariants: It turns out that $r_{123} := (X_1 X_2 X_3)^+$, being associated with the special partition $[1, 1, 1]$, is an indecomposable invariant, that $\{1, r_{12}, r_{13}, r_{23}, r_{123}\}$ is a minimal set of secondary invariants indeed, and that $\{l_i, q_i, r_{ij}$ for all $i \neq j\} \cup \{r_{123}\}$ is a minimal homogeneous generating set of S^G.

III Exercises and references

18 Exercises: Invariant algebras

(18.1) Exercise: Quadratic forms.
For $n \in \mathbb{N}$ let $\mathcal{V}$ be the set of n-ary complex quadratic forms over $\mathbb{C}$. Show that any $\mathrm{GL}_n(\mathbb{C})$-invariant continuous complex-valued map on $\mathcal{V}$ is constant.

(18.2) Exercise: Binary quadratic forms.
Let q be a binary quadratic form over $K \in \{\mathbb{C}, \mathbb{R}\}$ having discriminant Δ.
a) For $K = \mathbb{C}$ show that $\Delta = 0$ if and only if q is the square of a linear form.
b) For $K = \mathbb{R}$, show that $\Delta = 0$ if and only if q or $-q$ is a square.

(18.3) Exercise: Congruence of triangles.
A triangle $\Delta(P_1, P_2, P_3) \subseteq \mathbb{R}^2$ in the Euclidean plane $\mathbb{R}^2$ is uniquely determined by its vertices $P_i = [x_i, y_i] \in \mathbb{R}^2$. Hence the set of triangles can be identified with the **state space** $\mathbb{R}^6$ via $\Delta(P_1, P_2, P_3) \mapsto [x_1, y_1, x_2, y_2, x_3, y_3]$.

a) Triangles Δ and $\Delta'(P_1', P_2', P_3')$, where $P_i' = [x_i', y_i']$, are called **congruent**, if there are a permutation $\pi \in \mathcal{S}_3$ and a Euclidean transformation α on $\mathbb{R}^2$ such that $[x_i', y_i'] = [x_{i\pi}, y_{i\pi}]^\alpha$ für $i \in \{1, 2, 3\}$. Describe the structure of the latter symmetry group G, and show that congruence is an equivalence relation.

b) Show that G acts naturally via automorphisms on the $\mathbb{R}$-algebras $\mathcal{A} := \mathrm{Maps}(\mathbb{R}^6, \mathbb{R})$ and $R := \mathcal{A} \cap \mathbb{R}[X_1, Y_1, X_2, Y_2, X_3, Y_3]$.

A function $F \in \mathcal{A}$ is called **geometric**, if it is G**-invariant**, that is we have $F^g = F$ for all $g \in G$. Show that the sets $\mathcal{A}^G$ and R^G of geometric (polynomial) functions are $\mathbb{R}$-subalgebras of $\mathcal{A}$.

c) Show that letting

$$A(\Delta) := \left| \det \left(\begin{bmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{bmatrix} \right) \right|,$$

and $C(\Delta) := S_{12} + S_{13} + S_{23}$, where $S_{ij}(\Delta) := \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$, defines geometric functions A and C. What is their geometric interpretation? Are they polynomial? Are the functions S_{ij} geometric as well?

d) A set of geometric functions which uniquely determines all congruence classes of triangles is called **defining**. Show that both the (three) elementary symmetric functions in S_{12}, S_{13}, S_{23}, and the elementary symmetric functions in $S_{12}^2, S_{13}^2, S_{23}^2$ are defining sets. What is the geometric interpretation?

e) Show that any $\mathbb{R}$-algebra generating set of R^G is defining. Actually, the elementary symmetric functions in $S_{12}^2, S_{13}^2, S_{23}^2$ are an $\mathbb{R}$-algebra generating set of R^G; try to prove this. Write A^2 as a polynomial in $S_{12}^2, S_{13}^2, S_{23}^2$.

(18.4) Exercise: Geometric functions.
Keeping the notation of Exercise (18.3), find defining sets, and the $\mathbb{R}$-algebra of geometric (polynomial) functions for **i)** the points in $\mathbb{R}^2$, and **ii)** the lines in $\mathbb{R}^2$.

(18.5) Exercise: Invariant algebras.
a) Let G and H be groups, let V be a $K[G]$-module, and let W be a $K[H]$-module. Show that $V \oplus W$ becomes a $K[G \times H]$-module, that $S[V \oplus W] \cong S[V] \otimes S[W]$, and that $S[V \oplus W]^{G \times H} \cong S[V]^G \otimes S[W]^H$.
b) Let G be a finite group, and let V be a $K[G]$-module. For $d \in \mathbb{N}_0$ show that $S[V]_d^G \neq \{0\}$ only if $|\rho_V(G) \cap Z(\mathrm{GL}(V))|$ divides d.

(18.6) Exercise: Factorial invariant algebras.
Let K be a field, let G be a group having only the trivial one-dimensional K-representation, and let V be a $K[G]$-module. Show that $S[V]^G$ is factorial.

Hint. For $f \in S[V]$ consider the G-action on the associated primary ideals.

(18.7) Exercise: Invariant fields.
Let K be a field, let G be a finite group, let V be a $K[G]$-module such that $n := \dim_K(V) \in \mathbb{N}_0$, and let $\{f_1, \ldots, f_n\} \subseteq S[V]$ be algebraically independent. (Why does such a set always exist?) Show that there is $f \in S(V)^G$ such that $S(V)^G = K(f_1, \ldots, f_n, f)$. Can this be achieved with less than n polynomials?

(18.8) Exercise: Jacobian and Hessian determinants.
Let K be a field, let G be a group, let V be a $K[G]$-module with associated **determinant representation** $\det_V \colon G \to K^* \colon g \mapsto \det(\rho_V(g))$, and let $S := K[X_1, \ldots, X_n]$ be the associated polynomial algebra, where $n := \dim_K(V)$.

a) For $f_1, \ldots, f_n \in S$ let $\det(J(f_1, \ldots, f_n)) := \det([\frac{\partial f_i}{\partial X_j}]_{ij}) \in S$ be their Jacobian determinant. If the f_i are homogeneous, show that $\det(J(f_1, \ldots, f_n))$ is homogeneous as well, and express its degree in terms of the degree of the f_i.

Show that for $g \in G$ we have $\det(J(f_1^g, \ldots, f_n^g)) = \det_V(g) \cdot \det(J(f_1, \ldots, f_n))^g$. Conclude that whenever $\det_V$ is the trivial representation, and $f_1, \ldots, f_n \in S^G$, then we have $\det(J(f_1, \ldots, f_n)) \in S^G$ as well.

b) For $f \in S$ let $H(f) := \det([\frac{\partial^2 f}{\partial X_i \partial X_j}]_{ij}) \in S$ denote the corresponding **Hessian determinant**. If f is homogeneous, show that $H(f)$ is homogeneous as well, and express its degree in terms of the degree of f.

Show that for $g \in G$ we have $H(f^g) = \det_V(g)^2 \cdot H(f)^g$. Conclude that whenever $\det_V^2$ is the trivial representation, and $f \in S^G$, then we have $H(f) \in S^G$ as well.

(18.9) Exercise: The cyclic group of order 2.
Let K be a field such that $\mathrm{char}(K) \neq 2$, and let $G := \langle z \rangle \cong C_2$, where $z := \mathrm{diag}[-1, -1] \in \mathrm{GL}_2(K)$. Letting $S := K[X, Y]$ be the associated polynomial

algebra, show that as graded K-algebras we have the **presentation**

$$S^G = K[X^2, XY, Y^2] \cong K[A, B, C]/(AC - B^2),$$

where $K[A, B, C]$ is the polynomial algebra with degrees $[2, 2, 2]$.

(18.10) Exercise: The cyclic group of order 3.
Let K be a field such that $\mathrm{char}(K) \neq 3$, let $G := \langle z \rangle \cong C_3$ act on K^2 by

$$z \mapsto \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix},$$

and let $S := K[X, Y]$ be the associated polynomial algebra. Compute a minimal homogeneous generating set of S^G, and show that Noether's degree bound is sharp in this case. How does this relate to Exercise (18.13)?

