# Lectures on representations of finite groups and invariant theory

Dmitri I. Panyushev

Independent University of Moscow, Bol'shoi Vlasevskii per. 11, 119002 Moscow, Russia

*E-mail address*: panyush@mccme.ru

This work was supported in part by SFB/TR12 and RFBI Grant 05-01-00988.

# Contents

CHAPTER I

# Representation theory of finite groups

## I.1. Basic definitions and examples

$\Bbbk$ is the ground field;

$G$ is a finite group; the neutral element of $G$ is denoted by $\mathbb{1}$.

$E$ is a $\Bbbk$-vector space. (Usually, $\dim_{\Bbbk}(E) < \infty$.)

$\mathrm{Aut}_{\Bbbk}(E) \subset \mathrm{End}_{\Bbbk}(E) = \{f : E \to E \mid f \text{ is } \Bbbk\text{-linear}\}$.

**Definition 1.** A *linear representation of $G$ in $E$* is a group homomorphism $\rho : G \to \mathrm{Aut}_{\Bbbk}(E)$.

That is, a representation is a triple $(G, \rho, E)$. However, we will say abusing the language that $\rho$ is a representation; $E$ is also called a *representation space* of $G$ or a *$G$-module*. Whenever we wish to stress that $E$ corresponds to $\rho$, we write $E_\rho$ for it.

- $\dim E_\rho = \deg \rho$ is the *degree* of the representation $\rho$.

Let $\boldsymbol{e} = (e_1, e_2, \dots, e_n)$ be a basis for $E$. Then $\mathrm{Aut}_{\Bbbk}(E) \simeq GL_n(\Bbbk)$ and $\rho_{(\boldsymbol{e})} : G \to GL_n(\Bbbk)$ is a *matrix representation* of $G$. Here $\rho_{(\boldsymbol{e})}(\sigma)$ is a non-singular $n \times n$ matrix for any $\sigma \in G$.

**Definition 2.** Two matrix representations $\rho_i : G \to GL_{n_i}(\Bbbk)$, $i = 1, 2$, are said to be *equivalent* if $n_1 = n_2$ and there is $C \in GL_{n_1}(\Bbbk)$ such that $C^{-1}\rho_1(\sigma)C = \rho_2(\sigma)$ for any $\sigma \in G$.

**Definition 3.** Two linear representations $\rho_i : G \to \mathrm{Aut}_{\Bbbk}(E_i)$, $i = 1, 2$, are said to be *equivalent* (*isomorphic*) if $\dim E_1 = \dim E_2$ and there is an isomorphism $C : E_1 \to E_2$ such that $C\rho_1(\sigma) = \rho_2(\sigma)C$ for any $\sigma \in G$.

Notation: $\rho_1 \simeq \rho_2$.

We do not distinguish equivalent representations. Our goal is to describe the representations of $G$ up to equivalence.

**I.1.1. Basic constructions.** Let $X$ be a finite set. The set of all $\Bbbk$-valued functions on $X$ is a finite-dimensional $\Bbbk$-vector space; $\dim_{\Bbbk} \Bbbk[X] = \#X$. The group of all bijections $X \to X$, denoted $\mathrm{Aut}\,(X)$, is isomorphic to a symmetric group. Any $\sigma \in \mathrm{Aut}\,(X)$ induces the linear transformation $\sigma_*$ of $\Bbbk[X]$ defined by the formula

$(\sigma_* f)(x) = f(\sigma^{-1}x)$, $f \in \Bbbk[X]$, $x \in X$.

The role of $\sigma^{-1}$ in the right hand side is that it guarantees us the right order in compositions: we then have $(\sigma\tau)_* = \sigma_*\tau_*$.

Any group homomorphism $s : G \to \mathrm{Aut}\,(X)$ defines the linear representation $\rho_s$ of $G$ in $\Bbbk[X]$ by the formula:

$$\rho_s(\sigma) = s(\sigma)_* .$$

This $\rho_s$ is called the *permutation representation* associated with $(s, X)$.

$1^o$. $X = G$ and $G$ acts on itself by left multiplications. That is, $s(\sigma_1)\sigma_2 = \sigma_1\sigma_2$. Here $\rho_s = L$, the *left regular* representation of $G$ in $\Bbbk[G]$.

