Algorithmic Aspects of Invariant Theory

Diplomarbeit
zur Erlangung des akademischen Grades
"Diplom-Ingenieur"
in der Studienrichtung **Informatik**

Thomas Bayer
Research Institute for Symbolic Computation
Johannes Kepler Universität Linz
Thomas.Bayer@risc.uni-linz.ac.at

Eingereicht am 8.4.1998 bei a.Univ.-Prof. Dr. Peter Paule

Contents

Preface

Invariant theory has its origin in the 18th and 19th century. Mathematicians like C.F. Gauss, A. Cayley, J. Sylvester and P. Gordon studied invariant theory. Then in 1890 D. Hilbert solved the fundamental problem whether invariant rings are finitely generated as algebras with nonconstructive methods, which were considered to be "theology" at that time. Hilbert responded the criticism in 1893 with a constructive proof. Hilbert's striking results seem to have killed invariant theory for a long time. But with the rise of computers, mathematicians and computer scientists again gained interest in invariant theory.

In this thesis we are concerned with constructive invariant theory of finite matrix groups over arbitrary fields following the book of B. Sturmfels [43] an the work of G. Kemper [22], [23]. We provide a theoretical study of the existing algorithms, present a new algorithm for the intersection of invariant rings, and a Mathematica implementation of almost all presented algorithms in the `Invariants` package.

The structure of this thesis is as follows :
In **Chapter 1** we state the required background from commutative algebra and representation theory. Only those results are proved where the author was not able to find a direct proof in the literature. For all other proofs we give a reference. **Chapter 2** is an introduction to invariant theory of finite groups and forms the theoretical heart of this thesis. In Section 2.1 we treat the symmetric polynomials and in Section 2.2 we give an introduction to invariant theory from a representation theoretic point of view. Section contains the finiteness theorems of E. Noether and D. Hilbert. In Section 2.4 we present Molien's Theorem and in Section 2.5 consider the Cohen-Macaulay property of invariant rings. All stated results, which will be used later, are proved. **Chapter 3** contains the description of algorithms for computing invariant rings. In Section 3.1 we describe the algorithms of Dade and Kemper for the computation of primary invariants, a straightforward algorithm for the computation of secondary invariants in the nonmodular case and Kemper's algorithm for the computation of secondary invariants

in the modular case. In Section 3.2 we present a new algorithm for the computation of the intersection of invariant rings. **Chapter 4** is devoted to the study selected topics. In Section 4.1 we study the invariant theory of complex representations of finite abelian groups and present algorithms for the computation of primary and secondary invariants and fundamental invariants without using Gröbner bases. In Section 4.2 we study of invariant theory of the tensor and exterior algebra and prove an analogue to Molien's theorem. For the tensor algebra we solve the problem of the finite generation of the invariant ring for Abelian groups. A summation example from R. Stanley together with a slight generalization is presented in Section 4.3. In Section 4.4 we show how the invariant theory of $SL_d(\mathbf{C})$ can be used to prove theorems in projective geometry. **Chapter 5** contains a documentation of my Mathematica package `Invariants.`

What's new

Some results of this thesis seem to be new, namely :

Section 3.1.1 : Proposition 18.

Section 3.2 : All results with the exception of Lemma 13.

Section 4.1 : All algorithms.

Section 4.2.1 : All results.

Section 4.3 : The generalization to characters.

Acknowledgments

I am very grateful to my supervisor Peter Paule for accepting the topic, for all the discussions and for showing me the beauty of mathematics. I owe many thanks to Gregor Kemper from IWR Heidelberg and Josef Schicho from RISC-Linz for the useful discussions. Furthermore I am very grateful to Bruno Buchberger for all his effort in teaching RISC students. I want to thank my parents for their moral support. Finally I am particularly grateful to Heidi for her patience and warm presence.

Chapter 1

Preliminaries

In this chapter we state the necessary prerequisites in representation theory and commutative algebra.

Convention With $\mathbf{N}$ we denote the positive integers without 0, with $\mathbf{N}_0$ the positive integers containing 0 and with $\mathbf{C}$ the complex numbers. For $n \in \mathbf{N}$ the elements of $\mathbf{N}_0^n$ will be denoted with bold letters, i.e. we write $\boldsymbol{\alpha} \in \mathbf{N}_0^n$ and $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_n)$. For any $\boldsymbol{\alpha}$ we define $|\boldsymbol{\alpha}| := \sum_{i=1}^n \alpha_i$. If $x_1, x_2, ..., x_n$ are variables then $\mathbf{x}^{\boldsymbol{\alpha}} := \prod_{i=1}^n x_i^{\alpha_i}$. With $\mathbf{K}$ we denote an arbitrary field. Any reference to a Theorem (Proposition, Lemma, ...) in this thesis is of the form Theorem $C.S.N$ which denotes Theorem N in Section S of chapter C.

1.1 Groups, Rings and Modules.

We present some basic notions of algebra and refer to any algebra book for more details.

Definition 1 *Let G be a nonempty set and $\cdot : G \times G \to G$ be a binary operation. G is a* ***group*** *iff the following 3 conditions are satisfied.*
(a) $\exists 1_G \in G : \forall \sigma \in G \; 1_G \cdot \sigma = \sigma \cdot 1_G = \sigma,$
(b) $\forall \sigma \in G : \exists \tau \in G \; \sigma \cdot \tau = \tau \cdot \sigma = 1_G, \forall \sigma \in G$
(c) $\forall \sigma, \tau, \rho \in G : (\sigma \cdot \tau) \cdot \rho = \sigma \cdot (\tau \cdot \rho).$
The group G is ***Abelian*** *(commutative) iff $\forall \sigma, \tau \in G : \sigma \cdot \tau = \tau \cdot \sigma$. The set $[\sigma] := \{\tau \cdot \sigma \cdot \tau^{-1} \mid \tau \in G\}$ is the* ***conjugacy class*** *of $\sigma \in G$.*

Note that the conjugacy classes of G are a partition of G.

Definition 2 *Let R be a nonempty set, $+ : R \times R \to R$ and $\cdot : G \times G \to G$ be binary operations. R is a* ***ring*** *iff the following 4 conditions are satisfied.*

(a) R is an Abelian group w.r.t. $+$,
(b) $\forall r,s,t \in R : (r \cdot s) \cdot t = r \cdot (s \cdot t)$,
(c) $\forall r,s,t \in R : (r + s) \cdot t = r \cdot s + r \cdot t$,
(d) $\forall r,s,t \in R : r \cdot (s + t) = r \cdot s + r \cdot t$.
*R is **commutative** iff $\forall r,s \in R : r \cdot s = s \cdot r$. R is a ring with **unity** iff $\exists 1_R \in R : \forall r \in r\ 1_R \cdot r = r$. An element $r \in R$ is called **nilpotent** iff there exists $n \in \mathbf{N}$ s.t. $r^n = 0$.*

Definition 3 *Let $R \subseteq S$ be commutative rings with unity. A map $\pi : S \to R$ is a **projection** iff π is surjective and $\pi\mid_R = id$. The map π is $R-$**linear** iff $\pi(r \cdot s) = r \cdot \pi(s)$ for all $r \in R$ and $s \in S$.*

We will now introduce the concept of group actions which plays an important not only in representation theory, but also in many areas of mathematics, e.g. in algebraic combinatorics. For more details on group actions we refer to Kerber [25]

Definition 4 *Let G be a group and M be a nonempty set. A **group-action** of G on M is a map*

$$\begin{aligned} G \times M &\to M, \\ (\sigma, m) &\mapsto \sigma x \end{aligned}$$

s.t.

$$\begin{aligned} 1_G m &= m, \\ \sigma(\tau m) &= (\sigma\tau) m \end{aligned}$$

*for all $m \in M$ and $\sigma, \tau \in G$. M is called a **(left)** $G-$**set**.*

Since all rings in this thesis contain a unit element, we define modules only over rings with unity.

Definition 5 *Let R be a ring w.r.t. the operations $+_R$ and $\cdot_R$, M be a nonempty set, and $+ : M \times M \to M$ and $\cdot : R \times M \to M$ be binary operations. M is an $R-$**module** iff*
(a) M is an Abelian group w.r.t. $+$,
(b) $\forall r,s \in R : \forall m \in M\ (r \cdot_R s) \cdot m = r \cdot (s \cdot m)$,
(c) $\forall r \in R : \forall m,n \in M\ r \cdot (m + n) = r \cdot m + r \cdot n$,
(d) $\forall r,s \in R : \forall m \in M\ (r +_R s) \cdot m = r \cdot m + s \cdot m$,
(e) $\forall m \in M : 1_R \cdot m = m$.
*We say that R acts on M or that M is a left $R-$module. M is **finitely generated** iff there exists a set $m_1, m_2, ..., m_k$ of elements of M s.t. for all $f \in M$ we have $f = \sum_{i=1}^{k} r_i \cdot_R m_i$ for some $r_i \in R$. $\langle m_1, m_2, ..., m_k \rangle_R := \{\sum_{i=1}^{k} r_i \cdot_R m_i \mid r_i \in R\}$. A submodule I of R, considered as an $R-$module is called and **ideal**. The ideal I is **prime** if $\forall r,s \in R : r \cdot s \in I, r \notin I \Rightarrow s \in I$.*

1.2 Representation Theory

In part one we define basic notions of representation theory of finite groups, omitting all proofs. We consider only complex representations, because all properties which we need are invariant w.r.t. complex conjugation, and refer to Fulton and Harris [14], Sagan [34] or Simon [41] for the proofs and further details. Part two is devoted to the investigation of invariant subspaces and we prove some results which will be used in Chapter 2.

1.2.1 Basics

In the sequel let G be a finite group and V be a finite dimensional $\mathbf{C}-$vector-space of dimension d. With $GL(V)$ we denote the set of all invertible linear transformations of V. We write $\mathbf{C}^d$ instead of V if we have fixed a basis for V and $GL_d(\mathbf{C})$ instead of $GL(V)$. If $\{e_1, e_2, ..., e_d\}$ is a basis of V then the coordinate representation of $v = \sum_{i=1}^d \lambda_i e_i$ is abbreviated by $\widehat{v}$, i.e. $\widehat{v} = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_d \end{pmatrix}$ and $\widehat{v}_i = \lambda_i$. The coordinate representation of $v^* \in V^*$ is the row vector $(\lambda_1, \lambda_2, ..., \lambda_d)$. By $\langle \_, \_ \rangle$ we denote the usual inner product of V,i.e., for $v, w \in V$ we have $\langle v, v \rangle = \langle \widehat{v}, \widehat{w} \rangle = \sum_{i=1}^d \widehat{v}_i \widehat{w}_i$. If $M \in GL_d(\mathbf{C})$ then M_{ij} denotes the matrix entry in the $i-$th row and $j-$th column. M_i denotes the $i-$th row.

Definition 6 *A (complex)* ***representation*** *of G is a homomorphism*

$$\begin{array}{rcl} \rho & : & G \to GL(V) \\ \sigma & \longmapsto & \rho(\sigma). \end{array}$$

The integer d is the ***degree*** *of the representation. If we have chosen a basis of V then*

$$\rho : G \to GL_d(\mathbf{C})$$

is called a matrix representation.

The *trivial representation* is the homomorphism $\rho_{triv}(\sigma) := 1_{GL(V)}$ for all $\sigma \in G$. In the sequel we do not distinguish between the linear map $\rho(\sigma) : V \to V, v \mapsto \rho(\sigma)(v)$ and the corresponding matrix representation $\rho(\sigma) : \mathbf{C}^d \to \mathbf{C}^d, \widehat{v} \mapsto \rho(\sigma) \cdot \widehat{v}$.

Definition 7 *If ρ and ρ' are matrix representations of G with degree m and m' respectively, then the sum of ρ and ρ' is the matrix representation of degree $m+m'$, defined by*

$$\begin{array}{rcl} \rho \oplus \rho' & : & G \longrightarrow GL_{m+m'}(\mathbf{C}) \\ \sigma & \longmapsto & \begin{pmatrix} \rho(\sigma) & \mathbf{0} \\ \mathbf{0} & \rho'(\sigma) \end{pmatrix}. \end{array}$$

We abbreviate the sum $\underbrace{\rho \oplus \rho \oplus \ldots \oplus \rho}_{n \text{ times}}$ with $n\rho$.

Equipped with the action " $\cdot$ " of G on V, defined by

$$\sigma \cdot v := \rho(\sigma) \cdot v \tag{1.1}$$

for all $\sigma \in G$ and $v \in V$, the vectorspace V is called a $\mathbf{G}-$**space**.

Definition 8 *A subspace $W \subseteq V$ is* $\mathbf{G}-$***invariant*** *if for all $w \in W$ and $\sigma \in G$ we have $\rho(\sigma)(w) \in W$. The restriction of ρ on W, denoted by ρ_W, is also a representation of G with degree* $\dim W$. *The representation ρ is called* ***reducible*** *if W is nontrivial, otherwise we say that ρ is* ***irreducible****. If there exists a subspace W' s.t. $V = W \oplus W'$ and W and W' are $G-$invariant then ρ is called* ***completely reducible****.*

Note that all complex representations of finite groups are completely reducible.

With the choice of a suitable basis for V we can decompose the matrix representation ρ into ρ_W and $\rho_{W'}$, i.e. $\rho = \rho_W \oplus \rho_{W'}$.

Definition 9 *Let V, V' be complex vectorspaces of dimension d and $\varphi : V \to V'$ be an isomorphism. Two representations $\rho : G \to GL_d(\mathbf{V})$, and $\rho' : G \to GL_d(\mathbf{V'})$ are* ***equivalent,*** *which we denote with $\rho \cong \rho'$, iff for all $\sigma \in G$ the diagram*

$$\begin{array}{ccc} V & \xrightarrow{\rho(\sigma)} & V \\ \varphi \downarrow & & \varphi \downarrow \\ V' & \xrightarrow{\rho'(\sigma)} & V' \end{array}$$

commutes.

From now on we consider matrix representations. For matrix representations ρ, ρ' we obtain

$$\rho \cong \rho' \Longleftrightarrow \exists M \in GL_d(\mathbf{C}) \forall \sigma \in G : \rho(\sigma) = M^{-1} \rho'(\sigma) M.$$

It is one of the aims of representation theory to decompose a given representation of G in simpler (irreducible, if possible) ones. Let k denote the number of conjugacy classes of G.

Theorem 1 *(a) There are only finitely many non-equivalent irreducible complex representations $\rho_1, ..., \rho_k$ of G. Furthermore each (finite dimensional) representation ρ of G can be decomposed uniquely into irreducible ones, i.e. there exist $a_1, ..., a_k \in \mathbf{N}_0$ s.t.*

$$\rho \cong a_1\rho_1 \oplus ... \oplus a_k\rho_k. \tag{1.2}$$

(b) Let d_i denote the degree of the representation ρ_i. Then

$$|G| = \sum_{i=1}^{k} d_i^2.$$

■

Let $\{e_\sigma \mid \sigma \in G\}$ be a basis of the $|G|$−dimensional vectorspace $\mathbf{C}^{|G|}$. The linear extension of the group action $\sigma * e_\tau := e_{\sigma\tau}$ is equivalent to the *regular representation* $\rho_{reg} := \sum_{i=1}^{k} d_i\rho_i$.

Corollary 1 *If G is Abelian then $k = |G|$ and $d_i = 1$ for $1 \leq i \leq |G|$.* ■

A very important tool for studying representations are characters. Let $M \in GL_d(\mathbf{C})$ we define $trace(M) := \sum_{i=1}^{d} M_{ii}$.

Definition 10 *Let ρ be a matrix representation of G. The mapping $\chi_\rho(\sigma) := trace(\rho(\sigma))$ is the* ***character*** *of ρ. A character is* ***linear*** *iff there exists a representation ρ of degree 1 s.t. $\chi = \chi_\rho$.*

We omit ρ if the representation is clear from the context. Note that the linearity of χ_ρ implies that $\rho(\sigma) \cdot \widehat{v} = \chi_\rho(\sigma)\widehat{v}$ for all $\sigma \in G$ and $v \in V$ and that the representation ρ is irreducible.

Lemma 1 *A character χ is linear iff χ is a group homomorphism $\chi : G \to \mathbf{C}\backslash\{0\}$.*

Proof. Let χ be linear and ρ be a representation of degree 1 s.t. $\chi = \chi_\rho$. So $\chi(\sigma) = \chi_\rho(\sigma) = \rho(\sigma)$. Conversely assume that χ is a group homomorphism. Then $\chi(1_G) = 1$ and $\rho : G \to GL_1(\mathbf{C}), \rho(\sigma) := \chi(\sigma)$ is the required representation. ■

Since $trace(A) = trace(BAB^{-1})$ the characters are class functions on G, i.e. they are constant on each conjugacy class. For two arbitrary characters χ, χ' of representations of G an inner product $\langle \_, \_ \rangle_G$ can be defined as follows

$$\langle \chi, \chi' \rangle_G := \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma)\chi'(\sigma^{-1}).$$

This inner product provides a simple test for irreducibility, see, e.g., Fulton and Harris [14], Sagan [34] or Simon [41].

Let $\rho_1, \rho_2, ..., \rho_k$ be the irreducible, non-equivalent representations of G with $\rho_1 = \rho_{triv}$ and define $\chi_i := \chi_{\rho_i}$. Let $\rho \cong a_1\rho_1 \oplus ... \oplus a_k\rho_k$ be the decomposition of $\rho : G \to GL_d(\mathbf{C})$ according to Theorem 1.2.1.

Theorem 2 *(a) The representation ρ is irreducible iff $\langle \chi_\rho, \chi_\rho \rangle_G = 1$.*
(b) The degree of ρ equals $\chi_\rho(1_G)$, hence $d_i = \chi_i(1_G)$.
(c) We have $a_i = \langle \chi_\rho, \chi_i \rangle_G$.

Proof. For the proof of (a) and (c) we refer, e.g., .to Fulton and Harris [14], corollary 2.15 and corollary 2.16 respectively. (b) follows from $trace(\rho(1_G)) = d$. ■

For the regular representation we have $\chi_{reg}(e) = \sum_{i=1}^k d_i^2 = |G|$. Note that the characters $\chi_1, \chi_2, ..., \chi_k$ are orthonormal w.r.t. $\langle \_, \_ \rangle_G$, i.e. for $i, j \in \{1, 2, ..., k\}$ we have $\langle \chi_i, \chi_j \rangle_G = \delta_{i,j}$. If the characters $\chi_1, \chi_2, ..., \chi_k$ are known then any matrix representation ρ can be decomposed according to Theorem 1.2.1 as follows : $\rho \cong \langle \chi_\rho, \chi_i \rangle_G \rho_1 \oplus ... \oplus \langle \chi_\rho, \chi_i \rangle_G \rho_k$. It is sufficient to have a table of the values of the characters $\chi_1, \chi_2, ..., \chi_k$ on the conjugacy classes of G which is called the **character table**.

As an example we compute the character table of S_3. The group $S_3 = \{e, (12), (13), (23), (123), (213)\}$ is generated by the elements (12) and (123) and has three conjugacy classes $K_1 = \{e\}, K_2 = \{(12), (13), (23)\}$ and $K_3 = \{(123), (213)\}$. We have to find three non-equivalent irreducible representations of degree d_1, d_2, d_3 s.t. $d_1^2 + d_2^2 + d_3^2 = 6$. Firstly we analyze the trivial representation $\rho_{triv} : S_3 \to \mathbf{C}$, $\pi \mapsto 1$ for all $\pi \in S_3$ and the alternating representation $\rho_{alt} : S_3 \to \mathbf{C}$, $\pi \mapsto sign(\pi)$. Both are irreducible since $\langle \chi_{triv}, \chi_{triv} \rangle = \frac{1}{6}(1+1+1+1+1+1) = 1$ and $\langle \chi_{alt}, \chi_{alt} \rangle = \frac{1}{6}(1+(-1)^2+(-1)^2+(-1)^2+1+1) = 1$. So $d_1 = d_2 = 1$. It remains to find ρ_3 of degree 2. As a third one we consider the *permutation representation*

$$\begin{aligned} \rho_{perm} &: S_3 \to GL_3(\mathbf{C}), \\ (12) &\longmapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \\ (123) &\longmapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. \end{aligned} \tag{1.3}$$

If $\{e_1, e_2, e_3\}$ is a basis for $\mathbf{C}^3$ then the space spanned by $\langle e_1 + e_2 + e_3 \rangle$ is an S_3- invariant subspace of $\mathbf{C}^3$. Hence ρ_{perm} is reducible (this follows also from the fact that the third representation must have degree 2) and we can split off ρ_1 and ρ_2 from ρ_{perm}. Since $\langle \chi_{triv}, \chi_{perm} \rangle = \frac{1}{6}(3+1+1+1+0+0) = 1$ and $\langle \chi_{alt}, \chi_{perm} \rangle = \frac{1}{6}(3-1-1-1+0+0) = 0$ we can split off ρ_{triv} and obtain the representation ρ_3 because ρ_3 does not contain any of the two representations ρ_1 and ρ_2 and has degree 2. Since we know the characters χ_1 and χ_2 and $\chi_3(e) = 2$ we can compute the two missing values of χ_3 from the orthogonality of the characters. The orthogonality yields the equations

$$\begin{aligned} 0 &= \langle \chi_{triv}, \chi_3 \rangle_G = \frac{1}{6}(2 + 3\chi_3(K_2) + 2\chi_3(K_3)), \\ 0 &= \langle \chi_{alt}, \chi_3 \rangle_G = \frac{1}{6}(2 - 3\chi_3(K_2) + 2\chi_3(K_3)). \end{aligned}$$

So S_3 has the character table

S_3	K_1	K_2	K_3
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

.

Note that for permutation groups the regular representation coincides with the permutation representation.

1.2.2 Invariant Subspaces

Let G be a finite group with non-equivalent irreducible representations $\rho_1, \rho_2, \ldots, \rho_k$ and let $\chi_1, \chi_2, \ldots, \chi_k$ be the corresponding characters. Let $\rho : G \to GL_d(\mathbf{C})$ be a representation of G with degree d and assume that for the chosen basis we have $\rho = a_1\rho_1 \oplus \ldots \oplus a_k\rho_k$ for some $a_i \in \mathbf{N}_0$. Set $V = \mathbf{C}^d$.

Definition 11 *Let $a_i \neq 0$. We denote the maximal invariant subspace of ρ_i with $V_{\chi_i}^{\rho(G)}$. If $a_i = 0$ then we set $V_{\chi_i}^{\rho(G)} = \{0\}$.*

Proposition 1 *Let χ_i be linear. Then*

$$V_{\chi_i}^{\rho(G)} = \{v \in V \mid \forall \sigma \in G : \rho(\sigma) \cdot \widehat{v} = \chi_i(\sigma)\widehat{v}\}.$$

Proof. After a suitable reordering of the $\rho_i's$ assume that $i = 1$ (note that ρ_1 need not be the trivial representation). It follows from the decomposition that $\rho(\sigma)$ is a block-diagonal matrix for $\sigma \in G$ and that the block $a_1\rho_1$ affects precisely the first a_1 coordinates. ■

From character theory we obtain the following result.

Lemma 2 *Let ρ_j be s.t. χ_j is linear. Then dimension of $V_{\chi_i}^{\rho(G)}$ equals $\langle \chi_\rho, \chi_i \rangle$, i.e.,*

$$\dim V_{\chi_i}^{\rho(G)} = \frac{1}{|G|} \sum_{\sigma \in G} \chi_\rho(\sigma)\chi_i(\sigma^{-1}).$$

The computation of a basis for this subspace is an important topic in invariant theory and can be done by an application of the Reynolds operator

$$\mathfrak{R}^{\rho(G)}_{\chi_i}(v) := \frac{1}{|G|}\sum_{\sigma\in G}\chi_i(\sigma^{-1})\sigma\cdot v$$

to a basis of V. Note how the action "$\cdot$" depends on ρ, cf. (1.1). In Chapter 2 we take $V = \mathbf{K}[x_1, x_2, ..., x_n]_d$ and consider the action of a matrix group $G \le GL_n(\mathbf{C})$ by linear substitution in the variables. We are interested in the computation of a basis for $V^{\rho(G)}_{\chi_i}$ for linear characters χ_i.

Proposition 2 *(a) Let χ_i be linear. Then the Reynolds operator is a projection onto $V^{\rho(G)}_{\chi_i}$.*
(b) Let $i \neq j$ and χ_i, χ_j be linear. Then we have $V^{\rho(G)}_{\chi_i} \cap V^{\rho(G)}_{\chi_j} = \{0\}$.

Proof. (a) Let $v \in V^{\rho(G)}_{\chi_i}$. Then $\mathfrak{R}^{\rho(G)}_{\chi_i}(v) = \frac{1}{|G|}\sum_{\sigma\in G}\chi_i(\sigma^{-1})\sigma\cdot v = \frac{1}{|G|}\sum_{\sigma\in G}\chi_i(\sigma^{-1})\chi_i(\sigma)v = \langle\chi,\chi\rangle_G v = v$. Now assume $v \notin V^{\rho(G)}_{\chi_i}$ and consider $\tau\cdot\mathfrak{R}^{\rho(G)}_{\chi_i}(v) = \tau\cdot\frac{1}{|G|}\sum_{\sigma\in G}\chi_i(\sigma^{-1})\sigma\cdot v = \frac{1}{|G|}\sum_{\sigma\in G}\chi_i(\sigma^{-1})\tau\sigma\cdot v = \frac{1}{|G|}\sum_{\sigma\in G}\chi_i(\sigma^{-1}\tau)\sigma\cdot v = \chi_i(\tau)\frac{1}{|G|}\sum_{\sigma\in G}\chi_i(\sigma^{-1})\sigma\cdot v = \chi_i(\tau)\mathfrak{R}^{\rho(G)}_{\chi_i}(v)$.
For the proof of (b) we assume $v \in V^{\rho(G)}_{\chi_i}$. Since $\chi_i \neq \chi_j$ there exits $\sigma \in G$ s.t. $\chi_i(\sigma) \neq \chi_j(\sigma)$, hence $\chi_i(\sigma)v = \rho(\sigma)\cdot v = \chi_j(\sigma)v$ which implies $v = 0$. ■

1.3 Artinian and Noetherian Rings

Let R be a commutative ring with unity and M be an $R-$module.

Definition 12 *M satisfies the ascending chain condition (ACC) iff every strictly ascending sequence of submodules*

$$M_1 \subsetneq M_2 \subsetneq ...$$

is finite. Conversely, M satisfies the descending chain condition (DCC) iff every strictly descending sequence of submodules

$$M_1 \supsetneq M_2 \supsetneq ...$$

is finite.

Definition 13 *M is a **Noetherian (Artinian)** $R-$module iff M satisfies the ACC (DCC). The ring R is **Noetherian (Artinian)** iff it is a Noetherian (Artinian) module over itself.*

Note that any ideal $I \trianglelefteq R$ is a submodule of the $R-$module R and vice versa.

Proposition 3 *The following conditions are equivalent :*
(a) R is Noetherian,
(b) Every ideal of R has a finite basis,
(c) Every collection of ideals has a maximal element.

Proof. See, e.g., Zariski and Samuel [49] vol. I, ch. III, Theorem 15 of 10. ■

We now state Hilbert's Basis Theorem, which was the first step in his proof that the ring of invariants is finitely generated.

Theorem 3 *(Hilbert 1890) If R is Noetherian then $R[t]$ is Noetherian.*

Proof. See, e.g., Cox et. al. [9] ch. 2, Theorem 4 of § 5 or Eisenbud [13] Theorem 1.2 of ch. 1. ■

Corollary 2 *The polynomial ring $\mathbf{K}[x_1, x_2, ..., x_n]$ is Noetherian.*

We present two useful criteria for checking whether a ring is Noetherian.

Proposition 4 *(a) The homomorphic image of a Noetherian ring is Noetherian.*
(b) If R is Noetherian and M is a finitely generated $R-$module then M is Noetherian.
(c) M is Noetherian iff each submodule of M is finitely generated.

Proof. (a) See, e.g., Eisenbud [13], corollary 1.3 of ch. 2. (b) See, e.g., Eisenbud [13], Proposition 1.4 of ch. 1.
(c) Let $0 \neq N \leq M$ be a submodule and η_1 be a nontrivial element of N. We set $\eta_i := N \backslash \langle \eta_1, \eta_2, ..., \eta_{i-1} \rangle$ and claim $\langle \eta_1, \eta_2, ..., \eta_n \rangle = N$ for some $n \in \mathbf{N}$. Otherwise the sequence $\langle \eta_1 \rangle \subsetneq \langle \eta_1, \eta_2 \rangle \subsetneq ...$ is strictly ascending and contradicts the assumption that M is Noetherian. Conversely assume that $N_1 \subsetneq N_2 \subsetneq ...$ is a strictly ascending chain. The submodule $N = \bigcup_i N_i$ has a finite basis and which is contained in N_j for some $j \in \mathbf{N}$. ■

1.4 Graded Algebras, Modules and the Hilbert Series

Definition 14 *A commutative ring R, which has a decomposition*

$$R = \bigoplus_{d=0}^{\infty} R_d$$

as abelian groups w.r.t. $+$, that satisfies

$$R_iR_j \subseteq R_{i+j} \text{ for all } i,j \in \mathbf{N}$$

*is called a **graded** ring. An element of R_d for some $d \in \mathbf{N}$ is called a homogenous element of degree d.*

A simple example of a graded ring is the polynomial ring $\mathbf{K}[x_1, x_2, ..., x_n]$. Let $\mathbf{K}[x_1, x_2, ..., x_n]_d$ denote the vectorspace of homogenous polynomials of degree d, then

$$\mathbf{K}[x_1, x_2, ..., x_n] = \bigoplus_{d=0}^{\infty} \mathbf{K}[x_1, x_2, ..., x_n]_d.$$

Definition 15 *Let R be a graded ring and M be an $R-$module. M is called a **graded module** if it has a decomposition*

$$M = \bigoplus_{i=0}^{\infty} M_i$$

as abelian groups and

$$R_iM_j \subseteq M_{i+j} \text{ for all } i,j \in \mathbf{N}.$$

Definition 16 *A $\mathbf{K}-$**algebra** is a commutative ring S with unity s.t. the following two conditions hold :*
(a) S is a $\mathbf{K}-$vectorspace,
(b) $\forall c \in \mathbf{K} \forall r,s \in S : c(r \cdot s) = cr \cdot s = r \cdot cs = (r \cdot s)c$.
*S is **graded** iff S is graded as a ring and each component S_d is a $\mathbf{K}-$vectorspace.*
*S is **finitely generated** as a $\mathbf{K}-$algebra iff there exists a finite set $\{f_1, ..., f_m\} \subseteq S$ s.t. the homomorphism*

$$\begin{aligned} \varphi &: \mathbf{K}[y_1, y_2, ..., y_m] \to S, \\ p(y_1, y_2, ..., y_m) &\mapsto p(f_1, f_2, ..., f_m). \end{aligned}$$

*is surjective. In this case we denote S with $\mathbf{K}[f_1, f_2, ..., f_m]$. If we replace $\mathbf{K}$ by a commutative ring R (with unity) and require that S is an $R-$module, then S is called an $R-$**algebra**.*

Note that any (graded) $\mathbf{K}-$algebra is a (graded) module over itself with basis $\{1\}$.

Definition 17 *Let R be a graded $\mathbf{K}-$algebra and M be a graded $R-$module. The **Hilbert series** of M is defined by*

$$H(M,t) := \sum_{d=0}^{\infty} \dim_{\mathbf{K}}(M_d) \cdot t^d,$$

*where $\dim_{\mathbf{K}}(M_d)$ denotes the dimension of M_d as a $K-$vectorspace. The **Hilbert function** of M is the numerical function $H_M(d) := \dim_{\mathbf{K}}(M_d)$.*

For details on the Hilbert function and series we refer to Stanley [37] and Eisenbud [13]. The next result is an important tool for the computation of the Hilbert series in invariant theory.

Lemma 3 *Let $\theta_1, \theta_2 ..., \theta_n \in \mathbf{K}[x_1, x_2, ..., x_n]$ be algebraically independent, homogenous elements of degree $d_1, d_2, ..., d_n$ respectively. Then*

$$H(\mathbf{K}[\theta_1, \theta_2, ..., \theta_n], t) = \prod_{i=1}^{n} \frac{1}{1 - t^{d_i}}.$$

Proof. See, e.g., Sturmfels [43], Lemma 2.2.3 of ch. 2. ■

In the sequel let R be a noetherian commutative ring with unity.

Definition 18 *The **(Krull-)dimension** of R, denoted with $\dim R$, is the supremum of the lengths of chains of distinct prime ideals of R. The length of the chain*

$$P_r \supsetneq P_{r-1} \supsetneq ... \supsetneq P_0$$

is taken to be r. The dimension of an ideal $I \trianglelefteq R$ is the dimension of R/I.

The next theorem is a different characterization of the dimension of a $\mathbf{K}-$algebra R. We denote the maximal number of algebraically independent elements of R over $\mathbf{K}$ with $\operatorname{transdeg}_{\mathbf{K}} R$.

Theorem 4 *Let R be a finitely generated graded $\mathbf{K}-$algebra with no nilpotent elements. Then*

$$\dim R = \operatorname{trans\,deg}_{\mathbf{K}} R.$$

Proof. See, e.g., Zariski and Samuel [49], vol. II, ch. VII. § 7 or Eisenbud [13], Theorem A in section 8.2.1. ■

Proposition 5 *Let $I \trianglelefteq R$ be an ideal. For any prime ideal $P \trianglelefteq R$ which is minimal over I we have $\dim R/I = \dim R/P$.*

Proof. Let

$$P_r \supsetneq P_{r-1} \supsetneq ... \supsetneq P_1 \supsetneq P \supseteq I \tag{1.4}$$

be a chain with prime ideals $P_1, ..., P_r \trianglelefteq R$ of maximal length. If I is not prime then $\{0\}$ is not a prime ideal in R/I and the chain (1.4) maps bijectively to a maximal chain of length r in R/I. Conversely, the assumption that I is prime implies that $P = I$ and the length of the chain (1.4) equals r. ■

Definition 19 *Let $f_1, f_2, ..., f_m \in \mathbf{K}[x_1, x_2, ..., x_n]$ for some $m \in \mathbf{N}$. The set $\mathbf{V_K}(f_1, f_2, ..., f_m) := \{v \in \mathbf{K}^n \mid f_1(v) = f_2(v) = ... = f_m(v) = 0\}$ is the* ***variety*** *of $f_1, f_2, ..., f_m$. A subset $\mathfrak{V} \subseteq \mathbf{K}^n$ is an* ***(affine algebraic) variety*** *iff there exist $g_1, g_2, ..., g_{m'} \in \mathbf{K}[x_1, x_2, ..., x_n]$ s.t. $\mathbf{V_K}(g_1, g_2, ..., g_{m'}) = \mathfrak{V}$. The ideal $\mathbf{I_K}(\mathfrak{V}) = \{f \in \mathbf{K}[x_1, x_2, ..., x_n] \mid f(v) = 0$ for all $v \in \mathfrak{V}\}$ is the ideal of $\mathfrak{V}$.*

Proposition 6 *Let $\overline{\mathbf{K}}$ denote the algebraic closure of $\mathbf{K}$,$\mathfrak{V} \subseteq \overline{\mathbf{K}}^n$ be an affine algebraic variety and $I = \langle f_1, f_2, ..., f_m\rangle \trianglelefteq \mathbf{K}[x_1, x_2, ..., x_n]$ s.t. $\mathbf{V}_{\overline{\mathbf{K}}}(f_1, f_2, ..., f_m) = \mathfrak{V}$. Then the following conditions are equivalent.*
(a) $\mathfrak{V}$ is finite.
(b) R/I is Artinian.
(c) $\dim I = 0$.

Proof. For the proof of (a) $\Leftrightarrow$ (b) we refer, e.g., to Eisenbud [13], corollary 2.15 of ch. 2. The proof of (b) $\Leftrightarrow$ (c) follows, e.g., from Proposition 1.4.5 and from Theorem 2.14 of ch. 2 of Eisenbud [13]. ■

Definition 20 *Let $R \subseteq S$ be commutative rings with unity.*
(a) $f \in S$ is ***integral*** *over R iff there exists a polynomial $p \in R[t]$ s.t. $p(f) = 0$.*
(b) S is ***integral*** *over R if $R \subseteq S$ and each $s \in S$ is integral over R.*

Proposition 7 *(a) Let $R \subseteq S$ be commutative rings with unity. If S is generated by elements integral over R then S is integral over R.*
(b) Let $R \subseteq S \subseteq T$ be commutative rings with unity s.t. S is integral over R and T is integral over S. Then T is integral over R.

Proof. (a) see, e.g., Eisenbud [13], Theorem.4.2 of ch. 4.
(b)See, e.g., Bosch [5], corollary 5 of section 3.3. ■

Proposition 8 *An $R-$algebra S is finitely generated as an $R-$module iff S is generated as an $R-$algebra by finitely many integral elements.*

Proof. See, e.g., Eisenbud [13], corollary 4.5 of ch. 4 ■

Proposition 9 *Let $R \subseteq S$ be commutative Noetherian rings with unity s.t. S is integral over R. Then* $\dim R = \dim S$.

Proof. Follows, e.g., from Eisenbud [13], proposition 9.2 of ch. 9 ■

Theorem 5 *(Noether Normalization Lemma) Let R be a $\mathbf{K}-$algebra of Krull dimension n which is generated as a $\mathbf{K}-$algebra by finitely many homogenous elements. Then there exist n algebraically independent homogenous elements $\theta_1, \theta_2 ..., \theta_n \in R$ s.t. R is a finitely generated as a $\mathbf{K}[\theta_1, \theta_2 ..., \theta_n]-$module.*

Proof. See, e.g., Zariski and Samuel [49], vol. II, ch. VII. § 7, Theorem 25, or Eisenbud [13], Theorem 13.3 in section 13.1. ■

Definition 21 *Let R and $\theta_1, \theta_2 ..., \theta_n$ be as in Theorem 1.4.5. The elements $\theta_1, \theta_2 ..., \theta_n$ are called a* ***homogenous system of parameters (hsop)*** *for R.*

Theorem 6 *(Krull's Principal Ideal Theorem) Let R be a graded commutative ring of Krull dimension n and $f_1, f_2, ..., f_k \in R$ homogenous elements. Then*

$$\dim R / \langle f_1, f_2, ..., f_k \rangle \geq n - k.$$

Proof. See, e.g., Eisenbud [13], Theorem 10.2 of ch. 10. ■

Lemma 4 *Let $I = \langle f_1, f_2, ..., f_k \rangle \trianglelefteq \mathbf{K}[x_1, x_2, ..., x_n]$ be an ideal generated by homogenous polynomials $f_1, f_2, ..., f_k$. If $h \in I$ then there exist homogenous polynomials $p_1, p_2, ..., p_k$ s.t. $h = \sum_{i=1}^{k} p_i f_i$ and $\deg p_i = \deg h - \deg f_i$ or $p_i = 0$.*

Proof. Since $h \in I$ we have $h = \sum_{i=1}^{k} r_i f_i$ for some $r_i \in \mathbf{K}[x_1, x_2, ..., x_n]$. Let $d = \deg f, d_i = \deg f_i$.and let m be the largest degree of the monomials occurring in any of the f_i's. With $r_i^{(j)}$ we denote the homogenous component of r_i of degree j. Then we have

$$h = \sum_{i=1}^{k} \underbrace{r_i^{(d-d_i)} f_i}_{\deg = d} + \sum_{i=1}^{k} \sum_{j=0, j \neq d_i}^{m} \underbrace{r_i^{(j)} f_i}_{\deg \neq d}.$$

Since h is homogenous of degree d all monomials in the second sum must cancel, therefore $h = \sum_{i=1}^{k} r_i^{(d-d_i)} f_i$. ■

1.5 Gröbner Basics

The ideal operations (comparison, dimension, intersection) in the presented algorithms are done with Gröbner bases. We refer to Buchberger [7], [8], Becker and Weispfennig [3], Cox et. al. [9] and Winkler [47] for further details. For this section let $R = \mathbf{K}[x_1, x_2, ..., x_n]$.

Definition 22 *A product $p = \prod_{i=1}^{n} x_i^{\alpha_i}$ is a **monomial** of degree $|\boldsymbol{\alpha}| = \sum_{i=1}^{n} \alpha_i$. $(\alpha_1, \alpha_2, ..., \alpha_n)$ is called the **degree vector** of p.*

In the sequel we identify the monomials of R with their degree vectors.