(18.11) Exercise: The dihedral group of order 8.
Let K be a field such that $\mathrm{char}(K) \neq 2$, and let $G := \langle s, t \rangle \cong D_8$, where

$$s := \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \in \mathrm{GL}_2(K) \quad \text{and} \quad t := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in \mathrm{GL}_2(K).$$

Letting $S := K[X, Y]$ be the associated polynomial algebra, show that $S^G = K[X^2 + Y^2, X^2Y^2]$. Determine the Hilbert series of S^G. Is S^G polynomial? How does this relate to (6.6)?

(18.12) Exercise: The dihedral group of order $2(p+1)$.
Let K be a field such that $\mathrm{char}(K) = p > 0$, where $p \equiv 3 \pmod 4$, and let $(a + bT) \in \mathbb{F}_p[T]/(T^2 + 1) \cong \mathbb{F}_{p^2}$ have order $p + 1$. Moreover, let $V := K^2$, let $S := K[X, Y]$ be the associated polynomial algebra, and let $G := \langle s, t \rangle$, where

$$s := \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \in \mathrm{GL}_2(K) \quad \text{and} \quad t := \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in \mathrm{GL}_2(K).$$

a) Show that t has order $p+1$, such that $t^s = t^{-1}$. Conclude that $G \cong D_{2(p+1)}$.
b) Show that $S^G = K[X^2 + Y^2, X^{p+1} + Y^{p+1}]$. How does this relate to (6.6)?

(18.13) Exercise: Cyclic groups.
Let K be a field, let $k \in \mathbb{N}$ such that $\mathrm{char}(K) \nmid k$, let $\zeta_k \in K$ be a primitive k-th root of unity, and let $G := \langle z \rangle \cong C_k$. We consider representations $G \to \mathrm{GL}_2(K)$, and let $S := K[X, Y]$ be the associated polynomial algebra.

a) We consider the representation given by $z \mapsto \mathrm{diag}[\zeta_k, \zeta_k]$, for which we have already seen that $S^G = K[f_0, \ldots, f_k]$, where $f_i := X^iY^{k-i} \in S$ for $i \in \{0, \ldots, k\}$. Show that as graded K-algebras we have the presentation

$$S^G \cong K[F_0, \ldots, F_k]/(F_0F_k - F_iF_{k-i}; 1 \leq i \leq \lfloor\frac{k}{2}\rfloor),$$

where $K[F_0, \ldots, F_k]$ is polynomial with degrees $[k, \ldots, k]$.

b) We consider the representation given by $z \mapsto \operatorname{diag}[\zeta_k, \zeta_k^{-1}]$, for which we have already seen that $S^G = \bigoplus_{i=0}^{k-1}(X^iY^i \cdot R)$ as graded K-algebras, where $R := K[X^k, Y^k]$. Show that as graded K-algebras we have the presentation

$$S^G \cong K[F_1, \ldots, F_k, F_k']/(F_kF_k' - F_iF_{k-i}; 1 \leq i \leq \lfloor \frac{k}{2} \rfloor),$$

where $K[F_1, \ldots, F_k, F_k']$ is polynomial with degrees $[2, 4, \ldots, 2(k-1), k, k]$.

(18.14) Exercise: Generic representations of cyclic groups.
Let $G := \langle z \rangle \cong C_k$ be the cyclic group of order $k \in \mathbb{N}$, and let K be a field such that $\operatorname{char}(K) \nmid k$ containing a primitive k-th root of unity ζ_k.
a) We consider the representation $G \to \mathrm{GL}_n(K) \colon z \mapsto \operatorname{diag}[\zeta_k^{e_i}; i \in \{1, \ldots, n\}]$, where $e_1, \ldots, e_n \in \mathbb{Z}$ and $n \in \mathbb{N}$. Letting $S := K[X_1, \ldots, X_n]$ be the associated polynomial algebra, show that S^G is generated by the monomials

$$\{\prod_{i=1}^{n} X_i^{a_i} \in S;\, a_1, \ldots, a_n \in \{0, \ldots, k\},\, \sum_{i=1}^{n} a_ie_i \equiv 0 \pmod{k}\}.$$

b) In particular, letting $k_1, \ldots, k_n \in \mathbb{N}$ be pairwise coprime such that $k = \prod_{i=1}^{n} k_i$, and $z \mapsto \operatorname{diag}[\zeta_{k_i}; i \in \{1, \ldots, n\}]$, show that $S^G = K[X_1^{k_1}, \ldots, X_n^{k_n}]$.

(18.15) Exercise: Number of generators.
Let K be field, let G be a finite group such that $\operatorname{char}(K) \nmid |G|$, and let V be a $K[G]$-module such that $n := \dim_K(V) \in \mathbb{N}_0$.
a) Show that $S[V]^G$ is generated by at most $\binom{n+|G|}{n}$ homogeneous elements.
b) Let $G := \langle z \rangle \cong C_k$ be the cyclic group of order $k \in \mathbb{N}$, let K contain a primitive k-th root of unity ζ_k, and let G act on $V = K^n$ by $z \mapsto \zeta_k \cdot E_n$. Show that the minimal homogeneous generating sets of $S[V]^G$ consist of $\binom{n+k-1}{n-1}$ elements of degree p. (Thus the above bound is essentially sharp.)

(18.16) Exercise: The cyclic group of order p.
Let K be a field such that $\operatorname{char}(K) = p > 0$, let $V := K^2$, and let $S := K[X, Y]$ be the associated polynomial algebra.
a) Let $G := \langle z \rangle \cong C_p$ act by

$$z \mapsto \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in \mathrm{GL}_2(K).$$

Show that $S^G = K[X, Y^p - X^{p-1}Y]$, so that S^G is polynomial and Noether's degree bound holds. Show that the trace ideal equals $S^G_{\{1\}} = (X^{p-1}) \trianglelefteq S^G$.
b) Let $H := \langle z, s \rangle \cong C_p \colon C_{p-1}$ act by $s \mapsto \operatorname{diag}[\zeta_{p-1}^{-1}, \zeta_{p-1}] \in \mathrm{GL}_2(K)$, and let $U := \langle z, s, t \rangle \cong (C_p \colon C_{p-1}) \times C_{p-1}$ act by $t \mapsto \operatorname{diag}[\zeta_{p-1}, 1] \in \mathrm{GL}_2(K)$. Determine generating sets of S^H and S^U. Are these invariant algebras polynomial?

(18.17) Exercise: The dihedral group of order $2p$.
Let K be a field such that $\mathrm{char}(K) = p \geq 3$, let $V := K^2$, let $S := K[X, Y]$ be the associated polynomial algebra, and let $G := \langle s, t \rangle \cong D_{2p}$.
i) Show that $S^G = K[X, (Y^p - X^{p-1}Y)^2]$, where G acts by

$$s \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \in \mathrm{GL}_2(K) \quad \text{and} \quad t \mapsto \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in \mathrm{GL}_2(K).$$

ii) Show that $S^G = K[X^2, Y^p - X^{p-1}Y]$, where G acts (contragrediently) by

$$s \mapsto \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \in \mathrm{GL}_2(K) \quad \text{and} \quad t \mapsto \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in \mathrm{GL}_2(K).$$

Moreover, for both actions, determine the Hilbert series of S^G. Is S^G polynomial? Show that G is a pseudoreflection group. How many pseudoreflections are there? Does Theorem (8.2) hold?

(18.18) Exercise: Bertin's example.
Let K be a field such that $\mathrm{char}(K) = 2$, let $G := \langle z \rangle \cong C_4$, let $V := K[G]$ be the regular $K[G]$-module, with respect to the K-basis $\{1, z, z^2, z^3\} \subseteq V$, and let $S := K[X_1, \ldots, X_4]$ be the associated polynomial algebra. Determine the Hilbert ideal of S^G. Does Hilbert's Finiteness Theorem hold? Does Benson's Lemma hold for $S^G_+ \trianglelefteq S^G$?

(18.19) Exercise: An inadmissible counterexample.
Let K be a field, let $G := K^+$ act on K^2 by

$$K \to \mathrm{GL}_2(K) \colon t \mapsto \begin{bmatrix} 1 & 0 \\ t & 1 \end{bmatrix},$$

and let $S := K[X, Y]$ be the associated polynomial algebra.
a) Show that $(X^2) \trianglelefteq S$ is a G-invariant ideal, so that $R := S/(X^2)$ becomes a graded K-algebra, on which G acts faithfully by automorphisms of graded K-algebras. Is R a domain, or factorial, or a polynomial algebra?
b) Show that the set $R^G \subseteq R$ of G-fixed points in R is a K-algebra again, which is generated by the image of $\{XY^n \in S; n \in \mathbb{N}_0\}$ with respect to the natural epimorphism $S \to R$. Conclude that R^G is *not* a finitely generated K-algebra.