$2^o$. $X = G$ and $G$ acts on itself by right multiplications. That is, $s(\sigma_1)\sigma_2 = \sigma_2(\sigma_1)^{-1}$. Here $\rho_s = R$, the *right regular* representation of $G$ in $\Bbbk[G]$.

**Exercise 1.** *Prove that $L \simeq R$.* [Hint: Use the inversion $s \mapsto s^{-1}$.]

$3^o$. The adjoint representation of $G$ in $\Bbbk[G]$. Here $X = G$ and $\mathrm{Ad}\,(\sigma_1)\sigma_2 = (\sigma_1)^{-1}\sigma_2\sigma_1$.

$4^o$. The restriction of a representation to a subgroup. If $H$ is a subgroup of $G$, then $\rho|_H : H \to \mathrm{Aut}_{\Bbbk}(E)$ is a representation of $H$.

$5^o$. If $H$ is a subgroup of $G$, then take $X = G/H$ and define $s : G \to \mathrm{Aut}\,(G/H)$ by the formula $s(\sigma_1)\sigma_2 H = (\sigma_1\sigma_2)H$. This yields a representation of $G$ in the space $\Bbbk[G/H]$.

$6^o$. More generally, let $\bar{E}$ be an $H$-module (via $\bar{\rho} : H \to \mathrm{Aut}_{\Bbbk}(\bar{E})$). Consider the finite-dimensional vector space

$$E = \{f : G \to \bar{E} \mid f(gh^{-1}) = \bar{\rho}(h)f(g)\} .$$

It becomes a $G$-module in a very natural way. Define $\rho : G \to \mathrm{Aut}_{\Bbbk}(E)$ by

$$(\rho(\sigma)f)(g) = f(\sigma^{-1}g), \quad \sigma, g \in G .$$

The representation $\rho$ is called the *induced representation*. Notation: $\rho = \mathrm{Ind}_H^G(\bar{\rho})$. If $\dim \bar{E} = 1$ and $\bar{\rho} \equiv 1$, then $E$ is naturally isomorphic to $\Bbbk[G/H]$ and we obtain Example $5^0$ as a particular case of this construction.

$7^o$. If $(\rho, E), (\rho', E')$ are $G$-modules, then $\mathrm{Hom}_{\Bbbk}(E, E')$ is again a $G$-module. For $f \in \mathrm{Hom}_{\Bbbk}(E, E')$ and $\sigma \in G$, we set

$$(\sigma{\cdot}f)(x) = \rho'(\sigma)(f(\rho(\sigma^{-1})x)) .$$

$8^o$. The *dual* (contragredient) representation. Since $E^* = \mathrm{Hom}_{\Bbbk}(E, \Bbbk)$, it is a special case of Example $7^o$. We write $\rho^*$ for the representation dual to $\rho$.

$9^o$. If $(G, \rho, E)$ and $(G, \mu, V)$ are two representations, then $\rho \otimes \mu : G \to \mathrm{Aut}_{\Bbbk}(E \otimes V)$ defines a representation, which is called the *tensor product* of $\rho$ and $\mu$.

**Exercise 2.** *The $G$-modules $\mathrm{Hom}_{\Bbbk}(E, E')$ and $E^* \otimes E'$ are naturally isomorphic.*

## I.2. Invariant subspaces and complete reducibility

Let $(G, \rho, E)$ be a representation.

**Definition 4.** $U \subset E$ is an *invariant* (or $G$-*invariant*) subspace if $\rho(\sigma)U \subset U$ for all $\sigma \in G$.

Any invariant subspace yields the *subrepresentation* and the *factor-representation* of $G$:

$$\begin{cases} \rho_U : G \to GL(U) = \mathrm{Aut}_{\Bbbk}(U), \quad \rho_U(\sigma) = \rho(\sigma)|_U \\ \rho_{E/U} : G \to GL(E/U) = \mathrm{Aut}_{\Bbbk}(E/U), \quad \rho_{E/U}(\sigma)(v+U) = \rho(\sigma)(v) + U. \end{cases}$$

If $U \oplus U' = E$ is a vector space decomposition, then we obtain in the matrix form:
$\rho(\sigma) = \begin{pmatrix} \rho_U(\sigma) & * \\ 0 & \rho_{E/U}(\sigma) \end{pmatrix}$.