Definition 23 *Let $\mathbf{x}^{\boldsymbol{\alpha}}$ and $\mathbf{y}^{\boldsymbol{\beta}}$ be monomials. $\mathbf{x}^{\boldsymbol{\alpha}} < \mathbf{y}^{\boldsymbol{\beta}}$ iff there exists $k \in \{1, 2, ..., n\}$ s.t. $\alpha_i = \beta_i$ for $1 \leq i \leq k-1$ and $\alpha_k < \beta_k$. $\mathbf{x}^{\boldsymbol{\alpha}} \leq \mathbf{y}^{\boldsymbol{\beta}}$ iff $\mathbf{x}^{\boldsymbol{\alpha}} < \mathbf{y}^{\boldsymbol{\beta}}$ or $\mathbf{x}^{\boldsymbol{\alpha}} = \mathbf{y}^{\boldsymbol{\beta}}$. The ordering $<$ is called the lexicographic ordering.*

Definition 24 *Let $f \in R$. The leading monomial of f, denoted by $LM(f)$, is the greatest monomial in f w.r.t. $<$. The leading coefficient of $f, LC(f)$, is the coefficient of $LM(f)$. The leading tern of f is $LT(f) = LC(f) \cdot LM(f)$.*

Definition 25 *Let $I \trianglelefteq R$ be an ideal. $\{f_1, f_2, ..., f_m\} \subseteq I$ is a **Gröbner basis** of I iff $\langle LT(f_1), LT(f_2), ..., LT(f_m)\rangle = \langle LT(f) \mid f \in I\rangle$.*

Note that if $\{f_1, f_2, ..., f_m\}$ is a Gröbner basis of I then $I = \langle f_1, f_2, ..., f_m\rangle$. The main result was introduced by Buchberger in his Ph.D. thesis, cf. [7].

Theorem 7 *(Buchberger 1965) For any ideal $I \trianglelefteq R$ there exists a finite Gröbner basis.*

Proof. We refer to (loc. cit.). ■

1.6 Tensor, Symmetric, and Alternating Powers

Let $\mathbf{K}$ be a field, V and W be $\mathbf{K}-$vectorspaces of dimension m and n with bases $\{a_1, a_2, ..., a_m\}$ and $\{b_1, b_2, ..., b_n\}$.

[1] The terminus Gröbner Basics is due to B. Sturmfels.

Definition 26 *The **tensor product** of V and W is the $\mathbf{K}-$vectorspace $V \otimes W$ with basis $\{a_i \otimes b_j \mid 1 \le i \le m, 1 \le j \le n\}$ subject to the relations*
(a) $\forall c \in \mathbf{K}, v \in V, w \in W : cv \otimes w = v \otimes cw$
(b) $\forall v, v' \in V, w \in W : (v + v') \otimes w = v \otimes w + v' \otimes w$
(c) $\forall v \in V, w, w' \in W : v \otimes (w + w') = v \otimes w + v \otimes w'$.
*For $d \in \mathbf{N}$ the $d-$**th tensor power** of V is defined inductively by*

$$\begin{aligned} \bigotimes^1 V \; &: = V, \\ \bigotimes^d V \; &: = V \otimes \bigotimes^{d-1} V. \end{aligned}$$

Definition 27 *The **symmetric product** of V and W is the $\mathbf{K}-$vectorspace $V \circ W := V \otimes W / \langle v \otimes w - w \otimes v \mid v \in V, w \in W \rangle$.For $d \in \mathbf{N}$ the $d-$**th symmetric power** of V is defined inductively by*

$$\begin{aligned} Sym^1 V \; &: = V, \\ Sym^d V \; &: = V \circ Sym^{d-1} V. \end{aligned}$$

Note that $v_1 \circ v_2 = v_2 \circ v_1$ for any $v_1, v_2 \in V$.

Definition 28 *The **alternating product** of V and W is the $\mathbf{K}-$vectorspace $V \wedge W := V \otimes W / \langle v \otimes v \mid v \in V, w \in W \rangle$.For $d \in \mathbf{N}$ the $d-$**th exterior power** of V is defined inductively by*

$$\begin{aligned} \bigwedge^1 V \; &: = V, \\ \bigwedge^d V \; &: = V \wedge \bigwedge^{d-1} V. \end{aligned}$$

Note that $v_1 \wedge v_2 = -v_2 \wedge v_1$ for any $v_1, v_2 \in V$.

For details and properties we refer, e.g., to Appendix 2 of Eisenbud [13] and Appendix B of Fulton and Harris [14].

Chapter 2

Invariant Theory of Finite Groups

In the first section we start with the well known symmetric and alternating polynomials. Section 2 contains basic definitions of invariant theory and in section 3 we state three finiteness theorems. In Section 4 we present Molien's Theorem and in section 5 we introduce the Cohen-Macaulay property.

For a historical account we refer, e.g., to Decker and Jong [11] or Smith [39].

2.1 Symmetric Polynomials

In this section we consider the ring of all symmetric polynomials and demonstrate a lot of concepts which will be investigated in the latter chapters. Throughout this section let $\mathbf{K}$ be an algebraically closed field of characteristic 0 and let $n \in \mathbf{N}$.

Let S_n denote the symmetric group of n letters. We define the following group action " $\cdot$ " of S_n on the ring $\mathbf{K}[x_1, x_2, ..., x_n]$. For $\pi \in S_n$ and $f \in \mathbf{K}[x_1, x_2, ..., x_n]$ we define

$$\pi \cdot f(x_1, x_2, ..., x_n) := f(x_{\pi^{-1}(1)}, x_{\pi^{-1}(2)}, ..., x_{\pi^{-1}(n)}).$$

We want to describe the ring

$$\mathbf{K}[x_1, x_2, ..., x_n]^{S_n} := \{f \in \mathbf{K}[x_1, x_2, ..., x_n] : \forall \pi \in S_n : \pi \cdot f = f\}$$

which is the invariant ring of S_n w.r.t. the action " $\cdot$ ".

Definition 29 *A polynomial $f \in \mathbf{K}[x_1, x_2, ..., x_n]$ is **symmetric** if and only if for all $\pi \in S_n$ we have $\pi \cdot f(x_1, x_2, ..., x_n) = f(x_1, x_2, ..., x_n)$.*

So the ring $\mathbf{K}[x_1, x_2, ..., x_n]^{S_n}$ is just the ring of all symmetric polynomials. We put the usual grading on the ring $\mathbf{K}[x_1, x_2, ..., x_n]$, i.e. $\mathbf{K}[x_1, x_2, ..., x_n]_d := \{f \in \mathbf{K}[x_1, x_2, ..., x_n] : f$ homogenous of degree $d\}$. We are also interested in the generating function

$$H^{S_n}(t) = \sum_{d=0} \dim_{\mathbf{K}}(\mathbf{K}[x_1, x_2, ..., x_n]_d^{S_n}) \cdot t^d$$

which is the Hilbert series of the ring $\mathbf{K}[x_1, x_2, ..., x_n]^{S_n}$.

Definition 30 *Let $x_1, x_2, ..., x_n$ be variables. The polynomials $\sigma_1, \sigma_2, ..., \sigma_n \in \mathbf{K}[x_1, x_2, ..., x_n]$ defined by*

$$\sigma_k(x_1, x_2, ..., x_n) := \sum_{1 \leq i_1 < i_2 < ... < i_k \leq n} \prod_{j=1}^{k} x_{i_j} \text{ for } 1 \leq k \leq n$$

*are the **elementary symmetric polynomials.** We set $\sigma_0(x_1, x_2, ..., x_n) = 1$ and $\sigma_{n+i}(x_1, x_2, ..., x_n) = 0$ for $i \in \mathbf{N}$. With σ_k^n we denote $\sigma_k(x_1, x_2, ..., x_n)$ if the integer n is not clear from the context.*

Let $f = x^3 + bx^2 + cx + d$ with roots α_1, α_2 and α_3, so $f = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$. Expansion gives

$$f = x^3 - (\alpha_1 + \alpha_2 + \alpha_3) \cdot x^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) \cdot x - \alpha_1\alpha_2\alpha_3.$$

This means, the coefficients are elementary symmetric polynomials in the roots of f; namely :

$$\begin{aligned} b &= -\alpha_1 - \alpha_2 - \alpha_3 = -\sigma_1(\alpha_1, \alpha_2, \alpha_3), \\ c &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = \sigma_2(\alpha_1, \alpha_2, \alpha_3), \\ d &= \alpha_1\alpha_2\alpha_3 = -\sigma_3(\alpha_1, \alpha_2, \alpha_3). \end{aligned}$$

Proposition 10 *(a) Let $k \in \mathbf{N}$, $k \leq n$. Then $\sigma_k^{n+1} = \sigma_k^n + x_{n+1}\sigma_{k-1}^n$.*
(b) Let $\alpha_1, \alpha_2, ..., \alpha_n \in \mathbf{K}$. Then

$$\prod_{i=1}^{n}(x - \alpha_i) = \sum_{i=0}^{n}(-1)^i x^{n-i}\sigma_i(\alpha_1, \alpha_2, ..., \alpha_n). \tag{2.1}$$

Proof. (a) Follows from Definition 2.1.30.
We prove (b) by induction on n. For $n = 1$ we have $x - \alpha_1 = x\sigma_0(\alpha_1) - \sigma_1(\alpha_1)$. So for a fixed $n \in \mathbf{N}$ assume (2.1). Then we have $\prod_{i=1}^{n+1}(x - \alpha_i) = \sum_{i=0}^{n}(-1)^i x^{n-i}\sigma_i^n \cdot (x - \alpha_{n+1}) = \sum_{i=0}^{n}(-1)^i x^{n+1-i}\sigma_i^n - \sum_{i=0}^{n}(-1)^i x^{n-i}\alpha_{n+1}\sigma_i^n =$

$\sum_{i=0}^{n}(-1)^i x^{n+1-i}\sigma_i^n + \sum_{i=1}^{n+1}(-1)^i x^{n+1-i}\alpha_{n+1}\sigma_{i-1}^n = x^{n+1}\sigma_0^n + \sum_{i=1}^{n+1}(-1)^i x^{n+1-i}$ $(\sigma_i^n + \alpha_{n+1}\sigma_{i-1}^n) = x^{n+1} + \sum_{i=1}^{n+1}(-1)^i x^{n+1-i}\sigma_i^{n+1} = \sum_{i=0}^{n+1}(-1)^i x^{n+1-i}\sigma_i^{n+1}$. ■

The next theorem is due to C.F. Gauss, who needed this theorem for his second proof of the fundamental theorem of algebra. The proof contains probably the first explicit statement of the lexicographic ordering.

Theorem 8 *Every symmetric polynomial $f \in \mathbf{K}[x_1, x_2, ..., x_n]$ can be written as a unique polynomial in the elementary symmetric polynomials $\sigma_1, \sigma_2, ..., \sigma_n$.*

Proof. We follow the proof of Theorem 3 of § 1 of ch. 7 in Cox et. al. [9]. We use the lexicographic order on the variables $x_1, x_2, ..., x_n$. Let $f \in \mathbf{K}[x_1, x_2, ..., x_n]$ be a symmetric polynomial and let $t = a \cdot x_1^{\alpha_1} x_2^{\alpha_2} ... x_n^{\alpha_n}$ be the leading term of f. Then $\alpha_1 \geq \alpha_2 \geq ... \geq \alpha_n$. Otherwise assume $\alpha_i < \alpha_{i+1}$, set $\pi = (i, i+1) \in S_n$ and consider $\pi \cdot f(x_1, x_2, ..., x_n)$. The monomial $x_1^{\alpha_1} x_2^{\alpha_2} ... x_i^{\alpha_{i+1}} x_{i+1}^{\alpha_i} ... x_n^{\alpha_n}$ is contained in f but it is strictly larger than $x_1^{\alpha_1} x_2^{\alpha_2} ... x_n^{\alpha_n}$, a contradiction. Let $h = \sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3} \cdot ... \cdot \sigma_n^{\alpha_n}$, then for the leading term of h we have

$$\begin{aligned} LT(h) &= LT(\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3} \cdot ... \cdot \sigma_n^{\alpha_n}) \\ &= LT(\sigma_1^{\alpha_1-\alpha_2})LT(\sigma_2^{\alpha_2-\alpha_3}) \cdot ... \cdot LT(\sigma_n^{\alpha_n}) \\ &= x_1^{\alpha_1-\alpha_2}(x_1x_2)^{\alpha_2-\alpha_3} \cdot ... \cdot (x_1x_2 \cdot ... \cdot x_n)^{\alpha_n} = x_1^{\alpha_1}x_2^{\alpha_2}...x_n^{\alpha_n}. \end{aligned} \tag{2.2}$$

The polynomial $f_1 = f - a \cdot h$ is symmetric since f and $a \cdot h$ are. Clearly we have $LT(f_1) < LT(f)$ and if we repeat the above process we get a sequence $LT(f) > LT(f_1) > LT(f_2) > ....$ Since $<$ is a well-ordering, the sequence terminates at f_m for some m which implies that $f_m = 0$. So $f = ah + a_1h_1 + ... + a_mh_m$. Uniqueness follows if the $\sigma_1, \sigma_2, ..., \sigma_n$ are algebraically independent. So assume that there exists a nontrivial $p \in \mathbf{K}[y_1, y_2, ..., y_n]$ s.t. $p(\sigma_1, \sigma_2, ..., \sigma_n) = 0$. Let $a \cdot y_1^{\alpha_1} y_2^{\alpha_2} ... y_n^{\alpha_n}$ be the leading term of p, then from (2.2) it follows that $LT(\,p(\sigma_1, \sigma_2, ..., \sigma_n)) = x_1^{\alpha_1+\alpha_2+...+\alpha_n} x_2^{\alpha_2+...+\alpha_n} ... x_n^{\alpha_n}$. Since the map

$$(\alpha_1, \alpha_2, ..., \alpha_n) \mapsto (\alpha_1 + \alpha_2 + ... + \alpha_n, \alpha_2 + ... + \alpha_n, ..., \alpha_n)$$

is injective there is nothing to cancel $LT(\,p(\sigma_1, \sigma_2, ..., \sigma_n))$, so $p(\sigma_1, \sigma_2, ..., \sigma_n) \neq 0$ in $\mathbf{K}[x_1, x_2, ..., x_n]$, a contradiction. ■

The above theorem implies that $\mathbf{K}[x_1, x_2, ..., x_n]^{S_n} = \mathbf{K}[\sigma_1, \sigma_2, ..., \sigma_n]$ and that $\sigma_1, \sigma_2, ..., \sigma_n$ are algebraically independent. From Lemma 1.4.3 we obtain

$$H^{S_n}(t) = \prod_{i=1}^{n} \frac{1}{1-t^i}.$$

Example 1 *In the case $n = 3$ the ring of symmetric polynomials equals*

$$\mathbf{K}[x_1, x_2, x_3]^{S_3} = \mathbf{K}[x_1 + x_2 + x_3, x_1x_2 + x_1x_3 + x_2x_3, x_1x_2x_3]$$

with corresponding Hilbert series

$$H^{S_3}(t) = \frac{1}{(1-t)(1-t^2)(1-t^3)} = 1+t+2\,t^2+3\,t^3+4\,t^4+5\,t^5+7\,t^6+\mathrm{O}(t^7).$$

2.2 Introduction to Invariant Theory

Many algebraic equations and polynomials have symmetries and according to F. Klein's "Erlanger Programm" a polynomial describes a geometric property if it is invariant under the corresponding transformation group. The group clearly depends on the geometry e.g. affine and projective geometry have different transformation groups. In Section 4.4 we study geometric properties which are invariant w.r.t. $SL_n(\mathbf{C})$, i.e. we study projective geometry.

For finite groups with representations over a field of characteristic 0 we develop invariant theory in the frame of representation theory. If the characteristic of the field is greater than 0 we take a purely ring-theoretic approach. We start with characteristic 0.

Let $\mathbf{K}$ be a field of characteristic 0 and V be a $\mathbf{K}-$vectorspace of dimension n. We chose a basis $\{e_1, e_2, ..., e_n\}$ of V and denote the dual basis of V^* with $X_1, X_2, ..., X_n$. We have chosen the isomorphism

$$\begin{aligned} {}^* &: V \to V^*, \\ v^*(w) &: = \langle \widehat{v}, \widehat{w} \rangle \text{ for all } w \in V \end{aligned}$$

Therefore we consider the elements $\widehat{v}$ of V as column vectors and the elements $\widehat{v}^*$of V^* as row vectors. Note that in coordinate representation the map * corresponds to the transposition. It follows that $(v^*)^* = v$. Let $\rho : G \to GL_n(\mathbf{K})$ be a representation of a finite group G. The representation $\rho : G/\ker\rho \to GL_n(\mathbf{K})$ is faithful and equivalent to ρ, so it suffices to treat faithful representations.

Definition 31 *The **dual representation** ρ^* of ρ is defined as follows.*

$$\begin{aligned} \rho^* &: G \to GL(V^*), \\ \sigma &\mapsto \rho^*(\sigma), \\ \rho^*(\sigma)(v^*))(w) &: = \left\langle \widehat{v}, \rho(\sigma^{-1}) \cdot \widehat{w} \right\rangle. \end{aligned}$$

We define a group action $\cdot$ of G on V^* via

$$\sigma \cdot f := \rho^*(\sigma)(f)$$

for $\sigma \in G$ and $f \in V^*$. In the sequel we construct the matrix representation $\widetilde{\rho}$ which is equivalent to ρ^*. We define

$$\begin{array}{rcl} \widetilde{\rho} & : & G \to GL_n(\mathbf{K}), \\ \sigma & \mapsto & \rho(\sigma^{-1})^T \end{array}$$

and from $\widetilde{\rho}(\sigma\tau) = \rho\left((\sigma\tau)^{-1}\right)^T = \rho\left(\tau^{-1}\sigma^{-1}\right)^T = \left(\rho\left(\tau^{-1}\right) \cdot \rho\left(\sigma^{-1}\right)\right)^T = \rho\left(\sigma^{-1}\right)^T \cdot \rho\left(\tau^{-1}\right)^T = \widetilde{\rho}(\sigma) \cdot \widetilde{\rho}(\tau)$ it follows that $\widetilde{\rho}$ is indeed a representation.

Proposition 11 *(a) For $\sigma \in G$ and $v, w \in V$ we have*

$$\left\langle \widehat{v}, \rho(\sigma^{-1}) \cdot \widehat{w} \right\rangle . = \left\langle \rho(\sigma^{-1})^T \cdot \widehat{v}, \widehat{w} \right\rangle .$$

(b) The diagram

$$\begin{array}{ccc} V & \stackrel{\widetilde{\rho}(\sigma)}{\longrightarrow} & V \\ {}^*\downarrow & & {}^*\downarrow \\ V^* & \stackrel{\rho^*(\sigma)}{\longrightarrow} & V^* \end{array}$$

is commutative.

Proof. For the proof of (a) we refer, e.g., to Klingenberg [27], Theorem 3.3.1.
(b) We have to show that $\left(\widetilde{\rho}(\sigma) \cdot \widehat{v}\right)^* (w) = \rho^*(v^*)(w)$ for all $v, w \in V$. Now

$$\left(\widetilde{\rho}(\sigma) \cdot \widehat{v}\right)^* (w) = \left\langle \widetilde{\rho}(\sigma) \cdot \widehat{v}, \widehat{w} \right\rangle = \left\langle \rho(\sigma^{-1})^T \cdot \widehat{v}, \widehat{w} \right\rangle = \left\langle \widehat{v}, \rho(\sigma^{-1}) \cdot \widehat{w} \right\rangle = \rho^*(v^*)(w).$$

■

It follows from the above proposition that the representation that $\widetilde{\rho}$ is equivalent to ρ^*, hence it is sufficient to consider the properties of the matrix representation $\widetilde{\rho}$.

Definition 32 *Let W be a finite-dimensional $\mathbf{K}-$vectorspace and $\rho' : G \to GL(W)$ be a representation of G. The $d-$th* ***symmetric power*** *of ρ' is the representation*

$$\begin{array}{rcl} Sym^d \rho' & : & G \to GL(Sym^d W), \\ Sym^d \rho'(\sigma)(w_1 \circ w_2 \circ ... \circ w_d) & = & \left(\rho'(\sigma)(w_1)\right) \circ \left(\rho'(\sigma)(w_2)\right) \circ ... \circ \left(\rho'(\sigma)(w_d)\right). \end{array}$$

If ρ' is a matrix representation we replace $\rho'(\sigma)(w_i)$ with $\rho'(\sigma) \cdot w_i$.

We extend the group action $\cdot$ to $Sym^d V^*$ via

$$\sigma \cdot f := (Sym^d \rho^*)(f)$$

for all $\sigma \in G$. Hence we can use the representation $Sym^d \widetilde{\rho}$ to study the properties of the group action $\cdot$ on $Sym^d V^*$.

We set $\mathbf{K}[V] := \bigoplus_{d=0}^{\infty} Sym^d V^*$, and from the isomorphism

$$\begin{aligned} \phi \quad &: \quad \mathbf{K}[x_1, x_2, ..., x_n] \to \mathbf{K}[V], \\ \sum_{\boldsymbol{\alpha} \in \mathbf{N}_0^n} a_{\boldsymbol{\alpha}} \mathbf{x}^{\boldsymbol{\alpha}} \quad &\longmapsto \quad \bigoplus_{\boldsymbol{\alpha} \in \mathbf{N}_0^n} a_{\boldsymbol{\alpha}} \mathbf{X}^{\boldsymbol{\alpha}} \end{aligned}$$

we obtain an action of G on the polynomial ring in n variables in the following way.

$$\begin{aligned} G \times \mathbf{K}[x_1, x_2, ..., x_n] \quad &\to \quad \mathbf{K}[x_1, x_2, ..., x_n], \\ \sigma \cdot f \quad &: \quad = \phi^{-1}(\sigma \cdot \phi(f)). \end{aligned}$$

Lemma 5 *For all $\sigma \in G$ we have $\sigma \cdot X_i = \sum_{j=1}^{n} \rho(\sigma^{-1})_{ij} X_j$.*

Proof. Let $v \in V$ and $(\sigma \cdot X_i)(\widehat{v}) = X_i(\rho(\sigma^{-1}) \cdot \widehat{v}) = \sum_{j=1}^{n} \rho(\sigma^{-1})_{ij} \widehat{v}_j = \left(\sum_{j=1}^{n} \rho(\sigma^{-1})_{ij} X_j\right)(\widehat{v})$. ■

Proposition 12 *For all $\sigma \in G$ and $f \in \mathbf{K}[x_1, x_2, ..., x_n]$ we have*

$$(\sigma \cdot f)(x_1, x_2, ..., x_n) = f\left(\left(\rho(\sigma^{-1}) \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \right)^T \right). \tag{2.3}$$

Proof. Let $f = \sum_{\boldsymbol{\alpha} \in \mathbf{N}_0^n} a_{\boldsymbol{\alpha}} \mathbf{x}^{\boldsymbol{\alpha}}$ and $\sigma \in G$. We obtain

$$\begin{aligned} (\sigma \cdot f)(x_1, x_2, ..., x_n) &= \phi^{-1}(\sigma \cdot \phi(f(x_1, x_2, ..., x_n))) \\ &= \phi^{-1}\left(\sigma \cdot \bigoplus_{\boldsymbol{\alpha} \in \mathbf{N}_0^n} a_{\boldsymbol{\alpha}} \mathbf{X}^{\boldsymbol{\alpha}}\right) = \phi^{-1}\left(\bigoplus_{\boldsymbol{\alpha} \in \mathbf{N}_0^n} a_{\boldsymbol{\alpha}} (\sigma \cdot \mathbf{X})^{\boldsymbol{\alpha}}\right) \\ &= \phi^{-1}\left(\bigoplus_{\boldsymbol{\alpha} \in \mathbf{N}_0^n} a_{\boldsymbol{\alpha}} (\sigma \cdot X_1)^{\alpha_1} \circ (\sigma \cdot X_2)^{\alpha_2} \circ ... \circ (\sigma \cdot X_n)^{\alpha_n}\right) \\ &= \phi^{-1}\left(\bigoplus_{\boldsymbol{\alpha} \in \mathbf{N}_0^n} a_{\boldsymbol{\alpha}} \left(\sum_{j=1}^{n} \rho(\sigma^{-1})_{1j} X_j\right)^{\alpha_1} \circ ... \circ \left(\sum_{j=1}^{n} \rho(\sigma^{-1})_{nj} X_j\right)^{\alpha_n}\right) \end{aligned}$$

$$= \sum_{\boldsymbol{\alpha}\in\mathbf{N}_0^n} a_{\boldsymbol{\alpha}} \left(\sum_{j=1}^n \rho(\sigma^{-1})_{1j}x_j\right)^{\alpha_1} \circ \ldots \circ \left(\sum_{j=1}^n \rho(\sigma^{-1})_{nj}x_j\right)^{\alpha_n}$$
$$= f\left(\sum_{j=1}^n \rho(\sigma^{-1})_{1j}x_j, \sum_{j=1}^n \rho(\sigma^{-1})_{2j}x_j, \ldots, \sum_{j=1}^n \rho(\sigma^{-1})_{nj}x_j\right)$$

as required. ■

Convention : If G is already a matrix group then we consider the identity representation , i.e. $\rho = id$. If we want to emphasize the representation ρ of G we write $\rho(G)$ instead of G. Otherwise we assume that G is already a matrix group (the image of ρ) and neglect the identity representation. If we emphasize the representation theoretic aspect we denote $\mathbf{K}[x_1, x_2, ..., x_n]$ by $\mathbf{K}[V]$.

Example 2 *Let $f = x^2 + xy + y^2 \in \mathbf{C}[x, y]$ and $\sigma^{-1} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$. The variety of f is an ellipse. Applying σ^{-1} to f yields*

$$\begin{aligned}
\sigma \cdot f(x, y) &= f\left(\left(\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}\right)^T\right) = f(\frac{1}{\sqrt{2}}(x-y), \frac{1}{\sqrt{2}}(x+y)) \\
&= \frac{1}{2}(x-y)^2 + \frac{1}{2}(x-y)(x+y) + \frac{1}{2}(x+y)^2 \\
&= \frac{3}{2}x^2 + \frac{1}{2}y^2.
\end{aligned}$$

So we have eliminated the xy term by rotating the axes $45°$ degree and the ellipse is in normal form. Since a circle remains invariant under rotations, so does the polynomial $x^2 + y^2 - 1$ which follows from an easy calculation.

If $char(\mathbf{K}) > 0$ then we define the group action $\cdot$ via

$$\sigma \cdot f(x_1, x_2, ..., x_n) := f\left(\left(\rho(\sigma^{-1}) \cdot (x_1, ..., x_n)^T\right)^T\right) \tag{2.4}$$

for $\sigma \in G$ and $f \in \mathbf{K}[x_1, x_2, ..., x_n]$.

In the sequel let G be a finite group with a faithful representation $\rho : G \to GL_n(\mathbf{K})$.

Definition 33 *A polynomial $f \in \mathbf{K}[x_1, x_2, ..., x_n]$ is an (absolute)* ***invariant*** *w.r.t. G iff for all $\sigma \in G$*

$$\sigma \cdot f = f.$$

The set of all invariant polynomials w.r.t. G is denoted by

$$\mathbf{K}[x_1, x_2, ..., x_n]^G := \{f \in \mathbf{K}[x_1, x_2, ..., x_n] | \forall \sigma \in G : \sigma \cdot f = f\}.$$

*If χ is a linear character of G then f is a **relative** $\chi-$ **invariant** w.r.t. G iff for all $\sigma \in G$*

$$\sigma \cdot f = \chi(\sigma) f.$$

The set of all relative $\chi-$ invariant polynomials w.r.t. G is denoted by

$$\mathbf{K}[x_1, x_2, ..., x_n]^G_\chi := \{f \in \mathbf{K}[x_1, x_2, ..., x_n] | \forall \sigma \in G : \sigma \cdot f = \chi(\sigma) f\}.$$

*If $char(\mathbf{K}) \nmid |G|$ then we speak of **nonmodular** invariant theory, otherwise of **modular** invariant theory*

Proposition 13 *The set $\mathbf{K}[x_1, x_2, ..., x_n]^G$ is a graded ring and $\mathbf{K}[x_1, x_2, ..., x_n]^G_\chi$ is a graded $\mathbf{K}[x_1, x_2, ..., x_n]^G$ module (but not a ring).*

Proof. We obtain a grading for $\mathbf{K}[x_1, x_2, ..., x_n]^G$ from $(\mathbf{K}[x_1, x_2, ..., x_n]^G)_d := \mathbf{K}[x_1, x_2, ..., x_n]_d \cap \mathbf{K}[x_1, x_2, ..., x_n]^G$. In the same manner we obtain a grading for $\mathbf{K}[x_1, x_2, ..., x_n]^G_\chi$ by defining $(\mathbf{K}[x_1, x_2, ..., x_n]^G_\chi)_d := \mathbf{K}[x_1, x_2, ..., x_n]_d \cap \mathbf{K}[x_1, x_2, ..., x_n]^G_\chi$ for a linear character χ of G.
Let $f, g \in \mathbf{K}[x_1, x_2, ..., x_n]^G$ and $\sigma \in G$. The proof of the first claim follows from $(f+g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$. For a linear character χ of G and $h \in \mathbf{K}[x_1, x_2, ..., x_n]^G_\chi$ we have $\sigma \cdot (fh)(x) = (\sigma \cdot f(x)) (\sigma \cdot h(x)) = f(x) (\chi(\sigma) h(x)) = \chi(\sigma)(fh)(x)$. ■

Remark 1 *In general $\mathbf{K}[x_1, x_2, ..., x_n]^G_\chi$ is not a free $\mathbf{K}[x_1, x_2, ..., x_n]^G-$module which can be seen from the following example. We set $R = \mathbf{K}[x_1, x_2]$. Let $G = \mathbf{Z}_2 = \{1, -1\}$, $\rho : G \to GL_2(\mathbf{C})$ be a representation with $\rho(-1) = \langle diag(-1, -1) \rangle$ and $\chi(-1) = -1$ be a linear character. The invariant ring equals $R^{\rho(\mathbf{Z}_2)} = \mathbf{C}[x_1^2, x_2^2] \oplus x_1 x_2 \mathbf{C}[x_1^2, x_2^2]$. Since x_1 and x_2 are relative χ invariants we have $R^G_\chi = x_1 R^G + x_2 R^G$ with the nontrivial relation $x_1 \cdot x_2^2 - x_2 \cdot x_1 x_2 = 0$.*
But we will see in section 2.5 that $\mathbf{K}[x_1, x_2, ..., x_n]^G_\chi$ is a free $\mathbf{K}[\theta_1, \theta_2 ..., \theta_n]$ module provided that $\mathbf{K}[x_1, x_2, ..., x_n]^G$ is Cohen-Macaulay and $\theta_1, \theta_2 ..., \theta_n$ is an hsop for $\mathbf{K}[x_1, x_2, ..., x_n]^G$.

Let χ be a linear character of G and $d \in \mathbf{N}$. We can use the representation-theoretic methods from above to study the homogenous components of $\mathbf{K}[V]^G$ and $\mathbf{K}[V]^G_\chi$, namely we consider $V^* = (\mathbf{K}[V]^G)_1$ (or $V^* = (\mathbf{K}[V]^G_\chi)_1$) as a finite-dimensional $\mathbf{K}-$vectorspace. Then for $d \in \mathbf{N}$ we have $Sym^d V^* =$

$(\mathbf{K}[V]^G)_d$ with induced representation $Sym^d\rho^*$, which has the same properties as $Sym^d\widetilde{\rho}$. Let $a_1\rho_1 \oplus a_2\rho_2 \oplus ...a_k\rho_k$ be the decomposition of $Sym^d\widetilde{\rho}$ in irreducible representations , cf. Theorem 1.2.1 (k is the number of conjugacy classes of G). The number of linearly independent $\chi-$ invariants equals the dimension of the invariant subspace of the representation $a_j\rho_j$ which corresponds to χ. We define analogous projection operators for this action.

Definition 34 *Let χ be a linear character of G and $char(\mathbf{K}) \nmid |G|$. The Reynolds operator of G is the map*

$$\begin{aligned} \mathfrak{R}_\chi^G &: \mathbf{K}[V] \to \mathbf{K}[V]_\chi^G, \\ \mathfrak{R}_\chi^G(f) &: = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})\sigma\cdot f. \end{aligned}$$

We omit χ if it is the trivial character and abbreviate the map $\mathfrak{R}^G(f)$ with f^G.

The map $|G|\cdot\mathfrak{R}^G(f)$ is also called the transfer. If H is a subgroup of G then one can also define the relative transfer $f \mapsto \sum_{\sigma\in B}\sigma\cdot f$ for a set of representatives B of G/H. This map is useful in modular invariant theory, cf. Smith [39].

Proposition 14 *$\mathfrak{R}_\chi^G$ is a $\mathbf{K}[V]^G-$linear projection.*

Proof. For $f \in \mathbf{K}[V]^G$ and $g \in \mathbf{K}[V]$ we have $\mathfrak{R}_\chi^G(fg)(\mathbf{x}) = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})\sigma\cdot (fg)(\mathbf{x}) = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})(fg)(\sigma^{-1}\cdot\mathbf{x}) = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})\cdot f(\sigma^{-1}\cdot\mathbf{x})\cdot g(\sigma^{-1}\cdot \mathbf{x}) = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})\cdot f(\mathbf{x})\cdot g(\sigma^{-1}\cdot\mathbf{x}) = f(\mathbf{x})\frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})\cdot g(\sigma^{-1}\cdot\mathbf{x}) = (f\cdot R_\chi^G(g))(x)$.
Now let $\pi\in G$,then $\pi\cdot\mathfrak{R}_\chi^G(g)(\mathbf{x}) = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})g(\sigma^{-1}\pi^{-1}\cdot\mathbf{x}) = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1}\pi)g(\sigma^{-1}\cdot\mathbf{x}) = \chi(\pi)\frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})g(\sigma^{-1}\cdot\mathbf{x})$.
Let $g'\in\mathbf{K}[V]$. We have $\mathfrak{R}_\chi^G(g+g')(\mathbf{x}) = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})(g+g')(\sigma^{-1}\cdot\mathbf{x}) = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})\left(g(\sigma^{-1}\cdot\mathbf{x}) + g'(\sigma^{-1}\cdot\mathbf{x})\right) = \mathfrak{R}_\chi^G(g)(\mathbf{x}) + \mathfrak{R}_\chi^G(g')(\mathbf{x})$.
For $f\in\mathbf{K}[V]$ we have $\mathfrak{R}_\chi^G(\mathfrak{R}_\chi^G(f))(\mathbf{x}) = \mathfrak{R}_\chi^G\left(\frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})\sigma\cdot f\right)(\mathbf{x}) = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})\frac{1}{|G|}\sum_{\tau\in G}\chi(\tau^{-1})f(\sigma^{-1}\tau^{-1}\cdot\mathbf{x}) = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})\frac{1}{|G|}\sum_{\tau\in G}\chi(\sigma\tau^{-1})f(\tau^{-1}\cdot\mathbf{x}) = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})\chi(\sigma)\mathfrak{R}_\chi^G(f)(\mathbf{x}) = \mathfrak{R}_\chi^G(f)(\mathbf{x})$. ∎

We continue the example of the permutation representation from Section 1.2.1.

Example 3 *Let $\rho : S_3 \to GL_n(\mathbf{K})$ be the permutation representation of S_3 over a field with characteristic 0. Let V^* be the dual space of $\mathbf{K}^3$ with basis X_1, X_2, X_3, hence $V^* \cong \mathbf{K}[x_1, x_2, x_3]_1$. We consider the dual representation ρ^* on V^* and the representation $Sym^2\widetilde{\rho}$ on $Sym^2 V$.*
An arbitrary element $f \in \mathbf{V}^*$ equals $aX_1 + bX_2 + cX_3$ for some $a, b, c \in \mathbf{K}$. So f is invariant w.r.t. ρ^* if

$$\begin{aligned} aX_1 + bX_2 + cX_3 &= bX_1 + aX_2 + cX_3, \\ aX_1 + bX_2 + cX_3 &= cX_1 + aX_2 + bX_3. \end{aligned}$$

From these equations we obtain $a = b = c$. Note that f can be considered as a polynomials in the variables X_1, X_2, X_3 so the scalar multiplies of $X_1+X_2+X_3$ are the symmetric polynomials of degree 1. In representation theoretic terms we have computed the invariant subspace of the representation ρ^*, whose dimension is 1. The Reynolds map $\mathfrak{R}^{\rho^*(S_3)} : f \longmapsto \sum_{\pi \in S_3} \rho^*(\pi)(f)$ is a projection on the invariant subspace $\langle X_1 + X_2 + X_3 \rangle$ of V^*. The dimension of this subspace is the number of occurrences of the trivial representation in the decomposition of the representation ρ^*. Since $\rho^* \cong \widetilde{\rho}$ this dimension can be calculated with characters, namely

$$\begin{aligned} \dim (V^*)^{\rho^*(S_3)} &= \left\langle \chi_{triv}, \chi_{\widetilde{\rho}} \right\rangle = \frac{1}{|S_3|} \sum_{\pi \in S_3} \chi_{\widetilde{\rho}}(\pi) \\ &= \frac{1}{6}(3 + 1 + 1 + 1 + 0 + 0) = 1. \end{aligned}$$

Now we treat $Sym^2 V^*$ and consider the representation $Sym^2\widetilde{\rho}$ on $Sym^2 V$ (instead of $Sym^2\rho^*$). Let $\{x_1, x_2, x_3\}$ be a basis of V,then a basis for the vectorspace $Sym^2 V$ is given by $B = \{x_1^2, x_1x_2, x_1x_3, x_2^2, x_2x_3, x_3^2\}$. The induced representation $Sym^2\widetilde{\rho}$ of S_3 is given by

$$(12) \longmapsto \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$(123) \longmapsto \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

The vector (or polynomial) $f = c_1x_1^2 + c_2x_1x_2 + c_3x_1x_3 + c_4x_2^2 + c_5x_2x_3 + c_6x_3^2$ *is symmetric if*

$$\begin{aligned} Sym^2\widetilde{\rho}((12)) \cdot \widehat{f} &= \widehat{f}, \\ Sym^2\widetilde{\rho}((123)) \cdot \widehat{f} &= \widehat{f}. \end{aligned}$$

If we apply the Reynolds map $\mathfrak{R}^{Sym^2\widetilde{\rho}(S_3)} : \widehat{f} \longmapsto \frac{1}{6}\sum_{\pi \in S_3} Sym^2\rho^*(\pi) \cdot \widehat{f}$ *to all monomials in* B *we obtain the set* $\{x_1^2 + x_2^2 + x_3^2, x_1x_2 + x_1x_3 + x_2x_3\}$ *which is a basis for* $(Sym^2V)^{Sym^2\widetilde{\rho}(S_3)}$. *So we have*

$$\begin{aligned} \dim\Big((Sym^2V^*)^{Sym^2\rho^*(S_3)}\Big) &= \langle \chi_{triv}, \chi_{Sym^2\widetilde{\rho}} \rangle = \frac{1}{|S_3|}\sum_{\pi \in S_3} \chi_{Sym^2\widetilde{\rho}}(\pi) \\ &= \frac{1}{6}(6+2+2+2+0+0) = 2. \ \Box \end{aligned}$$

According to Sturmfels [43] the following problems are often called the fundamental problems of invariant theory.

1. Find a set $\{f_1, f_2..., f_m\}$ of generators for the invariant subring $\mathbf{K}[x_1, x_2, ..., x_n]^G$ of $\mathbf{K}[x_1, x_2, ..., x_n]$.

2. Describe the algebraic relations among the generators $\{f_1, f_2..., f_m\}$ (syzygies).

3. Give an algorithm for rewriting an arbitrary invariant polynomial $f \in \mathbf{K}[x_1, x_2, ..., x_n]^G$ in terms of $\{f_1, f_2..., f_m\}$.

4. Given a geometric property P. Find the corresponding invariants (or covariants[1]) and vice versa. Is there an algorithm for this translation from geometry to algebra.

We describe solutions for problem (1), (2) and (3). In Section 2.1 we have solved problems (1),(2) and (3) for the group S_n. For problem (4) we describe a partial solution in Section 4.4

We extend problem (1) to $\mathbf{K}[x_1, x_2, ..., x_n]_\chi^G$ for a linear character χ of G. In the next section we prove certain finiteness statements for $\mathbf{K}[x_1, x_2, ..., x_n]^G$ and $\mathbf{K}[x_1, x_2, ..., x_n]_\chi^G$. For all groups (finite and infinite) in this text the invariant ring is finitely generated. The general case is precisely Hilbert's 14'th problem, namely : Given $G \leq GL(\mathbf{C}^n)$, is $\mathbf{K}[x_1, x_2, ..., x_n]^G$ finitely generated as a $\mathbf{K}-$algebra. A famous result of Nagata provides a negative answer, cf. [29]

[1]We refer, e.g., to ch. 3 of Sturmfels [43] for a definition.