(18.20) Exercise: Nagata's counterexample.
Let $\{a_{ij} \in \mathbb{C}; i \in \{1, \ldots, 16\}, j \in \{1, \ldots, 3\}\}$ be algebraically independent over $\mathbb{Q}$, and let $G \leq \mathrm{GL}_{32}(\mathbb{C})$ be the group of all block diagonal matrices

$$\mathrm{diag}\left[c_i \cdot \begin{bmatrix} 1 & b_i \\ 0 & 1 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{C}); i \in \{1, \ldots, 16\} \right],$$

where $\prod_{i=1}^{16} c_i = 1$ and $\sum_{i=1}^{16} b_i a_{ij} = 0$, for $j \in \{1, \ldots, 3\}$. Show that the invariant algebra $S[\mathbb{C}^{32}]^G$ is *not* a finitely generated $\mathbb{C}$-algebra. (At least try.)

(18.21) Exercise: Contragredient modules.
Let K be a field, let G be a finite group, let V be a $K[G]$-module, and let V^* be the associated contragredient $K[G]$-module.
a) Show that $S[V^*]_d \cong (S[V]_d)^*$ as $K[G]$-modules, for $d \in \mathbb{N}_0$.
b) Assume that $\operatorname{char}(K) \nmid |G|$. Show that we have $H_{S[V]^G} = H_{S[V^*]^G} \in \mathbb{Q}(T)$.
c) Assume that $\operatorname{char}(K) = 0$. Show that $S[V]^G$ is polynomial if and only if $S[V^*]^G$ is polynomial. In this case, are $S[V]^G$ and $S[V^*]^G$ (graded) isomorphic?

(18.22) Exercise: Birman's identity.
Let G be a finite group, let K be a field such that $\operatorname{char}(K) \nmid |G|$, let V be a $K[G]$-module such that $n := \dim_K(V) \in \mathbb{N}_0$, and let $\chi_V \colon G \to K$ be the associated character. Show that $H_{S[V]^G} = \frac{1}{|G|} \cdot \sum_{g \in G} \exp\left(\sum_{d \geq 1} \frac{1}{d} \cdot \chi_V(g^d) T^d\right) \in \mathbb{Q}[[T]]$.

(18.23) Exercise: Molien's formula for semi-invariants.
Let G be a finite group, let K be a field such that $\operatorname{char}(K) \nmid |G|$, let $\lambda \colon G \to K^*$ be a one-dimensional representation, and let V be a $K[G]$-module such that $n := \dim_K(V) \in \mathbb{N}_0$. Show that the set of semi-invariants $S[V]^G_\lambda \subseteq S[V]$ is a graded $S[V]^G$-module, and that its Hilbert series is given as $H_{S[V]^G_\lambda} = \frac{1}{|G|} \cdot \sum_{g \in G} \frac{\lambda(g)^{-1}}{\det(E_n - T \cdot \rho_V(g))} \in \mathbb{Q}(T)$, where we identify λ with its Brauer lift.

(18.24) Exercise: Stanley's identity.
Let G be a finite group, let K be a field such that $\operatorname{char}(K) \nmid |G|$, let V be a $K[G]$-module such that $n := \dim_K(V) \in \mathbb{N}_0$, and let $\lambda \colon G \to K^* \colon g \mapsto \det(\rho_V(g))^{-1}$ be the contragredient of the associated determinant representation. Show that $H_{S[V]^G}(T^{-1}) = (-T)^n \cdot H_{S[V]^G_\lambda} \in \mathbb{Q}(T)$. In particular, conclude $S[V]^G_\lambda \neq \{0\}$.

(18.25) Exercise: Sums of roots of unity.
For $k \in \mathbb{N}$ find $\sum_{i=0}^{k-1} \frac{1}{|1-\zeta_k^i|^2} \in \mathbb{C}$, where $\zeta_k \in \mathbb{C}$ is a primitive k-th root of unity.

(18.26) Exercise: Regular representation of cyclic groups.
Let $G := \langle z \rangle \cong C_n$ be the cyclic group of order $n \in \mathbb{N}$, and let $V := \mathbb{C}[G]$ be the regular $\mathbb{C}[G]$-module, given by the action of G on the $\mathbb{C}$-basis $\{1, z, \ldots, z^{n-1}\}$. Show that the Hilbert series of $S[V]^G$ is $H_{S[V]^G} = \frac{1}{n} \cdot \sum_{d \in \mathbb{N},\, d \mid n} \frac{\varphi(d)}{(1-T^d)^{\frac{n}{d}}} \in \mathbb{Q}(T)$, where $\varphi \colon \mathbb{N} \to \mathbb{N}$ is Euler's totient function.

(18.27) Exercise: Abelian groups of order 8.
Let K be a field such that $\operatorname{char}(K) \neq 2$ containing a primitive 4-th root of unity ζ_4, let $V := K^3$, and let $S := K[X, Y, Z]$ be the associated polynomial algebra. Moreover, let $G := \langle y \rangle \times \langle z \rangle \cong C_2 \times C_4$ act on V by $y \mapsto \operatorname{diag}[-1, -1, 1]$ and $z \mapsto \operatorname{diag}[1, 1, \zeta_4]$, and let $H := \langle a, b, c \rangle \cong C_2^3$ act on V by $a \mapsto \operatorname{diag}[-1, 1, 1]$ and $b \mapsto \operatorname{diag}[1, -1, 1]$ and $c \mapsto \operatorname{diag}[1, 1, -1]$.

Determine S^G and S^H, show that S^G and S^H are not isomorphic as K-algebras, but have the same Hilbert series $H_{S^G} = H_{S^H} = \frac{1}{(1-T^2)^3} \in \mathbb{Q}(T)$,

(18.28) Exercise: Nakajima's example.
Let p be a prime, and let

$$G := \left\{ \begin{bmatrix} 1 & 0 & a+b & b \\ 0 & 1 & b & b+c \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \in \mathrm{GL}_4(\mathbb{F}_p); a,b,c \in \mathbb{F}_p \right\} \leq \mathrm{GL}_4(\mathbb{F}_p).$$

Show that G is generated by pseudoreflections, where $|G| = p^3$, but the associated invariant algebra $S[\mathbb{F}_p^4]^G$ is not polynomial.

(18.29) Exercise: Reflection representation 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 trivial $\mathbb{Q}[\mathcal{S}_n]$-submodule, and that $V := W/W'$ is an absolutely irreducible faithful reflection representation of $\mathcal{S}_n$.
b) Determine $\{f_1, \ldots, f_{n-1}\} \subseteq S[V]^{\mathcal{S}_n}$ homogeneous and algebraically independent such that $\deg(f_i) = i+1$ and $S[V]^{\mathcal{S}_n} = \mathbb{Q}[f_1, \ldots, f_{n-1}]$.

(18.30) Exercise: Polyhedral groups.
We consider the regular tetrahedron and the regular octahedron, embedded into Euclidean 3-space, centered at the origin. Let $\widehat{\mathcal{T}} \leq O_3(\mathbb{R})$ and $\widehat{\mathcal{O}} \leq O_3(\mathbb{R})$ be their full symmetry groups, respectively, let $\mathcal{T} := \widehat{\mathcal{T}} \cap \mathrm{SO}_3(\mathbb{R})$ and $\mathcal{O} := \widehat{\mathcal{O}} \cap \mathrm{SO}_3(\mathbb{R})$ be their rotational symmetry groups, also called the **tetrahedral** and **octahedral groups**, respectively. Let $S := S[\mathbb{R}^3]$.

a) Show that $\widehat{\mathcal{T}} = \{\pm E_3\} \times \mathcal{T}$, where $\mathcal{T} \cong \mathcal{A}_4$, and that $\widehat{\mathcal{T}}$ is generated by reflections and irreducible. Conclude that $S^{\widehat{\mathcal{T}}}$ is polynomial with degrees $[2,3,4]$. (It is the group $G_{2,2,3}$ in the Shephard-Todd classification.)