**Definition 5.** A representation $(G, \rho, E)$ is said to be *irreducible*, if $\{0\}$ and $E$ are the only invariant subspaces. In this case, the $G$-module $E$ is said to be *simple*.

We say that an invariant subspace is *non-trivial* if it is different from $\{0\}$ and $E$. An invariant subspace $U$ is said to be *minimal* if $U \neq 0$ and $\rho|_U$ is irreducible.

**Example I.2.1.** The monomial representation of the symmetric group $\Sigma_n$.
Let $e_1, \dots, e_n$ be a a basis of an $n$-dimensional space $E$. For a permutation $\sigma \in \Sigma_n$, we set $M(\sigma)(e_i) = e_{\sigma(i)}$. Obviously, $\Bbbk(e_1 + \ldots + e_n)$ is an invariant subspace, hence $M$ is not irreducible. Next, $E_0 = \{\sum x_i e_i \mid x_i \in \Bbbk \ \& \ \sum x_i = 0\}$ is a complementary invariant subspace.

**Exercise 3.** *Prove that $E_0$ is a simple $\Sigma_n$-module.*
[Hint: if $\sigma_{12}(x) \neq x$, then $\sigma_{12}(x) - x$ is proportional to $e_1 - e_2$.]

**Definition 6.** A representation $(G, \rho, E)$ is said to be *completely reducible* if every invariant subspace $U \subset E$ has an invariant complement.

*Notation*: $E^G = \{x \in E \mid \rho(\sigma)x = x \ \forall \sigma \in G\}$. It is an invariant subspace of $E$.

**Lemma I.2.2.** *If $\#G$ is invertible in $\Bbbk$, then $E^G$ has a unique invariant complement.*

*Proof.* Consider the operator

$$T_G : E \to E, \qquad T_G(x) = \frac{1}{\#G} \sum_{\sigma \in G} \sigma x.$$

Clearly, $T_G$ is a projection of $E$ to $E^G$. Furthermore, $T_G(\sigma x) = T_G(x)$ for any $x \in E$, $\sigma \in G$. Hence $\ker(T_G)$ is an invariant complement to $E^G$. Assume that $E'$ is another invariant complement to $E^G$. Applying $T_G$ to $E'$, we obtain $T_G(E') \subset E' \cap E^G = \{0\}$. Therefore $E' \subset \ker(T_G)$ and hence they are equal for dimension reason. □

**Lemma I.2.3.** *If $V, V'$ are $G$-modules and $\varphi : V \to V'$ is a surjective $G$-homomorphism, then $\varphi|_{V^G} : V^G \to (V')^G$ is surjective, too.*

*Proof.* Consider the commutative diagram:

$$\begin{tikzcd} V \arrow[r] \arrow[d, "T_G"'] & V' \arrow[d, "T_G"] \\ V^G \arrow[r] & (V')^G \end{tikzcd}$$

whose vertical arrows are surjective in view of Lemma I.2.2. □

**Definition 7.** Let $(G, \rho_i, E_i)$, $i = 1, 2$, be two representations of $G$. A mapping $\varphi \in \mathrm{Hom}_{\Bbbk}(E_1, E_2)$ is called a *$G$-homomorphism* or *intertwining operator* if $\varphi(\rho_1(\sigma)x) = \rho_2(\sigma)\varphi(x)$ for any $\sigma \in G, x \in E_1$. The set of all intertwining operators is denoted by $\mathrm{Hom}_G(E_1, E_2)$.

If $\varphi$ is a $G$-homomorphism, then $\ker \varphi$ and $\mathrm{Im}\, \varphi$ are invariant subspaces.

**Example I.2.4.** $C \in \mathrm{Hom}\,(E_1, E_2)$ is a $G$-homomorphism if and only if $C$ is a $G$-fixed vector in $\mathrm{Hom}\,(E_1, E_2)$. That is, $\mathrm{Hom}_G(E_1, E_2) = (\mathrm{Hom}\,(E_1, E_2))^G$.