Example 4 *Let* $G = V_4 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ *be a representation of* $\mathbf{Z}_2 \times \mathbf{Z}_2$. *A polynomial* $f \in \mathbf{C}[x_1, x_2]$ *is invariant w.r.t.* G *if*

$$f(x_1, x_2) = f(-x_1, x_2) = f(x_1, -x_2) = f(-x_1, -x_2).$$

So we have

$$\begin{aligned} f(x_1, x_2) &= f(-x_1, x_2) \Leftrightarrow \sum_{i,j} a_{i,j} x_1^i x_2^j = \sum_{i,j} a_{i,j} (-x_1)^i x_2^j = \sum_{i,j} (-1)^i a_{i,j} x_1^i x_2^j \\ &\Longleftrightarrow \\ a_{i,j} &= (-1)^i a_{i,j} \Longleftrightarrow a_{i,j} = 0 \text{ for } i \text{ odd.} \end{aligned}$$

With the same computation we obtain $f(x_1, x_2) = f(x_1, -x_2) \Leftrightarrow a_{i,j} = (-1)^j a_{i,j} \Leftrightarrow j$ *is odd. So* x_1 *and* x_2 *appear to an even power in* f *and therefore* f *can be written as* $f(x_1, x_2) = g(x_1^2, x_2^2)$ *for some* $g \in \mathbf{C}[y_1, y_2]$. *Conversely each polynomial of this form is invariant w.r.t.* V_4 *so we have*

$$\mathbf{C}[x_1, x_2]^{V_4} = \mathbf{C}[x_1^2, x_2^2].$$

Since x_1^2 *and* x_2^2 *are algebraically independent, the Hilbert series of* $\mathbf{C}[x_1, x_2]^{V_4}$ *can be computed with Lemma 1.4.3, namely*

$$H(\mathbf{C}[x_1^2, x_2^2], t) = \frac{1}{(1 - t^2)^2}.$$

2.3 Three Finiteness Theorems

In his talk at the international mathematical congress 1900 Hilbert posed 21 problems. The fourteenth problem was concerned with invariant theory.

Is the ring of invariants always finitely generated as a $\mathbf{C}-$ *algebra ?*

In general, the answer is negative, which was first shown by Nagata in 1959 (cf. [29]), where he presented a counterexample. But in the case of linear reductive groups[2] over $\mathbf{C}$, or finite groups over fields $\mathbf{K}$ with characteristic 0 or $p > 0$, for a prime p, the invariant ring is finitely generated as a $\mathbf{K}-$algebra. We restrict ourselves to finite groups and present three different proofs for the finiteness of the invariant ring, each with individual advances and disadvantages.

In this section we identify the group G with the image $\rho(G)$ for a matrix representation $\rho : G \to GL_n(\mathbf{K})$.

[2]For a definition we refer, e.g., to Derksen [12].

2.3.1 Noether's General Approach

We present E. Noether's characteristic-free approach for finite groups, cf. Noether [31]. Let $\mathbf{K}$ be a field and $G \leq GL_n(\mathbf{K})$ be a finite group.

Lemma 6 *The ring* $\mathbf{K}[x_1, x_2, ..., x_n]$ *is integral over* $\mathbf{K}[x_1, x_2, ..., x_n]^G$.

Proof. Let $i \in \{1, 2, ..., n\}$ and consider $P_i(t) = \prod_{\sigma \in G}(\sigma \cdot x_i - t)$. The polynomial P_i is contained in $\mathbf{K}[x_1, x_2, ..., x_n][t]$ and obviously $P_i(x_i) = 0$. If we let G act on the coefficients of P_i w.r.t. t, which we denote by p_{ij} for $1 \leq j \leq \deg P_i(t)$, we obtain $\sigma \cdot P_i(t) = P_i(t)$ for all $\sigma \in G$. So the coefficients of P_i are invariant w.r.t. G. Since each x_i is integral over $\mathbf{K}[x_1, x_2, ..., x_n]^G$ the claim follows from Proposition 1.4.7. ■

Theorem 9 *(Noether 1926) The invariant ring* $\mathbf{K}[x_1, x_2, ..., x_n]^G$ *is a finitely generated* $\mathbf{K}-$*algebra.*

Proof. Let A be the $\mathbf{K}-$algebra, which is generated from the coefficients of the P_i, i.e. $A = \mathbf{K}[p_{ij}]$. It is clear that $\mathbf{K}[x_1, x_2, ..., x_n]$ is a finitely generated $A-$ algebra (take $x_1, ..., x_n$) and from Lemma 2.3.6 and Proposition 1.4.8 it follows that $\mathbf{K}[x_1, x_2, ..., x_n]$ is also finitely generated as an $A-$module. From $p_{ij} \in \mathbf{K}[x_1, x_2, ..., x_n]^G$ it follows that $\mathbf{K}[x_1, x_2, ..., x_n]^G$ is an $A-$submodule of $\mathbf{K}[x_1, x_2, ..., x_n]$. Since A is the image of a Noetherian ring (take, for instance, $y_k \mapsto p_{ij}$) it follows from Proposition 1.3.4 (a) and (b) that A is Noetherian and $\mathbf{K}[x_1, x_2, ..., x_n]$ is a Noetherian $A-$module. Now Proposition 1.3.4 (c) implies that $\mathbf{K}[x_1, x_2, ..., x_n]^G$ is finitely generated as an $A-$module, and, since A is a finitely generated $\mathbf{K}-$algebra, $\mathbf{K}[x_1, x_2, ..., x_n]^G$ is finitely generated as a $\mathbf{K}-$algebra. ■

Note that if $f \in \mathbf{K}[x_1, x_2, ..., x_n]^G$ then each homogenous component of f is contained in $\mathbf{K}[x_1, x_2, ..., x_n]^G$. Therefore we can chose a set of homogenous generators.

Corollary 3 *There exists an hsop* $\theta_1, \theta_2, ..., \theta_n$ *for* $\mathbf{K}[x_1, x_2, ..., x_n]^G$.

Proof. From $\dim \mathbf{K}[x_1, x_2, ..., x_n] = n$, Lemma 2.3.6 and Proposition 1.4.9 it follows that $\dim \mathbf{K}[x_1, x_2, ..., x_n]^G = n$. Hence Noether's Normalization Lemma (Lemma 1.4.5) implies that there are n algebraically independent elements $\theta_1, \theta_2, ..., \theta_n$ s.t. $\mathbf{K}[x_1, x_2, ..., x_n]^G$ is finitely generated as a module over $\mathbf{K}[\theta_1, \theta_2, ..., \theta_n]$. ■

The module in the above proof need not be free. The drawback of this result is, that it is neither constructive nor gives a degree bound, also it holds only for finite groups.

Definition 35 *Let $\theta_1, \theta_2, ..., \theta_n \in \mathbf{K}[x_1, x_2, ..., x_n]^G$ be an hsop for $\mathbf{K}[x_1, x_2, ..., x_n]^G$ and let $\eta_1, \eta_2, ..., \eta_m$ be a minimal generating set of $\mathbf{K}[x_1, x_2, ..., x_n]^G$ as a $\mathbf{K}[\theta_1, \theta_2, ..., \theta_n]-$module. The elements $\theta_1, \theta_2, ..., \theta_n$ are called **primary invariants** and the elements $\eta_1, \eta_2, ..., \eta_m$ are called **secondary invariants** of $\mathbf{K}[x_1, x_2, ..., x_n]^G$. We call $(\deg\theta_1, \deg\theta_2, ..., \deg\theta_n)$ the degrees of the hsop $\theta_1, \theta_2, ..., \theta_n$.*

2.3.2 Noether's Degree Bound

The following theorem of E. Noether (cf. [30]) is constructive, but does not hold over arbitrary fields. Let $\mathbf{K}$ be a field and $G \leq GL_n(\mathbf{K})$ be a finite group. The restriction to the nonmodular case comes from the application of the Reynolds operator.

Theorem 10 *(Noether 1916) Let $\mathbf{K}$ be a field of $char(\mathbf{K}) > |G|!$ or $char(\mathbf{K}) = 0$. Then $\mathbf{K}[x_1, x_2, ..., x_n]^G$ is generated as a $\mathbf{K}-$ algebra by at most $\binom{|G|+n}{n}$ invariants of degree not exceeding $|G|$. In particular*

$$\mathbf{K}[x_1, x_2, ..., x_n]^G = \mathbf{K}[\mathfrak{R}^G(\mathbf{x}^{\boldsymbol{\beta}}) : |\boldsymbol{\beta}| \leq |G|].$$

Proof. We follow the proof of Theorem 5 of § 3 of ch. 7 in Cox et. al. [9]. Since $\mathfrak{R}^G$ is linear it suffices to show that for all $\boldsymbol{\alpha} \in \mathbf{N}^n$ we can express $\mathfrak{R}^G(\mathbf{x}^{\boldsymbol{\alpha}})$ as a polynomial in the $\mathfrak{R}^G(\mathbf{x}^{\boldsymbol{\beta}})$ for $|\boldsymbol{\beta}| \leq |G|$. Let $k \in \mathbf{N}$ be fixed.

$$(x_1 + x_2 + ... + x_n)^k = \sum_{|\boldsymbol{\alpha}|=k} a_{\boldsymbol{\alpha}} \mathbf{x}^{\boldsymbol{\alpha}} \tag{2.5}$$

If A_i denotes the $i-$th row of $A = (a_{i,j}) \in G$ then $A^{-1} \cdot \mathbf{x}^{\boldsymbol{\alpha}} = \prod_{i=1}^n (A_i \cdot \mathbf{x})^{\alpha_i}$. Let $u_1, u_2, ..., u_n$ be new variables and substitute $u_i A_i \cdot \mathbf{x}$ for x_i in (2.5). Then we obtain

$$(u_1 A_1 \mathbf{x} + u_2 A_2 \mathbf{x} + ... + u_n A_n \mathbf{x})^k = \sum_{|\boldsymbol{\alpha}|=k} a_{\boldsymbol{\alpha}} \prod_{i=1}^n (A_i \cdot \mathbf{x})^{\alpha_i} \mathbf{u}^{\boldsymbol{\alpha}} = \sum_{|\boldsymbol{\alpha}|=k} a_{\boldsymbol{\alpha}} (A^{-1} \cdot \mathbf{x}^{\boldsymbol{\alpha}}) \mathbf{u}^{\boldsymbol{\alpha}}.$$

Let $U_A = u_1 A_1 \mathbf{x} + u_2 A_2 \mathbf{x} + ... + u_n A_n \mathbf{x}$. If we sum over G we get

$$\begin{aligned} S_k \ :&= \sum_{A \in G} (U_A)^k = \sum_{A \in G} \sum_{|\boldsymbol{\alpha}|=k} a_{\boldsymbol{\alpha}} (A^{-1} \cdot \mathbf{x})^{\boldsymbol{\alpha}} \mathbf{u}^{\boldsymbol{\alpha}} & (2.6) \\ &= \sum_{|\alpha|=k} \sum_{A \in G} a_{\boldsymbol{\alpha}} (A^{-1} \cdot \mathbf{x})^{\boldsymbol{\alpha}} \mathbf{u}^{\boldsymbol{\alpha}} & (2.7) \\ &= |G| \sum_{|\boldsymbol{\alpha}|=k} a_{\boldsymbol{\alpha}} \mathfrak{R}^G(\mathbf{x}^{\boldsymbol{\alpha}}) \mathbf{u}^{\boldsymbol{\alpha}}. \end{aligned}$$

Since S_k is a power sum in the $|G|$ quantities U_A (for $A \in G$) it is a symmetric polynomial in U_A for $A \in G$. Hence it can be written as a polynomial in the $|G|$ power sums $S_1, ..., S_{|G|}$. So

$$S_k = P\left(S_1, ..., S_{|G|}\right) \text{ for some } P \in \mathbf{K}[y_1, y_2, ..., y_{|G|}].$$

Substituting in (2.6) we obtain

$$|G| \sum_{|\boldsymbol{\alpha}|=k} a_{\boldsymbol{\alpha}} \mathfrak{R}^G(\mathbf{x}^{\boldsymbol{\alpha}}) \mathbf{u}^{\boldsymbol{\alpha}} = P\left(|G| \sum_{|\boldsymbol{\beta}|=1} a_{\boldsymbol{\beta}} \mathfrak{R}^G(\mathbf{x}^{\boldsymbol{\beta}}) \mathbf{u}^{\boldsymbol{\beta}}, ..., |G| \sum_{|\boldsymbol{\beta}|=|G|} a_{\boldsymbol{\beta}} \mathfrak{R}^G(\mathbf{x}^{\boldsymbol{\beta}}) \mathbf{u}^{\boldsymbol{\beta}}\right).$$

Expansion and coefficient comparison yields the desired result. ■

Definition 36 *Let $h_1, h_2, ..., h_m$ be homogenous invariants s.t.* $\mathbf{K}[h_1, h_2, ..., h_m] = \mathbf{K}[x_1, x_2, ..., x_n]^G$. *Then $h_1, h_2, ..., h_m$ are called **fundamental invariants** of* $\mathbf{K}[x_1, x_2, ..., x_n]^G$.

We have seen that for any finite group G the invariant ring is finitely generated. Moreover, one can derive a simple algorithm for computing a generating set of the invariant ring from the above Theorem.

Algorithm *Invariants*$(G) :=$
invariants $:= \{\}$;
for all $\boldsymbol{\alpha} \in \mathbf{N}^n$ with $|\boldsymbol{\alpha}| \leq \binom{|G|+n}{n}$ **do**
. *invariants* $:=$ *invariants* $\cup \left\{\mathfrak{R}^G(\mathbf{x}^{\boldsymbol{\alpha}})\right\}$;
end for;

The algorithm is not very practical which can be seen from the following example.

Example 5 *The invariant ring of the permutation representation of S_3 equals* $\mathbf{K}[x, y, z]^{S_3} = \mathbf{K}[x + y + z, xy + xz + yz, xyz]$. *But if we compute the generators with the above algorithm, we obtain the following set with 22 elements* : $\{x + y + z, x\,y\,z, x^2\,y^2\,z^2, x\,y + x\,z + y\,z, x^2 + y^2 + z^2, x^2\,y + x\,y^2 + x^2\,z + y^2\,z + x\,z^2 + y\,z^2, x^2\,y\,z + x\,y^2\,z + x\,y\,z^2, x^2\,y^2 + x^2\,z^2 + y^2\,z^2, x^2\,y^2\,z + x^2\,y\,z^2 + x\,y^2\,z^2, x^3 + y^3 + z^3, x^3\,y + x\,y^3 + x^3\,z + y^3\,z + x\,z^3 + y\,z^3, x^3\,y\,z + x\,y^3\,z + x\,y\,z^3, x^3\,y^2 + x^2\,y^3 + x^3\,z^2 + y^3\,z^2 + x^2\,z^3 + y^2\,z^3, x^3\,y^2\,z + x^2\,y^3\,z + x^3\,y\,z^2 + x\,y^3\,z^2 + x^2\,y\,z^3 + x\,y^2\,z^3, x^3\,y^3 + x^3\,z^3 + y^3\,z^3, x^4 + y^4 + z^4, x^4\,y + x\,y^4 + x^4\,z + y^4\,z + x\,z^4 + y\,z^4, x^4\,y\,z + x\,y^4\,z + x\,y\,z^4, x^4\,y^2 + x^2\,y^4 + x^4\,z^2 + y^4\,z^2 + x^2\,z^4 + y^2\,z^4, x^5 + y^5 + z^5, x^5\,y + x\,y^5 + x^5\,z + y^5\,z + x\,z^5 + y\,z^5, x^6 + y^6 + z^6\}$.

2.3.3 Hilbert's Approach.

In this Section we present Hilbert's Finiteness Theorem which is contained in his landmark paper *"Über die Theorie der Algebraischen Formen"* in 1890, where D. Hilbert proved that for reductive groups $G \leq GL_n(\mathbf{C})$ the ring of invariants is finitely generated as a $\mathbf{C}-$algebra, cf. Hilbert [18]. There he used nonconstructive methods, namely he introduced his Basis Theorem as a Lemma (Theorem 3 in section 1.3). At this time this was a radical new approach and P. Gordon, the "King of Invariants" exclaimed *"Das ist nicht Mathematik, das ist Theologie"*. Hilbert responded three years later with his paper *"Über die Vollen Invariantensysteme"*, cf. Hilbert [19], where he presented a constructive proof. This paper is considerably deeper w.r.t. construction and contains the Nullstellensatz, the Syzygy Theorem and the Hilbert function. In his Ph.D. thesis H. Derksen was able to make the proof of Hilbert's Finiteness Theorem from 1890 constructive, cf. Derksen [12]. Hilbert's Finiteness Theorem holds for all matrix groups which admit a projection map that satisfies the Reynolds properties. Note that such matrix groups need not be finite.

Theorem 11 *(Hilbert 1890) Let $\mathbf{K}$ be a field and $G \leq GL_n(\mathbf{K})$ be a finite group s.t. $char(\mathbf{K}) \nmid |G|$. Then $\mathbf{K}[x_1, x_2, ..., x_n]^G$ is finitely generated as a $\mathbf{K}-$algebra.*

Proof. Let $R = \mathbf{K}[x_1, x_2, ..., x_n]$ and R_+^G be the set of homogenous elements of R^G of positive degree. Hilbert's basis Theorem implies that the ideal $\left\langle R_+^G \right\rangle \trianglelefteq R$ can be generated by finitely many homogenous invariant polynomials $h_1, ..., h_k$. We claim that $R^G = \mathbf{K}[h_1, ..., h_k]$. It is clear that $\mathbf{K}[h_1, ..., h_k] \subseteq R^G$. Now assume that this inclusion is strict and take $f \in R^G \backslash \mathbf{K}[h_1, ..., h_k]$ homogenous of minimal degree. Since $f \in \left\langle R_+^G \right\rangle$ we have $f = \sum_{i=1}^k p_i h_i$ for some homogenous polynomials $p_i \in R$ with $\deg p_i = \deg f - \deg h_i$ (cf. Lemma 1.4.4). The polynomial f is invariant and therefore

$$f = \mathfrak{R}^G(f) = \sum_{i=1}^{k} \mathfrak{R}^G(p_i h_i) = \sum_{i=1}^{k} \mathfrak{R}^G(p_i) h_i.$$

From $f \notin \mathbf{K}[h_1, ..., h_k]$ we conclude that for some j the polynomials p_j is not a constant and $\mathfrak{R}^G(p_j) \neq 0$, so

$$\deg p_j = \deg \mathfrak{R}^G(p_j) < \deg f,$$

but $\mathfrak{R}^G(p_j) \in R^G$, a contradiction to the minimality assumption. ■

The above proof implies that any ideal basis of $\langle R_+^G \rangle$, which consists of homogenous invariant polynomials, is also an algebra basis for $\mathbf{K}[x_1, x_2, ..., x_n]^G$. This property is very important for the intersection algorithm, presented in Section 3.2.

2.4 Molien's Theorem

Let $\mathbf{K}$ be a field of characteristic $0, G$ be a finite group and $\rho : G \to GL_n(\mathbf{K})$ be a faithful representation and $V = \mathbf{K}^n$. We are interested in the number of linearly independent homogenous invariants of degree $d \in \mathbf{N}$, i.e., we want to know the Hilbert series of $\mathbf{K}[V]^{\rho(G)}$ and of $\mathbf{K}[V]_\chi^{\rho(G)}$ for a linear character χ of G, which we denote with $H^{\rho(G)}$ and $H_\chi^{\rho(G)}$ respectively. So we are interested in the formal power series

$$H_\chi^{\rho(G)}(t) = \sum_{d=0}^{\infty} \dim_{\mathbf{K}}(\mathbf{K}[V]_\chi^{\rho(G)})_d \cdot t^d.$$

If $char(\mathbf{K}) = 0$ we can proceed as follows. From the results in Section 2.2 we know that for a given representation $\rho : G \to GL_n(\mathbf{K})$ it is sufficient to consider the equivalent representation $\widetilde{\rho}(\sigma) = \rho(\sigma^{-1})^T$. We compute the dimension of the graded component $(\mathbf{K}[V]_\chi^{\widetilde{\rho}(G)})_d$ for each $d \in \mathbf{N}$ with the aid of representation theory. Note that $\dim Sym^d V = \binom{n+d-1}{d-1} =: N$. We transform the representation $Sym^d \rho^*$, which acts on the $N-$dimensional vectorspace $\mathbf{K}[V]_d$, to the representation $Sym^d \widetilde{\rho}$, which acts on $\mathbf{K}^N$. The dimension of $(\mathbf{K}[V]_\chi^{\widetilde{\rho}(G)})_d$ equals the dimension of the invariant subspace of the representation belonging to the character χ. Hence

$$\dim_{\mathbf{K}}(\mathbf{K}[V]_\chi^{\rho(G)})_d = \langle \chi_{Sym^d \widetilde{\rho}}, \chi \rangle .$$

Lemma 7 *Let $\sigma \in G$ and $A = \rho(\sigma)$ with eigenvalues $\lambda_1, \lambda_2, ..., \lambda_n$ and assume $char(\mathbf{K}) = 0$.*
(a) If A is of finite order (i.e. $A^k = E$ for some $k \in \mathbf{N}$) then A can be diagonalized, i.e. there exists T s.t. $TAT^{-1} = diag(\lambda_1, \lambda_2, ..., \lambda_n)$..
(b) $trace(A) = \sum_{i=1}^n \lambda_i$.
(c) The eigenvalues of $Sym^d \rho(\sigma)$ are the elements $\prod_{i=1}^n \lambda_i^{\alpha_i}$ for all $\boldsymbol{\alpha} \in \mathbf{N}_0^n$ with $|\boldsymbol{\alpha}| = d$.

Proof. (a) Assume that A is not diagonalizable. Let $l > 1$ and B be a $l \times l$ Jordan-block of the Jordan normal form of A with the eigenvalue λ (of order α) of A in the diagonal and $B_{i,i+1} = 1$ for $1 \leq i \leq l - 1$. Note that such a

block exists, otherwise A would be a diagonal matrix. Since $A^k = I$ we have $\alpha \mid k$ and $B^k = I$, but $\left(B^k\right)_{1,2} = k \cdot \lambda^{k-1}$, a contradiction.
(b) follows from (a) and the fact that *trace* is constant on conjugacy classes.
(c) W.l.o.g. we assume that $A = diag(\lambda_1, \lambda_2, ..., \lambda_n)$. The $\binom{n+d-1}{d-1}$ monomials of degree d form a basis of $Sym^d\left(\mathbf{C}^n\right)^*$. If $f = \prod_{j=1}^{d} x_{i_j}$ is a monomial, then $\rho^*(\sigma)(f) = \prod_{j=1}^{d} \lambda_{i_j} x_{i_j} = \prod_{j=1}^{d} \lambda_{i_j} \prod_{j=1}^{d} x_{i_j}$. The claim follows from the isomorphism * (cf. Proposition 2.2.11 (b)). ■

In the sequel we denote the identity matrix of $GL_n(\mathbf{K})$ with I and identify G with $\rho(G)$.

Theorem 12 *(Molien 1897) Let χ be a linear character of G.*
(a) If $char(\mathbf{K}) = 0$ then the Hilbert series of $\mathbf{K}[V]^G_\chi$ equals

$$H^G_\chi(t) = \frac{1}{|G|} \sum_{\sigma \in G} \frac{\chi(\sigma)}{\det(I - t\sigma)}.$$

(b) Assume $char(\mathbf{K}) = p > 0$ for a prime p and $p \nmid |G|$. Choose primitive all $|G|-$roots of unity $\{\lambda\}$ in $\mathbf{K}$ and $\left\{\widetilde{\lambda}\right\}$ in $\mathbf{Q}$. Let $\lambda_\sigma^{k_1}, \lambda_\sigma^{k_2}, ..., \lambda_\sigma^{k_n}$ be the eigenvalues of $\sigma \in G$ and set

$$\Phi_\sigma(t) = \prod_{i=1}^{n} (1 - t\widetilde{\lambda}_\sigma^{k_i}).$$

Then the Hilbert series of $\mathbf{K}[V]^G$ equals

$$H^G(t) = \frac{1}{|G|} \sum_{\sigma \in G} \Phi_\sigma(t).$$

The formulation of part (b) is due to Decker and Jong [11]. We present a proof for fields with characteristic 0. For the general case we refer, e.g., to Smith [39].
Proof. We denote the eigenvalues of $\rho(\sigma) \in G$ with $\lambda_{\sigma,1}, \lambda_{\sigma,2}, ..., \lambda_{\sigma,n}$. From Lemma 2.4.7 (c) it follows that

$$\chi_{_{Sym^d \rho}}(\sigma) = \sum_{d_1 + d_2 ... + d_n = d} \lambda_{\sigma,1}^{d_1} \lambda_{\sigma,2}^{d_2} \cdot ... \cdot \lambda_{\sigma,n}^{d_n}.$$

From the previous discussion we obtain

$$H^G_\chi(t) \quad = \quad \sum_{d=0}^{\infty} \left\langle \chi_{Sym^d \widetilde{\rho}}, \chi \right\rangle \cdot t^d = \sum_{d=0}^{\infty} \frac{1}{|G|} \sum_{\sigma \in G} \chi_{_{Sym^d \widetilde{\rho}}}(\sigma) \chi(\sigma^{-1}) \cdot t^d$$

$$\begin{aligned}
&= \sum_{d=0}^{\infty}\frac{1}{|G|}\sum_{\sigma\in G}\chi_{Sym^d\rho}(\sigma^{-1})\chi(\sigma^{-1})\cdot t^d\\
&= \sum_{d=0}^{\infty}\frac{1}{|G|}\sum_{\sigma\in G}\sum_{d_1+d_2...+d_n=d}\lambda_{\sigma,1}^{d_1}\lambda_{\sigma,2}^{d_2}\cdot\ldots\cdot\lambda_{\sigma,n}^{d_n}\chi(\sigma)\cdot t^d\\
&= \frac{1}{|G|}\sum_{\sigma\in G}\sum_{(d_1,d_2,\ldots,d_n)\in\mathbf{N}_0^n}\lambda_{\sigma,1}^{d_1}\lambda_{\sigma,2}^{d_2}\cdot\ldots\cdot\lambda_{\sigma,n}^{d_n}\chi(\sigma)\cdot t^{d_1+d_2...+d_n}\\
&= \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma)\frac{1}{(1-\lambda_{\sigma,1}t)}\cdot\frac{1}{(1-\lambda_{\sigma,2}t)}\cdot\ldots\cdot\frac{1}{(1-\lambda_{\sigma,n}t)}\\
&= \frac{1}{|G|}\sum_{\sigma\in G}\frac{\chi(\sigma)}{\det(I-t\sigma)}.\ \blacksquare
\end{aligned}$$

Example 6 *We compute the Hilbert series of $\mathbf{C}[V]^{V_4}$ (cf. Example 2.2.4). We have*

$$\begin{aligned}
H^{V_4}(t) &= \frac{1}{4}\left(\frac{1}{1-2\,t+t^2}+\frac{1}{1+2\,t+t^2}+\frac{1}{1-t^2}+\frac{1}{1-t^2}\right)\\
&= \frac{1}{(1-t^2)^2}=\sum_{k=0}^{\infty}(k+1)t^{2k}\\
&= 1+2\,t^2+3\,t^4+4\,t^6+5\,t^8+6\,t^{10}+7\,t^{12}+8\,t^{14}+\mathrm{O}(t^{15}).
\end{aligned}$$

Since $H^{V_4}(t)=H(\mathbf{C}[V]^{V_4},t)$ we have found a generating set for the invariant ring in Example 2.2.4.

Remark 2 *For finite groups $G,G'\leq GL_n(\mathbf{K})$ the property $H^G(t)=H^{G'}(t)$ is not sufficient for $G=G'$. Furthermore $H^G(t)=\prod_{i=1}^n\frac{1}{1-t^{d_i}}$ for some $d_i\in\mathbf{N}$ does not imply that there exists an hsop of degree $(d_1,d_2,\ldots,d_n)$, cf. Example 4.1.20.*

2.5 The Invariant Ring is Cohen-Macaulay

In Section 2.3.1 we have seen that there exists an hsop $\theta_1,\theta_2,\ldots,\theta_n$ s.t. $\mathbf{K}[x_1,x_2,\ldots,x_n]^G$ is a finitely generated $\mathbf{K}[\theta_1,\theta_2,\ldots,\theta_n]-$module. In this section we show that if $char(\mathbf{K})\nmid|G|$ then $\mathbf{K}[x_1,x_2,\ldots,x_n]^G$ is a finitely generated *free* $\mathbf{K}[\theta_1,\theta_2,\ldots,\theta_n]$ module, i.e., there exist homogenous $\eta_1,\eta_2,\ldots,\eta_m\in\mathbf{K}[x_1,x_2,\ldots,x_n]^G$ s.t.

$$\mathbf{K}[x_1,x_2,\ldots,x_n]^G=\bigoplus_{i=1}^m\eta_i\mathbf{K}[\theta_1,\theta_2,\ldots,\theta_n].$$

This is equivalent to the fact that $\mathbf{K}[x_1, x_2, ..., x_n]^G$ is a Cohen-Macaulay ring. For details on Cohen-Macaulay rings we refer to Eisenbud [13].

In the sequel let R be a $\mathbf{K}-$algebra of Krull-dimension n which is generated by finitely many homogenous elements.

Definition 37 *The* $\mathbf{K}-$*algebra (or ring)* R *is* ***Cohen-Macaulay*** *iff there exists an hsop* $\theta_1, \theta_2, ..., \theta_n$ *s.t.* R *is a finitely generated, free* $\mathbf{K}[\theta_1, \theta_2, ..., \theta_n]-$*module. Let* $\eta_1, \eta_2, ..., \eta_m$ *be a module basis for* R*. The decomposition*

$$R = \bigoplus_{i=1}^{m} \eta_i \mathbf{K}[\theta_1, \theta_2, ..., \theta_n]$$

is called the ***Hironaka decomposition*** *of* R *w.r.t.* $\theta_1, \theta_2, ..., \theta_n$*.*

Note that the Hironaka decomposition is by no means unique. This can be seen, e.g., from Example 2.5.8.

Definition 38 *The elements* $\theta_1, \theta_2 ..., \theta_k \in R$ *are called a* ***regular sequence*** *in* R *iff* $\langle \theta_1, \theta_2 ..., \theta_k \rangle \subsetneq R$ *and* θ_i *is not a zerodivisor in* $R/\langle \theta_1, \theta_2, ..., \theta_{i-1} \rangle$ *for* $1 \leq i \leq k$*.*

We provide a different characterization of the Cohen-Macaulay property.

Lemma 8 *The algebra* R *is Cohen-Macaulay iff there exists an hsop* $\theta_1, \theta_2 ..., \theta_n$ *which is also a regular sequence.*

Proof. Assume that R is a free $\mathbf{K}[\theta_1, \theta_2 ..., \theta_n]-$module with basis $\eta_1, ..., \eta_m$ and that θ_k is a zerodivisor in $R/\langle \theta_1, \theta_2 ..., \theta_{k-1} \rangle$. So there are elements $p_1, ..., p_{k-1} \in R$ and $p_k \notin \langle \theta_1, \theta_2 ..., \theta_{k-1} \rangle$ s.t.

$$\sum_{i=1}^{k-1} p_i \theta_i = p_\kappa \theta_k. \tag{2.8}$$

Since $p_i \in R$ for $1 \leq i \leq k$ we have $p_i = \sum_{j=1}^{m} \eta_j q_j^{(i)}$ for some $q_j^{(i)} \in \mathbf{K}[\theta_1, \theta_2, ..., \theta_n]$. Furthermore there exists some $j' \in \{1, 2, ..., m\}$ s.t. $0 \neq q_{j'}^{(k)} \notin \langle \theta_1, \theta_2 ..., \theta_{k-1} \rangle$ (otherwise $p_k \in \langle \theta_1, \theta_2 ..., \theta_{k-1} \rangle$). Note that this implies $q_{j'}^{(k)} \notin \mathbf{K}[\theta_1, \theta_2 ..., \theta_{k-1}]$. Substitution in (2.8) yields $\sum_{i=1}^{k} \sum_{j=1}^{m_i} \eta_j q_j^{(i)} \theta_i = 0$. Since R is a free module, we have $\sum_{i=1}^{k-1} q_j^{(i)} \theta_i + q_j^{(k)} \theta_k = 0$ for $1 \leq j \leq k$. But for j' we have

$$\sum_{i=1}^{k-1} \underbrace{q_{j'}^{(i)} \theta_i}_{\in \mathbf{K}[\theta_1, \theta_2, ..., \theta_n]} = \underbrace{q_{j'}^{(k)} \theta_k}_{\in \mathbf{K}[\theta_k, \theta_{k+1}, ..., \theta_n]}.$$

which is a contradiction since θ_i is not contained in the right-hand side for $1 \leq i \leq k-1$. For the proof of the converse we refer to the proof of lemma 3.3 of Stanley [38]. ■

We mention another characterization of Cohen-Macaulay algebras without proof, because we do not make use of it.

Theorem 13 *The* $\mathbf{K}-$*algebra* R *is Cohen-Macaulay iff for each hsop* $\theta_1, \theta_2 ...,$ θ_n R *is a free* $\mathbf{K}[\theta_1, \theta_2, ..., \theta_n]$ *module.*

Proof. See, e.g., Sturmfels [43], Theorem 2.3.1. in ch. 2. ■

Corollary 4 *The polynomial ring* $\mathbf{K}[x_1, x_2, ..., x_n]$ *is Cohen-Macaulay.*

Proof. Obviously the variables $x_1, x_2, ..., x_n$ are algebraically independent and $\mathbf{K}[x_1, x_2, ..., x_n]$ is a free $\mathbf{K}[x_1, x_2, ..., x_n]-$module with basis $\{1\}$. ■

Corollary 5 *Let* R *be a Cohen-Macaulay algebra with Hironaka decomposition* $R = \bigoplus_{i=1}^m \eta_i \mathbf{K}[\theta_1, \theta_2, ..., \theta_n]$. *The Hilbert series of* R *equals*

$$\sum_{i=1}^{m} t^{\deg(\eta_i)} \cdot H(\mathbf{K}[\theta_1, \theta_2, ..., \theta_n], t).$$

Proof. *Follows from Lemma 1.4.3.* ■

Lemma 9 *Let* $R \subseteq S$ *be finitely generated* $\mathbf{K}-$*algebras of Krull dimension* n, *and* $\pi : S \to R$ *be an* $R-$*linear projection. Then :*
(a) $IS \cap R = I$ *for each* $I \trianglelefteq R$.
(b) Each regular sequence $\theta_1, ..., \theta_n$ *of* S *with* $\theta_i \in R$ *for* $1 \leq i \leq n$ *is already a regular sequence of* R.

Proof. (a) Let $x \in I$ and $s \in S$ and suppose $xs \in R$, then $xs = \pi(xs) = x \cdot \pi(s) \in I$.
(b) Now let $\theta_1, \theta_2, ..., \theta_n$ be a regular sequence in S with $\theta_i \in R$ for $1 \leq i \leq n$. Assume that $p_k\theta_k = \sum_{i=1}^{k-1} p_i\theta_i$ for some $p_i \in R, (1 \leq i \leq k)$. But then $p_k\theta_k \in \langle \theta_1, \theta_2 ..., \theta_{k-1} \rangle \trianglelefteq S$, a contradiction. ■

The next theorem, which is the main result in this section, appeared first in Hochster and Eagon [21] although apparently it has been part of the "folklore" in commutative algebra since long.

Theorem 14 *(Hochster, Eagon 1971). Let* $G \leq GL_n(\mathbf{K})$ *be a finite group and char*$(\mathbf{K}) \nmid |G|$. *Then the invariant ring* $\mathbf{K}[x_1, x_2, ..., x_n]^G$ *is Cohen-Macaulay.*

Proof. It follows from the Noether Normalization Lemma (Theorem 1.4.5), from Proposition 1.4.8 and from Proposition 1.4.7 (a) that there exists an hsop $\theta_1, \theta_2 ..., \theta_n$ of $\mathbf{K}[x_1, x_2, ..., x_n]^G$ s.t. $\mathbf{K}[x_1, x_2, ..., x_n]^G$ is integral over $\mathbf{K}[\theta_1, \theta_2, ..., \theta_n]$. From Lemma 2.3.6 we know that $\mathbf{K}[x_1, x_2, ..., x_n]$ is integral over $\mathbf{K}[x_1, x_2, ..., x_n]^G$, hence Proposition 1.4.7 implies that $\mathbf{K}[x_1, x_2, ..., x_n]$ is integral over $\mathbf{K}[\theta_1, \theta_2, ..., \theta_n]$ and $\theta_1, \theta_2 ..., \theta_n$ is an hsop for $\mathbf{K}[x_1, x_2, ..., x_n]$. Since $\mathbf{K}[x_1, x_2, ..., x_n]$ is Cohen-Macaulay, the elements $\theta_1, \theta_2 ..., \theta_n$ are a regular sequence of $\mathbf{K}[x_1, x_2, ..., x_n]$, therefore it follows from Lemma 2.5.9 that they are a regular sequence of $\mathbf{K}[x_1, x_2, ..., x_n]^G$. Now Lemma 2.5.8 implies that $\mathbf{K}[x_1, x_2, ..., x_n]^G$ is Cohen-Macaulay. ■

Remark 3 *In general, Cohen-Macaulay rings R are defined to be rings with* $\operatorname{depth}(R) = \dim(R)$, *where* $\operatorname{depth}(R)$ *is the maximal integer m s.t. a regular sequence $\{\theta_1, \theta_2 ..., \theta_m\}$ exists. It is a basic fact in homological algebra that* $\operatorname{depth}(R) \leq \dim(R)$, *cf. Eisenbud [13]. This is precisely what we have done in the proof of Lemma 2.5.8 for finitely generated $\mathbf{K}-$algebras, namely if we have found an hsop $\{\theta_1, \theta_2 ..., \theta_n\}$ s.t. R is a free $\mathbf{K}[\theta_1, \theta_2, ..., \theta_n]$ module, than we show that we have found a regular sequence of length n, hence* $\operatorname{depth}(R) = n = \dim(R)$.

Example 7 *Let* $G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$ *be a representation of the cyclic group of order 4. The Hilbert series equals* $H(\mathbf{C}[V]^G, t) = \frac{1+t^2}{(1-t^2)(1-t^4)}$. *Using the* **`Invariants`** *package (cf. Chapter 5) we find the primary invariants $\theta_1 = x_1^2 + x_2^2$ and $\theta_1 = x_1^2 x_2^2$ of minimal degrees and the secondary invariants $\eta_1 = 1$ and $\eta_2 = x_1^3 x_2 - x_1 x_2^3$. Hence the corresponding Hironaka decomposition of $\mathbf{C}[x_1, x_2]^G$ equals*

$$\mathbf{C}[x_1, x_2]^G = \mathbf{C}[\theta_1, \theta_2] \oplus \eta_2 \mathbf{C}[\theta_1, \theta_2].$$

A different hsop of degree $(4, 4)$ is given in Example 3.1.10.

Once we have found primary invariants $\theta_1, \theta_2, ..., \theta_n$ we can compute the rank of $\mathbf{K}[x_1, x_2, ..., x_n]^G$ as a $\mathbf{K}[\theta_1, \theta_2, ..., \theta_n]-$module and the degrees of the secondary invariants.

Proposition 15 *Let $G \leq GL_n(\mathbf{K})$ be a finite group and $d_1, d_2, ..., d_n$ be the degrees of a set of primary invariants for $\mathbf{K}[x_1, x_2, ..., x_n]^G$. Then*
(a) the number of secondary invariants equals

$$r = \frac{d_1 d_2 ... d_n}{|G|},$$

(b) the degrees (together with their multiplicities) of the secondary invariants are the exponents of the generating function

$$H^G(t)\cdot\prod_{i=1}^{n}\left(1-t^{d_j}\right).$$

Proof. We follow the proof of proposition 2.3.6 in Sturmfels [43]. We equate the formula for the Hilbert series of $\mathbf{K}[x_1,x_2,...,x_n]^G$ from Corollary 2.5.5 with Molien's formula (Theorem 2.4.12)

$$\frac{1}{|G|}\sum_{\sigma\in G}\frac{1}{\det(I-t\sigma)}=\sum_{i=1}^{m}t^{\deg(\eta_i)}\cdot\prod_{j=1}^{n}\frac{1}{(1-t^{d_j})}\tag{2.9}$$

and multiply both sides with $(1-t)^n$. We obtain

$$\frac{1}{|G|}\sum_{\sigma\in G}\frac{(1-t)^n}{\det(I-t\sigma)}=\sum_{i=1}^{m}t^{\deg(\eta_i)}\cdot\prod_{j=1}\frac{1}{(1+t+t^2+...+t^{d_j-1})}.\tag{2.10}$$

We now consider the limit $t\to 1$ in (2.10). All summands $\frac{(1-t)^n}{\det(I-t\sigma)}$ of the left hand side converge to 0 except $\frac{(1-t)^n}{\det(I-tI)}$which converges to 1. Hence the left hand side converges to $\frac{1}{|G|}$. The right hand side converges to $\frac{1}{d_1d_2...d_n}$. Putting this together we get

$$\frac{1}{|G|}=\frac{t}{d_1d_2...d_n}$$

which proves (a). The proof of (b) follows from (2.9). ■.