Show that $H_{S^{\mathcal{T}}} = \frac{1+T^6}{(1-T^2)(1-T^3)(1-T^4)} \in \mathbb{Q}(T)$, and provide a homogeneous invariant $f \in S^{\mathcal{T}}$ of degree 6, such that $S^{\mathcal{T}} = S^{\widehat{\mathcal{T}}} \oplus f S^{\widehat{\mathcal{T}}}$.

b) Show that $\widehat{\mathcal{O}} = \{\pm E_3\} \times \mathcal{O}$, where $\mathcal{O} \cong \mathcal{S}_4$, and that $\widehat{\mathcal{O}}$ is generated by reflections and irreducible. Conclude that $S^{\widehat{\mathcal{O}}}$ is polynomial with degrees $[2,4,6]$. (It is the group $G_{2,1,3}$ in the Shephard-Todd classification.)

Show that $H_{S^{\mathcal{O}}} = \frac{1+T^9}{(1-T^2)(1-T^4)(1-T^6)} \in \mathbb{Q}(T)$, and provide a homogeneous invariant $g \in S^{\mathcal{O}}$ of degree 9, such that $S^{\mathcal{O}} = S^{\widehat{\mathcal{O}}} \oplus g S^{\widehat{\mathcal{O}}}$. How is this related to the irreducible reflection representation of $\mathcal{S}_4$?

(18.31) Exercise: A complex reflection group.
We consider the group $G := \mathrm{GL}_3(\mathbb{F}_2)$, which is the (up to isomorphism) unique (non-abelian) simple group of order 168.

a) Show that G has conjugacy classes having elements of order $[1,2,3,4,7,7|$, and that its irreducible complex representations have dimension $[1,3,3,6,7,8]$.

b) Let V be one of the (faithful) 3-dimensional irreducible $\mathbb{C}[G]$-modules, and let $\mathcal{S} \subseteq G$ be the set of involutions. Show that $|\mathcal{S}| = 21$, and that $s \in \mathcal{S}$ has trace $\chi_V(s) = -1$ on V. Conclude that $\widehat{G} := \langle -\rho_V(\mathcal{S}) \rangle \leq \mathrm{GL}_3(\mathbb{C})$ is a non-real complex pseudoreflection group, which is generated by reflections, and show that $\widehat{G} = \{\pm E_3\} \times G$. (It is the group G_{24} in the Shephard-Todd classification.)

c) Show that $S[V]^{\widehat{G}}$ is polynomial with degrees $[4, 6, 14]$. Moreover, show that $H_{S[V]^G} = \frac{1+T^{21}}{(1-T^4)(1-T^6)(1-T^{14})} \in \mathbb{Q}(T)$, and provide a homogeneous invariant $g \in S[V]^G$ of degree 21, such that $S[V]^G = S[V]^{\widehat{G}} \oplus g \cdot S[V]^{\widehat{G}}$.

(18.32) Exercise: Invariant forms.
Let G be a finite group, and let $n \in \mathbb{N}$.
a) If $G \leq \mathrm{GL}_n(\mathbb{C})$, show that there is $A \in \mathrm{GL}_n(\mathbb{C})$ such that $A^{-1}GA \leq U_n(\mathbb{C})$. If $G \leq \mathrm{GL}_n(\mathbb{R})$, show that there is $B \in \mathrm{GL}_n(\mathbb{R})$ such that $B^{-1}GB \leq O_n(\mathbb{R})$.
b) If $G \leq \mathrm{GL}_n(\mathbb{C})$ is irreducible, show that there is $C \in \mathrm{GL}_n(\mathbb{C})$ such that $C^{-1}GC \leq \mathrm{GL}_n(\mathbb{R})$ if and only if there is a non-zero quadratic G-invariant.

(18.33) Exercise: Pseudoreflection groups.
Let K be a field such that $\mathrm{char}(K) = 0$, let G be a finite group, let V be a faithful $K[G]$-module such that G is generated by pseudoreflections, let $d_1, \ldots, d_n \in \mathbb{N}$ be the associated degrees, where $n := \dim_K(V) \in \mathbb{N}_0$, and let $\zeta_m \in K$ be a primitive m-th root of unity, where $m \in \mathbb{N}$. Show that $\zeta_m \cdot E_n \in G$, if and only if $m \mid d_i$ for all $i \in \{1, \ldots, n\}$.

(18.34) Exercise: Basic invariants.
Let K be a field such that $\mathrm{char}(K) = 0$, let G be a finite group, let V be a $K[G]$-module such that $n := \dim_K(V) \in \mathbb{N}_0$, and let $S[V]^G = K[f_1, \ldots, f_n] = K[f'_1, \ldots, f'_n]$ be polynomial. Use Jacobian matrices to give an alternative proof that the associated multisets of degrees coincide.

(18.35) Exercise: Jacobian criterion.
Let K be a field of $\mathrm{char}(K) = 0$, let $K[\mathcal{X}] = K[X_1, \ldots, X_n]$ for $n \in \mathbb{N}_0$, let $p_{n,k} := \sum_{i=1}^n X_i^k \in K[\mathcal{X}]$ be the power sums for $k \in \mathbb{N}$, and let $e_{n,1}, \ldots, e_{n,n} \in K[\mathcal{X}]$ be the elementary symmetric polynomials, where $\deg(e_{n,i}) = i$. Use the Jacobian criterion to show directly that $\{p_{n,1}, \ldots, p_{n,n}\}$ and $\{e_{n,1}, \ldots, e_{n,n}\}$ are algebraically independent.

(18.36) Exercise: Newton identities.
a) Let K be a field, let $K[\mathcal{X}] = K[X_1, \ldots, X_n]$ where $n \in \mathbb{N}_0$, let $p_{n,k} := \sum_{i=1}^n X_i^k \in K[\mathcal{X}]$ be the power sums for $k \in \mathbb{N}$, and let $e_{n,0}, \ldots, e_{n,n} \in K[\mathcal{X}]$ be the elementary symmetric polynomials, where $\deg(e_{n,i}) = i$. Show that for $k \in \{1, \ldots, n\}$ we have $ke_{n,k} = \sum_{i=1}^k (-1)^{i-1} p_{n,i} e_{n,k-i}$.
b) Let $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) > n$. Determine all solutions $[x_1, \ldots, x_n] \in K^n$ of the system of equations $\sum_{i=1}^n x_i^k = 0$, where $k \in \{1, \ldots, n-1\}$.

(18.37) Exercise: Symmetric polynomials.
Let K be a field, let $\mathcal{S}_n$ act naturally on $K[\mathcal{X}] := K[X_1, \ldots, X_n]$, where $n \in \mathbb{N}_0$, and let $p_{n,k} := \sum_{i=1}^n X_i^k \in K[\mathcal{X}]$ be the power sums, for $k \in \mathbb{N}$. Show that $K[\mathcal{X}]^{\mathcal{S}_n} = K[p_{n,1}, \ldots, p_{n,n}]$ whenever $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) > n$. Is the assumption on the characteristic necessary?

(18.38) Exercise: Elementary symmetric polynomials.
Let K be a field, let $\mathcal{S}_n$ act naturally on $K[\mathcal{X}] = K[X_1, \ldots, X_n]$, where $n \in \mathbb{N}_0$, and let the monomials $\mathcal{X}^\alpha \in K[\mathcal{X}]$, for $\alpha \in \mathbb{N}_0^n$, be totally ordered **lexicographically** by letting $X_1 > \cdots > X_n$. Then the largest monomial occurring in a polynomial $0 \neq f \in K[\mathcal{X}]$ is called its **leading monomial**.
a) Let $0 \neq f \in K[\mathcal{X}]^{\mathcal{S}_n}$, and let $\mathcal{X}^\alpha$ be its leading monomial, where $\alpha = [\alpha_1, \ldots, \alpha_n] \in \mathbb{N}_0^n$. Show that α is a partition, that is $\alpha_1 \geq \cdots \geq \alpha_n$. Moreover, show that $\prod_{i=1}^n e_{n,i}^{\alpha_i - \alpha_{i-1}} \in K[\mathcal{X}]^{\mathcal{S}_n}$, where $\alpha_0 := 0$, has leading monomial $\mathcal{X}^\alpha$.
b) Give an algorithm utilizing the lexicographic order on the set of monomials to write a symmetric polynomial as a polynomial in the elementary symmetric polynomials $\{e_{n,1}, \ldots, e_{n,n}\}$. Compare this algorithm (which is actually due to Gauss) with the algorithm given in (9.3).
c) For $n \in \{1, \ldots, 4\}$ and $k \in \{1, \ldots, 4\}$, write the symmetric polynomials Δ_n^2 and $p_{n,k}$ as polynomials in the elementary symmetric polynomials.