**Theorem I.2.5** (Maschke). *If $\#(G)$ is invertible in $\Bbbk$, then every representation of $G$ is completely reducible.*

*Proof.* Let $U$ be an invariant subspace of a $G$-module $E$. Then

$$V = \mathrm{Hom}_{\Bbbk}(E, U) \to \mathrm{Hom}_{\Bbbk}(U, U) = V', \quad (f \in V) \mapsto f|_U,$$

is a surjective $G$-homomorphism. Hence

$$\psi : V^G = \mathrm{Hom}_G(E, U) \to \mathrm{Hom}_G(U, U) = (V')^G$$

is surjective, too. The space $(V')^G$ contains a distinguished element, namely, $id_U$. If $id_U = \psi(p)$, then $p : E \to U$ is a $G$-projection. Therefore $\ker\,(p)$ is a $G$-invariant complementary subspace. □

This is a general scheme of proving the complete reducibility, which applies in much more general context. The crucial point here is Lemma I.2.2 and the existence of the projection to the subspace of $G$-fixed points. The rest of the proof does not exploit the fact that $G$ is finite. In case of compact Lie groups, the averaging operator $T_G$ is replaced with the invariant integration on $G$.

**Corollary I.2.6.** *Any representation of $G$ is a direct sum of irreducible representations,*

**Remark.** It follows from the complete reducibility that any $G$-module $E$ can be presented as a direct sum of minimal invariant subspaces. In general, such a decomposition is not unique. A more coarse but canonical decomposition—thew so-called isotypic decomposition—will be discussed below.

**Theorem I.2.7** (Schur's Lemma)**.** *Let $\rho_1, \rho_2$ be irreducible representations of $G$ and $f : E_1 \to E_2$ a $G$-homomorphism.*

(i) *If $\rho_1 \not\simeq \rho_2$, then $f = 0$;*

(ii) *If $\rho_1 \simeq \rho_2$ and $f \neq 0$, then $f$ is an isomorphism; furthermore, if $\Bbbk = \bar{\Bbbk}$, then $\dim_{\Bbbk} \operatorname{Hom}_G(E_1, E_2) = 1$.*

*Proof.* (i) It follows from the fact the $\ker(f)$ and $\operatorname{Im}(f)$ are invariant subspaces.

(ii) If $f \neq 0$, then we must have $\ker(f) = 0$ and $\operatorname{Im}(f) = E_2$, i.e., $f$ is a $G$-isomorphism. Suppose $f_1, f_2 \in \operatorname{Hom}_G(E_1, E_2)$ are two $G$-isomorphisms. Then $s = f_2 f_1^{-1} : E_1 \to E_1$ is a $G$-isomorphism. If $\Bbbk = \bar{\Bbbk}$, then $s$ has a non-trivial eigenvector, i.e., $sv = \lambda v$ for some $v \in E_1$ and $\lambda \in \Bbbk$. Then $s - \lambda{\cdot}id$ is a $G$-homomorphism having non-trivial kernel. Hence $s = \lambda{\cdot}id$ and $f_2 = \lambda f_1$. □

From now on, we assume that $\Bbbk$ is algebraically closed and the orders of all finite groups under consideration are invertible in $\Bbbk$.

**Theorem I.2.8.** *Let $(G, \rho, E)$ and $(H, \mu, V)$ be two irreducible representations. Then $(G \times H, \rho \otimes \mu, E \otimes V)$ is also irreducible.*

*Proof.* We have $G = G \times \{e\} \subset G \times H$ and

$$\rho \otimes \mu|_G \simeq m\rho, \quad \text{where } \ m = \deg \mu\,.$$

It follows that any simple $G$-submodule of $E \otimes V$ is isomorphic to $E$ (induction on $m$ and an application of Schur's Lemma). Let $U$ be a minimal $G$-invariant subspace of $E \otimes V$. Then $U \simeq E$ as $G$-module, and we are going to prove that all such subspaces have a very special form.