Together with Moliens Theorem the above results lay the theoretical foundation for the computation of invariant rings of a finite groups $G\leq GL_n(\mathbf{K})$ with $char(\mathbf{K})\nmid|G|$, which we will discuss in the next chapter.

Example 8 *[The permutation representation of D_4.]*
We know from Section 2.1 that the symmetric polynomials $\sigma_1=x_1+x_2+x_3+x_4,\sigma_2=x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4,\sigma_3=x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4,\sigma_4=x_1x_2x_3x_4$ *are primary invariants for D_4 with degrees* $(1,2,3,4)$*. From Proposition 2.5.15 we obtain the number and degrees of the secondary invariants. There are* 3 *secondary invariants with generating function* $1+t^2+t^4$,*and the* **`Invariants`** *package delivers* $\eta_1=1,\eta_2=x_1x_3+x_2x_4$ *and* $\eta_3=x_1^2x_3^2+x_2^2x_4^2$*. With* $R=\mathbf{C}[\sigma_1,\sigma_2,\sigma_3,\sigma_4]$,*we have the following Hironaka decomposition of the invariant ring*

$$\mathbf{C}[x_1,x_2,x_3,x_4]^{D_4}=R\oplus\eta_2R\oplus\eta_3R$$

Note that a set of minimal primary invariants has degree $(1,2,2,4)$. *With the* **`Invariants`** *package we find* $\theta_1 = x_1 + x_2 + x_3 + x_4, \theta_2 = x_1x_3 + x_2x_4, \theta_3 = x_1x_2 + x_2x_3 + x_1x_4 + x_3x_4$ *and* $\theta_4 = x_1x_2x_3x_4$. *With these primary invariants the generating function for the secondary invariants equals* $1+t^3$, *hence there are only* 2 *secondary invariants of degree* 0 *and* 3 *left. We have* $\widetilde{\eta}_1 = 1$ *and* $\widetilde{\eta}_2 = x_1^2 + x_2^3 + x_3^3 + x_4^3$. *As above we set* $R = \mathbf{C}[\theta_1,\theta_2,\theta_3,\theta_4]$ *and obtain the following Hironaka decomposition*

$$\mathbf{C}[x_1,x_2,x_3,x_4]^{D_4} = R \oplus \widetilde{\eta}_2 R.$$

Let $G \leq GL_n(\mathbf{K})$ be a finite group, assume $char(\mathbf{K}) \nmid |G|$ and let $\theta_1,\theta_2,...,\theta_n$ and $\eta_1,\eta_2,...,\eta_m$ be primary and secondary invariants of $\mathbf{K}[x_1,x_2, ...,x_n]^G$ respectively.. In order to compute in $\mathbf{K}[x_1,x_2,...,x_n]^G$ it is sufficient to know the representations of the elements $\eta_i\eta_j$ for $1 \leq i \leq j \leq m$, i.e. to know the structure constants of the algebra $\mathbf{K}[x_1,x_2,...,x_n]^G$.

Example 9 *We compute the structure table of the invariant ring* $\mathbf{K}[x_1,x_2]^G$ *of Example 2.5.7. We have* $\eta_2^2 = \frac{3}{2}\theta_1^2\theta_2 - \frac{1}{2}\theta_1^4 - \theta_2^2$, *hence we have the following structure table :*

$\cdot$	1	η_2
1	1	η_2
η_2	η_2	$\frac{3}{2}\theta_1^2\theta_2 - \frac{1}{2}\theta_1^4 - \theta_2^2$

.

Chapter 3

Computing Invariant Rings

We present two different paradigms for computing the invariant ring of a finite group G, namely the computation of the invariant ring as a finitely generated module over a subring and the computation of algebra generators for the invariant ring. For the first paradigm several algorithms have been proposed, see, for example, Sturmfels [43], Kemper [23], Kemper and Steel [24] and Decker et. al. [10]. The algorithm of Kemper can also deal with the case $char(\mathbf{K}) \mid |G|$. They can be subsumed in the following schemes.

Scheme 1 :

1. Compute primary invariants $\theta_1, \theta_2, ..., \theta_n$.
2. Compute module generators of $\mathbf{K}[x_1, x_2, ..., x_n]^G$ as a $\mathbf{K}[\theta_1, \theta_2, ..., \theta_n]-$ module.

A description of this scheme can be found in Section 3.1. Also Kemper's algorithm is implemented in the `Invariants` package (with the restriction to the nonmodular case in step 2) described in the Appendix.

The second paradigm is based on computing a set of algebra generators for the invariant ring. Examples are the algorithm of E. Noether (algorithm *Invariants* in Section 2.3.2) for finite groups in the nonmodular case and the algorithm of H. Derksen for linear reductive groups $G \leq GL_n(\mathbf{C})$ (for a definition of linearly reductive groups we refer, e.g., to Derksen [12]. We note that any finite group $G \leq GL_n(\mathbf{C})$ is linearly reductive).

Scheme 2 :

1. Compute algebra generators for $\mathbf{K}[x_1, x_2, ..., x_n]^G$.

A discussion of Noether's algorithm can be found in Section 2.3.2.

Finally, we present a new method for computing the algebra basis of an invariant ring for a finite group $G = \langle \sigma_1, \sigma_2, ..., \sigma_k \rangle$ in the nonmodular case.

Scheme 3 :

1. Compute algebra generators for $\mathbf{K}[x_1, x_2, ..., x_n]^{\langle\sigma_i\rangle}$.
2. Intersect all $\mathbf{K}[x_1, x_2, ..., x_n]^{\langle\sigma_i\rangle}$ using the algebra generators.

For a description of step 1 we refer to Section 4.1 and for step 2 to Section 3.2.

3.1 Primary and Secondary Invariants

We present two different approaches for the computation of primary invariants which are due to E. Dade and G. Kemper, respectively. For the computation of secondary invariants we present a straightforward approach in the non-modular case, and an algorithm from Kemper for the modular case.

For the computation of invariant rings of permutation groups we refer to Göbel [15].

3.1.1 Primary Invariants

We present two different algorithms to find an hsop $\theta_1, \theta_2, ..., \theta_n$ for the invariant ring $\mathbf{K}[x_1, x_2, ..., x_n]^G$. It is clear (from Proposition 2.5.15) that the degrees of an hsop $\theta_1, \theta_2, ..., \theta_n$ should be as small as possible. Following Kemper we call an algorithm **optimal** if it computes an hsop of minimal degree, i.e. $\prod_{i=1}^n \deg\theta_i$ is minimal. The first algorithm is due to E. Dade and is one of the fastest, but has some restrictions on the ground field and does in general not find an optimal hsop. The second algorithm is Kemper's algorithm for computing an optimal hsop, which works in the non-modular and modular case.

Our presentation is by no means exhaustive. Several other algorithms are described in the literature. For the *successive* algorithm from Kemper we refer to Kemper [22] or to Decker et. al. [10] for an improved version. Various other algorithms are contained in Sturmfels [43].

Before we can describe the algorithms we need some technical results.

Lemma 10 *Let $\theta_1, \theta_2, ..., \theta_n$ be homogenous elements of $\mathbf{K}[x_1, x_2, ..., x_n]$ and let $\overline{\mathbf{K}}$ denote the algebraic closure of $\mathbf{K}$. Then*

$$\dim \mathbf{K}[x_1, x_2, ..., x_n]/\langle\theta_1, \theta_2, ..., \theta_n\rangle = 0 \Longleftrightarrow \mathbf{V}_{\overline{\mathbf{K}}}(\theta_1, \theta_2, ..., \theta_n) = \{0\}$$

Proof. Let $I = \langle\theta_1, \theta_2, ..., \theta_n\rangle$ be of dimension 0. Proposition 1.4.6 implies that $\mathbf{K}[x_1, x_2, ..., x_n]/I$ is Artinian and that the variety $\mathfrak{V} = \mathbf{V}_{\overline{\mathbf{K}}}(\theta_1, \theta_2, ..., \theta_n)$ is finite. Since the elements $\theta_1, \theta_2, ..., \theta_n$ are homogenous, for any $p \in \mathfrak{V}$ and

$c \in \overline{\mathbf{K}}$ the product $c \cdot p$ is also contained in $\mathfrak{V}$. But the field $\overline{\mathbf{K}}$ is infinite (the algebraic closure of any field is infinite), hence $\mathfrak{V} = \{0\}$. Conversely, assume that $\mathbf{V}_{\overline{\mathbf{K}}}(\theta_1, \theta_2, ..., \theta_n) = \{0\}$. Proposition 1.4.6 implies that the ring $\mathbf{K}[x_1, x_2, ..., x_n] / \langle \theta_1, \theta_2, ..., \theta_n \rangle$ is Artinian and therefore we have $\dim \mathbf{K}[x_1, x_2, ..., x_n] / \langle \theta_1, \theta_2, ..., \theta_n \rangle = 0$. ■

Lemma 11 *Let* $\theta_1, \theta_2, ..., \theta_n$ *be homogenous elements of* $\mathbf{K}[x_1, x_2, ..., x_n]^G$. *Then*

$$\theta_1, \theta_2, ..., \theta_n \textit{ is an hsop } \Longleftrightarrow \dim \mathbf{K}[x_1, x_2, ..., x_n] / \langle \theta_1, \theta_2, ..., \theta_n \rangle = 0.$$

Furthermore each set $\psi_1, \psi_2, ..., \psi_k$. *of homogenous elements of* $\mathbf{K}[x_1, x_2, ..., x_n]^G$ *can be extended to an hsop iff* $\dim \mathbf{K}[x_1, x_2, ..., x_n] / \langle \psi_1, \psi_2, ..., \psi_k \rangle = n - k$.

Proof. We denote $\mathbf{K}[x_1, x_2, ..., x_n]$ by R, define $I = \langle \theta_1, \theta_2, ..., \theta_n \rangle$ for an hsop $\theta_1, \theta_2, ..., \theta_n$ and let $P \supseteq I$ be a minimal prime ideal over I, so R/P is a finitely generated $\mathbf{K}-$algebra with no nilpotent elements. It follows from Proposition 1.4.5 that $\dim R/P = \dim R/I$. Now Theorem 1.4.4 implies that $\dim R/P$ equals the transcendence degree of R/P over $\mathbf{K}$. Since P contains n algebraically independent elements, the transcendence degree of R/P equals 0, hence $\dim R/I = 0$.
Conversely, assume that $\dim R / \langle \theta_1, \theta_2, ..., \theta_n \rangle = 0$. Since $R / \langle \theta_1, \theta_2, ..., \theta_n \rangle$ is Artinian, for each x_i there exists a power k_i s.t. $\langle x_i^{k_i} \rangle = \langle x_i^{k_i+1} \rangle$. Let $\kappa_1 = 1$ and $\kappa_2, \kappa_3, ..., \kappa_r$ be homogenous elements of R^G s.t. their images form a $\mathbf{K}-$vectorspace basis of $R^G / \langle \theta_1, \theta_2, ..., \theta_n \rangle_{R^G}$. We claim that $\kappa_1, \kappa_2, ..., \kappa_r$ is a generating set for the $\mathbf{K}[\theta_1, \theta_2, ..., \theta_n]-$module R^G. We show via induction on the degree d for homogenous $f \in R^G$ that f can be written in the form $\sum_{i=1}^n \kappa_{j_i} \theta_i$. For $d = 0$ there is nothing to prove. Now assume that $\deg f > 0$ and that f is not a $\mathbf{K}-$linear combination of the κ_i's. Therefore $f \in \langle \theta_1, \theta_2, ..., \theta_n \rangle_{R^G}$, i.e., $f = \sum_{i=1}^n p_i \theta_i$ for some homogenous $p_i \in R^G$ with $\deg p_i < d$ or $p_i = 0$. Since $p_i \in \mathbf{K}$ or $p_i = \sum_{j=1}^n \kappa_{k_j} \theta_j$ by assumption, the claim follows.
From Krull's Principal Ideal Theorem (Theorem 1.4.6) it follows, that each element ψ_i decrease the dimension of R at most by 1, so $\dim \mathbf{K}[V] / \langle \psi_1, ..., \psi_k \rangle = n - k$. ■

We can use the above results for the computation of an hsop in the following way. Once we have found homogenous elements $\theta_1, \theta_2, ..., \theta_k$ of $\mathbf{K}[x_1, x_2, ..., x_n]^G$, we compute the dimension of the ideal $\langle \theta_1, \theta_2, ..., \theta_k \rangle$ with the aid of Gröbner bases. Then we apply Lemma 3.1.11 to check whether $\theta_1, \theta_2, ..., \theta_n$ is an hsop. If $\dim \langle \theta_1, \theta_2, ..., \theta_n \rangle = 0$ then $\theta_1, \theta_2, ..., \theta_n$ is an hsop for R^G. Otherwise we discard the elements $\theta_1, \theta_2, ..., \theta_n$. Note that the above results enable us to perform the ideal computations in $\mathbf{K}[x_1, x_2, ..., x_n]$.

Dade's Algorithm

Originally described in Stanley [38] for fields of characteristic 0. V. Reiner and L. Smith have generalized the algorithm to groups $G \leq GL_n(\mathbf{K})$ over a field $\mathbf{K}$ with $|G|^{n-1} < |\mathbf{K}|$,cf. Reiner and Smith [32] or Smith [40]. This algorithm is rather fast, but produces in general primary invariants of too high degree, i.e. they do not form an optimal hsop. We set $V = \mathbf{K}^n$ and denote the orbit of $f \in \mathbf{K}[V]$ w.r.t. G with $G(f) := \{\sigma \cdot f \mid \sigma \in G\}$. Furthermore with $span_{\mathbf{K}}(v_1, v_2, ..., v_k)$ we denote the subspace of V which is spanned by the elements $v_1, v_2, ..., v_k \in V$.

Proposition 16 *Let $V = \mathbf{K}^n$ and $G \leq GL_n(\mathbf{K})$ be a finite group. Suppose that there exists a basis $f_1, f_2, ..., f_n \in V^*$ s.t.*

$$f_{i+1} \notin \bigcup_{\sigma_1,\sigma_2...,\sigma_i \in G} span_{\mathbf{K}}(\sigma_1 \cdot f_1, \sigma_2 \cdot f_2..., \sigma_i \cdot f_i) \text{ for } 1 \leq i \leq n-1. \quad (3.1)$$

Then the polynomials $F_i := \prod_{g \in G(f_i)} g$ for $1 \leq i \leq n$ form an hsop for $\mathbf{K}[V]^G$.

Proof. We first show that $F_i \in \mathbf{K}[V]^G$ for $1 \leq i \leq n$. For $\tau \in G$ we have $\tau \cdot G(f_i) = \{\tau\sigma \cdot f \mid \sigma \in G\} = G(f_i)$, hence $F_i \in \mathbf{K}[V]^G$. We claim that the variety $\mathbf{V}_{\overline{\mathbf{K}}}(F_1, F_2, ..., F_n) = \{0\}$ over the algebraic closure of $\mathbf{K}$. For each F_i the variety $\mathbf{V}(F_i) = \bigcup_{\sigma \in G} \ker(\sigma \cdot f_i)$. Since the linear forms $\sigma_1 \cdot f_1, \sigma_2 \cdot f_2..., \sigma_n \cdot f_n$ are linearly independent for any $\sigma_1, \sigma_2..., \sigma_i \in G$, the intersection of their kernels equals $\{0\}$. Hence

$$\begin{aligned}
\mathbf{V}(F_1, ..., F_n) &= \bigcap_{i=1}^{n} \mathbf{V}(F_i) = \bigcap_{i=1}^{n} \bigcup_{\sigma_i \in G} \ker(\sigma_i \cdot f_i) \\
&= \bigcup_{\sigma_1,\sigma_2...,\sigma_i \in G} \bigcap_{i=1}^{n} \ker(\sigma_i \cdot f_i) = \{0\}.
\end{aligned}$$

From Lemma 3.1.10 and Lemma 3.1.11 it follows that the elements $F_1, F_2, ..., F_n$ are an hsop in $\mathbf{K}[V]$ and, since $\mathbf{K}[V]$ is integral over $\mathbf{K}[V]^G$, they are already an hsop for $\mathbf{K}[V]^G$. ■

We refer to (3.1) as the **Dade condition**. A basis $f_1, f_2, ..., f_n$ of V^* which satisfies the Dade condition is called a **Dade basis**.

Proposition 17 *Let $V = \mathbf{K}^n$ and $G \leq GL_n(\mathbf{K})$ be a finite group. If $|G|^{n-1} < |\mathbf{K}|$ then there exists a Dade basis for $\mathbf{K}[V]^G$.*

Proof. Let $f_1, f_2, ..., f_n$ be linearly independent elements of V^*. Note that for $1 \leq i \leq n$ the cardinality of the subspace $span_{\mathbf{K}}(\sigma_1 \cdot f_1, \sigma_2 \cdot f_2 ..., \sigma_i \cdot f_i)$ is $|\mathbf{K}|^i$ and therefore the set $\bigcup_{\sigma_1,\sigma_2...,\sigma_i \in G} span_{\mathbf{K}}(\sigma_1 \cdot f_1, \sigma_2 \cdot f_2 ..., \sigma_i \cdot f_i)$ has cardinality $|G|^i\ |\mathbf{K}|^i$. If $i = n-1$ we have $|G|^{n-1}\ |\mathbf{K}|^{n-1} < |\mathbf{K}|^n = |V^*|$, hence one can always find an element f_{i+1} satisfying (3.1). ■

Example 10 *Let* $G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$ *be a complex representation of the cyclic group of order* 4. *We start with* $f_1 = x$ *and obtain*

$$G(f_1) = \{-x, y, -y, x\},$$

so $F_1 = x^2y^2$. *Now we must choose* f_2 *s.t.* f_2 *is not contained in* $span_{\mathbf{C}}(x) \cup span_{\mathbf{C}}(y)$. *A suitable choice is* $f_2 = x + y$. *We get*

$$G(f_2) = \{-x-y, -x+y, x-y, x+y\},$$

so $F_2 = x^4 - 2\,x^2\,y^2 + y^4$. *So we have found an hsop of degree* $(4,4)$.*From Proposition 2.5.15 we conclude that the rank of* $\mathbf{K}[V]^G$ *as a* $\mathbf{K}[F1, F2]-$*module equals* 4 *and the generating function for the secondary invariants is* $1 + t^2 + t^4 + t^6$. *But an optimal hsop has degree* $(2,4)$ *and the generating polynomial equals* $1 + t^4$, *cf. Example 2.5.7.*

Algorithm Invariants(G)
  In : a finite group G s.t.$|G|^{n-1} < |\mathbf{K}|$
  Out : a Dade basis $F_1, ..., F_n$
  begin
  $B = \{\langle 0 \rangle\}$;
  for $i = 1$ **to** n **do**
  . select f_i s.t. $f_i \notin \bigcup_{b \in B} b$;
  . $F_i := \prod_{g \in G(f_i)} g$;
  . $B = \bigcup_{b \in B} \bigcup_{\sigma \in G} \langle b, \sigma \cdot f_i \rangle$;
  end
  end;

Kemper's Optimal Algorithm

This algorithm calculates always a minimal hsop for $\mathbf{K}[x_1, x_2, ..., x_n]^G$ and was introduced in Kemper [23]. We follow closely the presentation in (loc. cit.).

Theorem 15 *(Kemper 1997) Let* $\mathbf{K}$ *be an infinite field,* R *be a finitely generated graded* $\mathbf{K}-$*algebra with* $\dim R = n$ *and* $R_0 = \mathbf{K}$. *Let* $d_1, ..., d_k$ *be*

elements of $\mathbf{N}$. *The following two conditions are equivalent.*
(a) There are homogenous elements $f_1, f_2, ..., f_k \in R$ *with* $\deg f_i = d_i$ *for* $1 \leq i \leq k$, *s.t.*

$$\dim R/\langle f_1, f_2, ..., f_k\rangle = n - k.$$

(b) For each $M \subseteq \{1, 2, ..., k\}$ *we have*

$$\dim R/\left\langle \sum_{i\in M} R_{d_i}\right\rangle \leq n - |M|.$$

Proof. Let $f_1, f_2, ..., f_k \in R$ be homogenous with $\deg f_i = d_i$ for $1 \leq i \leq k$ s.t. $\dim R/\langle f_1, f_2, ..., f_k\rangle = n - k$. Assume that for some $M \subseteq \{1, 2, ..., k\}$ we have $\dim R/(\sum_{i\in M} R_{d_i}) > n - |M|$. From the estimation

$$\dim R/\langle f_i \mid i \in M\rangle \geq \dim R/\left\langle \sum_{i\in M} R_{d_i}\right\rangle > n - |M|$$

and from the fact the dimension of $R/\langle f_i \mid i \in \{1, 2, ..., k\}\backslash M\rangle$ is at least $k - |M|$ (compare Krull's Principal Ideal Theorem, Theorem 1.4.6), we obtain

$$\dim R/\langle f_1, f_2, ..., f_k\rangle > n - |M| - (k - |M|) = n - k,$$

a contradiction.
We prove (b) $\Rightarrow$ (a) by induction on k. For $k = 0$ there is nothing to prove. For $M \subseteq \{1, 2, ..., n\}$ we write

$$\dim_R(M) := \dim R/\left\langle \sum_{i\in M} R_{d_i}\right\rangle$$

Now let $k > 0$ and assume that for each $M \subseteq \{1, 2, ..., k\}$ we have

$$\dim_R(M) \leq n - |M|.$$

For $N \subseteq \{1, 2, ..., k-1\}$ we define the ideal P_N in the following way. If $\dim_R(N) = n - |N|$ then P_N denotes a minimal prime ideal properly containing $\left\langle \sum_{i\in N} R_{d_i}\right\rangle$ with $\dim R/P_N = n - |N|$. Otherwise we have $\dim_R(N) < n - |N|$ and we set $P_N = \{0\}$. From the assumption we have $\dim R/\langle R_{d_k}\rangle < n$ and therefore $\dim R/\left\langle \sum_{i\in N\cup\{k\}} R_{d_i}\right\rangle \leq n - |N| - 1 < n - |N|$. Hence R_{d_k} is not contained in P_N, so $P_N \cap R_{d_k}$is a proper subspace of R_{d_k}. Since $\mathbf{K}$ is infinite, there exists $f_k \in R_{d_k}$ not contained in any of the ideals P_N for $N \subseteq \{1, 2, ..., k-1\}$. Now let $\overline{R} = R/\langle f_k\rangle$ and note that $\dim \overline{R} = n - 1$. For any $N \subseteq \{1, 2, ..., k-1\}$ we have

$$\dim R/\left\langle \sum_{i\in N} R_{d_i} + f_k\right\rangle = \dim \overline{R}/\left\langle \sum_{i\in N} R_{d_i}\right\rangle \leq n - 1 - |N|.$$

The induction hypotheses implies that there exist $f_i \in R_{d_i}$ for $1 \leq i \leq k-1$ s.t. $\dim R/\langle f_1, f_2, ..., f_{k-1}\rangle = n - k + 1$. It follows from the inclusion $\langle f_1, f_2, ..., f_{k-1}\rangle \subseteq \left\langle \sum_{i=1}^{k-1} R_{d_i}\right\rangle$ that

$$\dim R/\langle f_1, f_2, ..., f_k\rangle = \dim \overline{R}/\langle f_1, f_2, ..., f_{k-1}\rangle = n - 1 - (k-1) = n - k. \blacksquare$$

Note that the implication $(a) \Rightarrow (b)$ still holds if the field $\mathbf{K}$ is finite. We obtain a corollary, which is very useful for the computation of primary invariants.

Corollary 6 *Let $\mathbf{K}$ be an infinite field, R be a finitely generated graded $\mathbf{K}-$algebra of Krull dimension n and let $d \in \mathbf{N}$. The following two conditions are equivalent.*
(a) There exist homogenous elements $f_1, f_2, ..., f_k \in R$ of degree d s.t.

$$\dim R/\langle f_1, f_2, ..., f_k\rangle = n - k,$$

(b)

$$\dim R/\langle R_d\rangle \leq n - k.$$

Proof. $(a) \Rightarrow (b)$ follows from the inclusion $\langle f_1, f_2, ..., f_k\rangle \subseteq \langle R_d\rangle$. For the converse let $d_1 = d_2 = ... = d_k = d$. Then the claim follows immediately from Theorem 3.1.15. ■

The important point of Kemper's Theorem is, that one can decide algorithmically whether an hsop of a given degree exists, provided that the dimension of ideals and bases for the homogenous components of R can be computed, which is possible in the context of invariant theory. One drawback is, that in order to check condition (b) one has to perform 2^k Gröbner bases computations in the worst case. The next proposition reduces the number of Gröbner bases computations to the number of different degrees d_i.

Proposition 18 *Let $\mathbf{K}$ be an infinite field, R be a finitely generated graded $\mathbf{K}-$algebra of Krull dimension n, and $d_1 < d_2 < ... < d_r$ with $r \leq n$ be natural numbers. Assume that $\alpha_i = n - \dim R/\left\langle \sum_{j=1}^{i} R_{d_j}\right\rangle > 0$ for $1 \leq i \leq r$ and set $k = \sum_{i=1}^{r} \alpha_i$. Then the following conditions are equivalent.*
(a) There exist a set of homogenous polynomials $\{f_1, f_2..., f_k\}$ which contains α_i polynomials of degree d_i, s.t.

$$\dim R/\langle f_1, f_2, ..., f_k\rangle = n - k,$$

(b)

$$\dim R > \dim R/R_{d_1} > \dim R/\langle R_{d_1} + R_{d_2}\rangle > ... > \dim R/\langle \textstyle\sum_{i=1}^{r} R_{d_i}\rangle = n-k.$$

Proof. We prove both directions with induction on r and remark that for $r = 0$ there is nothing to prove. We start with $(a) \Rightarrow (b)$. Let $r > 0$ and $f_1, f_2..., f_k$

be homogenous polynomials which satisfy (a) and let $t = \sum_{i=1}^{r-1} \alpha_i$. From the hypothesis we know that $\dim R/\left\langle \sum_{i=1}^{r-1} R_{d_i} \right\rangle = \dim R/\langle f_1, f_2, ..., f_t\rangle = n - t$. Since $\alpha_r > 0$ we have

$$\dim R/\langle f_1, f_2, , ..., f_{t+\alpha_r}\rangle = n - t - \alpha_r < \dim R/\left\langle \sum_{i=1}^{r-1} R_{d_i} \right\rangle,$$

hence $\dim R/\left\langle \sum_{i=1}^{r-1} R_{d_i} \right\rangle > \dim R/\langle \sum_{i=1}^{r} R_{d_i} \rangle$.
Let $r > 0$ and assume that (b) holds. We denote $\dim R/\left\langle \sum_{j=1}^{i} R_{d_j} \right\rangle$ by $\dim_R(i)$. From the hypothesis we know that there exist $f_1, f_2, ..., f_{k-\alpha_r}$ which satisfy the degree requirements from (a) and that $\dim R/\langle f_1, f_2, ..., f_{k-\alpha_r}\rangle = \dim_R(r-1)$ It follows from the assumption $\dim_R(r-1) > \dim_R(r)$ and from Corollary 3.1.6 that there exist α_r polynomials $f_{k-\alpha_{r-1}+1}, ..., f_{\alpha_r} \in R_{d_r}$ s.t. $\dim R/\langle f_1, f_2, ..., f_k\rangle = n - k$. ■

The computation of the dimension of $\dim R/\left\langle \sum_{j=1}^{i} R_{d_j} \right\rangle$ for $1 \leq i \leq r$ can be performed by the following subroutine, which we will describe schematically.

Dimension $(\mathbf{K}[x_1, x_2, ..., x_n]/\langle g_1, ..., g_{m_1}\rangle, \langle f_1, ..., f_{m_2}\rangle)$
In: The basis of a homogenous ideal $I \trianglelefteq \mathbf{K}[x_1, x_2, ..., x_n]/\langle g_1, ..., g_{m_1}\rangle$(each f_i is homogenous).
Out: The Krull dimension of I.
begin
$B := \mathit{GroebnerBasis}(g_1, ..., g_{m_1}, f_1, ..., f_k, \{x_1, ..., x_n\})$; // any ordering
$h(t) :=$ Hilbert polynomial of the ideal generated by B;
return$(\deg h(t))$;
end;

Algorithms for the computation of the Hilbert polynomial can be found in ,e.g., Bayer and Stillman [1] or Bigatti et. al.[4]. An introduction to Hilbert polynomials and a different algorithm for the dimension can be found, e.g., in Cox et. al. [9], see also Becker and Weispfennig [3].

The enumeration of degree vectors plays a fundamental role and in our implementation it requires three additional functions, namely *InitDegree*, *AdmissibleQ*, and *NextDegree.* These algorithms can be exchanged by others, but must fulfill the following specification :

InitDegree $(G, \mathbf{K})$

In: a finite matrix group $G \leq GL_n(\mathbf{K})$, a field $\mathbf{K}$;
Out : -
Initialization of the degree enumeration..

AdmissibleQ $(\mathbf{d})$

In: a degree vector $\mathbf{d}$.
Out: $True$, iff there might exist primary invariants, $False$ otherwise.
if $char(\mathbf{K}) \nmid |G|$ **and** $|G| \mid \prod_{i=1}^{n} d_i$ **and** there are enough invariants of degree d_i for $1 \leq i \leq n$, **then return**$(True)$;
else return$(False)$;
end;

NextDegree $(\mathbf{d})$

In: a degree vector $\mathbf{d}$.
Out: a degree vector $\mathbf{d}'$ satisfying $\prod_{i=1}^{n} d_i \leq \prod_{i=1}^{n} d_i'$.

We now present Kemper's algorithm for computing primary invariants of least degree. A rough description of the algorithm is as follows.
In the main loop the algorithm enumerates degree vectors in an increasing way w.r.t. a multiplicative ordering (cf. the introduction of Section 3.1.1), and checks if an hsop with the given degree vector might exist. In the non-modular case simple criteria are the Hilbert series or the Cohen-Macaulay property (check if there are enough invariants, if $H^G(t)$ times a polynomial is a polynomial), then it uses condition (b) of Proposition 3.1.18. If all these requirements are met, the algorithm *TryDegrees* is called. In the case of an infinite ground field, *TryDegrees* always returns an hsop. This is guaranteed from Proposition 3.1.18. If the ground field is finite, then an hsop might not exist, and the algorithm does not leave the main loop.
Warning : The enumeration must deliver all possible degree vectors in the correct order. Otherwise the algorithm does not produce a set of primary invariants of least degree.

Algorithm *PrimaryInvariants*$(G, \mathbf{K})$

In: a finite matrix group $G \leq GL_n(\mathbf{K})$, a field $\mathbf{K}$;
Out: A minimal hsop.
$found := False$;
$\mathbf{dv} = \{0, 0, ..., 0\}$;
InitDegree$(G, \mathbf{K})$;
while $found = False$ **do**
. **dv** $:= NextDegree(\mathbf{dv})$;
. **if** AdmissibleQ$(\mathbf{dv})$ **then begin**
. $\mathbf{d} = Union(\mathbf{dv})$; // set-theoretic union
. $i = 1; dimension = n; loop := True$;
. **while** $loop$ **do**
. $dd = \dim R/(\sum_{j=1}^{i} R_{dj})$;
. **if** $dimension > dd$ **then** $dimension = dd$;
. **else** $loop = False$;
. **if** $i < |\mathbf{d}|$**then** $i := i + 1$;
. **else** $loop = False$;
. **end-while**;
. **if** $i = |\mathbf{d}|$ **then** $\{\theta_1, \theta_2, ..., \theta_n\} :=$*TryDegrees*$(\mathbf{d}, G)$;
. **if** $\{\theta_1, \theta_2, ..., \theta_n\} \neq \{0, 0, ..., 0\}$ **then** $found := True$;
. **end-if**;
end-while;
return$(\{\theta_1, \theta_2, ..., \theta_n\})$;
end;

If the field $\mathbf{K}$ is infinite and we have found a degree vector, then we "only" have to find the polynomials $\theta_1, \theta_2, ..., \theta_n$. In the case that $\mathbf{K}$ is finite, the algorithm tries to find polynomials $\theta_1, \theta_2, ..., \theta_n$. The algorithm performs a loop over a finite-dimensional $\mathbf{K}-$vectorspace V. The idea of how one can perform such a loop is due to Kemper (loc. cit.). Let $b_1, b_2, ..., b_m$ be a basis of V. We distinguish the two cases:

Case 1 $|\mathbf{K}| = \infty$: Take an injective map $\iota : \mathbf{N_0} \hookrightarrow \mathbf{K}$ and enumerate the elements of $\mathbf{N}_0^n$ w.r.t. to a total degree ordering. For any such $(k_1, k_2..., k_n) \in \mathbf{N}_0^n$ consider the element $\sum_{i=1}^{n} \iota(k_i) \cdot b_i \in V$.

Case 2 $|\mathbf{K}| = q < \infty$: Take a bijection $\iota : \{0, 1, ..., q-1\} \to \mathbf{K}$ and enumerate the elements of $\{0, 1, ..., q-1\}^n$ w.r.t. to a total degree ordering on $\mathbf{N}_0^n$, restricted on $\{0, 1, ..., q-1\}^n$. For any such $(k_1, ..., k_n) \in \{0, 1, ..., q-1\}^n$ consider the element $\sum_{i=1}^{n} \iota(k_i) \cdot b_i \in V$.

The algorithm below is a simplified version of the algorithm *TryDegrees* from Kemper (loc. cit.). The algorithm loops over a finite-dimensional vectorspace V. If the ground field $\mathbf{K}$ is infinite, termination is guaranteed from Proposition 3.1.18, and, if $|\mathbf{K}| < \infty$, there are only finitely many combinations.

Algorithm *TryDegrees*($R, G, \{d_1, d_2, ..., d_r\}, \{\alpha_1, \alpha_2, ..., \alpha_r\}$)
In: a finite matrix group $G \leq GL_n(\mathbf{K})$, a degree vector $\mathbf{d}, \alpha$
Out: A minimal hsop, if it exists, $\{0, 0, ..., 0\}$ otherwise.
if $m = 0$ **then return**($\{\}$);
for $(\theta_1, \theta_2, ..., \theta_{\alpha_1}) \in R_{d_1}$ **do**
. $k := 1$;
. **while** $\dim R/\left((\theta_1, ..., \theta_{\alpha_1}) + \sum_{i=1}^{k} R_{d_i}\right) = n - \sum_{i=1}^{k} \alpha_k$
. **and** $k \leq r$**do**
. $k := k + 1$**;**
. **end;**
. **if** $k = r + 1$ **then**
. $\overline{R} := R/(\theta_1, \theta_2, ..., \theta_{\alpha_1})$;
. $\{\theta_{\alpha_1+1}, \theta_{\alpha_1+2}, , ..., \theta_n\} :=$
. $TryDegrees(\overline{R}, \{d_1, d_2, ..., d_r\}, \{\alpha_2, \alpha_3, ..., \alpha_r\}, G)$;
. **end;**
. **if** $\{\theta_{\alpha_1+1}, ..., \theta_n\} \neq \{0, ..., 0\}$ **then return**($\{\theta_1, ..., \theta_{\alpha_1}, \theta_{\alpha_1+1}, ..., \theta_n\}$);
end;
return($\{0, ..., 0\}$);
end;

The following example is taken from Rötteler [33] (example 4.3.2)

Example 11 *Let* $G = \left\langle \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \right\rangle$. *The group G is used in Sloane [36] in order to compute the weight enumeration polynomial of an error-correcting code, and also to show that a code with certain specific properties does not exist. For details we refer to (loc. cit.). The order of G equals* 192 *and from Molien's Theorem we obtain*

$$H^G(t) = \frac{1}{(1 - t^8)(1 - t^{24})}.$$

The implementation of the algorithm PrimaryInvariants *in the* ***`Invariants`*** *package returns the following hsop :*

$$\begin{aligned} \theta_1 &= x^8 + 14\, x^4\, y^4 + y^8, \\ \theta_2 &= x^{24} - \frac{1288x^{20}y^4}{3} + \frac{7429x^{16}y^8}{3} + \frac{7429x^8y^{16}}{3} - \frac{1288x^4y^{20}}{3} + y^{24}. \end{aligned}$$

Since $H(\mathbf{C}[\theta_1,\theta_2],t) = H^G(t)$ *the invariant ring equals* $\mathbf{C}[x,y]^G = \mathbf{C}[\theta_1,\theta_2]$.

3.1.2 Secondary Invariants

We present two algorithms, one for the non-modular and one for the modular case, which is due to Kemper (cf. Kemper [22]). These algorithms take as an input a set $\theta_1,\theta_2,...,\theta_n$ of primary invariants, and compute a module basis for the invariant ring over $\mathbf{K}[\theta_1,\theta_2,...,\theta_n]$. In the sequel we abbreviate $\mathbf{K}[x_1,x_2,...,x_n]$ with $\mathbf{K}[V]$ (cf. Section 2.2).

Nonmodular Case

Let $\mathbf{K}$ be a field and $G \leq GL_n(\mathbf{K})$ be a finite group and s.t. $char(\mathbf{K}) \nmid |G|$. From the Hilbert series $H^G(t)$ and the degrees of the primary invariants we can immediately compute the rank r of $\mathbf{K}[V]^G$ as a $\mathbf{K}[\theta_1,\theta_2,...,\theta_n]-$module and the degrees of the secondary invariants, using Proposition 2.5.15. In the sequel let $\theta_1,\theta_2,...,\theta_n$ be primary invariants of G and r be the rank of $\mathbf{K}[V]^G$ as a $\mathbf{K}[\theta_1,\theta_2,...,\theta_n]-$module and $A = \mathbf{K}[\theta_1,...,\theta_n]$.

The next two propositions are of technical nature and will be needed in the algorithm.

Proposition 19 *The elements* $\eta_1,\eta_2...,\eta_r \in \mathbf{K}[V]^G$ *are an* $A-$*module basis for* $\mathbf{K}[V]^G$ *iff* $\eta_1,\eta_2,...,\eta_r$ *are a basis of* $\mathbf{K}[V]^G/A_+\mathbf{K}[V]^G$ *as a* $\mathbf{K}-$*vectorspace.*

Proof. Assume that $\eta_1,\eta_2,...,\eta_r$ is a basis of $\mathbf{K}[V]^G$ and there exists a relation $\sum_{i=1}^r \lambda_i\eta_i + \sum_{i=1}^m a_ih_i = 0$ for some $\lambda_i \in \mathbf{K}, a_i \in A_+$ and $h_i \in \mathbf{K}[V]^G$. Each h_i can be written as $h_i = \sum_{j=1}^r \eta_j p_j^{(i)}$, so $\sum_{i=1}^r \lambda_i\eta_i + \sum_{i=1}^m \sum_{j=1}^r \eta_j a_i p_j^{(i)} = 0$, which would imply that $\mathbf{K}[V]^G$ is not a free module.
Conversely, we assume that the elements $\eta_1,\eta_2,...,\eta_m$ are a $\mathbf{K}-$vectorspace basis of $\mathbf{K}[V]^G/A_+\mathbf{K}[V]^G$. We show that $M = \sum_{i=1}^r \eta_i A = \mathbf{K}[V]^G$ via induction on the degree. Let $f \in \mathbf{K}[V]^G$ be a homogenous element of degree $d > 0$. The image of f in $\mathbf{K}[V]^G/A_+\mathbf{K}[V]^G$ equals

$$f = \sum_{i=1}^r \lambda_i\eta_i + \sum_{i=1}^m a_ih_i$$

for some $\lambda_i \in \mathbf{K}, a_i \in A_+$ and $h_i \in \mathbf{K}[V]^G$. Now $\deg(a_ih_i) = d$, hence $\deg(h_i) < d$, which implies $h_i \in M$, hence each h_i is of the form $h_i = \sum_{j=1}^r \eta_j a_j^{(i)}$. ■

Proposition 20 *The elements* $\eta_1,\eta_2,...,\eta_r \in \mathbf{K}[V]^G$ *are a* $A-$*module basis for* $\mathbf{K}[V]^G$ *iff their images are linearly independent in* $\mathbf{K}[V]/\langle\theta_1,\theta_2,...,\theta_n\rangle$ *(w.r.t.* $\mathbf{K}$*).*

Proof. Let $\eta_1, \eta_2, ..., \eta_r$ be an $A-$module basis of $\mathbf{K}[V]^G$. We claim that the canonical map $\varphi : \mathbf{K}[V]^G/A_+\mathbf{K}[V]^G \to \mathbf{K}[V]/\langle\theta_1, ..., \theta_n\rangle$ is injective. If $\varphi(p) = 0$ for some $p \in \mathbf{K}[V]^G/A_+\mathbf{K}[V]^G$ then $p \in \langle\theta_1, ..., \theta_n\rangle$, so $p = \sum_{i=1}^n h_i\theta_i$ for some $h_i \in \mathbf{K}[V]$. Now $p = \mathfrak{R}^G(p) = \sum_{i=1}^n \mathfrak{R}^G(h_i)\theta_i$, hence $p \in A_+\mathbf{K}[V]^G$. This implies that the elements $\eta_1, \eta_2, ..., \eta_m$ are linearly independent. Conversely assume that $\eta_1, \eta_2, ..., \eta_r$ are linearly independent in $\mathbf{K}[V]/\langle\theta_1, \theta_2, ..., \theta_n\rangle$. In particular they are linearly independent in the vectorspace $\mathbf{K}[V]^G/A_+\mathbf{K}[V]^G$. But dim $\mathbf{K}[V]^G/A_+\mathbf{K}[V]^G = r$, hence they form a basis. ■

Proposition 21 *Let B be an $A-$module basis of $\mathbf{K}[V]$. Then the set $\mathfrak{R}^G(B) = \left\{\mathfrak{R}^G(b) \mid b \in B\right\}$ contains an $A-$module basis for $\mathbf{K}[V]^G$.*

Proof. It follows from the Reynolds properties, that $\mathfrak{R}^G$ is an $A-$module homomorphism. But $\mathfrak{R}^G$ is also a projection. ■

Now we can state an algorithm for computing secondary invariants. Kemper and Steel [24] give a refined version of this algorithm, which computes a subset of irreducible secondary invariants, where a secondary invariant is irreducible if it cannot be written as a polynomial in the primary invariants and the remaining secondary invariants. The set of primary invariants together with the irreducible secondary invariants form a minimal set of fundamental invariants. For details, see (loc. cit.).