(18.39) Exercise: Göbel's algorithm.
Let K be a field, let $\mathcal{S}_n$ act naturally on $K[\mathcal{X}] = K[X_1, \ldots, X_n]$, where $n \in \mathbb{N}_0$, and let $G \leq \mathcal{S}_n$. Give an algorithm utilizing Göbel's Theorem to write a G-invariant polynomial as a polynomial in the elementary symmetric polynomials $\{e_{n,1}, \ldots, e_{n,n}\}$ and the orbit sums $(\mathcal{X}^\alpha)^+$, where $\alpha \in \mathbb{N}_0$ is $(n-1)$-special.

(18.40) Exercise: Direct products of symmetric groups.
a) Let $\mathcal{S} := \mathcal{S}_{n_1} \times \cdots \times \mathcal{S}_{n_r} \leq \mathcal{S}_n$ be a **Young subgroup**, where $r \in \mathbb{N}$ and $n = \sum_{i=1}^r n_i \in \mathbb{N}$, let K be a field, and let $\mathcal{S}$ act on $K[\mathcal{X}_1, \ldots, \mathcal{X}_r]$, where $\mathcal{X}_i := \{X_{i,1}, \ldots, X_{i,n_i}\}$, and where the i-th direct factor acts naturally on $\mathcal{X}_i$ and fixes the other indeterminates. Show that $K[\mathcal{X}_1, \ldots, \mathcal{X}_r]^{\mathcal{S}}$ is a polynomial algebra, and determine a set of basic invariants.
b) Use this to give improved versions of the algorithms in Exercise (18.38) for Young subgroups, and to give an improved version of Göbel's algorithm in Exercise (18.39) for intransitive permutation groups.

(18.41) Exercise: Trace ideal.
a) Let K be a field, let $\mathcal{S}_n$ act naturally on $K[\mathcal{X}] = K[X_1, \ldots, X_n]$, where $n \in \mathbb{N}_0$, and let $G \leq \mathcal{S}_n$. Show that the trace ideal $\mathrm{Tr}^G(K[\mathcal{X}]) \trianglelefteq K[\mathcal{X}]^G$ is generated by $\mathrm{Tr}^G(\mathcal{X}^\alpha)$, where $\alpha \in \mathbb{N}_0$ is $(n-1)$-special such that $p \nmid [G \colon \mathrm{Stab}_G(\mathcal{X}^\alpha)]$.
b) Let $\mathrm{char}(K) = 2$ and $n \geq 2$. Show that $\mathrm{Tr}^{\mathcal{S}_n}(K[\mathcal{X}]) = \Delta_n \cdot K[\mathcal{X}]^{\mathcal{S}_n}$
c) Let $\mathrm{char}(K) = 2$ and $n \geq 2$. Give a similar description of $\mathrm{Tr}^{\mathcal{A}_n}(K[\mathcal{X}])$.

Hint for c). Consider $(n-1)$-special partitions of length at least $n-3$.

(18.42) Exercise: Galois resolvents.
Let K be a field, let $f \in K[X]$ be separable of degree $n \in \mathbb{N}$, having roots $\{x_1, \ldots, x_n\}$ in a splitting field $K \subseteq L$, let $\mathrm{Aut}_K(L) \cong A \leq \mathcal{S}_n$ be the Galois group of f. Moreover, for $H \leq G \leq \mathcal{S}_n$ such that $A \leq G$ let $\pi_H^G \colon G \to \mathcal{S}_{H\backslash G}$ be the action homomorphism of G with respect to H, and for $F \in K[X_1, \ldots, X_n]^H$ let $\rho := \rho_H^G(F)(x_1, \ldots, x_n) \in K[X]$ be the associated resolvent. If ρ is separable, show that ρ has Galois group isomorphic to $\pi_H^G(A)$.

(18.43) Exercise: Generalized quaternion groups.
Let K be a field containing a primitive $2k$-th root of unity ζ_{2k}, where $k \geq 2$, let $G \cong Q_{4k}$ be the generalized quaternion group of order $4k$, where

$$G := \left\langle \begin{bmatrix} \zeta_{2k} & 0 \\ 0 & \zeta_{2k}^{-1} \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\rangle \leq \mathrm{GL}_2(K),$$

and let $S := K[X, Y]$ be the associated polynomial algebra.
a) Show that the Hilbert series of S^G is given as $H_{S^G} = \frac{1+T^{2k+2}}{(1-T^4)(1-T^{2k})} \in \mathbb{Q}(T)$.
b) Find primary invariants $\{f_1, f_2\} \subseteq S^G$ such that $\deg(f_1) = 4$ and $\deg(f_2) = 2k$, and secondary invariants $\{g_1, g_2\} \subseteq S[V]^G$ such that $\deg(g_1) = 0$ and $\deg(g_2) = 2k+2$, yielding the Hironaka decomposition $S^G = \bigoplus_{i=1}^2 (g_i \cdot K[f_1, f_2])$. Conclude that $\{f_1, f_2\}$ are optimal primary invariants, and that $\{f_1, f_2, g_2\}$ is a minimal generating set of S^G.
c) Show that as graded K-algebras we have the presentation

$$S^G \cong K[A, B, C]/(C^2 - AB^2 + 4A^{k+1}),$$

where $K[A, B, C]$ is the polynomial algebra with degrees $[4, 2k, 2k+2]$.

(18.44) Exercise: An abelian group of order 8.
Let K be a field such that $\mathrm{char}(K) \neq 2$ containing a primitive 4-th root of unity ζ_4, let $V := K^3$, let $S := K[X, Y, Z]$ be the associated polynomial algebra, and let $G := \langle y \rangle \times \langle z \rangle \cong C_2 \times C_4$ act on V by $y \mapsto \mathrm{diag}[-1, -1, 1]$ and $z \mapsto \mathrm{diag}[1, 1, \zeta_4]$; recall that the Hilbert series of S^G equals $H_{S^G} = \frac{1}{(1-T^2)^3} \in \mathbb{Q}(T)$.
a) Show that there is no set of primary invariants $\{f_1, f_2, f_3\} \subseteq S^G$ such that $\deg(f_1) = \deg(f_2) = \deg(f_2) = 2$.
b) Find primary invariants $\{f_1, f_2, f_3\} \subseteq S^G$ such that $\deg(f_1) = \deg(f_2) = 2$ and $\deg(f_3) = 4$, and secondary invariants $\{g_1, \ldots, g_m\} \subseteq S^G$ for some $m \in \mathbb{N}$, yielding the Hironaka decomposition $S^G = \bigoplus_{i=1}^m (g_i \cdot K[f_1, \ldots, f_3])$. Are $\{f_1, f_2, f_3\}$ optimal primary invariants? Find a minimal generating set of S^G.

(18.45) Exercise: Depth of invariant algebras.
Let K be a field, let G be a finite group, let V be a $K[G]$-module such that $\dim_K(V) \geq 2$. Show that $\mathrm{depth}(S[V]^G) \geq 2$.

(18.46) Exercise: Depth of invariant algebras.
Let K be a field, let G be a finite group, let $H \leq G$, let V be a $K[G]$-module such that $n := \dim_K(V) \in \mathbb{N}_0$, and let $S := S[V]$.
a) Show that $\operatorname{depth}(S^H) = \operatorname{depth}_{S^G}(S^H)$, where the latter denotes the depth of S^H as an S^G-module.
b) Assume that $\operatorname{char}(K) \nmid [G\colon H]$. Show that $\operatorname{depth}(S^G) \geq \operatorname{depth}(S^H)$.
c) Conclude that S^G is Cohen-Macaulay whenever $n \leq 2$.

(18.47) Exercise: Cohen-Macaulay property.
Let p be a prime, let K be a field such that $\operatorname{char}(K) = p$, and for the following p-groups G let V be the natural $K[G]$-module, and let V^* be the associated contragredient $K[G]$-module. For both $S[V]^G$ and $S[V^*]^G$ provide a set of primary invariants and an associated minimal set of secondary invariants, as well as a minimal homogeneous generating set; moreover, decide about their Cohen-Macaulayness and polynomiality:
a) Let $G \cong C_p^2$ be given as

$$G := \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in \mathrm{GL}_3(\mathbb{F}_p); a, b \in \mathbb{F}_p \right\} \leq \mathrm{GL}_3(\mathbb{F}_p).$$

Show that $S[V^*]^G$ is polynomial, while $S[V]^G$ is not, but is Cohen-Macaulay.
b) Let $G \cong C_p^4$ be given as

$$G := \left\{ \begin{bmatrix} 1 & 0 & 0 & a & 0 & 0 & d \\ 0 & 1 & 0 & 0 & b & 0 & d \\ 0 & 0 & 1 & 0 & 0 & c & d \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \in \mathrm{GL}_7(\mathbb{F}_p); a, b, c, d \in \mathbb{F}_p \right\} \leq \mathrm{GL}_7(\mathbb{F}_p).$$

Show that $S[V]^G$ is polynomial, while $S[V^*]^G$ is not even Cohen-Macaulay.