Let $f_1, \dots, f_m$ be a basis for $V$. Then for any $u \in U$ we have

$$u = \sum_{i=1}^{m} \alpha_i \otimes f_i, \quad \alpha_i \in E\,.$$

In this way, we obtain the mappings $\phi_i : U \to E$, $\phi_i(u) = \alpha_i$, $i = 1, \dots, m$. Clearly, $\phi_i \in \operatorname{Hom}_G(U, E)$ for each $i$. Hence $\phi_i = c_i \phi$, where $\phi$ is a fixed isomorphism of $U$ and $E$, and $c_i \in \Bbbk$. Hence $u = \sum_i c_i \phi(u) \otimes f_i = \phi(u) \otimes \sum_i c_i f_i$. Thus, $U$ is of the form $E \otimes \{v\}$ for $v = \sum_i c_i f_i \in V$.

Let $W$ be a non-trivial $G \times H$-invariant subspace. Then $W \supset E \otimes \{v_0\}$ for some $v_0$ and hence $W \supset E \otimes \operatorname{span}\{Hv_0\}$. Since $\mu$ is irreducible, $\operatorname{span}\{Hv_0\} = V$. □

## I.3. The decomposition of the group algebra

The vector space $\Bbbk[G]$ has a natural structure of a $\Bbbk$-algebra, which we consider later. In this section, we regard $\Bbbk[G]$ only as a $\Bbbk$-vector space and a $G$-module.

Let $(\rho, E)$ be an arbitrary representation of $G$ and $(\rho_{ij}(s))$ is a matrix of $\rho(s)$ with respect to some basis of $E$. Then $\rho_{ij} \in \Bbbk[G]$ and we set

$$M(\rho) = \mathrm{span}\{\rho_{ij} \mid i,j = 1,\dots,\dim E\} \subset \Bbbk[G]\ .$$

We say that $M(\rho)$ is the *space of matrix coefficients* of $\rho$. First, notice that $M(\rho)$ does not depend on the choice of a basis. Indeed,

$$M(\rho) = \mathrm{span}\{x \mapsto \mathrm{tr}\,(\xi{\cdot}\rho(x)) \mid \xi \in \mathrm{End}_{\Bbbk}(V)\}. \tag{I.3.1}$$

It suffices to consider the spaces of matrix elements only for irreducible representations. For, if $\rho \simeq \rho_1 \oplus \rho_2$, then $M(\rho) = M(\rho_1) + M(\rho_2)$.

The crucial observation is that $\mathrm{End}_{\Bbbk}(E)$ and $\Bbbk[G]$, which are $G$-modules as yet, can be regarded as $G\times G$-modules. The representation of $G\times G$ in $\Bbbk[G]$ is obtained by combining the left and right regular representations of $G$. For this reason, it will be denoted '$LR$'.

- For $\xi \in \mathrm{End}_{\Bbbk}(E)$, we set $(g_1, g_2){\cdot}\xi = \rho(g_1)\xi\rho(g_2)^{-1}$;
- For $f \in \Bbbk[G]$, we set $(LR(g_1, g_2)f)(x) = f(g_2^{-1}xg_1)$.

Consider the linear mapping

$$\mu : \mathrm{End}_{\Bbbk}(E) \to \Bbbk[G], \quad \mu(\xi)(g) := \mathrm{tr}\,(\xi{\cdot}\rho(g)).$$

It follows from Eq. (I.3.1) that $\mathrm{Im}\,\mu = M(\rho)$.

**Proposition I.3.1.**
1. *$\mu$ is a $G \times G$-homomorphism.*
2. *If $\rho$ is irreducible, then $\mu$ is a monomorphism and thereby* $\dim M(\rho) = (\deg \rho)^2$.

*Proof.* 1. We have to prove that $\mu((g_1, g_2){\cdot}\xi)(g) = (LR(g_1, g_2){\cdot}\mu(\xi))(g)$ for any $g \in G$. Here

$$\text{LHS} = \mathrm{tr}\,(\rho(g_1)\xi\rho(g_2)^{-1}\rho(g)) \quad \text{and} \quad \text{RHS} = \mu(\xi)(g_2^{-1}gg_1) = \mathrm{tr}\,(\xi{\cdot}\rho(g_2^{-1}gg_1)).$$

Now, the equality follows from the standard properties of the trace.