Algorithm *SecondaryInvariants*$(G, \langle\theta_1, \theta_2, ..., \theta_n\rangle)$
In: The group G, an hsop $\theta_1, \theta_2, ..., \theta_n$ for $\mathbf{K}[V]^G$.
Out:Secondary invariants $\{\eta_1, \eta_2..., \eta_r\}$ of $\mathbf{K}[V]^G$.
begin
$p = H^G(t) \cdot \prod_{i=1}^n (1 - t^{\deg\theta_i})$; // $p = 1 + \sum_{i=1}^d c_i t^{d_i}$
$B =$ an $A-$module basis of $\mathbf{K}[V]$;
$\eta_1 = 1$;
for $i = 2$ **to** d **do**
. select c_i linearly independent elements η_{i_j} of $\mathfrak{R}^G(B_{d_i})$;
end;
return$(\eta_1, \eta_2, ..., \eta_r)$;
end.

Example 12 (The permutation representation of C_5) *An optimal hsop has degree $(1, 2, 2, 3, 5)$ so the generating function for the secondary invariants equal $1 + 3t^3 + 4t^4 + 3t^5 + t^8$. The* `invariants` *package delivers the following primary invariants for $\mathbf{C}[x_1, x_2, x_3, x_4, x_5]^G$:*

$$\theta_1 = x_1 + x_2 + x_3 + x_4 + x_5,$$

$$\begin{aligned}
\theta_2 &= x_1x_3 + x_1x_4 + x_2x_4 + x_2x_5 + x_3x_5,\\
\theta_3 &= x_1x_2 + x_2x_3 + x_3x_4 + x_1x_5 + x_4x_5,\\
\theta_4 &= x_1x_2x_4 + x_1x_3x_4 + x_1x_3x_5 + x_2x_3x_5 + x_2x_4x_5,\\
\theta_5 &= x_1x_2x_3x_4x_5.
\end{aligned}$$

and 12 *secondary invariants :*

$$\begin{aligned}
&\{1, x_1^2\,x_2 + x_2^2\,x_3 + x_3^2\,x_4 + x_4^2\,x_5 + x_1\,x_5^2, x_1^2\,x_3 + x_2^2\,x_4 + x_1\,x_4^2 + x_3^2\,x_5 + x_2\,x_5^2,\\
&x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3, x_1^3\,x_2 + x_2^3\,x_3 + x_3^3\,x_4 + x_4^3\,x_5 + x_1\,x_5^3,\\
&x_1^3\,x_3 + x_2^3\,x_4 + x_1\,x_4^3 + x_3^3\,x_5 + x_2\,x_5^3, x_1\,x_3^3 + x_1^3\,x_4 + x_2\,x_4^3 + x_2^3\,x_5 + x_3\,x_5^3,\\
&x_1^4 + x_2^4 + x_3^4 + x_4^4 + x_5^4, x_1^4\,x_2 + x_2^4\,x_3 + x_3^4\,x_4 + x_4^4\,x_5 + x_1\,x_5^4,\\
&x_1^4\,x_3 + x_2^4\,x_4 + x_1\,x_4^4 + x_3^4\,x_5 + x_2\,x_5^4, x_1\,x_3^4 + x_1^4\,x_4 + x_2\,x_4^4 + x_2^4\,x_5 + x_3\,x_5^4,\\
&x_1^8 + x_2^8 + x_3^8 + x_4^8 + x_5^8\}.
\end{aligned}$$

If we denote the secondary invariants with $\eta_1, \eta_2, ..., \eta_{12}$*,respectively, we obtain the Hironaka decomposition*

$$R^{C_5} = \bigoplus_{i=1}^{12} \eta_i \mathbf{C}[\theta_1, \theta_2, \theta_3, \theta_4, \theta_5].$$

If we had taken the symmetric polynomials as primary invariants then we would have been forced to compute 25 *secondary invariants w.r.t. the generating function* $1 + t^2 + 3t^3 + 4t^4 + 6t^5 + 4t^6 + 3t^7 + t^8 + t^{10}$.

Modular Case

We follow Kemper [22]. In this section $\mathbf{K}$ denotes a finite field, $G \leq GL_n(\mathbf{K})$ a finite group and $\theta_1, \theta_2, ..., \theta_n$ primary invariants of G. Furthermore we assume that $char(\mathbf{K}) \mid |G|$. Set $A = \mathbf{K}[\theta_1, \theta_2, ..., \theta_n]$ and let B be a generating set of G. We reduce the problem to the non-modular case by choosing a subgroup $H \leq G$ s.t. $char(\mathbf{K}) \nmid |H|$. A good choice would be a $p'-$Sylow subgroup with a prime $p' \neq p$. Note that the trivial group $\{1_{GL_n(\mathbf{K})}\}$ always fulfills the requirement. Then we compute an $A-$module basis $\{b_1, b_2, ..., b_r\}$ of $\mathbf{K}[V]^H$ with the algorithm SecondaryInvariants. Finally we impose $G-$invariance conditions on the elements of $\mathbf{K}[V]^H$, which leads us to a system of linear equations. We have $h \in \mathbf{K}[V]^H \cap \mathbf{K}[V]^G = \mathbf{K}[V]^G$ iff $\sigma \cdot h = h$ for all $\sigma \in G$. Let $h = \sum_{i=1}^r b_i(x)p_i(\theta_1, \theta_2, ..., \theta_n)$. Then $\sigma \cdot h = h$ iff

$$\sum_{i=1}^{r} (b_i(x) - \sigma \cdot b_i(x))p_i(\theta_1, \theta_2, ..., \theta_n) = 0.$$

So we solve the system of $|B|$ linear equations over $\mathbf{K}[V]$

$$\sum_{i=1}^{r}(b_i(x)-\sigma\cdot b_i(x))z_i=0,\ \text{for } \sigma\in B \tag{3.2}$$

and intersect the solution module M with A^r.

Proposition 22 *With the notation from above let $\{c_1,c_2,...,c_m\}$ be a basis of $M\cap A^r$ and set*

$$\eta_k=\sum_{i=1}^{r} b_i\cdot c_{k,i},\ \textit{for } 1\le k\le m.$$

Then $\eta_1,\eta_2,...,\eta_m$ form a module basis of $\mathbf{K}[V]^G$.

Proof. For $1\le k\le m$ we have $c_{k,i}\in A$ and from (3.2) we obtain $\sum_{i=1}^{r} b_i(x)c_{k,i}=\sum_{i=1}^{r}\sigma\cdot b_i(x)c_{k,i}$. Conversely, let $f=\sum_{i=1}^{r}a_ib_i\in\mathbf{K}[x_1,x_2,...,x_n]^G$ for some $a_i\in A$. Since $f^*=f$ it follows from (3.2) that $(a_1,a_2,...,a_r)\in M\cap A^r$, so $(a_1,a_2,...,a_r)=\sum_{i=1}^{m}\widetilde{a}_ic_i$ for some $\widetilde{a}_i\in A$ and we have $f=\sum_{i=1}^{r}\widetilde{a}_i\eta_i$. ■

The computation of the basis $\{c_1,c_2,...,c_m\}$ of $M\cap A^r$ can be done with the following Lemma, which appears in Kemper (loc. cit.).

Lemma 12 *(Kemper 1996) Let $R=\mathbf{K}[x_1,x_2,...,x_n]$, $M=\sum_{i=1}^{m}R\cdot b_i\le R^r$ be a submodule, $S=\mathbf{K}[x_1,...,x_n,t_1,...,t_n]$ and $T=\mathbf{K}[t_1,t_2,...,t_n]$. Set*

$$\widetilde{M}=\sum_{i=1}^{m}S\cdot b_i+\sum_{i=1}^{n}(t_i-\theta_i)\cdot S^r\le S^r$$

and

$$\widetilde{M}_T=\widetilde{M}\cap T^r.$$

Then with $\phi:T^r\to A^r, t_i\mapsto\theta_j$, we have

$$\phi(\widetilde{M}_T)=M\cap A^r.$$

Proof. We denote $t_1,...,t_n$ with $\mathbf{t}$ and $\theta_1,...,\theta_n$ with $\boldsymbol{\theta}$. Let $\pi:R^r\to R^r/M$ be the canonical projection and $\overline{\psi}:S^r\to R^r$ the induced homomorphism from ϕ. We claim that the kernel of the homomorphism $\psi=\pi\circ\overline{\psi}$ equals $\widetilde{M}$. For $f=\sum_{i=1}^{m}s_i(\mathbf{x},\mathbf{t})\cdot b_i+\sum_{i=1}^{n}(t_i-\theta_i)\cdot s_i'\in\widetilde{M}$ we obtain $\overline{\psi}(f)=\sum_{i=1}^{s}s_i(\mathbf{x},\boldsymbol{\theta})\cdot b_i\in M$, hence $\pi\circ\overline{\psi}(f)=0$. We show the other inclusion in two steps. Firstly, let p be a monomial in T and e_i be a basis element of

S^r. We show via induction on the degree d of $p(t_1, ..., t_n)$ that $(p(t_1, ..., t_n) - p(\theta_1, ..., \theta_n)) \cdot e_i \in \widetilde{M}$. For $d = 0$ there is nothing to show. If $d > 0$ then $p(t_1, ..., t_n) = t_j p'(t_1, ..., t_n)$ for some j and $p' \in T$ with $\deg p' = d - 1$. It follows from the induction hypothesis that $(p'(t_1, ..., t_n) - p'(\theta_1, ..., \theta_n)) \cdot e_i \in \widetilde{M}$. So

$$\begin{aligned}(p(\mathbf{t}) - p(\boldsymbol{\theta})) \cdot e_i &= (t_j p'(\mathbf{t}) - \theta_j p'(\boldsymbol{\theta}) + \theta_j p'(\mathbf{t}) - \theta_j p'(\mathbf{t})) \cdot e_i \\ &= ((t_j - \theta_j) \cdot p'(\mathbf{t}) + \theta_j \cdot (p'(\mathbf{t}) - p'(\boldsymbol{\theta}))) \cdot e_i \in \widetilde{M}.\end{aligned}$$

Now a monomial $s \in S$ can be written as $s = r(\mathbf{x})p(\mathbf{t})$, and we obtain

$$(r(\mathbf{x})p(\mathbf{t}) - r(\mathbf{x})p(\boldsymbol{\theta})) \cdot e_i = r(\mathbf{x}) \cdot (p(\mathbf{t}) - p(\boldsymbol{\theta})) \cdot e_i \in \widetilde{M}.$$

So for each $(s_1, s_2, ..., s_r) \in S^r$ we have

$$(s_1, ..., s_r) - (s_1 |_{t_j=\theta_j}, s_2 |_{t_j=\theta_j}, ..., g_r |_{t_j=\theta_j}) \in \widetilde{M}. \tag{3.3}$$

If $\psi(s_1, s_2, ..., s_r) = 0$, then $(s_1, s_2, ..., s_r) \in M$, and it follows from (3.3) that $(s_1 |_{t_j=\theta_j}, s_2 |_{t_j=\theta_j}, ..., s_r |_{t_j=\theta_j}) \in M \subseteq \widetilde{M}$, which proves the claim.
Now we obtain $\ker(\psi|_{T^t}) = \ker(\psi) \cap T^r = \widetilde{M}_T$, and we have

$$\psi(T^r) = A^r/(A^r \cap M)$$

The the first homomorphism theorem implies that

$$T^r/\widetilde{M}_T \cong A^r/(A^r \cap M),$$

which is an isomorphism induced by ϕ, hence $\phi(\widetilde{M}_T) = A^r \cap M$. ■

The following algorithm for computing the intersection of M and A^r uses Gröbner bases of modules, which were introduced by Möller and Mora [28], who also extended the Buchberger algorithm to this case.

Algorithm *Module-Ring-Intersection*(B, R)
In: module generators $b_1, ..., b_s$ for M, algebra generators for A.
Out: Module generators $c_1, ..., c_m \in A^r$ for $M \cap A^r$.
begin
$S := \mathbf{K}[x_1, ..., x_n, t_1, ..., t_n]$;
$\{e_1, ..., e_r\}$:=canonical basis of S^r;
$\widetilde{M}$:= the module generated by $b_i, i \in \{1, ..., s\}$ and $(t_i - \theta_i) \cdot e_j, i \in \{1, ..., n\}, j \in \{1, ..., r\}$;
$\prec :=$ a term order on $\widetilde{M}$ with x_i greater than any monomial in the t_j;
$B := GroebnerBasis(\widetilde{M}, \{x_1, ..., x_n, t_1, ..., t_n\}, \prec)$;
$B_T := B \cap (\mathbf{K}[t_1, t_2, ..., t_n])^r$;
$\{c_1, ..., c_m\} := \phi(B_T)$;
return$(\{c_1, ..., c_m\})$**;**
end;

We can now present Kemper's algorithm for the computation of secondary invariants.

Algorithm *SecondaryInvariants*$(B, \langle\theta_1, ..., \theta_n\rangle)$
In: A generating set B of the group G, an hsop $\theta_1, ..., \theta_n$.
Out:Secondary invariants $\{\eta_1, ..., \eta_m\}$.
begin
let $H \leq G$ s.t. $char(\mathbf{K}) \nmid |H|$; // default $H := \{1\}$
$\{b_1, ..., b_s\}$:=*SecondaryInvariants*$(H, \langle\theta_1, ..., \theta_n\rangle)$; // non-modular
Let $M \leq \mathbf{K}[x_1, x_2, ..., x_n]^r$ be the solution module of the following linear system

$$\sum_{i=1}^{r}(\eta_i(x) - \sigma \cdot \eta_i(x)) \cdot z_i = 0, \text{ for } \sigma \in B;$$

This amounts to the calculation of a syzygy module;
$\{c_1, ..., c_m\}$:= a basis of $M \cap \mathbf{K}[\theta_1, ..., \theta_n]^r$
for $i := 1$ **to** m **do** $\eta_i := \sum_{j=1}^{r} c_{ij} \cdot b_j$; **end**;
return$(\eta_1, ..., \eta_m)$;
end.

Remark 4 *For the computation of syzygy modules we refer, e.g., to Becker and Weispfennig [3] or Winkler [47].*

3.2 Fundamental Invariants

In this section we present an new algorithm for computing the intersection of invariant rings of finite groups $G_1, G_2 \leq GL_n(\mathbf{K})$ which are given in terms of fundamental invariants in the nonmodular case. The result is a set of fundamental invariants for the ring $\mathbf{K}[x_1, x_2, ..., x_n]^{G_1} \cap \mathbf{K}[x_1, x_2, ..., x_n]^{G_2}$. This leads to a new approach for computing the invariant ring of a finite group $G = \langle \sigma_1, ..., \sigma_k \rangle \leq GL_n(\mathbf{K})$ in the nonmodular case. First one computes fundamental invariants for the invariant rings $\mathbf{K}[x_1, x_2, ..., x_n]^{\langle \sigma_i \rangle}$ for $1 \leq i \leq k$, which can be done for $\mathbf{K} = \mathbf{C}$ with the algorithms from Section 4.1. Then it is clear that the invariant ring equals

$$\mathbf{K}[x_1, x_2, ..., x_n]^G = \bigcap_{i=1}^{k} \mathbf{K}[x_1, x_2, ..., x_n]^{\langle \sigma_i \rangle}. \tag{3.4}$$

Also the algorithm can be used if the fundamental invariants of several invariant rings of some groups $G_1, G_2, ..., G_k$ are already known, and one wants to compute the invariant ring of the group $G = \langle G_1 \cup G_2 \cup ... \cup G_k \rangle$.

3.2.1 The Intersection Algorithm

Let $R = \mathbf{K}[x_1, x_2, ..., x_n], G_1, G_2$ and G be finite subgroups of $GL_n(\mathbf{K})$ s.t. $G = \langle G_1 \cup G_2 \rangle$, where $\langle G_1 \cup G_2 \rangle$ denotes the group generated by the elements of G_1 and G_2, and assume $char(\mathbf{K}) \nmid |G|$. Suppose that the two invariant rings $R^{G_1} = \mathbf{K}[f_1, ..., f_{m_1}]$ and $R^{G_2} = \mathbf{K}[g_1, ..., g_{m_2}]$ are given in terms of fundamental invariants. We present an algorithm which computes the algebra basis $\{h_1, h_2, ..., h_m\}$ of the intersection of R^{G_1} and R^{G_2}, i.e.

$$R^{G_1} \cap R^{G_2} = \mathbf{K}[h_1, h_2, ..., h_m] = R^G.$$

The restriction to the nonmodular case comes from the fact that the algorithm is based on the proof of Hilbert's finiteness Theorem (Theorem 2.3.11) and holds therefore only for a field $\mathbf{K}$ with $char(\mathbf{K}) \nmid |G|$. The following theorem is the key to the algorithm.

Theorem 16 *Let $G \leq GL_n(\mathbf{K})$ be a finite group with subgroups G_1 and G_2 s.t. $G = \langle G_1 \cup G_2 \rangle$. Let $\langle R_+^G \rangle \trianglelefteq R$ denote the ideal generated by all homogenous elements of positive degree from R^G. Let $I = \langle f_1, ..., f_{m_1} \rangle = \langle g_1, ..., g_{m_2} \rangle \trianglelefteq R$ be a proper ideal in R for homogenous elements $f_i \in R^{G_1}$ and $g_j \in R^{G_2}$,respectively, then*

$$I \supseteq \langle R_+^G \rangle \Longrightarrow I = \langle R_+^G \rangle.$$

Note : In general, $I \subsetneq \langle R_+^G \rangle$.

Proof. If $G_1 = G_2$ then $G = G_1$ and $R^G = R^{G_1}$. If $I \supseteq \langle R_+^G \rangle$ then $I = \langle R_+^G \rangle$ because $\langle R_+^G \rangle$ is the largest ideal which can be generated from the invariants of positive degree. Therefore we may assume $R^{G_1} \neq R^{G_2}$. We denote the Reynolds operator of the groups G_k by ^{*_k} for $k = 1, 2$ and of the group G with *. Suppose $I \supsetneq \langle R_+^G \rangle$ and let $h \in I \backslash \langle R_+^G \rangle$ be a homogenous element of minimal degree. Then, according to Lemma 1.4.4, we can write h in the following form :

$$h = \sum_{i=1}^{m_1} p_i f_i$$

for some homogenous polynomials p_i with $\deg p_i = \deg h - \deg f_i$. At least one of the p_i 's is a nonzero constant, otherwise each f_i is contained in $\langle R_+^G \rangle$ because of the minimality of h. W.l.o.g. we may assume $h = f_1$. Since I is also generated by $g_1, ..., g_{m_2}$ we have

$$f_1 = \sum_{i=1}^{m_2} r_i g_i = \sum_{i=1}^{m_2} \lambda_i \underbrace{g_i}_{\notin < R_+^G >} + \sum_{i=1}^{m_2} s_i \underbrace{g_i}_{\in < R_+^G >} .$$

for some homogenous polynomials r_i with $\deg r_i = \deg f_1 - \deg g_i$ (cf. Lemma 1.4.4). Note that any g_i with $\deg(g_j) < \deg(f_1)$ is contained in $\langle R_+^G \rangle$ because of the minimality of the degree of f_1. It follows that all λ_i are contained in $\mathbf{K}$ and at least one is nonzero. An application of the Reynolds operator to f_1 yields $f_1^{*_2} = \sum_{i=1}^{m_2} \lambda_i g_i + \sum_{i=1}^{m_2} s_i^{*_2} g_i$ and we have

$$f_1 - f_1^{*_2} = \sum_{i=1}^{m_2} (s_i - s_i^{*_2}) g_i \in \langle R_+^G \rangle ,$$

so $f_1 \equiv f_1^{*_2} \bmod \langle R_+^G \rangle$. Note that the ideal $\langle R_+^G \rangle$ is $G-$ invariant.
Now choose generators $G_1 = \langle \sigma_1 ..., \sigma_a \rangle$ and $G_2 = \langle \tau_1 ..., \tau_b \rangle$. We show via induction on the length l of products of the elements from $\{\sigma_1 ..., \sigma_a, \tau_1, ..., \tau_b\}$ that $f_1 \equiv \gamma \cdot f_1 \equiv f_1^{*_2} \equiv \gamma \cdot f_1^{*_2} \bmod \langle R_+^G \rangle$ for all $\gamma \in G$. The case $l = 0$ is trivial. So assume that $\gamma \in G$ is a product of $l - 1$ elements from the set $\{\sigma_1 ..., \sigma_a, \tau_1, ..., \tau_b\}$ and

$$f_1 \equiv \gamma \cdot f_1 \equiv f_1^{*_2} \equiv \gamma \cdot f_1^{*_2} \bmod \langle R_+^G \rangle . \qquad (+)$$

For $\gamma\sigma_j$ we have $\gamma\sigma_j \cdot (f_1 - f_1^{*_2}) = \gamma \cdot f_1 - \gamma\sigma_j \cdot f_1^{*_2}$, so $\gamma\sigma_j \cdot f_1^{*_2} \equiv \gamma \cdot f_1$ and the induction hypothesis implies that $f_1 \equiv \gamma\sigma_j \cdot f_1 \equiv \gamma\sigma_j \cdot f_1^{*_2} \bmod \langle R_+^G \rangle$. Also for $\gamma\tau_k$ we have $\gamma\tau_k \cdot (f_i - f_i^{*_2}) = \gamma\tau_k \cdot f_i - \gamma \cdot f_i^{*_2}$, so $\gamma\tau_k \cdot f_i \equiv \gamma \cdot f_i^{*_2} \equiv \gamma \cdot f_i$. Thus we have

$$f_1^* = \frac{1}{|G|} \sum_{\sigma \in G} \sigma \cdot f_1 \equiv \frac{1}{|G|} \sum_{\sigma \in G} f_1 \bmod \langle R_+^G \rangle .$$

Hence

$$f_1 \equiv f_1^* \bmod \left\langle R_+^G \right\rangle .$$

The polynomial f_1^* is contained in R^G, in particular $f_1^* \in \left\langle R_+^G \right\rangle$ so $f_1 \equiv f_1^* \equiv 0 \bmod \left\langle R_+^G \right\rangle$ which implies $f_1 \in \left\langle R_+^G \right\rangle$, a contradiction. ■

It is sufficient to know an ideal basis for $\left\langle R_+^G \right\rangle$ containing only homogenous elements, because the Reynolds images of the generators are a set of fundamental invariants for G.

Lemma 13 *Let $\langle h_1, h_2, ..., h_m \rangle$ be a set of arbitrary homogenous generators of the ideal $\left\langle R_+^G \right\rangle \trianglelefteq R$. Then $R^G = \mathbf{K}[h_1^*, h_2^*, ..., h_m^*]$.*

Proof. It is sufficient to show that each homogenous invariant of degree > 0 is contained in $\langle h_1^*, ..., h_m^* \rangle$. Assume the converse and let $h = \sum_{i=1}^m p_i h \in \langle h_1, h_2, ..., h_m \rangle \setminus \langle h_1^*, h_2^*, ..., h_m^* \rangle$ be a homogenous invariant of minimal degree for some $p_i \in \mathbf{K}[x_1, x_2, ..., x_n]$. Note that for a homogenous $f \in R$ of with $\deg(f) < \deg(h)$ we have $f \in \langle h_1, h_2, ..., h_m \rangle \Leftrightarrow f \in \langle h_1^*, h_2^*, ..., h_m^* \rangle$. As in the above proof we write $h = \sum_{i=1}^m \lambda_i h_i + \sum_{i=1}^m s_i h_i$ for $\lambda_i \in \mathbf{K}$ and $s_i \in \mathbf{K}[x_1, x_2, ..., x_n]$ with $s_i = 0$ or $\deg(s_i) > 0$. Now the minimality of h implies that $\sum_{i=1}^m s_i h_i \in \langle h_1^*, h_2^*, ..., h_m^* \rangle$, so $\sum_{i=1}^m s_i h_i = \sum_{i=1}^m \widetilde{s}_i h_i^*$ for some $\widetilde{s}_i$. But $h = h^* = \sum_{i=1}^m \lambda_i h_i^* + \sum_{i=1}^m \overline{s}_i h_i^*$, a contradiction. Hence the ideal $\langle h_1^*, h_2^*, ..., h_m^* \rangle$ contains all homogenous invariants of positive degree, and we have $\langle h_1^*, h_2^*, ..., h_m^* \rangle = \left\langle R_+^G \right\rangle = \langle h_1, h_2, ..., h_m \rangle$. ■

For a different proof see Derksen [12] Lemma 2.2 of ch. 1.

We can now state the intersection algorithm. The algorithm computes a basis for the ideal $\left\langle R_+^G \right\rangle$ and applies the Reynolds operator to each basis element.

Algorithm *Intersection*($\langle f_1, f_2, ..., f_{m_1} \rangle$,$\langle g_1, g_2, ..., g_{m_2} \rangle$, $*$)

In: Algebra generators $f_1, f_2, ..., f_{m_1}$ for R^{G_1} and $g_1, g_2, ..., g_{m_2}$ for R^{G_2}.
The Reynolds operator * for the group $\langle G_1 \cup G_2 \rangle$.
Out: Algebra generators $h_1, h_2, ..., h_m$ for $R^{\langle G_1 \cup G_2 \rangle}$.
begin
$I_1 := \langle f_1, f_2, ..., f_{m_1} \rangle$;
$I_2 := \langle g_1, g_2, ..., g_{m_2} \rangle$;
while $I_1 \neq I_2$ **do**
. $I := I_1 \cap I_2$;
. $I_1 := \left\langle I \cap R^{G_1} \right\rangle$; // Intersection of I with the subring R^{G_1}.
. $I_2 := \left\langle I \cap R^{G_2} \right\rangle$; // Intersection of I with the subring R^{G_2}.
end;
return(I_1^*); // Apply the Reynolds operator to each basis element.
end *Intersection.*

For comparing two ideals and for the computation of their intersection we refer to Cox et. al.. [9] and Becker and Weisspfennig [3]. The computation of the intersection of an ideal with an invariant ring is described in section 2.6 of Sturmfels [43].

The termination and correctness of the algorithm follows from the next two theorems.

Lemma 14 *In each iteration of the while loop the ideal* $\left\langle R_+^G \right\rangle$ *is contained in* $I_1 \cap I_2$.

Proof. Follows from the inclusion of ideals $\langle f_1, f_2, ..., f_{m_1} \rangle \supseteq \left\langle R_+^G \right\rangle$ and $\langle g_1, g_2, ..., g_{m_2} \rangle \supseteq \left\langle R_+^G \right\rangle$ and the equality $R^G = R^{G_1} \cap R^{G_2}$. ■

Theorem 17 *The algorithm Intersection terminates.*

Proof. Consider the residue class ring $\overline{R} = R/\left\langle R_+^G \right\rangle$. Since $\overline{R}$ is zero-dimensional it is Artinian, hence each strictly descending sequence $\left\{\overline{J}_k\right\}$ of ideals must stabilize, i.e. $\overline{J}_N = \overline{J}_{N+k}$ for some $N \in \mathbf{N}$ and all $k \in \mathbf{N}$. Let J_n be the intersection $I_1 \cap I_2$ in the $n-$th iteration of the while loop and denote the image of J_n in $\overline{R}$ with $\overline{J}_n$. We obtain a strictly descending sequence of ideals in $\overline{R}$, hence after a finite number of steps the sequence stabilizes. The proof follows from the fact, that the ideals in $\overline{R}$ correspond uniquely to ideals in R containing $\left\langle R_+^G \right\rangle$. ■

Theorem 18 *The algorithm* Intersection *is correct.*

Proof. It follows from Theorem 3.2.17 that $I_1 = I_2$ after a finite number of iterations of the while loop. Now Lemma 3.2.14 implies that I_1 and I_2 satisfy the condition of Theorem 3.2.16. Let $h_1, h_2, ..., h_m \in R^{G_1}$ be a set of homogenous generators for the ideal I_1, then we know from Lemma 3.2.13 that $R^G = \mathbf{K}[h_1^*, h_2^*, ..., h_m^*]$. ■

Example 13 *Let* $\mathbf{K} = \mathbb{F}_5, \sigma_1 = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 0 & 3 \\ 1 & 2 \end{pmatrix}$ *and* $G = \langle \sigma_1, \sigma_2 \rangle$. *Note that* $|G| = 96$. *The subgroup* $\langle \sigma_1 \rangle$ *has order* 8 *and* $R^{\langle \sigma_1 \rangle}$ *is generated by the fundamental invariants*

$$\begin{aligned} F_1 &= \{x^4 + x^2y^2 + y^4, x^3y + 4x^2y^2 + 4xy^3 + 3y^4, \\ &\quad x^8 + 2x^3y^5 + 4x^2y^6 + 3xy^7 + 2y^8, x^7y + 2x^3y^5 + 2x^2y^6 + 2xy^7 + 4y^8\} \end{aligned}$$

The subgroup $\langle \sigma_2 \rangle$ *has order* 4 *and* $R^{\langle \sigma_2 \rangle}$ *is generated by the fundamental invariants*

$$F_2 = \{x^2 + 3xy + y^2, x^3 + 3xy^2 + y^3, x^4 + 3x^2y^2 + 4xy^3 + y^4\}$$

The fundamental invariants F_1 and F_2 have been found with the implementation of Kemper's algorithms in the computer algebra system Magma (cf. [6]). Now we call Intersection$(F_1, F_2, \mathfrak{R}^G)$ *(from the* `Invariants` *package) and obtain fundamental invariants for R^G,namely*

$$\begin{aligned} h_1 &= 3x^{12} + x^{11}y + 3x^{10}y^2 + x^8y^4 + 4x^7y^5 + \\ &\quad 2x^5y^7 + x^4y^8 + 2x^2y^{10} + 3xy^{11} + 3y^{12}, \\ h_2 &= 2x^8 + x^7y + x^6y^2 + 2x^5y^3 + 3x^4y^4 + 4x^3y^5 + 4x^2y^6 + 3xy^7 + 2y^8. \end{aligned}$$

Hence

$$\mathbb{F}_5[x,y]^G = \mathbb{F}_5[h_1, h_2].$$

3.2.2 Computation of Fundamental Invariants

From the observation (3.4) we can derive a simple algorithm for the computation of the fundamental invariants of the invariant ring of $G = \langle \sigma_1, ..., \sigma_k \rangle \leq GL_n(\mathbf{K})$ in the nonmodular case. An algorithm for the computation the fundamental invariants of a cyclic group $\langle \sigma \rangle \leq GL_n(\mathbf{C})$ can be found in section 4.1.

Algorithm *InvariantRing*$(\sigma_1, ..., \sigma_k)$
In: Generators $\sigma_1, ..., \sigma_k$ for the finite group $G \leq GL_n(\mathbf{K})$.
Out: Algebra generators $h_1, ..., h_m$ for $\mathbf{K}[V]^G$.
begin
Compute a generating set H for $\mathbf{K}[V]^{\langle \sigma_1 \rangle}$;
for $i := 2$ **to** k **do**
. Compute a generating set B for $\mathbf{K}[V]^{\langle \sigma_i \rangle}$;
. Compute the Reynolds operator * for $\langle \sigma_1, ..., \sigma_i \rangle$;
. $H :=$*Intersection*$(H, B, ^*)$;
end;
return(H);

We conclude with two examples.

Example 14 *Let* $G_1 = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle, G_2 = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$ *and* $G = \langle G_1 \cup G_2 \rangle$ *be subgroups of $GL_n(\mathbf{C})$. Now $\mathbf{C}[V]^{G_1} = \mathbf{C}[x^2+y^2, x^4+y^4, x^3\,y - x\,y^3]$ and $\mathbf{C}[V]^{G_2} = \mathbf{C}[x, y^2]$. Using the algorithm Intersection we obtain algebra generators for $\mathbf{C}[x,y]^G = \mathbf{C}[x^2+y^2, \frac{1}{2}(x^4+y^4)]$. In the last step of the algorithm, the Reynolds operator is applied to the generators $\{y^4, x^2+y^2\}$ of the ideal $\left\langle \mathbf{C}[x,y]^G_+ \right\rangle$.*

Example 15 *Let* $\sigma_1 = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ *and* $\sigma_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$. *From Example 5.4.37 we obtain fundamental invariants for* $G_1 = \langle \sigma_1 \rangle$, *namely*

$$F_1 = \{x^2 + y^2, z^2, xyz, x^2z - y^2z, x^2y^2, x^3y - xy^3\}.$$

Fundamental invariants for $G_2 = \langle \sigma_2 \rangle$ *can be easily computed, we take primary and secondary invariants (without* 1*) of* G_2, *i.e.*

$$F_2 = \{x + y + z, xy + xz + yz, xyz, x^2y + xz^2 + y^2z\}.$$

We set $G = \langle \sigma_1, \sigma_2 \rangle$ *and call* $\mathrm{Intersection}(F_1, F_2, \mathfrak{R}^G)$ *and obtain*

$$\begin{aligned} h_1 &= x^2 + y^2 + z^2, \\ h_2 &= xyz, \\ h_3 &= 2x^4 + x^2y^2 + 2y^4 + x^2z^2 + y^2z^2 + 2z^4. \end{aligned}$$

Since $H^G(t) = H(\mathbf{C}[h_1, h_2, h_3], t)$ *the result is correct.*

It is an interesting question whether the algorithm Intersection can be generalized to linear reductive groups. If so, it might be an alternative to Derksen's algorithm.

Chapter 4

Selected Topics

In this chapter we deal with various aspects of invariant theory. In the first section we present specialized algorithms for Abelian groups. In section 2 we study the induced action of the dual representation on the tensor and exterior algebra. In section 3 we present Stanley's summation example and in section 4 we how one can prove theorems in projective geometry with invariant theory.

4.1 Abelian Groups

In this section we present a Gröbner bases free algorithm for the computation of the invariant ring of a finite Abelian group. For a different approach (with one Gröbner basis computation) we refer to Sturmfels [43], section 2.5.

Let G be a finite abelian group and ρ be any $n-$dimensional faithful representation of G. Since each irreducible representation of an abelian group is one-dimensional (cf. Corollary 1.2.1), the matrices $\rho(\sigma) \in GL_n(\mathbf{C}), \sigma \in G$ can be diagonalized simultaneously and contain roots of unity in the diagonal. This additional structure information can be used for the computation of the invariant ring of $\rho(G)$.
Convention : We only consider faithful representations. If $G = \mathbf{Z}_{n_1} \times ... \times \mathbf{Z}_{n_k}$ and $\rho : G \to GL_n(\mathbf{C})$ has non-trivial kernel H, then we consider the induced representation $\rho' : G/H \to GL_n(\mathbf{C}), gH \mapsto \rho(g)$. Since the roots of unity play such an important role we need an abbreviation for them.

Definition 39 *For $k \in \mathbf{N}$ we define $\xi_k := \exp(2\pi i/k)$.*

In the first two sections we study faithful representations of finite cyclic groups, which are generated by diagonal matrices, in section three we treat arbitrary finite cyclic groups. In section four we show how one can compute the invariant ring of arbitrary faithful representations ρ of finite abelian groups $\mathbf{Z}_{n_1} \times ... \times \mathbf{Z}_{n_k}$ from the knowledge of $\rho_{|\mathbf{Z}_{n_j}}$ for $1 \leq j \leq k$.

None of the presented algorithms use Gröbner bases, but use only simple ideas from linear algebra.

4.1.1 Cyclic Groups - Diagonal Form (1)

We start with the simplest non-trivial case, namely with irreducible representations.

Proposition 23 *For $n \in \mathbf{N}$ the invariant ring of $\mathbf{Z}_n$ w.r.t. any irreducible representation ρ is simply the polynomial ring $\mathbf{K}[x^{|\rho|}],$. where $|\rho|$ denotes the order of the group $\rho(\mathbf{Z}_n)$.* ■

In the sequel we study reducible (faithful) representations of G. We begin with cyclic groups where all elements are diagonal matrices of the form $diag(\xi_{d_1}, \xi_{d_2}, ..., \xi_{d_n})$ for some $d_1, d_2, ..., d_n \in \mathbf{N}_0$.

Example 16 *Let $G = \{1, -1, -i, i\}$ be the cyclic group of order 4. Consider the representation $\rho(i^k) = \begin{pmatrix} (-1)^k & 0 & 0 \\ 0 & (-1)^k & 0 \\ 0 & 0 & i^k \end{pmatrix}$ for $k \in \{0, 1, 2, 3\}$. A monomial $x^a y^b z^c$ is invariant w.r.t. $\rho(G)$ if and only if $\rho(i) \cdot x^a y^b z^c = x^a y^b z^c$.It suffices to look at the exponents of this equation, hence*

$$\begin{aligned} (-x)^a(-y)^b(i \cdot z)^c &= x^a y^b z^c \Leftrightarrow \\ \exp(\frac{2\pi i}{2}a)\exp(\frac{2\pi i}{2}b)\exp(\frac{2\pi i}{4}c) &= 1 \Leftrightarrow \\ \exp(\frac{\pi i}{2}(2a+2b+c)) &= 1 \Leftrightarrow \\ 2a+2b+c &\equiv 0 \bmod 4. \end{aligned}$$

Therefore we consider the solution set of the equations

$$2a + 2b + c = 4p \text{ for } p \in \mathbf{N}_0. \tag{4.1}$$

For $p = 1$ we have the solutions $(2, 0, 0), (0, 2, 0), (0, 0, 4), (1, 1, 0), (0, 1, 2)$ and $(1, 0, 2)$. From the first 3 solutions we obtain primary invariants x^2, y^2, z^4 (cf. Lemma 3.1.10) and set $R = \mathbf{C}[x^2, y^2, z^4]$. From the remaining solutions we obtain secondary invariants xy, xz^2 and yz^2. In the case $p = 2$ we obtain the solutions $(0, 1, 6), (0, 2, 4), (0, 3, 2), (0, 4, 0), (1, 0, 6), (1, 1, 4), (1, 2, 2), (1, 3, 0)$,

$(2,0,4),(2,1,2),(2,2,0),(3,0,2),(3,1,0),(4,0,0)$. *For each such solution* $(\alpha_1, \alpha_2, \alpha_3)$ *it holds that* α_1 *or* $\alpha_2 \geq 2$ *or* $\alpha_3 \geq 4$. *So each monomial* $x^{\alpha_1}y^{\alpha_2}z^{\alpha_3}$ *can be expressed as a product of the primary and secondary invariants from above. The Hilbert series of the ring obtained so far can be computed with Proposition 2.5.5 and equals*

$$H(R\bigoplus xyR\bigoplus xz^2R\bigoplus yz^2,t) = \frac{1+t^2+2t^3}{(1-t^2)^2\cdot(1-t^4)}. \tag{4.2}$$

It remains to show that there are no more secondary invariants left, which can be done by comparing (4.2) *with* $H^{\rho(G)}(t)$. *The Hilbert series* $H^{\rho(G)}(t)$ *can be evaluated with Molien's Theorem (Theorem 2.4.12) equals* (4.2).