(18.48) Exercise: Cohen-Macaulay property of vector invariants.
Let p be a prime, let $G := \langle \pi \rangle \cong C_p$ be the cyclic group of order p, let K be a field such that $\operatorname{char}(K) = p$, let $V = W \oplus W \oplus W$ as $K[G]$-modules, where

$$\rho_W : G \to GL_2(K) \colon \pi \mapsto \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

let $S[V] = K[X_1, Y_1, X_2, Y_2, X_3, Y_3]$ be the associated polynomial K-algebra.
a) For $1 \leq i < j \leq 3$ let $h_{ij} := X_i Y_j - X_j Y_i \in S[V]$. 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 $[Y_1, Y_2, Y_3]$ is not a regular sequence in $S[V]^G$.

(18.49) Exercise: The dihedral group of order 10.
The dihedral group D_{10} is the symmetry group of the regular 5-gon in the Euclidean plane, hence its action on the vertices gives rise to the embedding $D_{10} \cong G := \langle t, s\rangle \leq \mathcal{S}_5$, where $t := (1,2,3,4,5)$ and $s := (1,4)(2,3)$. Let K be a field, let V be the associated permutation $K[G]$-module, and let $S := S[V]$.

a) Compute the Hilbert series H_{S^G} of the invariant algebra S^G, and show that Noether's degree bound holds for S^G, independently of the characteristic of K.

b) Let $\mathrm{char}(K) \neq 5$. Show that S^G is Cohen-Macaulay. Moreover, show that S^G has an optimal set of primary invariants of degrees $[1,2,2,3,5]$, and an associated set of secondary invariants of degrees $[1,3,4,4,5,8]$. Conclude that S^G has a minimal homogeneous generating set of degrees $[1,2,2,3,3,4,4,5,5]$.

c) Let $\mathrm{char}(K) = 5$. Show that S^G has an optimal set of primary invariants of degrees $[1,2,3,4,5]$, and an associated set of secondary invariants of degrees $[1,2,3,4,4,5,5,6,6,7,8,10]$. Conclude that S^G is Cohen-Macaulay, and has a minimal homogeneous generating set of degrees $[1,2,2,3,3,4,4,5,5,6]$.

(18.50) Exercise: The dihedral group of order 8.
Let K be a field such that $\mathrm{char}(K) \neq 2$, and let $G := \langle s, t\rangle \cong D_8$, where

$$s := \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \in \mathrm{GL}_2(K) \quad \text{and} \quad t := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in \mathrm{GL}_2(K).$$

Letting $S := K[X,Y]$ be the associated polynomial algebra, by Exercise (18.11) it is known that the invariant algebra S^G is polynomial with degrees $[2,4]$.

Find a homogeneous K-basis of the coinvariant algebra S_G, and show that its Hilbert series equals $H_{S_G} = 1+2T+2T^2+2T^3+T^4 \in \mathbb{Q}(T)$. Moreover, describe the action of G on the homogeneous components of S_G, and show that S_G is as a $K[G]$-module isomorphic to the regular module.

(18.51) Exercise: Broer's degree bound.
Let G be a finite group, let K be a field such that $\mathrm{char}(K) \nmid |G|$, let V be a $K[G]$-module such that $n := \dim_K(V) \in \mathbb{N}_0$, let $\lambda\colon G \to K^*\colon g \mapsto \det(\rho_V(g))^{-1}$, let $d \in \mathbb{N}_0$ be the minimum degree of a non-zero homogeneous semi-invariant with respect to λ (which by Exercise (18.24) exists), let $\{f_1,\ldots,f_n\}$ be a set of primary invariants such that $d_i := \deg(f_i) \in \mathbb{N}$, let $\{g_1,\ldots,g_m\}$ be a minimal set of secondary invariants such that $e_j := \deg(g_j) \in \mathbb{N}_0$, and let $e := \max\{e_1,\ldots,e_m\}$.

Show that $e + d = \sum_{i=1}^n (d_i - 1)$. What happens in the case $\rho_V(G) \leq \mathrm{SL}(V)$?

19 Exercises: Commutative algebra

(19.1) Exercise: Tensor products.
Let K be a field, let V and W be K-vector spaces, and let $V \otimes W$ be a tensor product of V and W over K (which we assume to exist).

a) Show that $V \otimes W$ is uniquely determined up to isomorphism of K-vector spaces, and that $V \otimes W \cong W \otimes V$ as K-vector spaces. Moreover, if U be a K-vector space, show that $(V \otimes W) \otimes U \cong V \otimes (W \otimes U)$ as K-vector spaces.

b) Let V and W be finitely generated, having K-bases $\{v_1, \ldots, v_n\} \subseteq V$ and $\{w_1, \ldots, w_m\} \subseteq W$, where $n := \dim_K(V)$ and $m := \dim_K(W)$. Show that $\{v_i \otimes w_j \in V \otimes W; i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}\} \subseteq V \otimes W$ is a K-basis.

c) Let R and S be K-algebras. Show that $R \otimes S$ becomes a K-algebra by letting $(f \otimes g)(f' \otimes g') := ff' \otimes gg'$, for $f, f' \in R$ and $g, g' \in S$; show that if R and S are commutative then so is $R \otimes S$, and if R and S are graded then so is $R \otimes S$.

(19.2) Exercise: Symmetric algebras.
Let K be a field, let V be a finitely generated K-vector space, let $T(V) = \bigoplus_{d \geq 0} V^{\otimes d}$ be the associated tensor algebra, and let $T(V)^- = \bigoplus_{d \geq 0} V^{\otimes d,-}$.

Show that $T(V)^-$ is a homogeneous ideal of $T(V)$, which is generated by

$$\{v \otimes w - w \otimes v \in V^{\otimes 2}; v, w \in V\} \subseteq V^{\otimes 2,-}.$$

(19.3) Exercise: Exterior algebras.
Let K be a field, let V be a finitely generated K-vector space, and let $T(V) = \bigoplus_{d \geq 0} V^{\otimes d}$ be the tensor algebra. Moreover, let $T(V)^+ \trianglelefteq T(V)$ be the (homogeneous) ideal generated by $\{v \otimes v \in V^{\otimes 2}; v \in V\}$, and let $\Lambda(V) := T(V)/T(V)^+ = \bigoplus_{d \geq 0} \Lambda^d(V)$ be the associated graded **exterior K-algebra**, whose homogeneous components are called the **exterior powers** of V.

a) For $d \in \mathbb{N}_0$ let $V^{\otimes d,+} := \langle (v_1 \otimes \cdots \otimes v_d) \cdot (1 + \pi); v_1, \ldots, v_d \in V, \pi \in \mathcal{S}_d \rangle_K \leq V^{\otimes d}$. Show that $V^{\otimes 2,+} \leq T(V)^+$. Moreover, show that if $\operatorname{char}(K) \neq 2$ then $T(V)^+$ is as an ideal generated by $V^{\otimes 2,+}$, and we have $T(V)^+ \cap V^{\otimes d} = V^{\otimes d,+}$, so that $\Lambda^d(V) = V^{\otimes d}/V^{\otimes d,+}$. (What happens in the case $\operatorname{char}(K) = 2$?)

b) Show that $\Lambda(V)$ is **graded commutative**, that is for $a \in \Lambda^d(V)$ and $b \in \Lambda^e(V)$ we have $ab = (-1)^{de} \cdot ba \in \Lambda(V)$. Which universal property does $\Lambda(V)$ have? Moreover, provide a K-basis of $\Lambda^d(V)$, for $d \in \mathbb{N}_0$, in terms of a given K-basis of V, and determine $\dim_K(\Lambda^d(V))$. Is $\Lambda(V)$ finite-dimensional, and if so, what is its K-dimension? What is the Hilbert series of $\Lambda(V)$?

c) Let G be a group, and assume that V is a $K[G]$-module. Show that $\Lambda(V)$ naturally becomes a graded G-algebra. Moreover, if G is finite such that $\operatorname{char}(K) \nmid |G|$, show that the Hilbert series of the invariant algebra $\Lambda(V)^G$ is given as $H_{\Lambda(V)^G} = \frac{1}{|G|} \cdot \sum_{g \in G} \det\big(\rho_V(1) + \rho_V(g) \cdot T\big) \in \mathbb{Q}(T)$.