2. The representation of $G \times G$ in $\mathrm{End}_{\Bbbk}(E)$ is isomorphic to $\rho \otimes \rho^*$. Therefore $\mathrm{End}_{\Bbbk}(E)$ is a simple $G \times G$-module, by virtue of Theorem I.2.8. Since $\mu \neq 0$, the kernel of $\mu$ must be trivial. □

This proposition immediately implies a number of important conclusions.

**Corollary I.3.2.**
*1. If $\rho \not\simeq \rho'$, then $M(\rho)$ and $M(\rho')$ are linearly independent.*
*2. Each irreducible representation of $G$ occurs as a subrepresentation of $L$ (or $R$).*
*3. The number of non-equivalent irreducible representations of $G$ is finite.*

*Proof.* 1. The spaces $M(\rho)$ and $M(\rho')$ afford non-equivalent representations of $G \times G$.
2. Considering $M(\rho)$ as the $G \times \{\mathbb{1}\}$-module, we see that $\rho$ occurs as a subrepresentation of $L$.

3. Follows from part 2 and the fact that $\Bbbk[G]$ is finite-dimensional. □

Let $\widehat{G}$ denote a complete set of pairwise non-equivalent irreducible representations of $G$. We also assume that $\widehat{G} = \{\rho_1, \dots, \rho_m\}$. In particular, $\#\widehat{G} = m$. Set $n_i = \deg \rho_i$.

**Theorem I.3.3.** *The $G \times G$-modules $M(\rho_1) \oplus \ldots \oplus M(\rho_m)$ and $\Bbbk[G]$ are isomorphic.*

*Proof.* We have already proved the inclusion "$\subset$". To prove the opposite inclusion, we show that any $f \in \Bbbk[G]$ is a sum of matrix coefficients of $R$. Let $f_1, \dots, f_N$ be a basis for $\Bbbk[G]$. Without loss of generality, we may assume that $f = f_1$. Then we have

$$g \mapsto f(g) = (R(g)f_1)(e) = \sum_i (R_{i1}(g)f_i)(e) = \sum_i f_i(e)R_{i1}(g) .$$

Hence $f = \sum_i f_i(e)R_{i1}$. Because $R \simeq \sum l_i\rho_i$, we conclude that $f \in \bigoplus_{i=1}^m M(\rho_i)$. □

**Corollary I.3.4.** $n_1^2 + \ldots + n_m^2 = \#(G)$.

**Corollary I.3.5.** $L \simeq R \simeq \sum_{i=1}^m n_i\rho_i$.

**Example I.3.6.** We have $\#(\Sigma_3) = 6$. It follows that $\Sigma_3$ has three representations of degree $1, 1$, and $2$.

## I.4. Characters of linear representations

Let $(G, \rho, E)$ be a linear representation. The function $\chi_\rho : \sigma \mapsto \operatorname{tr} \rho(\sigma)$ is called the *character of the representation $\rho$*. A *simple* or *irreducible* character is the character of an irreducible representation.

**Definition 8.** A function $f$ on the group $G$ is said to be *central* or *class function* if $f(\sigma^{-1}x\sigma) = f(x)$ for all $\sigma, x \in G$.

In other words, $f$ is central if it is invariant with respect to the adjoint representation of $G$ in $\Bbbk[G]$. The space of all central functions is denoted by $\Bbbk[G]^\#$. Since the central functions are just the functions that are constant on the conjugacy classes of $G$, $\dim \Bbbk[G]^\#$ equals the number of conjugacy classes.

Clearly, the character of any representation is a central function. For simplicity, we write $\chi_i$ in place of $\chi_{\rho_i}$.

**Theorem I.4.1.** *The simple characters $\chi_, \dots, \chi_m$ form a basis for $\Bbbk[G]^\#$.*

*Proof.* By Theorem I.3.3, the matrix coefficients of the irreducible representations form a basis in $\Bbbk[G]$. Since $\chi_i \in M(\rho_i)$, $\chi_1, \dots, \chi_m$ are linearly independent and therefore $m \leqslant \dim \Bbbk[G]^\#$. Hence we have to only prove that any central function is a $\Bbbk$-linear combination of characters $\chi_i$. Let $f \in \Bbbk[G]^\#$. Then $f = \sum f_i$, where $f_i \in M(\rho_i)$. We have $G \times G \supset \Delta_G \simeq G$ and the adjoint representation of $G$ is the restriction of $LR$ to $\Delta_G$. Hence each $f_i$ is central, too. Hence it suffices to prove that if $f \in M(\rho_i) \cap \Bbbk[G]^\#$, then $f = c\chi_i$ for some $c \in \Bbbk$.