We can generalize the observation from the preceding example. Let $m \in \mathbf{N}$ and $G = \mathbf{Z}_m$ with generator σ, i.e. $G = \{\sigma^i \mid 0 \leq i \leq m-1\}$. In the sequel we consider faithful representations $\rho : \mathbf{Z}_m \to GL_n(\mathbf{C})$ with $\rho(\sigma) = \begin{pmatrix} \xi_{d_1} & 0 & \dots & 0 \\ \vdots & \xi_{d_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \xi_{d_n} \end{pmatrix}$. We have $\mathrm{lcm}(d_1,...,d_n) = |\rho(G)| = m$. A monomial $\prod_{j=1}^n x_j^{\alpha_j}$ is invariant w.r.t. $\rho(G)$ iff

$$\begin{aligned} \rho(\sigma^{-1})\cdot\prod_{j=1}^n x_j^{\alpha_j} &= \prod_{j=1}^n(\xi_{d_j}x_j)^{\alpha_j} = \prod_{j=1}^n(\xi_{d_j})^{\alpha_j}\prod_{j=1}^n x_j^{\alpha_j} = \prod_{j=1}^n x_j^{\alpha_j} \quad (4.3)\\ &\Longleftrightarrow \\ \sum_{j=1}^n 2\pi i\cdot\frac{\alpha_j}{d_j} &= 2\pi i\cdot p \text{ for some } p\in\mathbf{Z}. \\ &\Longleftrightarrow \\ \sum_{j=1}^n \frac{\alpha_j\cdot m}{d_j} &= m\cdot p \text{ for some } p\in\mathbf{Z}. \quad (4.4) \end{aligned}$$

Definition 40 *In the context from above the equation*

$$\sum_{j=1}^n \frac{m}{d_j}a_j = m\cdot p \textit{ for some } p\in\mathbf{Z} \tag{4.5}$$

is called the ***characteristic equation*** *of* $\rho(G)$ *w.r.t.* p.

We do not drop m from both sides of the equation because we want to have equations over the positive integers.

Definition 41 *Let $n \in \mathbf{N}$ and $\rho(G) = \langle diag(\xi_{d_1}, \xi_{d_2}, ..., \xi_{d_n})\rangle$ for some $d_1, ...d_n \in \mathbf{N}$. We denote the order of $\rho(G)$ with m. For $p \in \mathbf{N}_0$ we denote the set of solutions of the characteristic equation of $\rho(G)$ w.r.t. p with $S_p(\rho(G), (d_1, ...d_n)) := \{(\alpha_1, ..., \alpha_n) \in \mathbf{N}_0^n \mid \sum_{j=1}^n \frac{\alpha_j \cdot m}{d_j \cdot} = m \cdot p$, each $\alpha_j < d_j$ for $1 \leq j \leq n\}$, and we define $S(\rho(G), (d_1, ...d_n), t) := \bigcup_{p=0}^t S_p(\rho(G), (d_1, ...d_n))$. Furthermore we set $S(\rho(G), (d_1, ...d_n)) := \bigcup_{p=0}^{n-1} S_p(\rho(G), (d_1, ...d_n), n-1)$.*

For a cyclic group, which is generated by a diagonal matrix of the above kind, the invariant ring can be easily computed.

Theorem 19 *Let $n \in \mathbf{N}$ and $\rho(G) = \langle diag(\xi_{d_1}, \xi_{d_2}, ..., \xi_{d_n})\rangle$ for some $d_1, ...d_n \in \mathbf{N}$. The primary invariants of $\rho(G)$ are given by $x_1^{d_1}, ..., x_n^{d_n}$. A set of secondary invariants is given by the monomials $\prod_{j=1}^n x_j^{\alpha_j}$ with $\boldsymbol{\alpha} \in S(\rho(G), (d_1, ..., d_n))$.*

Proof. The monomials $x_1^{d_1}, ..., x_n^{d_n}$ are invariant w.r.t. $\rho(G)$ and the set of their common zeros equals $\{0\}$. Now Lemma 3.1.10 and Lemma 3.1.11 imply that they are primary invariants of $\rho(G)$. We claim that there are no secondary invariants missing. From (4.4) we know that a monomial $\prod_{j=1}^n x_j^{\alpha_j}$ is invariant iff $\boldsymbol{\alpha}$ satisfies the characteristic equation for some $p \in \mathbf{N}$. Suppose that $\prod_{j=1}^n x_j^{\alpha_j}$ is an invariant and $\alpha_k \geq d_k$ for some k. Now we set $\beta_j = \alpha_j$ and $\gamma_j = 0$ if $\alpha_j < d_j$ and $\beta_j = \alpha_j - d_j$ and $\gamma_j = d_j$ otherwise, and obtain $\prod_{j=1}^n x_j^{\alpha_j} = \prod_{j=1}^n x_j^{\beta_j} \prod_{j=1}^n x_j^{\gamma_j}$ with $\beta_k < d_k$. The monomial $\prod_{j=1}^n x_j^{\gamma_j}$ is a product of primary invariants which proves the claim. We substitute $d_j - 1$ for a_j in the left hand side of (4.5) and obtain the estimation

$$\sum_{j=1}^n \frac{m}{d_j}(d_j - 1) < m \cdot n.$$

Therefore the elements of $S(\rho(G), (d_1, ...d_n))$ correspond to degree vectors of a set of secondary invariants. ■

Note that the number of equations to solve equals

$$\left\lfloor \sum_{j=1}^n \frac{1}{d_j}(d_j - 1) \right\rfloor < n. \tag{4.6}$$

4.1.2 Cyclic Groups-Diagonal Form (2)

We extend the above theory to all representations of cyclic groups, which are already diagonalized. Let $G = \langle \sigma \rangle$ be a cyclic group of order m and $\rho : G \rightarrow$

$GL_n(\mathbf{C})$ be a faithful representation with $\rho(\sigma) = \begin{pmatrix} \xi_{d_1}^{k_1} & 0 & \dots & 0 \\ \vdots & \xi_{d_2}^{k_2} & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \xi_{d_n}^{k_n} \end{pmatrix}$ for some $d_1, d_2, ...d_n, k_1, k_2, ..., k_n \in \mathbf{N}$ with $\gcd(k_j, d_j) = 1$ for $1 \leq j \leq n$. It follows with the same calculation as in (4.3) that a monomial $\prod_{j=1}^n x_j^{\alpha_j}$ is invariant w.r.t. $\rho(G)$ iff $\sum_{j=1}^n \frac{k_j \alpha_j m}{d_j.} = s \cdot m$ for some $s \in \mathbf{N}$. The characteristic equation of $\rho(G)$ w.r.t. p equals

$$\sum_{j=1}^n \frac{k_j \cdot m}{d_j} a_j = m \cdot p.$$

The following example shows that the estimation (4.6) is no longer valid, so in general we have to solve more than $n-1$ equations.

Example 17 *Let $G = \left\langle diag(\xi_5^2, \xi_5^3) \right\rangle$ (and take $\rho = id$). The characteristic equations of G w.r.t. p equals*

$$2a + 3b = 5 \cdot p.$$

We have the solutions $(1,1)$ for $p = 1, (2,2)$ for $p = 2, (3,3)$ for $p = 3$ and $(4,4)$ for $p = 4$. Hence the invariant ring $\mathbf{K}[x,y]^G$ is generated as a $\mathbf{K}[x^5, y^5]$ module by the monomials $1, xy, x^2y^2, x^3y^3, x^4y^4$. But we were forced to solve 4 equations, not 1 as one would expect from (4.6).

For computational purposes it would be nice to reduce the problem of finding the solutions $S(G, (d_1, d_2, \dots, d_n))$ to a cyclic group from Section 4.1.1 because for such groups we have at most $n-1$ equations to solve. The above example shows that this bound is not longer valid if we consider arbitrary cyclic groups.

Theorem 20 *Let $G = \left\langle diag(\xi_{d_1}^{k_1}, \xi_{d_2}^{k_2}, ..., \xi_{d_m}^{k_m}) \right\rangle \leq GL_m(\mathbf{C})$ be a cyclic group of order m s.t. $\gcd(k_j, d_j) = 1$ for $1 \leq j \leq n$ and set $G' = \left\langle diag(\xi_{d_1}, \xi_{d_2}, ..., \xi_{d_m}) \right\rangle$. The map*

$$\begin{array}{rcl} \varphi_G & : & S(G') \to S(G) \\ (\alpha_1, ..., \alpha_m) & \mapsto & (\alpha_1 \cdot k_1^{-1} \bmod d_1, ..., \alpha_m \cdot k_m^{-1} \bmod d_m), \end{array}$$

where the inverse of k_j is taken in $\mathbf{Z}_{d_j}$, is a bijection.

Proof. Assume $\sum_{j=1}^n \frac{1}{d_j} \alpha_j = p$ for some $p \in \mathbf{N}_0$. Then $\sum_{j=1}^n \frac{k_j}{d_j}(\alpha_j k_j^{-1}) = \sum_{j=1}^n \frac{1}{d_j} \alpha_j = p$. ■

Example 18 *We consider the same group $G = \left\langle diag(\xi_5^2, \xi_5^3)\right\rangle$ as in Example 17. The characteristic equations of G' w.r.t. s equals*

$$a + b = 5 \cdot s.$$

We have the solutions $(1,4),(2,3),(3,2)$ and $(4,1)$ for $s = 1$. From Theorem 4.1.19 we know that these are all solutions. We transform the solutions w.r.t. the map φ_G and obtain $(1,1),(2,2),(3,3),(4,4)$ as required.

4.1.3 Cyclic Groups-General Case

Let G be a cyclic group with generator σ and $\rho, \rho' : G \to GL_n(\mathbf{C})$ be faithful equivalent representations of G s.t. $\rho(\sigma) \cong \rho'(\sigma) = diag(\xi_{d_1}^{k_1}, \xi_{d_2}^{k_2}, ..., \xi_{d_m}^{k_m})$ for some $\mathbf{k}, \mathbf{d} \in \mathbf{N}^n$ with $\gcd(k_i, d_i) = 1$. Firstly we examine the eigenvectors of the dual action ρ^* on $(\mathbf{C}^n)^*$. If $v^* \in (\mathbf{C}^n)^*$ then v denotes the image of v^* under the isomorphism * (cf. Section 2.2).

Proposition 24 *For $v^* \in (\mathbf{C}^n)^*$ and $\lambda \in \mathbf{C} \setminus \{0\}$ we have*

$$\rho^*(\sigma)(v^*) = \lambda v^* \Longleftrightarrow \rho(\sigma^{-1})^T \cdot \widehat{v} = \lambda \widehat{v}.$$

Proof. From definition 2.2.31 we obtain

$$\begin{aligned} \rho^*(\sigma)(v^*) &= \lambda v^* \Longleftrightarrow \forall \widehat{w} \in \mathbf{C}^n : \left\langle \widehat{v}, \rho(\sigma^{-1}) \cdot \widehat{w} \right\rangle = \langle \lambda \cdot \widehat{v}, \widehat{w} \rangle \\ &\Longleftrightarrow \forall \widehat{w} \in \mathbf{C}^n : \left\langle \rho(\sigma^{-1})^T \cdot \widehat{v}, \widehat{w} \right\rangle = \langle \lambda \widehat{v}, \widehat{w} \rangle \\ &\Longleftrightarrow \rho(\sigma^{-1})^T \cdot \widehat{v} = \lambda \widehat{v}. \blacksquare \end{aligned}$$

Let $v_1, v_2, ..., v_n$ be the eigenvectors of $\rho(\sigma)^T$ with eigenvalues $\xi_{d_1}^{k_1}, \xi_{d_2}^{k_2}, ..., \xi_{d_m}^{k_m}$ respectively. From Proposition 4.1.24 and the above discussion we obtain

$$Sym^d \rho^*(\sigma^{-1})(v_{j_1}^* \circ v_{j_2}^* \circ \ldots \circ v_{j_d}^*) = \prod_{r=1}^{d} \xi_{d_{j_r}}^{k_{j_r}} (v_{j_1}^* \circ v_{j_2}^* \circ \ldots \circ v_{j_d}^*). \tag{4.7}$$

If we chose the basis $x_1, x_2, ..., x_n$ of $(\mathbf{C}^n)^*$we can consider the elements of $Sym^d(\mathbf{C}^n)^*$ as homogenous polynomials of degree d in the variables $x_1, x_2, ..., x_n$. It follows from (4.7) that $v_{j_1}^* \circ v_{j_2}^* \circ \ldots \circ v_{j_d}^*$ is invariant w.r.t. $\rho(G)$ iff $\sum_{r=1}^{d} \frac{k_{j_r} \cdot m}{d_{j_r} \cdot} = m \cdot p$ for some $p \in \mathbf{N}$. For the computation of the in variant ring $\mathbf{K}[V]^{\rho(G)}$ it suffices to compute the eigenvectors of $\rho(\sigma)^T$ and form the products of them, considering the elements of $S(G)$ as degree vectors.

Theorem 21 *The polynomials* $\left(v_j^*\right)^{d_j}$ *and* $\prod_{j=1}^n \left(v_j^*\right)^{\alpha_j}$ *,*$\boldsymbol{\alpha} \in S(G)$*, in the variables* $x_1, x_2, ..., x_n$ *are primary and secondary invariants for* $\rho(G)$ *respectively..*

Proof. Since $v_1, v_2, ..., v_n$ are linearly independent, the common zeros of the linear forms $v_1^*, v_2^*, ..., v_n^*$, considered as polynomials in $x_1, x_2, ..., x_n$ equal $\{0\}$. The proof follows from the fact that for $\boldsymbol{\alpha} \in S(G)$ the products $\prod_{j=1}^n \left(v_j^*\right)^{\alpha_j}$ are linearly independent and the Hilbert series of $\mathbf{K}[V]^{\rho(G)}$ equals the Hilbert series of $\mathbf{K}[V]^{\rho'(G)}$. ∎

A set of primary and secondary invariants of $\rho(G)$ can be constructed from the solution set $S(\rho'(G))$ and the eigenvectors of $\rho(\sigma)^T$.

Algorithm *Invariants*$(\langle\sigma\rangle)$

In : The generator $\sigma \in GL_n(\mathbf{C})$ of a cyclic group G.
Out : Primary invariants $\theta_1, \theta_2, ..., \theta_n$ and secondary invariants $\eta_1, \eta_2, ..., \eta_r$.
begin
$\left(\xi_{d_1}^{k_1}, \xi_{d_2}^{k_2}, ..., \xi_{d_m}^{k_m}\right)$:= the eigenvalues of σ^{-1};
$(v_1, v_2, ..., v_m)$:= the eigenvectors of $(\sigma^{-1})^T$;
The eigenvectors are written w.r.t. the basis $x_1, x_2, ..., x_n$.
for $j := 1$ **to** n **do** $\theta_j = \left(v_j^*\right)^{d_j}$ **end**;
$m := 1$;
for $\boldsymbol{\alpha} \in S(G)$ **do**
. $\eta_m = \prod_{j=1}^n \left(v_j^*\right)^{\alpha_j}$;
. $m := m + 1$;
end;
return$(\{\theta_1, \theta_2, ..., \theta_n\} \{\eta_1, \eta_2, ..., \eta_r\})$;
end.

Example 19 *Let* $\sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ *and* $G = \langle\sigma\rangle$ *be the cyclic group of order 4. The eigenvalues of* σ *are* i *and* $-i$*. The corresponding eigenvectors of* σ^T *are* $\widehat{v_1} = \begin{pmatrix} i \\ 1 \end{pmatrix}$ *and* $\widehat{v_2} = \begin{pmatrix} -i \\ 1 \end{pmatrix}$*. The primary invariants are*

$$\begin{aligned} \theta_1 &= (ix+y)^4 = x^4 - 4ix^3y - 6x^2y^2 + 4ixy^3 + y^4, \\ \theta_2 &= (-ix+y)^4 = x^4 + 4ix^3y - 6x^2y^2 - 4ixy^3 + y^4. \end{aligned}$$

The solution set $S(G)$*equals* $\{(0,0), (1,1), (2,2), (3,3)\}$*. Hence secondary invariants are given by*

$$\begin{aligned} \eta_1 &= 1, \\ \eta_2 &= (ix+y)(-ix+y), \\ \eta_3 &= (ix+y)^2(-ix+y)^2, \\ \eta_4 &= (ix+y)^3(-ix+y)^3. \end{aligned}$$

We have the Hironaka decomposition

$$\mathbf{K}[x,y]^G = \mathbf{K}[\theta_1,\theta_2] \oplus \eta_2\mathbf{K}[\theta_1,\theta_2] \oplus \eta_3\mathbf{K}[\theta_1,\theta_2] \oplus \eta_4\mathbf{K}[\theta_1,\theta_2].$$

4.1.4 Abelian Groups

We extend the results of the previous two sections to all faithful representations of finite abelian groups. In the sequel let $G = \langle \sigma_1, ..., \sigma_t \rangle$ be a finite abelian group and $\rho : G \to GL_n(\mathbf{C})$ be a faithful representation and set $V = \mathbf{C}^n$. Since G is abelian, there exists a matrix T s.t. $T\rho(\sigma)T^{-1}$ is a diagonal matrix for each $\sigma \in G$. Let $\rho'(\sigma) := T\rho(\sigma)T^{-1}$ with $\rho'(\sigma_j) = diag(\xi_{d_1^{(j)}}^{k_1^{(j)}}, \xi_{d_2^{(j)}}^{k_2^{(j)}}, ..., \xi_{d_m^{(j)}}^{k_m^{(j)}})$ be the corresponding representation of G.

Proposition 25 *Let $e_1, e_2, ..., e_n$ be the canonical basis of V and let T be a matrix, which diagonalizes $\rho(G)$ simultaneously. Then, for $1 \leq j \leq n$, $T^{-1}e_j$ is an eigenvector for $\sigma \in G$.*

Proof. From

$$T\sigma_k T^{-1} \cdot e_j = \lambda \cdot e_j$$

for some eigenvalue of σ_k it follows that

$$\sigma_k(T^{-1} \cdot e_j) = \lambda(T^{-1} \cdot e_j).$$

Hence $T^{-1} \cdot e_j$ is an eigenvector of σ_k with eigenvector λ. ■

The main result is contained in the next theorem.

Theorem 22 *Assume $\rho'(\sigma_r) = diag(\xi_{d_1^{(r)}}^{k_1^{(r)}}, \xi_{d_2^{(r)}}^{k_2^{(r)}}, ..., \xi_{d_m^{(r)}}^{k_m^{(r)}})$ with $\gcd(k_l^{(r)}, d_l^{(r)}) = 1$, and let $m_l = \mathrm{lcm}(d_l^{(1)}, ..., d_l^{(t)})$ for $1 \leq t \leq r$. If $d_l^{(r)} = 1$ then set $k_l^{(r)} = 0$. Set $u^{(r)} = \left\lfloor \sum_{j=1}^n \frac{k_j^{(r)}}{d_j^{(r)}}(m_j - 1) \right\rfloor$ and $S^{(r)} = \{\varphi_{(d_1^{(r)},...d_n^{(r)})}(\boldsymbol{\alpha}) \mid \boldsymbol{\alpha} \in S\langle \sigma_r \rangle, \{m_1, m_2, ..., m_n\}, u^{(r)}\}$. Then with*

$$M = \bigcap_{j=1}^{t} S^{(j)}.$$

the monomials $x_1^{m_1}, x_2^{m_2}, ... x_n^{m_n}$ are primary invariants and $\left\{\prod_{l=1}^n x_l^{\alpha_j} \mid \alpha \in M\right\}$ is a set of secondary invariants for $\mathbf{K}[V]^G$.

Proof. Follows using the same argumentation as in the proof of Theorem 4.1.19. ■

One could also compute the intersection of the invariant rings $\mathbf{K}[V]^{\langle \sigma_j \rangle}$ with the algorithm *Intersection* in Section 3.2.

Algorithm *Invariants*$(\langle\sigma_1, ..., \sigma_t\rangle, T)$

In : The generators $\sigma_j \in GL_n(\mathbf{C})$ of an abelian group G in diagonalized form, a matrix T which diagonalizes σ_k.
Out : Primary invariants $\theta_1, ..., \theta_n$ and secondary invariants $\eta_1, ..., \eta_r$ of $\mathbf{K}[V]^G$.
begin
for $j := 1$ **to** n **do** $v_j^* = T^{-1} \cdot x_j$ **end** // consider v_j^* as polynomials in $x_1, x_2, ..., x_n$.
for $j := 1$ **to** n **do** $m_j := \operatorname{lcm}(d_l^{(1)}, ..., d_n^{(t)}); \theta_j := \left(v_j^*\right)^{m_j}$ **end**
$M = \bigcap_{r=1}^{t} S^{(r)}$;
for $\boldsymbol{\alpha} \in M$ **do**
. $\eta_{\boldsymbol{\alpha}} := \prod_{l=1}^{n} \left(v_j^*\right)^{\alpha_j}$;
end;
return$(\{\theta_1, ..., \theta_n\}, \{\eta_{\boldsymbol{\alpha}} \mid \boldsymbol{\alpha} \in M\})$;
end.

Example 20 *Let* $G = \langle diag(-1, -1, 1), diag(1, 1, i)\rangle$. *We have* $m_1 = 2, m_2 = 2, m_3 = 4$, *so* $u^{(1)} = \left\lfloor \frac{1}{2} + \frac{1}{2} + 0 \right\rfloor = 1$ *and* $u^{(2)} = \left\lfloor 0 + 0 + \frac{3}{4} \right\rfloor = 1. S^{(1)} = \{(0, 0, 2), (1, 1, 0)\}$ *and* $S^{(2)} = \{(1, 1, 0)\}$. *We obtain* $\theta_1 = x_1^2, \theta = x_2^2, \theta = x_3^4$ *as primary invariants and* $\eta_1 = 1, \eta_2 = x_1 x_2$ *as secondary invariants. Note that the Hilbert series equals*

$$H^G(t) = \frac{1 + t^2}{(1 - t^2)^2(1 - t^4)} = \frac{1}{(1 - t^2)^3}$$

but an hsop with degree $(2, 2, 2)$ *does not exist.*

4.1.5 Fundamental Invariants

Let G be a finite abelian group and $\rho : G \to GL_n(\mathbf{C})$ be a faithful representation. We assume that the solution set M according to Theorem 4.1.22 of the preceding section has already been computed and we set $F = M \cup \{(m_1, 0...), (0, m_2, ...), ..., (0, ..., 0, m_n)\}$. We call $\boldsymbol{\alpha} \in F$ **irreducible** iff $\boldsymbol{\alpha}$ cannot be written as the sum of two elements from F. Note that the primary and the secondary invariants form a set of fundamental invariants.

Proposition 26 *The set of all irreducible elements of* F *correspond to a set of fundamental invariants.*

Proof. Follows from the definition of fundamental invariants. ■

Example 21 *In Example 4.1.19 the elements* $\theta_1, \theta_2, \eta_2$ *are fundamental invariants for* G.

We obtain the following algorithm for the computation of fundamental invariants of a finite abelian group $G = \langle \sigma_1, ..., \sigma_t \rangle \leq GL_n(\mathbf{C})$.

Algorithm *FundamentalInvariants*$(\langle \sigma_1, ..., \sigma_t \rangle, T)$

In : The generators $\sigma_j \in GL_n(\mathbf{C})$ of an abelian group G in diagonalized form, a matrix T which diagonalizes σ_k.
Out : Fundamental invariants $h_1, h_2, ..., h_k$ of $\mathbf{K}[V]^G$.
begin
for $j := 1$ **to** n **do** $v_j^* = T^{-1} \cdot x_j$ **end** // consider v_j^*as polynomials in $x_1, x_2, ..., x_n$.
for $j := 1$ **to** n **do** $m_j := \mathrm{lcm}(d_l^{(1)}, ..., d_n^{(t)})$; **end**
$M = \bigcap_{r=1}^t S^{(r)}$;
$F =$ the set of all irreducible $\boldsymbol{\alpha}$ of M; $k := 1$;
for $\boldsymbol{\alpha} \in F$ **do**
. $h_k := \prod_{l=1}^n \left(v_j^*\right)^{\alpha_j}$;
. $k := k + 1$;
end;
return$(\{h_1, h_2, ..., h_k\})$;
end.

4.1.6 Relative Invariants

We want to compute the module of relative invariants of abelian groups w.r.t. their characters. Let $G = \langle \sigma \rangle$ be a cyclic group of order m with representation $\rho : G \to GL_n(\mathbf{C})$, s.t. $\rho(\sigma) = diag(\xi_{d_1}, \xi_{d_2}, ..., \xi_{d_n})$ and let $\chi : G \to \mathbf{C}\backslash\{0\}$ be a character of a one-dimensional representation of G. A monomial $\prod_{j=1}^n x_j^{\alpha_j}$ is a relative χ invariant iff

$$\rho(\sigma^{-1}) \cdot \prod_{j=1}^n x_j^{\alpha_j} = \chi(\sigma) \prod_{j=1}^n x_j^{\alpha_j}. \tag{4.8}$$

Let $\chi(\sigma) = \xi_m^s$, then (4.8) is satisfied iff

$$\sum_{j=1}^n \frac{\alpha_j m}{d_j} = p \cdot m + s \text{ for some } p \in \mathbf{Z}. \tag{4.9}$$

We call this equation the characteristic s equation of G w.r.t. k. It follows from the estimation

$$\sum_{j=1}^n \frac{m}{d_j}(d_j - 1) < m \cdot n < m \cdot n + s$$

that it is enough to solve $n-1$ such equations. In the sequel let $\rho : G \to GL_n(\mathbf{C})$ be a representation s.t. $\rho(\sigma) = diag(\xi_{d_1}^{k_1}, \xi_{d_2}^{k_2}, ..., \xi_{d_n}^{k_n})$ with $\gcd(k_j, d_j) = 1$.

Definition 42 *For $p \in \mathbf{N}_0$ we denote the set of solutions of the characteristic s equation of G w.r.t. p with $S_{p,s}(G,(d_1,...d_n)) := \{(\alpha_1,...,\alpha_n) \in \mathbf{N}_0^n \mid \sum_{j=1}^n \frac{\alpha_j \cdot n}{d_j} = m \cdot p + s, each\ \alpha_j < d_j \ for\ 1 \le j \le n\}$, and we define $S_s(G,(d_1,...d_n),t) := \bigcup_{p=0}^t S_{p,s}(G,(d_1,...d_n))$*

Proposition 27 *Let ρ' be a representation of G s.t. $\rho'(\sigma) = \langle diag(\xi_{d_1}, \xi_{d_2}, ..., \xi_{d_n}) \rangle$. Then the set $M = \{\prod_{j=1}^n x_j^{\beta_j} \mid (\beta_1,...,\beta_n) = \varphi_G(\alpha_1,...,\alpha_n)$ for $(\alpha_1,...,\alpha_n) \in S_s(G,(d_1,...d_n),n-1)\}$ is a $\mathbf{C}[x_1^{d_1}, x_2^{d_2}, ..., x_n^{d_n}]-$module basis of $\mathbf{C}[x_1,x_2,...,x_n]_\chi^G$.*

Proof. Follows with the same arguments as the proof of Theorem 4.1.19. ■

Example 22 *Let $G = \{1, \sigma, \sigma^2, \sigma^3\}$ with representation $\rho(\sigma) = diag(-1, i, -i)$ and character $\chi(\sigma) = i$. Primary invariants of G are given by x^2, y^4 and z^4, so we set $R = \mathbf{C}[x^2, y^4, z^4]$. We compute the $R-$module of relative χ invariants. So we have to solve the equations*

$$\begin{aligned} 2a_1 + a_2 + 3a_3 &= 3, \\ 2a_1 + a_2 + 3a_3 &= 7, \\ 2a_1 + a_2 + 3a_3 &= 11. \end{aligned}$$

The solutions are $(0,0,1), (0,3,0), (1,1,0), (0,1,2), (1,2,1), (1,3,2), (1,1,3)$. *Hence*

$$\mathbf{C}[x,y,z]_\chi^G = zR \oplus y^3R \oplus xyR \oplus yz^2R \oplus xy^2zR \oplus xy^3z^2R \oplus xyz^3R.$$

The generalization to abelian groups is analogous to Section 4.1.4.

4.2 A Glimpse of Noncommutative Invariant Theory

So far we have considered the induced action of a finite group G on the symmetric powers of V^* for a representation $\rho : G \to GL(V)$. In this section we investigate the induced action of G on the tensor and alternating powers of V^* for a complex vectorspace V of dimension n. In the first section we consider the action of G on the tensor algebra. In the second subsection we treat the exterior algebra.

4.2.1 Invariants of the Tensor Algebra

Let G be a finite group and $\rho : G \to GL_n(\mathbf{C})$ be a faithful complex representation. For $d \in \mathbf{N}$ we define the $d-$th tensor power of ρ^* by

$$\otimes^d \rho^*(\sigma)(v_1^* \otimes v_2^* \otimes ... \otimes v_n^*) := \rho^*(\sigma)(v_1^*) \otimes \rho^*(\sigma)(v_2^*) \otimes ... \otimes \rho^*(\sigma)(v_n^*).$$

We define a group action analogously to Section 2.1, namely

$$\begin{aligned} \bullet \quad &: \quad G \times \otimes^d V^* \to \otimes^d V^*, \\ \sigma \bullet (v_1^* \otimes v_2^* \otimes ... \otimes v_n^*) \quad &: \quad = \rho^*(\sigma)(v_1^* \otimes v_2^* \otimes ... \otimes v_n^*). \end{aligned}$$

Definition 43 *Let $x_1, x_2, ..., x_n$ be a basis of V^*. We define the finitely generated noncommutative $\mathbf{C}-$algebra $\mathbf{C}\langle V \rangle$ as*

$$\mathbf{C}\langle V \rangle := \bigoplus_{d=0}^{\infty} \otimes^d V^*.$$

*If we want to emphasize the selected basis, we denote $\mathbf{C}\langle V \rangle$ by $\mathbf{C}\langle x_1, x_2, ..., x_n \rangle$. The elements of $\mathbf{C}\langle V \rangle$ are called **noncommutative polynomials**. We set $\mathbf{C}\langle V \rangle_d = \otimes^d V^*$. If f is of the form $x_{i_1} \otimes x_{i_2} \otimes ... \otimes x_{i_d}$ then f is called a **monomial** of degree d. We abbreviate $\underbrace{v \otimes v \otimes ... \otimes v}_{d-\ times}$ with v^d. The degree vector of f is the degree vector of f considered as a commutative monomial. If it is clear from the context we omit the word 'noncommutative'.*

Definition 44 *Let $G \leq GL_n(\mathbf{C})$ be a finite group and be χ a linear character of G.*

$$\mathbf{C}\langle x_1, x_2, ..., x_n \rangle_\chi^G := \{ f \in \mathbf{C}\langle x_1, ..., x_n \rangle \mid \sigma \bullet f = \chi(\sigma) f \text{ for all } \sigma \in G \}.$$

*The elements of $\mathbf{C}\langle x_1, x_2, ..., x_n \rangle^G$ are called **relative-χ noncommutative invariants** w.r.t. G. We omit χ if it is the trivial character.*

Since noncommutativity destroys the symmetry among the 'variables' $x_1, x_2, ..., x_n$, we use an exponential generating function for the Hilbert series.

Definition 45 *The Hilbert series of $\mathbf{C}\langle V \rangle_\chi^G$ is the exponential power series*

$$H(\mathbf{C}\langle V \rangle_\chi^G, t) := \sum_{d=0}^{\infty} \dim_{\mathbf{C}}(\mathbf{C}\langle V \rangle_\chi^G)_d \cdot \frac{t^d}{d!}.$$

As in Chapter 2 we need some knowledge of the eigenvalues of the tensor power.

Lemma 15 *Let $\lambda_1, ..., \lambda_n$ be the eigenvalues of $\rho(\sigma^{-1})$. Then the eigenvalues of $\otimes^d \widehat{\rho}(\sigma)$ are the elements $\prod_{j=1}^n \lambda_j^{\alpha_j}$ for $(\alpha_1, ..., \alpha_n)$ s.t. $\sum_{j=1}^n \alpha_j = d$ with multiplicity $d! \cdot \prod_{j=1}^n \frac{1}{\alpha_j!}$.*

Proof. From Lemma 2.4.7 we know that the eigenvalues are given by $\prod_{j=1}^n \lambda_j^{\alpha_j}$. The multiplicities follow from the permutation rule of elementary combinatorics. ■

Theorem 23 *Let $G \leq GL_n(\mathbf{C})$ be a finite group and be χ a linear character of G. The Hilbert series of $\mathbf{C}\langle V\rangle_\chi^G$ is given by*

$$H(\mathbf{C}\langle V\rangle^G, t) = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma)\prod_{i=1}^n \exp(\lambda_{\sigma,i}\cdot t)$$

where $\lambda_{\sigma,i}$ denotes the i-th eigenvalue of $\sigma \in G$.

Proof. From the previous discussion we obtain

$$\begin{aligned}
H(\mathbf{C}\langle V\rangle^G, t) &= \sum_{d=0}^\infty \left\langle \chi_{\otimes^d\widetilde{\rho}}, \chi\right\rangle \cdot \frac{t^d}{d!} = \sum_{d=0}^\infty \frac{1}{|G|}\sum_{\sigma\in G}\chi_{\otimes^d\widetilde{\rho}}(\sigma)\chi(\sigma^{-1})\cdot\frac{t^d}{d!} \\
&= \sum_{d=0}^\infty \frac{1}{|G|}\sum_{\sigma\in G}\chi_{\otimes^d\rho}(\sigma^{-1})\chi(\sigma^{-1})\cdot\frac{t^d}{d!} \\
&= \sum_{d=0}^\infty \frac{1}{|G|}\sum_{\sigma\in G}\sum_{d_1+d_2\ldots+d_n=d}\prod_{i=1}^n\frac{1}{d_i!}\lambda_{\sigma,1}^{d_1}\lambda_{\sigma,2}^{d_2}\cdot\ldots\cdot\lambda_{\sigma,n}^{d_n}\chi(\sigma)\cdot t^d \\
&= \frac{1}{|G|}\sum_{\sigma\in G}\sum_{(d_1,d_2,\ldots,d_n)\in\mathbf{N}^n}\chi(\sigma)\prod_{i=1}^n\frac{\lambda_{\sigma,i}^{d_i}}{d_i!}\cdot t^{d_1+d_2\ldots+d_n} \\
&= \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma)\prod_{i=1}^n\exp(\lambda_{\sigma,i}\cdot t) \blacksquare
\end{aligned}$$

Example 23 *Let G be the 3 dim. permutation representation of S_3 (cf. the example in section 2.1). The Hilbert series of $\mathbf{C}\langle V\rangle^G$ is given by*

$$H(\mathbf{C}\langle V\rangle^G, t) = \frac{1}{6}\left(2 + 3\,e^t + e^{3\,t}\right).$$

If we expand $H^G(t)$ in a Taylor series we obtain

$$1+t+2\frac{t^2}{2!}+5\frac{t^3}{3!}+14\frac{t^4}{4!}+41\frac{t^5}{5!}+122\frac{t^6}{6!}+365\frac{t^7}{7!}+1094\frac{t^8}{8!}+3281\frac{t^9}{9!}+\mathrm{O}(t^{10}).$$

Figure 4.1:

Definition 46 *A subalgebra S of $\mathbf{C}\langle V\rangle$ is* ***finitely generated*** *iff there exists a finite set $f_1, ..., f_m \in S$, s.t. for each element $f \in S$ there exists a polynomial $p \in \mathbf{C}\langle y_1, y_2, ..., y_m\rangle$ s.t. $f = p(f_1, f_2, ..., f_m)$.*

In the sequel we examine the problem whether $\mathbf{C}\langle V\rangle^G$ is finitely generated as a $\mathbf{C}-$algebra.

Example 24 *Let $G = \langle diag(-1,-1)\rangle$. The commutative invariant ring of G equals $\mathbf{C}[V]^G = \mathbf{C}[x_1^2, x_2^2] \oplus x_1x_2\mathbf{C}[x_1^2, x_2^2]$. The Hilbert series of $\mathbf{C}\langle V\rangle^G$ equals $\frac{1}{2}(e^{2t}+e^{-2t}) = \cosh(2t)$, with Taylor expansion $1+4\frac{t^2}{2!}+16\frac{t4}{4!}+64\frac{t^6}{6!}+256\frac{t^8}{8!}+1024\frac{t^{10}}{10!}+\mathrm{O}(t^{11})$ The linearly independent noncommutative invariants of G of degree 2 are $x_1\otimes x_1, x_2\otimes x_2, x_1\otimes x_2, x_2\otimes x_1$. We claim that $\mathbf{C}\langle V\rangle^G$ is generated by the noncommutative invariants of degree 2. As in the proof of Noethers Finiteness Theorem (Theorem 2.3.10) is suffices to show that each monomial can be generated by the invariants of degree 2. Let $f \in \mathbf{C}\langle V\rangle^G$ be a monomial of degree $d > 2$, so $f = x_{i1}\otimes x_{i2}\otimes \overline{f}$ for some $i_1, i_2 \in \{1,2\}$ and $\overline{f} \in \mathbf{C}\langle V\rangle^G$ of degree $d-2$. Since $x_{i1}\otimes x_{i2}$ is invariant, the claim follows with induction on the degree.*

Example 25 *Let $G = \langle diag(I,-I)\rangle$. We have $H(\mathbf{C}\langle V\rangle^G, t) = \frac{1}{4}(2+e^{2t}+e^{-2t})$, which Taylor expansion $1+2\frac{t^2}{2!}+8\frac{t4}{4!}+32\frac{t^6}{6!}+128\frac{t^8}{8!}+512\frac{t^{10}}{10!}+\mathrm{O}(t^{11})$. The solutions of the characteristic equation w.r.t. 1 are $(4,0),(1,1),(0,4)$. We claim that the noncommutative invariant ring $\mathbf{C}\langle V\rangle^G$ is not finitely generated. The monomial $x_1^n x_2^{n+4}$ is a commutative invariant of G. We claim that for $n \in \mathbf{N}$ the noncommutative monomial*

$$f_n = x_2^3\otimes \underbrace{x_1\otimes x_2\otimes x_1\otimes x_2 ... x_1\otimes x_2}_{n-times}\otimes x_2$$

is an invariant, which cannot be written as a product of invariants of lower degree. In figure 4.1 a point with coordinates (a,b) *corresponds to the commutative monomial* $x^a y^b$, *and the points "•" correspond to the commutative invariants. We consider the monomial* f_1 *as a path in figure 4.1. With* x_1 *we denote a step to the right, while* x_2 *denotes a step to the left. The path of* f_1 *is indicated with "∘". Since* f_1 *meets (commutative) invariants only at the beginning and at the end, there exists no invariant in between, hence* f_1 *cannot be written as a product of invariants of smaller degrees. The same holds for* f_d, *since the noncommutative invariant monomials are just permutations of commutative invariant monomials w.r.t. the position of the variables* $x_1, x_2, ..., x_n$.

We can generalize the observation from the preceding examples.

Theorem 24 *Let* $n \geq 2$ *and* $G \leq GL_n(\mathbf{C})$ *be a finite abelian group. Then* $\mathbf{C}\langle V\rangle^G$ *is finitely generated as a noncommutative* $\mathbf{C}-$*algebra iff there exists* $\lambda \in \mathbf{C}$ *s.t.* $G = \langle \lambda \cdot I\rangle$.