(19.4) Exercise: Noetherian modules.
Let R be a commutative ring and let M be an R-module.
a) Let $N \leq M$ be an R-submodule. Show that if M is Noetherian, then so are N and M/N; and conversely if both N and M/N are Noetherian, then so is M.

b) Show that M is Noetherian if and only if each submodule of M is finitely generated. Conclude that if R is Noetherian, then M is Noetherian if and only if M is finitely generated.
c) Let $S \subseteq R$ be a subring, such that S is a direct summand of R as an S-module. Show that if R is Noetherian then so is S.

(19.5) Exercise: Prime avoidance.
Let R be a commutative ring.
a) Let $P_1, \ldots, P_n \trianglelefteq R$ be ideals, for $n \in \mathbb{N}$, and assume that R is a K-algebra for an infinite field K, or that at most two of the P_i are not prime. Given $I \trianglelefteq R$ such that $I \subseteq \bigcup_{i=1}^n P_i$, show that there is $i \in \{1, \ldots, n\}$ such that $I \subseteq P_i$.
b) Let $I_1, \ldots, I_n \trianglelefteq R$ be ideals, for $n \in \mathbb{N}$, and let $P \trianglelefteq R$ be a prime ideal such that $\bigcap_{i=1}^n I_i \subseteq P$. Show that there is $i \in \{1, \ldots, n\}$ such that $I_i \subseteq P$.
c) Let R be Noetherian, let $I \trianglelefteq R$ be an ideal, and let $M \neq \{0\}$ be a finitely generated R-module. Show that either I contains a non-zerodivisor on M, or there is $0 \neq m \in M$ such that $I \subseteq \mathrm{ann}_R(m)$.

(19.6) Exercise: Prime avoidance.
We present a few examples to show how prime avoidance cannot be improved:
a) Let $R := \mathbb{F}_2[X,Y]/(X,Y)^2$. Show that $(X,Y) \trianglelefteq R$ is the union of three properly smaller ideals.
b) Let K be a field, let $R := K[X,Y]/(XY,Y^2)$, and let $P := (X) \trianglelefteq R$, and $Q := (Y) \trianglelefteq R$, and $I := (X^2, Y) \trianglelefteq R$. Show that the homogeneous elements of I are contained in $P \cup Q$, but $I \not\subseteq P$ and $I \not\subseteq Q$. Which of these ideals is prime?
c) Let K be an infinite field, let $R := K[X,Y]$, and let $I := (X,Y) \trianglelefteq R$. Show that I is contained in the union of an infinite set of prime ideals, neither of which contains I.

(19.7) Exercise: Localization.
Let R be a commutative ring, let $U \subseteq R$ be a multiplicatively closed subset such that $1 \in U$, and let M be an R-module.
a) Show that R_U is a commutative ring, and that $\nu \colon R \to R_U \colon r \mapsto \frac{r}{1}$ is a homomorphism of commutative rings. Moreover, show that M_U is an R_U-module, and that $M \to M_U \colon m \mapsto \frac{m}{1}$ is a homomorphism of R-modules.
b) Show that the localization R_U has the following universal property: If $\varphi \colon R \to S$ is a homomorphism of commutative rings such that $\varphi(U) \subseteq S^*$, then there is unique ring homomorphism $\widehat{\varphi} \colon R_U \to S$ such that $\nu \cdot \widehat{\varphi} = \varphi$.
c) Show that for $J \trianglelefteq R_U$ we have $(\nu^{-1}(J))_U = J$, and conclude that the map $\nu^{-1} \colon \{J \trianglelefteq R_U\} \to \{I \trianglelefteq R\}$ is an inclusion-preserving and intersection-preserving injection, mapping prime ideals to prime ideals.
d) Show that for an ideal $I \trianglelefteq R$ we have $I \subseteq \nu^{-1}(I_U) = \{f \in R; fu \in I \text{ for some } u \in U\} \trianglelefteq R$, and conclude that we have $I_U \neq R_U$ if and only if $I \cap U = \emptyset$. Moreover, show that for a prime ideal $P \trianglelefteq R$ we have $P = \nu^{-1}(P_U)$ if and only if $P \cap U = \emptyset$, in which case $P_U \trianglelefteq R_U$ is a prime ideal as well.

(19.8) Exercise: Local rings.
Let R be a local commutative ring, and let M be a finitely generated R-module. Show that M is **projective**, that is M is a direct summand of a free R-module, if and only if M is free.

(19.9) Exercise: Nakayama Lemma.
Let R be a commutative ring, let $I \trianglelefteq R$ be an ideal, let M be a finitely generated R-module, and let $\varphi \in \mathrm{End}_R(M)$.
a) If $\varphi(M) \leq MI$, show that there are $a_1, \ldots, a_n \in R$, for some $n \in \mathbb{N}$, such that $a_i \in I^i$ and $\varphi^n + \sum_{i=1}^{n} a_i \varphi^{n-i} = 0 \in \mathrm{End}_R(M)$.
b) If $MI = M$, show that there is $a \in \mathrm{ann}_R(M)$ such that $a \equiv 1 \pmod{I}$.
c) Show that φ is surjective if and only if φ is bijective [Vasconcelos, 1969].

(19.10) Exercise: Lemma of Gauss.
Let R be a factorial domain. Show the **Lemma of Gauss**, saying that the polynomial ring $R[X]$ is factorial again.

(19.11) Exercise: Integral closure.
Let $R \subseteq S$ be an extension of commutative rings.
a) Show that for $\overline{R} = \overline{R}^S := \{s \in S; s \text{ is integral over } R\} \subseteq S$ we have $\overline{\overline{R}} = \overline{R}$.
b) Show that if R is a factorial domain, then it is integrally closed.

(19.12) Exercise: Integral extensions.
Let $R \subseteq S$ be an integral extension of commutative rings.
a) Let S be a domain. Show that R is a field if and only if S is a field.
b) Let $Q \trianglelefteq S$ be a prime ideal. Show that Q is a maximal ideal of S if and only if $Q \cap R \trianglelefteq R$ is a maximal ideal of R.
c) Let $P \trianglelefteq R$ be a maximal ideal. Show that there is a prime ideal $Q \trianglelefteq S$ such that $P = Q \cap R$, and that any such Q is maximal.

(19.13) Exercise: Going up.
Let $R \subseteq S$ be an integral extension of domains, such that R is integrally closed.
a) Assume that S is integrally closed as well, and that the field extension $K := \mathrm{Q}(R) \subseteq \mathrm{Q}(S) =: L$ is normal. Given a prime ideal $P \trianglelefteq R$, show that the Galois group $\mathrm{Aut}_K(L)$ acts transitively on the set of prime ideals of S lying over P.
b) Let $P' \subseteq P \trianglelefteq R$ be prime ideals, and let $Q \trianglelefteq S$ be prime such that $Q \cap R = P$. Show that there is a prime ideal $Q' \trianglelefteq S$ such that $Q' \subseteq Q$ and $Q' \cap R = P'$.

(19.14) Exercise: Krull's Principal Ideal Theorem.
Let R be a Noetherian commutative ring, and let $P \trianglelefteq R$ be a prime ideal such that $\mathrm{ht}(P) = r$, for some $r \in \mathbb{N}_0$. Show that there are $f_1, \ldots, f_r \in R$ such that P is a minimal prime divisor of $(f_1, \ldots, f_r) \trianglelefteq R$.

(19.15) Exercise: Zero-dimensional algebras.
Let K be a field, and let R be a finitely generated commutative K-algebra. Show that $\dim(R) = 0$ if and only if $\dim_K(R) < \infty$.

(19.16) Exercise: Infinite dimension.
Let K be a field, let $R = K[X_1, X_2, \ldots]$ be the polynomial algebra in countably infinitely many variables, let $d_0 := 0$ and $d_i \in \mathbb{N}$ such that $d_i < d_{i+1}$, let $P_i := (X_{d_{i-1}+1}, \ldots, X_{d_i}) \trianglelefteq R$, for $i \in \mathbb{N}$, and let $U := R \setminus (\bigcup_{i \geq 1} P_i) \subseteq R$. Show that R_U is Noetherian such that $\dim(R_U) = \sup\{d_i - d_{i-1} \in \mathbb{N}; i \in \mathbb{N}\}$.