Proof. Let $G = \langle \lambda \cdot I\rangle$ for some $\lambda \in \mathbf{C}$ and let $d \in \mathbf{N}$ be minimal s.t. $\lambda^d = 1$. The solutions of the characteristic equation $\sum_{j=1}^n \alpha_j = d$ of G w.r.t. 1 form a hyperplane in $\mathbf{N}^n$. If $f = x_{i1} \otimes x_{i_2} \otimes ... \otimes x_{i_m} \in \mathbf{C}\langle V\rangle^G$ is an invariant of degree $m > d$, then the degree vector of $x_{i1} \otimes x_{i_2} \otimes ... \otimes x_{i_d}$ satisfies the characteristic equation of G w.r.t. 1. Hence, $x_{i_1} \otimes x_{i_2} \otimes ... \otimes x_{i_d}$ is an invariant of degree $d < m$, and the claim follows from induction on d.
In order to show the converse we distinguish 2 base cases. In the first case $G = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & \xi_d^k \end{pmatrix} \right\rangle$ with $\gcd(k,d) = 1$ and $d > 1$. For any $t \in \mathbf{N}$ the monomial $y \otimes x^t \otimes y^{d-1}$ cannot be written as a polynomial in the invariants of smaller degree since y and y^{d-1} are not invariant. In the second case we assume that $G = \left\langle \begin{pmatrix} \xi_{d_1}^{k_1} & 0 \\ 0 & \xi_{d_2}^{k_2} \end{pmatrix} \right\rangle$ for some $d_j, k_j \in \mathbf{N}$ with $k_j > 1, \gcd(d_j, k_j) = 1$ for $j = 1,2$ and $d_1 \neq d_2$ or $d_1 = d_2$ and $k_1 \neq k \bmod d_1$. Let (α_1, α_2) be the greatest solution w.r.t. lexicographical order of the characteristic equation of G w.r.t. 1 s.t. $(\alpha_1, \alpha_2) < (d_1, 0)$. Set

$$f_n' = x_2^{d_2-1} \otimes \underbrace{x_1^{\alpha_1} \otimes x_2^{\alpha_2} \otimes x_1^{\alpha_1} \otimes x_2^{\alpha_2} \otimes ... \otimes x_1^{\alpha_1} \otimes x_2^{\alpha_2}}_{n-times}.$$

We claim that the monomial

$$f_n = f_n' \otimes x_2$$

is an invariant of degree $n(\alpha_1+\alpha_2)+d_2$ which cannot be written as a polynomial in the invariants of smaller degrees. The degree vector of f_n equals $(n\cdot\alpha_1, n\cdot\alpha_2+d_2)$, hence f is an invariant of degree $n(\alpha_1+\alpha_2)+d_2$. Since (α_1,α_2) and $(0,d_2)$ are solutions of the characteristic equation of G w.r.t. 1, the elements $(\alpha_1-\beta_1,\alpha_2-\beta_2)$ for $\beta_j<\alpha_j$ and $(n\cdot\alpha_1,n\cdot\alpha_2+d_2-1)$ are no solutions of the characteristic equation w.r.t. 1. Hence for any n the monomial f'_{n-1} is not invariant and, if we multiply from the right the monomials $x_1$and x_2 in such a way that we get f_n we never obtain an invariant before reaching f_n. It is clear that we have considered all possible cases for 2×2 matrices.
Let $G=\langle\sigma_1,\sigma_2,...,\sigma_k\rangle \le GL_n(\mathbf{C})$ be a finite abelian group which is already in diagonal form and let m_l denote the order of the roots of unity $(\sigma_1)_{ll},(\sigma_k)_{ll},...,(\sigma_k)_{ll}$. W.l.o.g. assume that $\sigma_1=diag(\xi_{d_1}^{k_1},\xi_{d_1}^{k_1},...)$ with $d_1\neq d_2$ or $d_1=d_2$ and $k_1\neq k \bmod d_1$. If we replace d_1 with m_1 and d_2 with m_2 and take $\boldsymbol{\alpha}$ as the lexicographic largest solution of all characteristic equations of $\langle\sigma_j\rangle$ w.r.t. 1, then f_n is an invariant of degree $n(\alpha_1+\alpha_2)+m_2$ which cannot be written as a polynomial in the invariants of smaller degree. ■

4.2.2 Invariants of the Exterior Algebra

We proceed in a similar way. Let G be a finite group and $\rho: G\to GL_n(\mathbf{C})$ be a complex representation. For $d\in\mathbf{N}$ we define the $d-$th exterior power of ρ^* by

$$\wedge^d\rho^*(\sigma)(v_1^*\wedge v_2^*\wedge ...\wedge v_n^*) := \rho^*(\sigma)(v_1^*)\wedge\rho^*(\sigma)(v_2^*)\wedge ...\wedge\rho^*(\sigma)(v_n^*).$$

We define a group action analogous to chapter 2, section 1, namely

$$\begin{aligned} * &: G\times\wedge^d V^*\to\wedge^d V^*, \\ \sigma*(v_1^*\wedge v_2^*\wedge ...\wedge v_n^*) &: =\rho^*(\sigma)\left(v_1^*\wedge v_2^*\wedge ...\wedge v_n^*\right)\end{aligned}$$

Definition 47 *Let $x_1,x_2,...,x_n$ be a basis of V^*. We define the finitely generated $\mathbf{C}-$algebra $\mathbf{C}^{alt}\langle V\rangle$ as*

$$\mathbf{C}^{alt}\langle V\rangle := \bigoplus_{d=0}^{\infty}\wedge^d V^*.$$

The elements of $\mathbf{C}^{alt}\langle V\rangle$ are called ***skewsymmetric polynomials****. We set $\mathbf{C}^{alt}\langle V\rangle_d=\wedge^d V^*$. If we want to emphasize the selected basis, we denote $\mathbf{C}^{alt}\langle V\rangle$ by $\mathbf{C}^{alt}\langle x_1,...,x_n\rangle$.*

Definition 48 *Let $G \leq GL_n(\mathbf{C})$ be a finite group and be χ a linear character of G.*

$$\mathbf{C}^{alt}_{\chi} \langle V \rangle^{G} := \left\{ f \in \mathbf{C}^{alt} \langle V \rangle \mid \sigma * f = \chi(\sigma) f \text{ for all } \sigma \in G \right\}.$$

*The elements of $\mathbf{C}^{alt} \langle V \rangle$ are called **relative-χ skewsymmetric invariants**. We omit χ if it is the trivial character. The Hilbert series of $\mathbf{C}^{alt} \langle V \rangle^{G}$ is the power series*

$$H(\mathbf{C}^{alt}_{\chi} \langle V \rangle^{G}_{\chi}, t) := \sum_{d=0}^{\infty} \dim_{\mathbf{C}} (\mathbf{C}^{alt}_{\chi} \langle V \rangle^{G})_d \cdot t^d.$$

Note that the algebra $\mathbf{C}^{alt} \langle V \rangle$ is a complex vectorspace of dimension 2^n, therefore the invariant ring $\mathbf{C}^{alt} \langle V \rangle^{G}$ is always finitely generated.

Lemma 16 *Let $\lambda_1, \lambda_2, ..., \lambda_n$ be the eigenvalues of $\rho(\sigma^{-1})$ and $d \leq n$. The eigenvalues of $\wedge^d \rho(\sigma)$ are given by $\prod_{j=1}^{d} \lambda_{i_j}$ for $1 \leq i_1 < ... < i_d \leq n$.*

Proof. Follows from Lemma 2.4.7 and from the fact that $v \wedge v = 0$ for any $v \in V$. ■

Theorem 25 *Let $G \leq GL_n(\mathbf{C})$ be a finite group. The Hilbert series of $\mathbf{C}^{alt} \langle V \rangle^{G}$ equals*

$$H(\mathbf{C}^{alt} \langle V \rangle^{G}, t) = \frac{1}{|G|} \sum_{\sigma \in G} \det(1 + \sigma t) \chi(\sigma).$$

Proof.

$$\begin{aligned} H(\mathbf{C}^{alt} \langle V \rangle^{G}, t) &= \sum_{d=0}^{\infty} \left\langle \chi_{\wedge^d \tilde{\rho}}, \chi \right\rangle \cdot t^d = \sum_{d=0}^{\infty} \frac{1}{|G|} \sum_{\sigma \in G} \chi_{\wedge^d \tilde{\rho}}(\sigma) \chi(\sigma^{-1}) \cdot t^d \\ &= \sum_{d=0}^{n} \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma) \sum_{1 \leq i_1 < ... < i_d \leq n} \prod_{j=1}^{d} \lambda_{\sigma, i_j} t^d \\ &= \frac{1}{|G|} \sum_{\sigma \in G} \det(1 + \sigma \cdot t) \chi(\sigma). \blacksquare \end{aligned}$$

.

Example 26 *Let G be the $3-$dimensional permutation representation of S_3 (cf. Example 4.2.23). The Hilbert series of $\mathbf{C}^{alt} \langle V \rangle^{G}$ equals*

$$H(\mathbf{C}^{alt} \langle V \rangle^{G}, t) = 1 + t.$$

A basis of $\mathbf{C}^{alt} \langle V \rangle^{G}$ as a vectorspace is given by $1, x_1 + x_2 + x_3$.

Example 27 *Let* $\sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ *and* $G = \langle \sigma \rangle$. *The Hilbert series of* $\mathbf{C}^{alt}\langle V \rangle^G$ *equals* $1 + t^2$, *and a basis of* $\mathbf{C}^{alt}\langle V \rangle^G$ *is given by* 1 *and* $x_1 \wedge x_2$. *Note that* $\sigma^{-1} * x_1 \wedge x_2 = -x_2 \wedge x_1 = x_1 \wedge x_2$.

Example 28 *Let* $G = \langle diag(i,i) \rangle$. *We have* $H(\mathbf{C}^{alt}\langle V \rangle^G, t) = 1$, *hence* $\mathbf{C}^{alt}\langle V \rangle^G = \mathbf{C}$.

4.3 Stanley's Summation Example

We follow the presentation of Stanley [38]. Let $g \in \mathbf{N}$, and define $\xi_g := \exp(2\pi i/g)$. We set

$$S(g) := \sum_{k=1}^{g} \frac{1}{\left|1 - \xi_g^k\right|^2}.$$

This is essentially the sum asked for in Hemperly [17]. Before we show how a closed form of $S(g)$ can be computed using invariant theory, we consider an example.

Example 29 *For* $g = 4$ *we obtain* $S(4) = \sum_{k=1}^{4} \frac{1}{\left|1-i^k\right|^2} = \frac{5}{4}$.

Since

$$S(g) = \sum_{k=1}^{g} \frac{1}{(1 - \xi_g^k)(1 - \xi_g^{-k})}$$

we consider the sum

$$F(g,t) = \frac{1}{g} \sum_{k=1}^{g} \frac{1}{(1 - \xi_g^k \cdot t)(1 - \xi_g^{-k} \cdot t)}$$

which is the Hilbert series of the group $G = \left\langle \begin{pmatrix} \xi_g & 0 \\ 0 & \xi_g^{-1} \end{pmatrix} \right\rangle$. Then we have

$$S(g) = \lim_{t \to 1} \left(g \cdot H^G(t) - \frac{1}{(1-t)^2} \right). \tag{4.10}$$

We need some additional information about $H^G(t)$ to evaluate the above limit. With the results of Section 4.1 we can compute the invariant ring of G, namely

$$\mathbf{C}[x,y]^G = \bigoplus_{k=0}^{g-1} x^k y^k \cdot \mathbf{C}[x^g, y^g].$$

From Proposition 2.5.15 we know that the Hilbert series of $\mathbf{C}[x,y]^G$ equals

$$H^G(t) = \sum_{k=0}^{g-1} \frac{t^{2k}}{(1-t^g)^2}.$$

Now we can evaluate (4.10), namely

$$\begin{aligned} S(g) &= \lim_{t\to 1}\left(g \cdot \sum_{k=0}^{g-1} \frac{t^{2k}}{(1-t^g)^2} - \frac{1}{(1-t)^2}\right) \\ &= \frac{g^2-1}{12}. \end{aligned}$$

For $g=4$ we obtain $\frac{4^2-1}{12} = \frac{5}{4}$, as expected.

We can generalize the above sum and consider

$$S_n(g) := \sum_{k=1}^{g} \frac{1}{\left|1-\xi_g^k\right|^{2n}}.$$

Then the corresponding group G is generated by the matrix M, which is defined as follows : Let $\sigma = \begin{pmatrix} \xi_g & 0 \\ 0 & \xi_g^{-1} \end{pmatrix}$, then $M := diag(\underbrace{\sigma, ..., \sigma}_{n-times})$. E.g.

$$\begin{aligned} S_2(g) &= (g^2-1)(g^2+11)/2^4\cdot 3^2 \cdot 5, \\ S_3(g) &= (g^2-1)(2g^4+23g^2+191)/2^6\cdot 3^3\cdot 5\cdot 7, \end{aligned}$$

cf. Stanley [38] for more details.

Generalization to Characters. We extend Stanley's approach to sums of the form

$$S(g) := \sum_{k=1}^{g} \frac{\xi_g^k}{\left|1-\xi_g^k\right|^{2}}.$$

With $\chi(\xi_g^k) = \xi_g^k$, we can proceed as above, and consider

$$F_\chi(g,t) = \frac{1}{g}\sum_{k=1}^{g} \frac{\chi(\xi_g^k)}{(1-\xi_g^k\cdot t)(1-\xi_g^{-k}\cdot t)}$$

which is the Hilbert series of the group $G = \left\langle \begin{pmatrix} \xi_g & 0 \\ 0 & \xi_g^{-1} \end{pmatrix} \right\rangle$ w.r.t. the character χ. i.e. $H_\chi^G(t) = F_\chi(g,t)$. Hence

$$S(g) = \lim_{t\to 1}\left(g\cdot H_\chi^G(t) - \frac{1}{(1-t)^2}\right).$$

With the results of Section 4.1.4 we can compute the module of relative χ invariants of G, namely

$$\mathbf{C}[x,y]^G_\chi = \bigoplus_{k=0}^{g-2} x^{k+1}y^k \cdot \mathbf{C}[x^g,y^g] \oplus y^{g-1} \cdot \mathbf{C}[x^g,y^g].$$

So the Hilbert series equals

$$H^G_\chi(t) = \frac{\left(\sum_{k=0}^{g-2} t^{2k+1} + t^{g-1}\right)}{\left(1-t^g\right)^2}.$$

Hence we have

$$\begin{aligned} S(g) &= \lim_{t\to 1}\left(g \cdot \frac{\left(\sum_{k=0}^{g-2} t^{2k+1} + t^{g-1}\right)}{\left(1-t^g\right)^2} - \frac{1}{(1-t)^2}\right) \\ &= \frac{1}{12}\left(g^2 - 6g + 5\right). \end{aligned}$$

Remark 5 *By the same token one can find a closed form for the sum*

$$S(g) = \sum_{k=1}^{g} \frac{\xi_g^{c\cdot k}}{\left|1-\xi_g^k\right|^2}$$

for $c \in \mathbf{N}$. *The corresponding character is* $\chi(\xi_g^{c\cdot k}) = \xi_g^{c\cdot k}$.

4.4 Theorem Proving in Projective Geometry

Basically there are two different kinds of methods for proving geometric theorems, namely coordinate dependent and coordinate independent methods. The article of D. Wang [45] provides a very good overview. We show how one can use invariant theory for proving theorems in projective geometry in a coordinate-free manner.

Invariant theory should not only be seen as a special case of representation and ring theory, as we have done it in the first three chapters, it should also be seen under the point of view of the "Erlanger Programm" of F. Klein (cf. Klein [26]). In this paradigm a geometric property is a property which is invariant under the corresponding transformation group. A polynomial in the coordinates corresponds to a geometric property if it is invariant under the action of the transformation group belonging to the geometry on the coordinates. Therefore invariant theory describes precisely the geometric properties which can be expressed by polynomials. It also provides a coordinate free notation for geometric facts which will lead us to the Grassmann-Cayley algebra. The Grassmann Cayley algebra can be seen as a systematic translation table for geometric facts given in synthetic form into algebraic expressions. According to Sturmfels (in the preface of the reprint Hilbert [20]), a nineteenth-century mathematician would consider invariant theory as the bridge between algebra and geometry.

We will introduce the Grassmann-Cayley algebra as a tool for describing suitable facts and theorems in projective geometry. There are two operations in the Grassmann-Cayley algebra, namely the join, denoted by "$\vee$" and the meet, denoted by "$\wedge$". Under a suitable geometric fact we understand a fact which can be expressed in the Grassmann-Cayley algebra. So we have the following diagram:

$$\begin{array}{c}\text{Admissible Geometric fact (theorem)}\\ \downarrow\\ \text{Grassmann-Cayley algebra}\\ \downarrow\\ \text{Bracket algebra}\\ \downarrow\\ \text{Polynomials}\end{array}$$

In section 1 we introduce the bracket algebra and the straightening algorithm, a necessary technical tool, then in section 2 we present the Grassmann Cayley algebra with the join and the meet. Finally, in section 3 we demonstrate the use of the Grassmann Cayley for geometry theorem proving.

Notation : By $\mathbb{P}(\mathbf{C}^d)$ we denote the $d-1$ dim. projective space over $\mathbf{C}^d$. For the sake of simplicity we only treat the case, where the ground-field is $\mathbf{C}$.

We follow the presentation in Sturmfels [43] and refer to (loc. cit.) for all proofs.

4.4.1 Bracket Algebra

Let $X = (x_{ij})$ be a generic $n \times d$ matrix and $\mathbf{C}[x_{ij}]$ be the ring of polynomials on X. The matrix X is a configuration of n vectors in $\mathbf{C}^d$ or of n points in $\mathbb{P}(\mathbf{C}^d)$. We let the group $SL_d(\mathbf{C})$ act on X via right multiplication and denote the action by "$\circ$". Which polynomials correspond to geometric properties in the spirit of F. Klein's "Erlanger Programm", i.e. properties that are invariant under the action "$\circ$" of $SL_d(\mathbf{C})$?

Definition 49 *Let* $\Lambda(n,d) := \{[\lambda_1,...,\lambda_d] : 1 \leq \lambda_1 < \lambda_2 < ... < \lambda_d \leq n\}$. *We abbreviate* $[\lambda_1,...,\lambda_d]$ *with* $[\lambda]$. *The map* $\phi_{n,d} : \mathbf{C}[\Lambda(n,d)] \to \mathbf{C}[x_{ij}]$,

$$[\lambda] \mapsto \det \begin{pmatrix} x_{\lambda_1 1} & x_{\lambda_1 2} & \dots & x_{\lambda_1 d} \\ x_{\lambda_2 1} & x_{\lambda_2 2} & \dots & x_{\lambda_2 d} \\ \vdots & \vdots & \ddots & \vdots \\ x_{\lambda_d 1} & x_{\lambda_d 2} & \dots & x_{\lambda_d d} \end{pmatrix}$$

is called the ***generic coordinatization****. The* ***bracket ring*** $\mathfrak{B}_{n,d} \leq \mathbf{C}[x_{ij}]$ *is the ring generated by all* $d \times d$ *minors of* X.

Example 30 *Let* $X = \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ \vdots & \vdots & \vdots \\ x_{61} & x_{62} & x_{63} \end{pmatrix}$ *be a configuration of* 6 *points in* $\mathbb{P}^2$. *Then*

$$\begin{aligned} \phi_{6,3}([1,4,6]) &= x_{11}x_{42}x_{63} - x_{11}x_{62}x_{43} - x_{41}x_{12}x_{63} + x_{41}x_{62}x_{13} + x_{61}x_{12}x_{43} \\ &\quad - x_{61}x_{42}x_{13} \end{aligned}$$

vanishes iff the points $1, 4, 6$ *are collinear.*

Note that the image of $\phi_{n,d}$ coincides with $\mathfrak{B}_{n,d}$, and, since the map $\phi_{n,d}$ is in general not injective, we have $\mathfrak{B}_{n,d} \simeq \mathbf{C}[\Lambda(n,d)]/I_{n,d}$,where $I_{n,d}$ denotes the kernel of $\phi_{n,d}$. The ideal $I_{n,d}$ is called the ideal of syzygies. In order to compute in $\mathfrak{B}_{n,d}$ we need an algorithm for normal-form computation modulo $I_{n,d}$, i.e. we need Gröbner bases !

Straightening Algorithm

This algorithm from A. Young is an important tool in representation theory. It provides the computation of a Gröbner basis for $I_{n,d}$ in a purely combinatorial way. We use lexicographic order on brackets, i.e. $[\lambda] \preceq [\mu]$ iff $[\lambda]$ is lexicographic smaller than $[\mu]$. E.g. $[1,2,3] \preceq [1,2,4]$. We denote the induced degree-reverse-lexicographic order on $\mathbf{C}[\Lambda(n,d)]$ also by $\preceq$ and call it the *tableaux order*.

Definition 50 *Let* $[\lambda^{(1)}],...,[\lambda^{(k)}] \in \mathbf{C}[\Lambda(n,d)]$ *s.t.* $[\lambda^{(1)}] \preceq ... \preceq [\lambda^{(k)}]$. *We write the monomial* $T = [\lambda^{(1)}] \cdot ... \cdot [\lambda^{(k)}]$ *as follows*

$$T = \begin{bmatrix} \lambda_1^{(1)} & \lambda_2^{(1)} & \dots & \lambda_d^{(1)} \\ \lambda_1^{(2)} & \lambda_2^{(2)} & \dots & \lambda_d^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{(k)} & \lambda_2^{(k)} & \dots & \lambda_d^{(k)} \end{bmatrix}$$

*The tableau T is **standard** iff all columns of T are sorted.*

Let $[\lambda^{(1)}] = [1\,2\,3], [\lambda^{(2)}] = [1\,4\,5], [\lambda^{(3)}] = [2\,3\,4]$ and $[\lambda^{(4)}] = [3\,5\,6]$ be monomials. Then the tableau $[\lambda^{(1)}][\lambda^{(3)}][\lambda^{(4)}]$ is standard while $[\lambda^{(1)}][\lambda^{(2)}][\lambda^{(3)}]$ is a non-standard tableau.

Definition 51 *For $\tau \in \Lambda(n,d)$ we define the **complement** of τ to be the unique tuple $\tau^* \in \Lambda(n, n-d)$ s.t. $\tau \cup \tau^* = \{1,2,...,n\}$ (where we consider the tuples as sets).*

Definition 52 *Let $s \in \{1,2,...,d\}, \alpha \in \Lambda(n, s-1), \beta \in \Lambda(n, d+1)$ and $\gamma \in \Lambda(n, d-s)$. The **van der Waerden syzygy***

$$[[\alpha\ \dot{\beta}\ \gamma]] := \sum_{\tau \in \Lambda(d+1,s)} sign(\tau,\tau^*) \cdot [\alpha_1...\alpha_{s-1}\,\beta_{\tau_1^*}...\beta_{\tau_{d+1-s}^*}] \cdot [\beta_{\tau_1}...\beta_{\tau_s}\,\gamma_1...\gamma_s]. \tag{4.11}$$

*It is called a **straightening syzygy** :$\Leftrightarrow$ $\alpha_{s-1} < \beta_{s+1}$ and $\beta_s < \gamma_1$.*

Example 31 *Let $n = 6$,$d = 3$ and $s = 2$. Therefore $\alpha \in \Lambda(6,1), \beta \in \Lambda(6,4)$,$\gamma \in \Lambda(6,1)$. Let $\alpha = [1], \beta = [2\,3\,4\,5]$ and $\gamma = [6]$, hence we obtain a straightening syzygy. The sum in 4.11 is taken over the set $\Lambda(4,2) = \{[1\,2],[1\,3],[1\,4],[2\,3],[2\,4],[3\,4]\}$. The corresponding van der Waerden syzygy equals*

$$\begin{aligned}[[1\ \dot{2}\dot{3}\dot{4}\dot{5}\ 6]] &= \underline{[1\,4\,5][2\,3\,6]} - [1\,3\,5][2\,4\,6] + [1\,3\,4][2\,5\,6] - [1\,2\,5][3\,4\,6] \\ &\quad + [1\,2\,4][3\,5\,6] - [1\,2\,3][4\,5\,6].\end{aligned}$$

The underlined tableau is the non-standard one.

Theorem 26 *The set $S_{n,d}$ of all straightening syzygies is a Gröbner basis for $I_{n,d}$.* ■

We present the first part of the proof of the following corollary because it provides useful information for the computation of $S_{n,d}$. For a complete proof we refer to Sturmfels and White [42].

Corollary 7 *The standard tableaux form a $\mathbf{C}-$vector-space basis for the bracket ring $\mathfrak{B}_{n,d}$.*

Proof. (First part). It is sufficient to show that each bracket polynomial is congruent to a linear combination of standard tableaux modulo $I_{n,d}$. Let $k \in \mathbf{N}$ and $T = [\lambda^1][\lambda^2]....[\lambda^k]$ be a non-standard tableau. Since there are only finitely many tableaux smaller than T we can use induction and assume that T is the smallest tableau which is not contained in the span of the standard tableaux. There exist $i \in \{2, ..., k\}$ and $s \in \{2, ..., d\}$ s.t.$\lambda_s^{i-1} > \lambda_s^i$. Let $\alpha = [\lambda_1^{i-1}\, \lambda_2^{i-1} \ldots \lambda_{s-1}^{i-1}], \beta = [\lambda_1^i\, \lambda_2^i \ldots \lambda_s^i\, \lambda_s^{i-1} \ldots \lambda_d^{i-1}]$ and $\gamma = [\lambda_{s+1}^i \ldots \lambda_d^i]$. Then the initial tableau of $[[\alpha\ \dot{\beta}\ \gamma]] = [\lambda^{i-1}][\lambda^i]$ and the polynomial $F = T - [\lambda^1]...[\lambda^{i-2}][\lambda^{i+1}]...[\lambda^k][[\alpha\ \dot{\beta}\ \gamma]]$ is congruent to T modulo $I_{n,d}$. Since $F \prec T$, F can be written as a linear combinations of standard tableaux. We omit the proof that the set of standard tableaux is linearly independent. ■

With α, β and γ as in the above proof we have

$$LT([[\alpha\ \dot{\beta}\ \gamma]]) = [\underbrace{\lambda_1^{i-1}\, \lambda_2^{i-1} \ldots \lambda_{s-1}^{i-1}}_{\alpha}\underbrace{\lambda_s^{i-1} \ldots \lambda_d^{i-1}}_{\beta_{s+1\ldots d+1}}][\underbrace{\lambda_1^i\, \lambda_2^i \ldots \lambda_s^i}_{\beta_{1\ldots s}}\underbrace{\lambda_{s+1}^i \ldots \lambda_d^i}_{\gamma}].$$

Thus we get the two conditions $\alpha_{s-1} < \beta_{s+1}$ and $\beta_s < \gamma_1$ that are satisfied by straightening syzygies. Note that $s > 1$ since there cannot be a non-standard tableau with a violation of the ordering in the first column. Since $[\lambda^{i-1}] < [\lambda^i]$ we can derive another condition which is important for computational purposes. We have $\lambda_j^{i-1} \leq \lambda_j^i$ for $1 \leq j \leq s-1$ and there exists a $j^* \in \{1, 2, ..., s-1\}$ s.t. $\lambda_{j^*}^{i-1} < \lambda_{j^*}^i$. We call a 3-tupel (α, β, γ) of brackets which satisfies all these three conditions a **straightening tupel.**

Corollary 8 *Let $M_{n,d} = \{[[\alpha\ \dot{\beta}\ \gamma]] : (\alpha, \beta, \gamma)$ is a straightening tupel w.r.t. n and $d\}$. For $n, d \in \mathbf{N}$ with $n \geq d$ we have*

$$M_{n,d} = S_{n,d}.$$

Proof. The set $M_{n,d}$ contains all possible non-standard quadratic tableaux. ■

Note that in general this Gröbner basis is not reduced.

Definition 53 *The normal form reduction w.r.t. $S_{n,d}$ is called the* ***straightening algorithm****.*

Example 32 *Let $n = 4$ and $d = 2$. In this case the ideal $I_{n,d}$ is principal. For $s = 1$ we have $\alpha \in \Lambda(4, 0), \beta \in \Lambda(4, 3), \gamma \in \Lambda(4, 1)$ and for $s = 2$ we have $\alpha \in \Lambda(4, 1), \beta \in \Lambda(4, 3)$ and $\gamma \in \Lambda(4, 0)$. Without any conditions on the brackets α, β and γ we would have to compute 32 van der Waerden syzygies but only one is non-trivial (i.e. nonzero). Taking only the first two conditions into account we were forced to compute 22 van der Waerden syzygies with the same result as above. If we apply all conditions we have to compute only one van der Waerden syzygy, which turns out to be the non-trivial one, namely $[[1\ \dot{2}\dot{3}\dot{4}]] = \underline{[1\,4][2\,3]} - [1\,3][2\,4] + [1\,2][3\,4]$. The underlined tableau is non-standard.*

Now we consider the invariant subring $\mathbf{C}[x_{ij}]^{SL_d(\mathbf{C})} = \{f \in \mathbf{C}[x_{ij}] \mid f = f \circ \sigma$ for all $\sigma \in SL_d(\mathbf{C})\}$ w.r.t. the induced action of $SL_d(\mathbf{C})$ on $\mathbf{C}[x_{ij}]$.

Theorem 27 *(First Fundamental Theorem of Invariant Theory)*

$$\mathbf{C}[x_{ij}]^{SL_d(\mathbf{C})} = \mathbf{C}[\Lambda(n,d)]/I_{n,d} = \mathfrak{B}_{n,d}. \blacksquare$$

From the above theorem we see that precisely the bracket polynomials correspond to geometric properties.

4.4.2 The Grassmann-Cayley Algebra

Originally it was developed by H. Grassmann as a calculus for linear varieties. It is an invariant algebraic formalism for expressing statements in synthetic projective geometry. We will show how one can prove and guess theorems of projective geometry using the Grassmann-Cayley algebra. For more details we refer to Zaddach [50].

Definition 54 *Let V be a $d-$dimensional $\mathbf{C}-$vectorspace.*

$$\Lambda(V) := \bigoplus_{k=0}^{d} \Lambda^k(V),$$

where $\Lambda^k(V)$ denotes the k-fold exterior product of V. We denote the exterior product (the "join") by "$\vee$" instead of "$\wedge$". In the sequel the symbol "$\wedge$" will be used for the "meet". This notation has geometric reasons and will become clear later.

Let $\{e_1, ..., e_d\}$ be a basis of V. Then the set $\{e_{j_1} \vee ... \vee e_{j_k} \mid 1 \leq j_1 < ... < j_d \leq d\}$ is a basis for $\Lambda^k(V)$.

Definition 55 *Let $a_1, ..., a_k \in V$, $a_l = \sum_{j=1}^{d} a_{lj} e_j$. The **join** of $a_1, ..., a_k$ equals*

$$a_1 \vee ... \vee a_k = \sum_{1 \leq j_1 < ... < j_d \leq k} \begin{vmatrix} a_{1j_1} & a_{1j_2} & \cdots & a_{1j_k} \\ a_{2j_1} & \cdots & \cdots & a_{2j_k} \\ \vdots & \vdots & \vdots & \vdots \\ a_{kj_1} & a_{kj_2} & \cdots & a_{kj_k} \end{vmatrix} e_{j_1} \vee ... \vee e_{j_d}.$$

*An element $A \in \Lambda^k(V)$ is an **extensor** of step k. The extensor A of step k is **decomposable** if it can be written in the form $a_1 \vee ... \vee a_k$ for some $a_1, ..., a_k \in V$. Furthermore $\overline{A} = span_{\mathbf{C}}\{a_1, ..., a_k\}$.*

Grassmann called the join the *"Progressive Product".* The important property of the join is contained in the next theorem.

Theorem 28 *Let $A = a_1 \vee ... \vee a_k, B = b_1 \vee ... \vee b_j$ be two extensors. Then the extensor $A \vee B$ is non-zero iff $\{a_1, ..., a_k, b_1, ..., b_j\}$ is linearly independent. Then we also have $\overline{A} + \overline{B} = \overline{A \vee B} = span\{a_1, ..., a_k, b_1, ..., b_j\}$.* ■

The decomposable non-zero elements of $\Lambda^k(V)$ correspond to $k-$dimensional subspaces of V. Let A denote such an element and consider the subspace $A^* = \{w \in V : A \vee w = 0\}$. All elements of $\overline{A}$ are contained in A^*. If w is not contained in $\overline{A}$ then the set $\{a_1, ..., a_k, w\}$ is linearly independent and from Theorem 4.4.28 we derive that $A \vee w \neq 0$. So we have $A^* = \overline{A}$.

Definition 56 *Let $A = a_1 \vee ... \vee a_j$ and $B = b_1 \vee ... \vee b_k$ be two extensors of step j and k with $j + k \geq d$. The **join** of A and B is*

$$A \wedge B = \sum_{\pi \in Sh \subset S_j} sign(\pi)[a_{\pi(1)}\, a_{\pi(2)} \ldots a_{\pi(d-k)}\, b_1 \ldots b_k] \cdot a_{\pi(d-k+1)} \vee \cdots \vee a_{\pi(j)}$$

with $Sh = \{\pi \in S_j : \pi(1) < \pi(2) < ... < \pi(d-k)$ and $\pi(d-k+1) < \pi(d-k+2) < ... < \pi(j)\}$. These permutations are called shuffles. A useful notation for signed sums over shuffles is the dotted notation. One puts dots over the shuffled vectors, with the summation and sign implicit. So the meet of A and B is equal to

$$A \wedge B = [\dot{a}_1\, \dot{a}_2\ \ldots\ \dot{a}_{d-k}\ b_1 \ldots b_k] \cdot \dot{a}_{d-k+1} \vee \cdots \vee \dot{a}_j\ .$$

Grassmann called the meet the *Regressive Product.* It corresponds to intersection of subspaces provided that they span the whole space V.

Theorem 29 *Let $A = a_1 \vee ... \vee a_j$ and $B = b_1 \vee ... \vee b_k$ be two extensors. Then $A \wedge B$ is an extensor and $A \wedge B \neq 0$ iff $\overline{A} + \overline{B} = V$. Furthermore we have $\overline{A \wedge B} = \overline{A} \cap \overline{B}$ and $A \wedge B = (-1)^{(d-k)(d-j)} B \wedge A$.* ■

Example 33 *Let $a_1, a_2, b_1, b_2 \in \mathbb{P}(\mathbf{C}^3)$ be distinct points (and not coordinates). We have $j = k = 2$ with $j + k \geq 3$ and $Sh = S_2$.*

$$(a_1 \vee a_2) \wedge (b_1 \vee b_2) = \sum_{\pi \in S_2} sign(\pi)[a_{\pi(1)}\, b_1\, b_2] \cdot a_{\pi(2)} =$$

$$= [a_1\, b_1\, b_2] \cdot a_2 - [a_2\, b_1\, b_2] \cdot a_1.$$

Definition 57 *The algebra* $(\Lambda(V), \vee, \wedge)$ *is the* ***Grassmann-Cayley algebra*** *of* V. *An element of* $(\Lambda(V), \vee, \wedge)$ *involving only* $\vee$ *and* $\wedge$ *is called a* ***simple*** *Grassmann-Cayley expression.*

Remark 6 *For proving theorems we are interested in Grassmann-Cayley expressions of step* 0 *or* d, *where* d *is the dimension of the vector-space* V. *If a Grassmann-Cayley expression* $C(a, b, ...)$ *has step* k, $0 < k < d$, *then* $C(a, b, ...) = 0$ *is equivalent to the following universal quantified statement of step* d *:*

$$\forall x_1, ..., x_{d-k} \in V : C(a, b, ...) \vee x_1 ... \vee x_{d-k} = 0. \tag{4.12}$$

It is sufficient to take $x_1, ..., x_{d-k}$ *from a basis of* V, *so* (4.12) *is equivalent to a finite conjunction of bracket statements.*

Algorithm *GCtoBrackets*$(C(a, b...))$

Input : Grassmann-Cayley expression $C(a, b...)$ of step 0.
Output : bracket polynomial for $C(a, b, ...)$.
1. Replace each occurrence of a subexpression $(a_1 \vee ... \vee a_j) \wedge (b_1 \vee ... \vee b_k)$ in C by $[\dot{a}_1, ..., \dot{a}_{d-k}, b_1, ..., b_k]\ \dot{a}_{d-k+1} \vee ... \vee \dot{a}_j$.
2. Simplify using associativity of $\vee$ and $\wedge$, write $C(a, b, ...)$ as linear combinations of simple Grassmann-Cayley expressions.
3. Extract bracket factors from each expression. For the remaining factors return to step 1.

It is time to apply these techniques in a concrete example.

Example 34 *Let* $V = \mathbb{P}(\mathbf{C}^3)$. *Consider the points* $a = (1, 0, 0), d = (0, 1, 0)$ *and let* $v_1 = (1, 2, 3)$ *and* $v_2 = (2, 1, 3)$. *We define* $b = a + v_1 = (2, 2, 3)$,$c = a + 2 \cdot v_1 = (3, 4, 6)$ *and* $e = d + 3 \cdot v_2 = (6, 4, 9)$. *Note that* $b = d + v_2$. *We want to express the fact that* b *is the intersection point of* $\overline{ac}$ *and* $\overline{de}$ *(or,equivalently, that* b *lies both on* $\overline{ac}$ *and* $\overline{de}$, *cf. the next section). We get the following Grassmann Cayley expression :*

$$((a \vee c) \wedge (d \vee e)) \vee b = 0.$$

Step 1 of GCtoBrackets *yields*

$$([c\, d\, e]a - [a\, d\, e]c) \vee b.$$

With step 2 we get

$$[c\, d\, e]a \vee b - [a\, d\, e]c \vee b.$$

The bracket $[cde]$ *evaluates to* -9 *and* $[ade]$*evaluates to* 9. *We have*

$$a \vee b \;=\; \begin{vmatrix} 1 & 0 \\ 2 & 2 \end{vmatrix} e_1 \vee e_2 + \begin{vmatrix} 1 & 0 \\ 2 & 3 \end{vmatrix} e_1 \vee e_3 + \begin{vmatrix} 0 & 0 \\ 2 & 3 \end{vmatrix} e_2 \vee e_3 = \\ 2 \cdot e_1 \vee e_2 + 3 \cdot e_1 \vee e_3$$

and

$$c \vee b = -2 \cdot e_1 \vee e_2 + -3 \cdot e_1 \vee e_3$$

so

$$-9 \cdot a \vee b - (9 \cdot c \vee b) = 0.$$

Applications of the Grassmann-Cayley Algebra

We can transform a Grassmann-Cayley expression in a bracket polynomial (algorithmically) which expresses a property. Since bracket polynomials are invariant w.r.t. $SL_d(\mathbf{C})$ they express a *geometric* property (according to F. Klein). We have the diagram :

$$\begin{array}{c} \text{(1) Suitable Geometric fact (theorem)} \\ \downarrow \\ \text{(2) Grassmann-Cayley algebra} \\ \downarrow \\ \text{(3) Bracket algebra} \\ \downarrow \\ \text{(4) Polynomials} \end{array}$$

The translation (1) $\leftrightarrow$ (2) is done by hand, (3) $\rightarrow$ (4) is obvious (apply $\phi_{n,d}$). The translation (4) $\rightarrow$ (3) is the statement of Theorem 4.4.27, (2) $\rightarrow$ (3) is done by the algorithm *GCtoBrackets*. The remaining translation (3) $\rightarrow$ (2) is the only difficult one and is called Cayley factorization. Here an algorithm exists only for a special case (the multilinear one), see White [46]

Cayley Factorization Problem : Find an algorithm which satisfies the following specification.
Input : A homogenous bracket polynomial $P(a, b, ...)$.
Output : A tableau T of minimal degree s.t. $P \cdot T = C$ for some simple Grassmann Cayley expression $C(a, b, ...)$.

We demonstrate this by two applications from Sturmfels [43] in the projective plane $\mathbb{P}(\mathbf{C}^2)$. From Theorem 4.4.28 and from Theorem 4.4.29 we obtain the following translations of geometric facts into the Grassmann Cayley algebra. For $a, b \in \mathbb{P}(\mathbf{C}^2)$ we denote the line through a and b with $\overline{ab}$.

Translation Let a, b, c, d be distinct points in $\mathbb{P}(\mathbf{C}^2)$. The line $\overline{ab}$ is represented by $a \vee b$. The intersection point of the lines $\overline{ab}$ and $\overline{cd}$ is represented by $(a \vee b) \wedge (c \vee d)$.

Conditions Let a, b, c, d be points in $\mathbb{P}(\mathbf{C}^2)$. The points a, b, c are collinear iff $a \vee b \vee c = 0$. The point c is contained in the line $\overline{ab}$ iff $(a \vee b) \wedge c = 0$. The points a, b are equal iff $a \vee b = 0$.

In the sequel we abbreviate $a \vee b$ with ab.

Example 35 *Let a, b, c, d, e, f be distinct points in $\mathbb{P}(\mathbf{C}^3)$.*

$$\begin{gathered}\text{The lines } \overline{ab}, \overline{cd} \text{ and } \overline{ef} \text{ are concurrent} \\ \downarrow \\ (a \vee b) \wedge (c \vee d) \wedge (e \vee f) = 0 \\ \downarrow \\ [a\,b\,e][d\,c\,f] - [a\,b\,f][d\,c\,e] = 0 \\ \downarrow \\ a_1 b_2 e_3 c_1 d_2 f_3 + a_1 b_2 e_3 d_1 c_2 f_3 + \ldots = 0\end{gathered}$$

Without Cayley factorization we can use the following scheme for proving theorems in projective geometry.

Proof Scheme :

- Express all conditions in Grassmann Cayley expressions $C_1, \ldots, C_k$.
- Transform $C_1, \ldots, C_k$ into bracket polynomials $P_1, \ldots, P_k$ in normal form.
- Compare P_i with P_j, if necessary, find non-degenerate conditions.

Theorem 30 *(Desargues). The following 2 conditions are equivalent :*
(a) The corresponding sides of 2 (non-degenerated) triangles meet in collinear points.
(b) The lines spanned by the corresponding vertices are concurrent.

Proof. Let a, b, c and d, e, f denote the two non-degenerate triangles. We express part (a) in terms of the Grassmann-Cayley algebra and obtain

$$((a \vee b) \wedge (d \vee e)) \vee ((b \vee c) \wedge (e \vee f))) \vee ((a \vee c) \wedge (d \vee f)).$$

With the algorithm *GCtoBrackets* we transform the above expression into a bracket polynomial. Step 1 yields

$$([ade]b - [bde]a) \vee ([bef]c - [cef]b) \vee ([adf]c - [cdf]a).$$

Expansion gives

$([ade]b\vee[bef]c-[ade]b\vee[cef]b-[bde]a\vee[bef]c+[bde]a\vee[cef]b)\vee([adf]c-[cdf]a) =$

$([ade][bef]b\vee c-[ade][cef]b\vee b-[bde][bef]a\vee c+[bde][cef]a\vee b)\vee([adf]c-[cdf]a) =$

$$[ade][bef][adf]b\vee c\vee c-[bde][bef][adf]a\vee c\vee c+[bde][cef][adf]a\vee b\vee c-$$
$$[ade][bef][cdf]b\vee c\vee a-[bde][bef][cdf]a\vee c\vee a+[bde][cef][cdf]a\vee b\vee a.$$

From Theorem 4.4.28 we know that $b\vee c\vee c = a\vee c\vee c = a\vee c\vee a = a\vee b\vee a = 0$. For the remaining 2 extensors we have $a\vee b\vee c = [abc]e_1\vee e_2\vee e_3$ and $b\vee c\vee a = [bca]e_1\vee e_2\vee e_3$. Since we have identified $e_1\vee e_2\vee e_3$ with 1 we obtain

$$[bde][cef][adf][abc]-[ade][bef][cdf][bca]. \tag{4.13}$$

The application of the straightening algorithm to (4.13) yields

$$[abc][abc][def][def]-[abc][abe][cdf][def] \qquad \text{(a)}$$
$$-[abc][acb][bef][def]+[abc][ace][bdf][def]. \tag{4.14}$$

For part (b) we proceed as above obtain the Grassmann-Cayley expression

$$(a\vee d)\wedge(b\vee e)\wedge(c\vee f)$$

which transforms in the bracket polynomial

$$[acf][bde]-[abe][cdf]$$

with normal form

$$[ace][bdf]-[acd][bef]-[abe][cdf]-[abc][def]. \qquad \text{(b)}$$

At the moment we have (4.14) $\neq$ (4.15) , so there is something missing. Note the monomial $[abc][def]$ vanishes iff one (or both) triangles are degenerated, which we have excluded by assumption.. We have

$$\begin{aligned}
[ace][bdf]-[acd][bef]-[abe][cdf]-[abc][def] &= 0\\
&\Longleftrightarrow\\
[abc][def]\left([ace][bdf]-[acd][bef]-[abe][cdf]-[abc][def]\right) &= 0\\
&\Longleftrightarrow
\end{aligned}$$

$[abc][abc][def][def]-[abc][abe][cdf][def]-[abc][acb][bef][def]$
$+[abc][ace][bdf][def]=0$
which is the same as

$(a\vee b\wedge d\vee e)\vee(b\vee c\wedge e\vee f)\vee(a\vee c\wedge d\vee f) = 0 \Longleftrightarrow (a\vee d)\wedge(b\vee e)\wedge(c\vee f) = 0.$ ■

If a Cayley factorization were available, then bracket polynomial (4.14) could be rewritten as

$$[abc][def] \cdot ((a \vee d) \wedge (b \vee e) \wedge (c \vee f)) .$$

We would get the condition (b) from the theorem and the degenerate condition from the algorithm. This means that with a Cayley factorization one could construct new theorems in the following way :

Theorem Construction :

- Starting from a configuration of points $a, b, ...$, construct a Grassmann Cayley expression $C(a, b, ...)$ for the condition.
- Transform $C(a, b, ...)$ with the *GCtoBrackets* and the straightening algorithm in a bracket polynomial P which is in normal form.
- Apply Cayley factorization to P.

Example 36 *Discovering and proving geometric theorems :*
Let $a, b, c, d, e, f \in \mathbb{P}(\mathbf{C}^3)$. Under which "geometric" condition lie a, b, c, d, e, f on a common quadric ? A quadric $\sum_{i+j+k=2} v_{ijk} x^i y^j z^k$ is determined by the coefficients v_{ijk}. So we can reformulate our problem as follows. Find a synthetic interpretation or construction for the algebraic condition :

$$\begin{aligned}
\exists(v_{200}, v_{020}, v_{002}, v_{110}, v_{101}, v_{011}) \quad &\in \quad \mathbf{C}^6 \backslash \{0\} : \\
v_{200}a_1^2 + v_{020}a_2^2 + v_{002}a_3^2 + v_{110}a_1a_2 + v_{101}a_1a_3 + v_{011}a_2a_3 \quad &= \quad 0, \\
&\quad\ \ \vdots \\
v_{200}f_1^2 + v_{020}f_2^2 + v_{002}f_3^2 + v_{110}f_1f_2 + v_{101}f_1f_3 + v_{011}f_2f_3 \quad &= \quad 0.
\end{aligned}$$

Our goal is to compute a simple Grassmann-Cayley expression . In the first step we eliminate the coefficients v_{ijk}.

$$\det \begin{pmatrix} a_1^2 & a_2^2 & a_3^2 & a_1a_2 & a_1a_3 & a_2a_3 \\ b_1^2 & b_1^2 & b_1^2 & b_1b_2 & b_1b_3 & b_2b_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ f_1^2 & f_1^2 & f_1^2 & f_1f_2 & f_1f_3 & f_2f_3 \end{pmatrix} = 0. \tag{4.15}$$

The resulting polynomial has degree 12 *and* 720 *monomials and is invariant w.r.t. $SL_d(\mathbf{C})$. It follows from Theorem 27 that it can be written as a bracket polynomial. Using the straightening algorithm we find that* (4.15) *is equivalent to*

$$[abc][ade][bdf][cef] + [abd][ace][bcf][def] = 0. \tag{4.16}$$

Now we have to find a simple Grassmann-Cayley expression $C(a,b,c,d,e,f)$*, whose expansion equals* (4.16) *. In our example Cayley factorization yields (in a non-algorithmic way !) :*

$$((a \vee b) \wedge (d \vee e)) \vee ((b \vee c) \wedge (e \vee f)) \vee ((c \vee d) \wedge (f \vee a)) = 0.$$

This Grassmann Cayley expression is equivalent to the following synthetic statement :

The intersection points $\overline{ab} \cap \overline{de}, \overline{bc} \cap \overline{ef}, \overline{cd} \cap \overline{fa}$ *are collinear.*

This is precisely the contents of Pascal's Theorem.

4.4.3 The `GCAlg` Package

`GCAlg` is a Mathematica package for the bracket and Grassmann Cayley algebra. It provides algorithms for the construction of Grassmann Cayley expressions, for the transformation of Grassmann Cayley expressions into bracket polynomials, and for the manipulation of bracket polynomials, e.g. the straightening algorithm. It can be used for proving theorems of projective geometry with the proof scheme of section 4.4.2.No Cayley factorization is implemented.

Bracket Algebra

Data Types

`BracketT[`i_1`,`i_2`,...]`

Represents the bracket monomial $[i_1\ i_2\ ...]$.

`BracketPolynomialT`

Denotes the fact that a polynomial in BracketT can be used. Not implemented.

Algorithms

`BPrint[B_BracketPolynomialT]`

> returns the bracket polynomial. In order to print a bracket polynomial `B` in an compound statement, use `Print[BPrint[B]];`

`Bracket[`$\{i_1, i_2, ...\}$`]`

Constructs the bracket $[i_1\ i_2\ ...]$.

`Bracket[`B`_BracketPolynomialT]`

Sorts the brackets of B, i.e. $[2\ 1\ 3]$ is transformed to $-[1\ 2\ 3]$.

`Phi[`n,d`][`B`_BracketPolynomialT,x]`

Application of the generic coordinatization map $\phi_{n,d}(B)$, cf. definition 4.4.49. `x` is a variable.

`StraighteningSyzygies[`n, d`]`
  $>$ a list of all straightening syzygies w.r.t. n and d.
`VdWSyz[`n`][`α`_BracketT, `β`_BracketT, `γ`_BracketT]`
  Computes the corresponding van der Waerden syzygy, cf. definition

Grassmann Cayley Algebra

Data Types
`ExtT[`$\mathtt{i}_1$`,`$\mathtt{i}_2$`,...,`$\mathtt{i}_k$`]`
  Represents the extensor $i_1 \vee i_2 \vee ... \vee i_k$. of step k.
`JoinT[A,B]:`
  Denotes the join of the simple Grassmann Cayley expressions A and B.
`MeetT[A,B]:`
  Denotes the meet of the simple Grassmann Cayley expressions A and B.
  Algorithms
`GCPrint[A]`
  $>$ returns the Grassmann Cayley expression `A`. In order to print
  `A` in an compound statement, use `Print[GCPrint[A]]`;
Extensor`[`$\mathtt{i}_1$`,`$\mathtt{i}_2$`,...,`$\mathtt{i}_k$`]`
  The exteonsor formed from the points $\mathtt{i}_1$`,`$\mathtt{i}_2$`,...,`$\mathtt{i}_k$.
`JoinGC[A,B]`
  The join of of the simple Grassmann Cayley expressions A and B.
`Meet[A,B]`
  The meet of of the simple Grassmann Cayley expressions A and B.
`GCtoBrackets[`d`][`A`]`
  Transforms the simple Grassmann Cayley expression gc to a bracket
  polynomial. The entries in the brackets are the integers occuring in gc.

4.4.4 A Semi-automatic Proof of the Theorem of Desargues

We show how one can prove the Theorem of Desargues with the Mathematica package `GCAlg`. Compare the proof below with the proof of the Theorem in section 4.4.2 (Theorem 4.4.30).

We load the package and define the 6 points (labelled as $1, 2, 3, 4, 5, 6$).

```
<<GCAlg.m
a = Extensor[1];
b = Extensor[2];
c = Extensor[3];
d = Extensor[4];
```

```
e = Extensor[5];
f = Extensor[6];
```

We form the corresponding lines.

```
ab = JoinGC[a,b];
ac = JoinGC[a,c];
bc = JoinGC[b,c];
de = JoinGC[d,e];
df = JoinGC[d,f];
ef = JoinGC[e,f];
```

Now we compute the intersection points.

`p1 = Meet[ab,de]; GCPrint[p1]`

$(\mathbf{1} \vee \mathbf{2}) \wedge (\mathbf{4} \vee \mathbf{5})$

`p2 = Meet[ac,df]; GCPrint[p2]`

$(\mathbf{1} \vee \mathbf{3}) \wedge (\mathbf{4} \vee \mathbf{6})$

`p3 = Meet[bc,ef]; GCPrint[p3]`

$(\mathbf{2} \vee \mathbf{3}) \wedge (\mathbf{5} \vee \mathbf{6})$

We now formulate the condition C_1 that p_1,p_2,p_3 are collinear (condition (a) in Theorem 4.4.30).

```
tc1 = JoinGC[p1,p2];
C1 = JoinGC[tc1,p3]; GCPrint[C1]
```

$(\mathbf{1} \vee \mathbf{2}) \wedge (\mathbf{4} \vee \mathbf{5}) \vee (\mathbf{1} \vee \mathbf{3}) \wedge (\mathbf{4} \vee \mathbf{6}) \vee (\mathbf{2} \vee \mathbf{3}) \wedge (\mathbf{5} \vee \mathbf{6})$

We transform C_1 in a bracket polynomial.

`bp1 = Bracket[GCtoBrackets[3][C1]; BPrint[bp1]`

[1 2 3] [1 4 5] [2 5 6] [3 4 6] [1 2 3] [1 4 6] [2 4 5] [3 5 6]

We compute a Gröbner bases and apply the straightening algorithm to bp_1.

```
gb = StraighteningSyzygies[6,3];
vars = Brackets[6,3];
B1 = Straighten[gb][bp1,vars]; BPrint[B1]
```

- [1 2 3] [1 3 5] [2 4 6] [4 5 6] + [1 2 3] [1 3 4] [2 5 6] [4 5 6] + [1 2 3] [1 2 5] [3 4 6] [4 5 6] + [1 2 3]^2 [4 5 6]^2

Now we formulate the condition that the lines spanned by the corresponding vertices are concurrent.

```
ad = JoinGC[a,d];
be = JoinGC[b,e];
cf = JoinGC[c,f];
de = JoinGC[d, e];
df = JoinGC[d, f];
ef = JoinGC[e, f];
tc2 = Meet[ad,be];
C2 = Meet[tc2,cf]; GCPrint[C2]
```

$((\mathbf{1} \vee \mathbf{4}) \wedge (\mathbf{2} \vee \mathbf{5})) \wedge (\mathbf{3} \vee \mathbf{6})$

We transform `C2` in a bracket polynomial.

```
bp2 = Bracket[GCtoBrackets[3][C2]; BPrint[bp2]
```

[1 3 6] [2 4 5] - [1 2 5] [3 4 6]

We apply the straightening algorithm to `bp2`.

```
B2 = Straighten[gb][bp2,vars]; BPrint[B2]
```

[1 3 5] [2 4 6] - [1 3 4] [2 5 6] - [1 2 5] [3 4 6] - [1 2 3] [4 5 6]

We construct the factor F and check if `B1` equals `F*B2`.

```
F = Bracket[{1,2,3}] * Bracket[{4,5,6}];
B1 == Expand[F * B2]
```

True

4.4.5 Grassmannians

In section 1 we have constructed a Gröbner basis for $I_{n,d}$ in a purely combinatorial way, but we mention that there is a rich geometry associated with $I_{n,d}$. The variety of the ideal $I_{n,d}$ is called the Grassmann variety or Grassmannian $G_{n,d}$ which corresponds to the set of $k-$dimensional subspaces of $\mathbf{C}^n$. We briefly describe the first non-trivial Grassmannian, which turns out to be $G_{4,2}$. As we will see a point on $G_{4,2}$ corresponds to a decomposable extensor of step two (this generalizes to all Grassmannians $G_{n,d}$, i.e. the points correspond to decomposable extensors of step d). The vector space $\Lambda^2\mathbf{C}^4$ has dimension six and a basis is given by $\{e_1 \vee e_2, e_1 \vee e_3, e_1 \vee e_4, e_2 \vee e_3, e_2 \vee e_4, e_3 \vee e_4\}$ provided that $\{e_1, ..., e_4\}$ is a basis of $\mathbf{C}^4$. Let $a, b \in \mathbf{C}^4$, then $a \vee b \neq 0$ iff the subspaces (lines) generated by a and b have only the trivial intersection, namely the zero vector. It is then clear that they represent a line in $\mathbb{P}(\mathbf{C}^4)$. If we multiply a and b by (different) non-zero scalars we get back the same line, so $a \vee b$ should be the "same" as $\lambda \cdot a \vee b$. According to definition of the join, $a \vee b$ has coordinates $(x_1, x_2, ..., x_6)$, namely

$$\begin{aligned}
x_1 &= a_1b_2 - a_2b_1, \\
x_2 &= a_1b_3 - a_3b_1, \\
x_3 &= a_1b_4 - a_4b_1, \\
x_4 &= a_2b_3 - a_3b_2, \\
x_5 &= a_2b_4 - a_4b_2, \\
x_6 &= a_3b_4 - a_4b_3.
\end{aligned}$$

This is exactly the condition which an extensor $x \in \Lambda^2\mathbf{C}^4$ has to fulfill if it is simple. Since multiplication by scalars does not affect points in a projective space we construct a map from the set of lines in $\mathbb{P}(\mathbf{C}^4)$ into $\mathbb{P}(\Lambda^2\mathbf{C}^4)$.

$$\psi : \{\text{lines in } \mathbb{P}(\mathbf{C}^4)\} \longrightarrow \mathbb{P}(\Lambda^2\mathbf{C}^4),$$

$$(a, b) \longmapsto a \vee b.$$

The map ψ is called the Plücker embedding. The above equations can also be seen as a parameterization of the projective variety $G_{4,2}$ in $\mathbb{P}(\Lambda^2\mathbf{C}^4)$. We compute a Gröbner basis G for by $G_{4,2}$ by implicitation and obtain

$$G = [x_1x_6 - x_2x_5 + x_3x_4].$$

The monomial x_1x_6 corresponds to the bracket $[12][34]$, $-x_2x_5$ corresponds to $-[13][24]$ and x_3x_4 corresponds to $[14][23]$. This is exactly the Gröbner basis for $I_{4,2}$ in $\mathbf{C}[\Lambda(4, 2)]$ produced by the straightening algorithm as we have seen in Example 4.4.32. The straightening algorithm uses the additional structure information of the ideal $I_{n,d}$ for constructing a Gröbner basis in a purely combinatorial way.

Chapter 5

My `Invariants` Package

This Mathematica package provides an environment for computing examples in invariant theory of finite groups. It provides basic tools for working with finite matrix groups, polynomials and contains implementations of Kemper's optimal algorithm and the intersection algorithm. Almost all examples in this thesis have been computed with this package.

Limitations :

- The field **K** can be a finite extension of **Q** or a field with p elements for a prime p.
- The order of the matrix groups should not be too large (> 1000).
- Roots of unity can cause restrictions in practical computations (due to Mathematica).
- The algorithm `SecondaryInvariants` is only implemented in the nonmodular case.

5.1 Variables and Trace

VARIABLES

Stores a set of variables. If an algorithm from below is called without variables, then it will use `VARIABLES`.

`Profile[AlgName]`

Shows a profile of the running time for the algorithm `AlgName`.

See the description below for the algorithms, which provide this feature.

`Reset[AlgName]`

Before `Profile[AlgName]` is used, `Reset[AlgName]` must be called to reset the counters.

`SetVariables[{`$\mathtt{x}_1, \mathtt{x}_2, ..., \mathtt{x}_n$`}]`

Assigns $\{\mathtt{x}_1, \mathtt{x}_2, ..., \mathtt{x}_n\}$ to `VARIABLES`.

`ShowTrace[AlgName]`

Enables/Disables the trace for the algorithm `AlgName`.

See the description below for the algorithms, which provide this feature.

5.2 Data Types

Matrix Groups :

`MatrixGroupT[{`M_1,M_2, ...,M_k`}, p, finite]`

Represents the matrix group with the elements {M_1,M_2, ...,M_k} $\leq GL_n(\mathbf{K})$.

`p` is the characteristic of the field $\mathbf{K}$. Note that this is already a group.

`MatrixGroupT[GenT[`G_1,G_2, ...,G_k`], p, finite]`

Represents the matrix group which is generated by .the matrices G_1,G_2, ...,G_k $\in GL_n(\mathbf{K})$..

`p` is the characteristic of the field $\mathbf{K}$.

5.3 Algorithms

Invariant Theory :

`DegSecInvars[G_MatrixGroupT,{`$\theta_1, \theta_2, ..., \theta_n$`},{`$x_1, x_2, ..., x_n$`}:{},t_Symbol]`

$>$ the polynomial $H^G(t)/H(\mathbf{K}[\theta_1, \theta_2, ..., \theta_n], t)$.

The generating function for the secondary invariants of `G`. The coefficient of t^d equals the number of linearly independent secondary

invariants of degree d.

`DegSecInvars[hs_,{`$\theta_1, \theta_2, ..., \theta_n$`},{`$x_1, x_2, ..., x_n$`}:{},t_Symbol]`

$>$ the polynomial `hs`$/H(\mathbf{K}[\theta_1, \theta_2, ..., \theta_n], t)$.

`hs` is the Hilbert series of the invariant ring with primary invariants {$\theta_1, \theta_2, ..., \theta_n$}.

`HilbertSeries[G_MatrixGroupT,t_Symbol]`

$>$ the Hilbert series $H^G(t)$.

The characteristic of $\mathbf{K}$ is 0 or relative prime to $|$`G`$|$.

`HilbertSeries[G_MatrixGroupT,`χ`,t_Symbol]`

$>$ the Hilbert series $H^G_\chi(t)$.

Only for $characteristic(\mathbf{K}) = 0$.

`HilbertSeries[G_MatrixGroupT,t_Symbol,NC]`

$>$ the Hilbert series of the noncommutative invariant ring $\mathbf{K}\left\langle x_1, x_2, ..., x_n\right\rangle^G$.

Only for $characteristic(\mathbf{K}) = 0$.

`HilbertSeries[G_MatrixGroupT,t_Symbol,ALT]`

$>$ the Hilbert series of the noncommutative invariant ring $\mathbf{K}^{alt}\left\langle x_1, x_2, ..., x_n\right\rangle^G$.

Only for $characteristic(\mathbf{K}) = 0$.

`HomogenousInvariants[G_MatrixGroupT,d_Integer,vars_List]`
$>$ a basis of the $\mathbf{K}-$vectorspace $\left(\mathbf{K}[x_1, x_2, ..., x_n]^G\right)_d$.
If `G` contains an element list, then the Reynolds operator is applied (nonmodular case). If `G` is represented by generators the algorithm does not use the Reynolds operator. This is recommended for matrix groups with more than 50 elements (and mandatory in the modular case).

`HomogenousInvariants[R_,d_Integer,vars_List]`
$>$ a basis of the $\mathbf{K}-$vectorspace $\left(\mathbf{K}[x_1, x_2, ..., x_n]^G\right)_d$.
`R` is the Reynolds operator of `G`.

`HomogenousInvariants[G_MatrixGroupT,d_Integer,vars_List]`
$>$ a basis of the $\mathbf{K}-$vectorspace $\left(\mathbf{K}[x_1, x_2, ..., x_n]^G\right)_d$.
If `G` contains an element list, then the Reynolds operator is applied (nonmodular case). If `G` is represented by generators the algorithm does not use the Reynolds operator. This is recommended for matrix groups with more than 50 elements (and mandatory in the modular case).

`Invariants[G_MatrixGroupT,{`$\mathtt{x}_1, \mathtt{x}_2, ..., \mathtt{x}_n$`}:{}]`
$> \{f_1, f_2, ..., f_m\}$
A set of fundamental invariants for the ring $\mathbf{K}[x_1, x_2, ..., x_n]^G$.
Works only in the nonmodular case. This is an implementation of Noether's algorithm.

`InvReset`
Resets the timer to zero.

`InvRingIntersection[{`$\mathtt{f}_1$`,`$\mathtt{f}_2$`,...,`$\mathtt{f}_{m_1}$`},{`$\mathtt{g}_1$`,`$\mathtt{g}_2$`,...,`$\mathtt{g}_{m_2}$`},{`$\mathtt{x}_1, \mathtt{x}_2, ..., \mathtt{x}_n$`}]`
$> \{h_1, h_2, ..., h_r\}$
Fundamental invariants for the ring $\mathbf{K}[x_1, x_2, ..., x_n]^{G_1} \cap \mathbf{K}[x_1, x_2, ..., x_n]^{G_2}$
`{`$\mathtt{f}_1$`,`$\mathtt{f}_2$`,...,`$\mathtt{f}_{m_1}$`}` and `{`$\mathtt{g}_1$`,`$\mathtt{g}_2$`,...,`$\mathtt{g}_{m_2}$`}` are fundamental invariants of $\mathbf{K}[x_1, x_2, ..., x_n]^{G_1}$ and $\mathbf{K}[x_1, x_2, ..., x_n]^{G_2}$ respectively.
Works only in the nonmodular case.

`NumSecInvars[G_MatrixGroupT,{`$\theta_1, \theta_2, ..., \theta_n$`},{`$\mathtt{x}_1, \mathtt{x}_2, ..., \mathtt{x}_n$`}:{}]`
$>$ the rank of $\mathbf{K}[x_1, x_2, ..., x_n]^G$ as a $\mathbf{K}[\theta_1, \theta_2, ..., \theta_n]-$module.
Works only in the nonmodular case.

`PrimaryInvariants[G_MatrixGroupT,{`$\mathtt{x}_1, \mathtt{x}_2, ..., \mathtt{x}_n$`}:{}]`
$>$ `{`$\theta_1, \theta_2, ..., \theta_n$`}`
A set of minimal primary invariants for the group `G`.

`PrimaryInvariants[G_MatrixGroupT,hs,t,order,{`$\mathtt{x}_1, \mathtt{x}_2, ..., \mathtt{x}_n$`}:{}]`
$>$ `{`$\theta_1, \theta_2, ..., \theta_n$`}`
`G` is a finite matrix group, `hs` is the Hilbert series $H^G(t)$ and `order`$= |G|$.
A set of minimal primary invariants for the group `G`.

`PrimaryInvariants[G_PermGroupT,{`$\mathtt{x}_1, \mathtt{x}_2, ..., \mathtt{x}_n$`}:{}]`
$>$ `{`$\sigma_1, \sigma_2, ..., \sigma_n$`}`
The elementary symmetric polynomials. Requires the `PermGroup.m`

package, cf. Bayer [2].

`ReynoldsOperator[G_MatrixGroupT][F,{`$x_1, x_2, ..., x_n$`}:{}]`

$> \mathfrak{R}^G$(F)

F is a polynomial in {$x_1, x_2, ..., x_n$}. Works only in the nonmodular case.

`ReynoldsOperator[G_MatrixGroupT][F,`χ`,{`$x_1, x_2, ..., x_n$`}:{}]`

$> \mathfrak{R}^G_\chi$(F)

F is a polynomial in {$x_1, x_2, ..., x_n$}.Works only in the nonmodular case.

`RF[rList_List,F,{`$x_1, x_2, ..., x_n$`}:{}]`

$> \mathfrak{R}^G$(F)

F is a polynomial in {$x_1, x_2, ..., x_n$},rList is a list of rules for $\mathfrak{R}^G$.

Works only in the nonmodular case.

`RFM[G_MatrixGroupT,F,{`$x_1, x_2, ..., x_n$`}:{}]`

$> \frac{1}{LC(\mathfrak{R}^G(\mathtt{F}))} \cdot \mathfrak{R}^G(\mathtt{F})$

F is a polynomial in {$x_1, x_2, ..., x_n$}. Works only in the nonmodular case.

`RFM[G_MatrixGroupT]`

$>$ (F,{$x_1, x_2, ..., x_n$}) $\longmapsto$RFM[G_MatrixGroupT,F,{$x_1, x_2, ..., x_n$}]

`RFM[rList_List,F,{`$x_1, x_2, ..., x_n$`}:{}]`

$> \frac{1}{LC(\mathfrak{R}^G(\mathtt{F}))} \cdot \mathfrak{R}^G(\mathtt{F})$

F is a polynomial in {$x_1, x_2, ..., x_n$}. rList is a list of rules for $\mathfrak{R}^G$.

Works only in the nonmodular case.

`RFM[G_MatrixGroupT,`χ`][F,{`$x_1, x_2, ..., x_n$`}:{}]`

$> \frac{1}{LC(\mathfrak{R}^G_\chi(\mathtt{F}))} \cdot \mathfrak{R}^G_\chi(\mathtt{F})$

F is a polynomial in {$x_1, x_2, ..., x_n$}.

Works only in the nonmodular case.

`Rules[G_MatrixGroupT,{`$x_1, x_2, ..., x_n$`}:{}]`

$>$ {r_1,r_2, . . . ,r_m}

A set of rules for the action of the group on $\mathbf{K}[x_1, x_2, ..., x_n]$.

`Rules[G_MatrixGroupT,`χ`,{`$x_1, x_2, ..., x_n$`}:{}]`

$>$ {r_1,r_2, . . . ,r_m}

A set of rules for the action of the group on $\mathbf{K}[x_1, x_2, ..., x_n]$ w.r.t. the character χ.

`SecondaryInvariants[G_MatrixGroupT,{`$\theta_1, \theta_2, ..., \theta_n$`},{`$x_1, x_2, ..., x_n$`}:{}]`

$> \{\eta_1, \eta_2, ..., \eta_r\}$

A module basis for $\mathbf{K}[x_1, x_2, ..., x_n]^G$ as a $\mathbf{K}[\theta_1, \theta_2, ..., \theta_n]-$module.

Works only in the nonmodular case.

`TotalDegree[F,{`$x_1, x_2, ..., x_n$`}:{}]`

$>$ the total degree of F as a polynomial in {$x_1, x_2, ..., x_n$}.

Matrices :

`Add[m1_List, m2_List]`

$> diag$(m1,m2)

`Del[M_List, i_Integer, j_Integer]`
deletes the `i`-th row and `j`-th column of `M`.
`ToMatrix[perm_List]`
> the permutation matrix of the permutation `perm` in list representation.
`trace[M_List]`
> $\sum_{i=1}^{n} \mathtt{M}_{i,i}$
The trace of `M`.
Matrix Groups :
`Act[M,F,{`$\mathtt{x}_1, \mathtt{x}_2, ..., \mathtt{x}_n$`}]`
> $\mathtt{F}(\mathtt{M}^{-1}\{\mathtt{x}_1, \mathtt{x}_2, ..., \mathtt{x}_n\})$
The action of the matrix `M` on the polynomial `F`.
`Characterisitc[G_MatrixGroupT]`
> the characteristic of the field $\mathbf{K}$ of $\mathtt{G} \leq GL_n(\mathbf{K})$.
`Conj[MatrixGroupT[g_GenT, finite],M_List]`
> conjugates each generator with `M`.
`Degree[G_MatrixGroupT]`
> n iff $\mathtt{G} \leq GL_n(\mathbf{K})$.
`Element[G_MatrixGroupT][i_Integer]`
> the `i`-th element of `G`.
`Elements[MatrixGroupT[{`$\mathtt{M}_1, \mathtt{M}_2, ..., \mathtt{M}_k$`},ord,finite]]`
> $\{\mathtt{M}_1, \mathtt{M}_2, ..., \mathtt{M}_k\}$
`Enumerate[G_MatrixGroupT,F:id]`
> $\{\mathtt{F}[\sigma] : \sigma \in \mathtt{G}\}$ iff `G` contains a list of all elements.
> `Nil` otherwise.
`TypeOfRep[MatrixGroupT[elem_List, ord_, finite]]`
`rtype1` : `G` contains an element list.
`rtype3` : `G` contians only a generating set.
`Generators[G_MatrixGroupT]`
> $\{\mathtt{G}_1, \mathtt{G}_2, ..., \mathtt{G}_k\}$ iff `G` contains a list of generators
> `Nil` otherwise.
`MatrixGroup[gens_List,generate_:True]`
> `G`
The linear group generated by $\{\mathtt{G}_1, \mathtt{G}_2, ..., \mathtt{G}_k\}$.
<generate == True>
`G` contains a list of all elements
<generate == False>
`G` contains a list of the generators.
`MatrixGroup[PG_PermGroupT]`
> `G`
The corresponding matrix group `G` to the permutation group `PG`
`Map[F,G_MatrixGroupT]`

Maps the function F to all elements of G. G must contain a list of all elements.
Orbit[G_MatrixGroupT,p_,Action_]
> $\{$Action$[\sigma, \mathtt{p}] : \sigma \in$ G$\}$
Order[G_MatrixGroupT
> $|$G$|$
Print[G_MatrixGroupT]
Prints the group G.
Transform[MatrixGroupT[elem_List, ord_, finite], set_, Action_]
Partitions
Taken from Skiena [35].
Partitions[n_Integer]
> all partitions of n
Partitions[n_Integer,maxpart_Integer]
> all partitions of n where all summands are $\leq$maxpart.
NextPartition[p_List]
ReducedPartitions[n_Integer]
ReducedPartitions[part_List]]
Polynomials :
DegVec[M_,{$x_1, x_2, ..., x_n$}]
> the degree vector of the monomial M.
HeadTerm[f_,{$x_1, x_2, ..., x_n$},ordering:PTotal]
> the head term of the polynomial f.
PTotal is the total degree ordering and PLex the lexicographic ordering.
Monomials[{$x_1, x_2, ..., x_n$}:{},d_Integer]
> a set of all monomials in $x_1, x_2, ..., x_n$ with degree d
PLex[l1_List,l2_List]
> True if l1 is lexicographical smaller or equal than l2. False otherwise.
PolyToFun[f_,{$x_1, x_2, ..., x_n$}]
> Transforms the polynomial f in a Mathematica function with n parameters $x_1, x_2, ..., x_n$.
SymmPoly[{$x_1, x_2, ..., x_n$}]
> The elementary symmetric polynomials in the variables $x_1, x_2, ..., x_n$.

5.4 A small Demo

Example 37 *We compute the Hironaka decomposition of* $G = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \right\rangle$.

G has order 4.

```
m = {{0,1,0},{-1,0,0},{0,0,-1}};
G = MatrixGroup[{m}];
Print[G]
```

Order 4 , characteristic 0

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

```
hs = HilbertSeries[G,t];
```

$$\frac{-1+t-t^2-t^3}{(-1+t)^3\,(1+t)^2\,(1+t^2)}$$

```
Series[hs,{t,0,10}]
```

$$1 + 2t^2 + 2t^3 + 5t^4 + 4t^5 + 8t^6 + 8t^7 + 13t^8 + 12t^9 + 18t^{10} + O(t)^{11}$$

$\{\mathtt{p}_1,\mathtt{p}_2,\mathtt{p}_3\}$ `= PrimaryInvariants[G,{x,y,z}]`

$$\{x^2 + y^2, z^2, x^2y^2\}$$

```
SetVariables[{x,y,z}];
```

`NumSecInvars[G,{`$\mathtt{p}_1,\mathtt{p}_2,\mathtt{p}_3$`}]`

4

`DegSecInvars[hs,{`$\mathtt{p}_1,\mathtt{p}_2,\mathtt{p}_3$`},t]`

$$1 + 2t^3 + t^4$$

`gb = GroebnerBasis[{`$\mathtt{p}_1,\mathtt{p}_2,\mathtt{p}_3$`},{x,y,z}];`

$\{\mathtt{s}_2,\mathtt{s}_3\}$ `= HomogenousInvariants[G,3]`

$$\{xyz, x^2z - y^2z\}$$

```
hom4 = HomogenousInvariants[G,4]
```

$$\{x^2y^2, x^3y - xy^3, x^4 + y^4, z^4, x^2z^2 + y^2z^2\}$$

```
Map[PolynomialReduce[#,gb,{x,y,z}][[2]] &,hom4]
```

$$\{0, -2xy^3, 0, 0, 0\}$$

$\mathtt{s}_4$ `= hom4[[2]];`

Let $R = \mathbf{C}[\mathtt{p}_1, \mathtt{p}_2, \mathtt{p}_3]$. We have obtained the Hironaka decomposition

$$\mathbf{C}[x, y, z]^G = R \oplus \mathtt{s}_2R \oplus \mathtt{s}_3R \oplus \mathtt{s}_4R.$$

Bibliography

[1] Bayer, D., Stillman, M. *Computation of Hilbert Functions.* J. Symb. Comp. 14 : 31 - 50, 1992.

[2] Bayer, T. *Permutation Groups and Polya Theory in Mathematica.* RISC report (to appear).

[3] Becker, T., Weispfennig V., *Gröbner Bases.* Springer Verlag New York 1993.

[4] Bigatti, A. M., Caboara M., Robbiano L. *On the Computation of Hilbert-Poincare' Series.* AAECC 2 : 21 - 33, 1991.

[5] Bosch, S. *Algebra.* Springer Verlag Berlin Heidelberg New York, 1993.

[6] Bosma, W., Cannon, J., Playoust, C., *The Magma Algebra System I : The User Language.* J. Symb. Comp. 24, 1997.

[7] Buchberger B., *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD Thesis, University of Innsbruck, 1965.

[8] Buchberger B., *Gröbner Bases - an Algorithmic Method in Polynomial Ideal Theory.* In : Bose, N.K.(ed) : Multidimensional System Theory. D. Reidel, Dordrecht 1985 (pp 184 - 232).

[9] Cox, D. Little, J, O'Shea, D., *Ideals, Varieties, and Algorithms.* Springer Verlag, New York 1992.

[10] Decker W., Heydtmann A. E. , Schreyer F., *Generating a Noetherian Normalization of the Invariant Ring of a Finite Group*,J. Symb. Comp (to appear).

[11] Decker, W., Jong, T., *Gröbner Bases and Invariant Theory.* In : Buchberger, B., Winkler, F. (eds) : *33 Years of Gröbner Bases.*, Cambridge Univ. Press 1998.

[12] Derksen, H.,*Constructive Invariant Theory and the Linearization Problem.* PhD thesis 1997, University of Basel.

[13] Eisenbud, D. *Commutative Algebra with a View Toward Algebraic Geometry.* Graduate Texts in Mathematics 150, Springer Verlag, New York Berlin Heidelberg 1995.

[14] Fulton W., Harris, J. *Representation Theory.* Graduate Texts in Mathematics 129, Springer Verlag New York 1991.

[15] Göbel, M. *Computing Bases for Rings of Permutation-invariant Polynomials.* J. Symb. Comp. 19 : 285 - 291, 1995

[16] Harris, J. *Algebraic Geometry.* Graduate Texts in Mathematics 133, Springer Verlag, New York 1992.

[17] Hemperly, J., C. *Problem E2442.* Amer. Math. Monthly 80 : 1058, 1973.

[18] Hilbert, D. (1890). *Über die Theorie der Algebraischen Formen.* Collected Papers, Volume II, Springer Verlag Berlin Heidelberg New York 1970

[19] Hilbert, D. (1893). *Über die Vollen Invariantensysteme.* Collected Papers, Volume II, Springer Verlag Berlin Heidelberg New York1970

[20] Hilbert, D. (1897). *Theory of Algebraic Invariants.* Reprint, Cambridge Univ. Press 1993.

[21] Hochster, M, Eagon, J.A. *Cohen-Macaulay Rings, Invariant Theory, and the Generic Perfection of Determinantal Loci.* Am. J. Math. 93: 1020 - 1058, 1971.

[22] Kemper, G. *Calculating Invariant Rings of Finite Groups over Arbitrary Fields.* J. Symb. Comp. to appear.

[23] Kemper, G. *Calculating Optimal Systems of Parameters.* IWR Preprint **97-08**, Heidelberg 1997.

[24] Kemper G, Steel A. *Some Algorithms in Invariant Theory of Finite Groups.* Preprint 1997.

[25] Kerber, A. *Algebraic Combinatorics via Finite Group Actions.* BI-Wiss.-Verl. Mannheim-Wien-Zuerich 1991.

[26] Klein, F. (1872). *Das Erlanger Programm.* Ostwald's Klassiker der Exakten Wissenschaften Bd. 253, Verlag Harri Deutsch, Frankfurt/Main 1995.

[27] Klingenberg, W. *Lineare Algebra und Geometrie.* Springer Verlag, Berlin Heidelberg New York 1992.

[28] Möller, H. M., Mora, F. *New Constructive Methods in Classical Ideal Theory.* J. of Algebra 100 : 138 - 178, 1986.

[29] Nagata, M. *On the 14th Problem of Hilbert.* Am. J. Math. 81, 766 - 772, 1959.

[30] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen.* Math. Ann. 77 : 89 - 92, 1916,

[31] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher linearen Gruppen der Characteristik p.* Nachr. v. d. Ges. d. Wiss. zu Göttingen 28 - 35, 1926.

[32] Reiner, V., Smith, L. *Systems of Parameters for Rings of Invariants.* Preprint, Göttingen, 1996.

[33] Rötteler, M. *Invariantentheorie endlicher und kompakter Gruppen.* Diploma Thesis, University of Karlsruhe, 1997.

[34] Sagan, B. *The Symmetric Group.* Wadsworth & Brooks/Cole Mathematics series, Pacific Grove California 1991.

[35] Skiena, S. *Implementing Discrete Mathematics in Mathematica.* Addison-Wesley Reading MA, 1990.

[36] Sloane, N.A.J. *Error-Correcting Codes and Invariant Theory: New Applications of a Nineteenth-Century Technique.* Amer. Math. Monthly 84: 82 - 107, 1977.

[37] Stanley, R. *Hilbert Functions of Graded Algebras.* Adv. in Math. 28 : 57 - 83, 1978.

[38] Stanley, R. *Invariant Theory of Finite Groups and Their Applications to Combinatorics.* Bull.Amer.Math.Soc. Vol 1, nr. 3 ,1979.

[39] Smith, L. *Polynomial Invariants of Finite Groups.* A.K. Peters, Welesley 1995.

[40] Smith, L. *Polynomial Invariants of Finite Groups.* Bull. Am. Math. Soc. Vol 34, nr. 3 : 211-250, 1997.

[41] Simon, B. *Representations of Finite and Compact Groups.* Graduate Studies in Mathematics 10, American Mathematical Society 1996.

[42] Sturmfels, B., White N. *Gröbner Bases and Invariant Theory.* Adv.Math. 76 : 245 - 259, 1989

[43] Sturmfels, B. *Algorithms in Invariant Theory.* Texts and Monographs in Symbolic Computation, Springer Verlag Wien New York 1993.

[44] Vasconcelos, W. *Computational Methods in Commutative Algebra and Algebraic Geometry.* Algorithms and Computations in Mathematics, Springer Verlag Berlin Heidelberg New York 1997.

[45] Wang, D.*Geometry Machines : From AI to SMC.* in : Calmet, Campell, Pfalzgraf : *Artificial Intelligence and Symbolic Mathematical Computation*, p 213 - p 239. LNCS 1138, Springer Verlag, Berlin 1996.

[46] White N. *Multilinear Cayley Factorization.* J. Symb. Comput. 11: 421 - 438, 1991.

[47] Winkler, F. *Polynomial Algorithms in Computer Algebra.* Texts and Monographs in Symbolic Computation, Springer Verlag Wien 1997.

[48] Wu,W., *Mechanical Theorem Proving in Geometries.* Texts and Monographs in symbolic computation, Springer Verlag, Wien 1994.

[49] Zariski, O, Samuel, P. *Commutative Algebra.* Volume I and II. Reprint of the 1958-60 edition. Springer Verlag , New York 1979.

[50] Zaddach, A. *Grassmanns Algebra in der Geometrie.* BI-Wissenschafts Verlag, Mannheim; Leipzig; Wien; Zürich; 1994.