(19.17) Exercise: Graded fields of fractions.
Let K be a field, and let R be a finitely generated (non-negatively) graded K-domain. Then the associated **graded field of fractions** is defined as the **(non-connected) $\mathbb{Z}$-graded** K-algebra $\mathrm{GrQ}(R) := L = \bigoplus_{d \in \mathbb{Z}} L_d \subseteq \mathrm{Q}(R)$, where $L_d := \{\frac{f}{g} \in \mathrm{Q}(R); f \in R_{i+d}, g \in R_i \text{ for } i \in \mathbb{Z}\}_K$

a) Show that L is a K-domain containing R, which is graded in the appropriate sense, and that any non-zero homogeneous element of L has a homogeneous inverse, such that L_0 is a field, but that L in general is *not* a field.

If $L \neq L_0$, then let $L_0[X^{\pm 1}]$ be the algebra of Laurent polynomials over L_0 in the indeterminate X, where $\deg(X) := \min\{d \in \mathbb{N}; L_d \neq \{0\}\}$. Show that we have $L \cong L_0[X^{\pm 1}]$ as $\mathbb{Z}$-graded K-algebras, and that $\mathrm{Q}(R) = \mathrm{Q}(L) = L_0(X)$.

b) Let $R \subseteq S$ be finite, where S is a finitely generated graded K-domain, and let $M := \mathrm{GrQ}(S)$. Show that $L \subseteq M$ is a finite extension of **graded fields**, where actually M is a free L-module of finite rank $[M\colon L] := \mathrm{rk}_L(M) \in \mathbb{N}$, having an L-basis consisting of homogeneous elements of S.

Comparing with the (genuine) field extensions $L_0 \subseteq M_0$ and $\mathrm{Q}(R) \subseteq \mathrm{Q}(S)$, show that $[M_0\colon L_0] = [M\colon L] = [\mathrm{Q}(S)\colon \mathrm{Q}(R)]$. Give a reformulation of (the proof of) the degree theorem for $R \subseteq S$ in terms of their graded fields of fractions.

(19.18) Exercise: Carlson's Lemma.
Let K be a field, let R be a graded K-algebra, and let M and N be finitely generated graded R-modules. Show that any short exact sequence $\{0\} \to M \to M \oplus N \to N \to \{0\}$ of graded R-modules splits.

Hint. Consider $\{0\} \to \mathrm{Hom}_R(N, M)_0 \to \mathrm{Hom}_R(N, M \oplus N)_0 \to \mathrm{End}_R(N)_0$.

(19.19) Exercise: Hilbert series.
Let K be a field, and let $K[\mathcal{X}] := K[X_1, \ldots, X_n]$, for $n \in \mathbb{N}_0$, be the polynomial algebra in the indeterminates $X_1, \ldots, X_n$.
a) For the standard grading show that $\dim_K(K[\mathcal{X}]_d) = \binom{n+d-1}{d}$, for $d \in \mathbb{N}_0$.
b) Given any grading, letting $d_1, \ldots, d_n \in \mathbb{N}_0$, show that $K[\mathcal{X}]/(X_1^{d_1}, \ldots, X_n^{d_n})$ becomes a graded K-algebra, and determine its Hilbert series.

c) Show that $R := K[X_1, X_2, X_3]/(X_1^2 - X_2^2)$ becomes a graded K-algebra with respect to the degrees $[1, 1, 2]$, having Hilbert series $H_R = \frac{1}{(1-T)^2} \in \mathbb{Q}(T)$, but R is not a polynomial algebra. Is R a domain or factorial?

(19.20) Exercise: Coefficient growth.
Let $H := \frac{f}{\prod_{i=1}^{k}(1-T^{d_i})} = \sum_{d \geq 0} a_d T^d \in \mathbb{Q}((T))$, where $f \in \mathbb{Z}[T^{\pm 1}]$, $d_1, \ldots, d_k \in \mathbb{N}$, and $a_d \geq 0$. Show that there is $c \in \mathbb{N}_0$ such that the sequence $[\frac{a_d}{d^c} \in \mathbb{Q}; d \geq 0]$ is bounded, where for $\gamma(H) := -\nu_1(H) \geq 1$ the minimal choice is $c = \gamma(H) - 1$.

(19.21) Exercise: Hilbert polynomials.
Let K be a field, let R be a commutative graded K-algebra, having a homogeneous generating set of cardinality $k \in \mathbb{N}_0$, and let M be a finitely generated graded R-module. Show that there is a (unique) **Hilbert polynomial** $h \in K[T]$ of degree at most $k - 1$, such that $\dim_K(M_d) = h(d)$ for all $d \gg 0$.

Hint. Mimic the proof of Hilbert's Theorem on the shape of Hilbert series.

(19.22) Exercise: Noether normalization.
Let K be a field, and let R be a commutative graded K-algebra. Show that the following assertions are equivalent: **i)** R is Noetherian. **ii)** R is a finitely generated K-algebra. **iii)** The irrelevant ideal $R_+ \trianglelefteq R$ is finitely generated.

(19.23) Exercise: Homogeneous sets of parameters.
Let K be a field, and let $\mathcal{F}_1 := \{X, XY\}$ and $\mathcal{F}_2 := \{X^2, XY\}$.
a) For $i \in \{1, 2\}$, show that $\mathcal{F}_i \subseteq K[X, Y]$ is algebraically independent, but is not a regular sequence. Conclude that $\dim(K[\mathcal{F}_i]) = 2$, but $K[\mathcal{F}_i] \subseteq K[X, Y]$ is not a Noether normalization.
b) Find a homogeneous generating set of $K[X, Y]$ as a $K[\mathcal{F}_i]$-module, and determine the field of fractions $K(\mathcal{F}_i)$. How does $K(\mathcal{F}_i)$ relate to $K(X, Y)$?

(19.24) Exercise: Regular sequences.
Let K be a field.
a) Let $R := K[X^2, X^2Y, Y^2, Y^3] \subseteq K[X, Y]$. Show that $\{X^2, Y^2\}$ is a regular sequence in $K[X, Y]$, but not a regular sequence in R.
b) Let $R := K[X^4, X^3Y, XY^3, Y^4] \subseteq K[X, Y]$. Show that $\{X^4, Y^4\}$ is a homogeneous system of parameters of R, and that R is not Cohen-Macaulay.

20 References

Invariant theory

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

[2] E. Campbell, D. Wehlau: Modular invariant theory, Encyclopaedia of Mathematical Sciences 139, Springer, 2011.

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

[4] H. Kraft: Geometrische Methoden in der Invariantentheorie, 2. Aufl., Aspekte der Mathematik D1, Vieweg, 1985.

[5] M. Neusel: Invariant theory, Student Mathematical Library 36, American Mathematical Society, 2007.

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

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

[8] T. Springer: Invariant theory, Lecture Notes in Mathematics 585, Springer, 1977.

[9] R. Stanley: Invariants of finite groups and their applications to combinatorics, Bulletin of the American Mathematical Society 1 (3), 1979, 475—511.

[10] B. Sturmfels: Algorithms in invariant theory, Texts and Monographs in Symbolic Computation, Springer, 2008.

Algebra and Commutative Algebra

[11] M. Atiyah, I. MacDonald: Introduction to commutative algebra, Addison-Wesley, 1969.

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

[13] H. Cohen: A course in computational algebraic number theory, Graduate Texts in Mathematics 138, Springer, 1993.

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

[15] E. Kunz: Introduction to commutative algebra and algebraic geometry, Birkhäuser, 1985.

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

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

Groups and Reflection Groups

[18] N. Bourbaki: Éléments de mathématique, Fasc. XXXIV: Groupes et algèbres de Lie, Chapitre IV: Groupes de Coxeter et systèmes de Tits, Chapitre V: Groupes engendrés par des réflexions, Chapitre VI: systèmes de racines, Actualités Scientifiques et Industrielles 1337, Hermann, 1968.

[19] M. Broué: Introduction to complex reflection groups and their braid groups, Lecture Notes in Mathematics 1988, Springer, 2010.

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

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

[22] P. Landrock: Finite group algebras and their modules, London Mathematical Society Lecture Note Series 84, Cambridge University Press, 1983.