Recall that we have the $G \times G$-isomorphism $\mu : \operatorname{End}_{\Bbbk}(E_i) \xrightarrow{\sim} M(\rho_i)$. Hence $f = \mu(\xi)$ for some $\xi \in \operatorname{End}_{\Bbbk}(E_i)$. The assumption that $f$ is central translates to the condition $\rho_i(\sigma)\xi\rho_i(\sigma^{-1}) = \xi$ for any $\sigma \in G$. That is, $\xi \in \operatorname{End}_G(E_i)$. Therefore $\xi = c{\cdot}id_{E_i}$, in view of the Schur Lemma. It remains to observe that $\mu(id_{E_i})(g) = \operatorname{tr}(id_{E_i}\rho_i(g)) = \chi_i(g)$. Thus, $f = \mu(\xi) = c\chi_i$. □

**Corollary I.4.2.** *For a finite group $G$, the number of (the equivalence classes of) irreducible representations equals the number of conjugacy classes.*

If $\rho \simeq \sum_i k_i\rho_i$, then the each number $k_i$ is called the *multiplicity* (of $\rho_i$ in $\rho$).

**Corollary I.4.3.** *The multiplicities are well-defined. Up to equivalence, any representation of $G$ is uniquely determined by its character.*

*Proof.* If $\rho \simeq \sum k_i\rho_i$, then $\chi_\rho = \sum k_i\chi_i$. Since the irreducible characters are linearly independent, the last decomposition is unique. Hence the multiplicities $\{k_i\}$ are well-defined. □

**Exercise 4.** *Describe all the irreducible complex representations of the dihedral group $D_n = \langle a, b, \mid a^n = b^2 = 1\!\!1,\ bab^{-1} = a^{-1}\rangle$. Verify that $\#D_n = 2n$ and any $\sigma \in D_n$ is conjugate to $\sigma^{-1}$.*

## I.5. Orthogonality relations for characters and matrix elements

In this section, $\Bbbk = \mathbb{C}$. For $\alpha \in \mathbb{C}$, we let $\bar\alpha$ denote the complex-conjugate number.

**I.5.1. Invariant inner products.** Let $(G, \rho, E)$ be a representation of $G$. Let $(\ |\ )$ be a Hermitian positive-definite sesquilinear form on $E$. Recall that this means the following:

$$(x|y) = \overline{(y|x)}, \quad (\alpha_1x_1 + \alpha_2x_2|y) = \alpha_1(x_1|y) + \alpha_2(x_2|y), \quad \text{and } (x|x) > 0 \text{ for any } x \neq 0.$$

For brevity, we say that $(\ |\ )$ is an *inner product* on the complex vector space $E$. Letting

$$T(x|y) = \frac{1}{\#G}\sum_{\sigma\in G}(\sigma x|\sigma y),$$

we obtain an inner product satisfying the property $T(\sigma x|\sigma y) = T(x|y)$ for any $\sigma \in G$, $x, y \in E$. Such a product is said to be a $G$-ıinvariant inner product (on $E$). If $U \subset E$ is an invariant subspace, then $U^{\perp_T}$ is an invariant complementary subspace. Here $U^{\perp_T}$ stands for the orthocomplement of $U$ with respect to $T$. This yields another proof of complete irreducibility over $\mathbb{C}$.

The above argument also implies that, for any complex representation of $G$, there is a basis for $E$ in which all the matrices $\rho(\sigma)$, $\sigma \in G$, are Hermitian.

**Proposition I.5.1.** *If $\rho$ is irreducible, then a $G$-invariant Hermitian form on $E$ is unique, up to a scalar (real) multiple.*

*Proof.* Assume that $T_1, T_2$ are two inner products on $E$. Then there is a *positive* $\beta \in \mathbb{R}$ such that the $G$-invariant form $f_1 + \beta f_2$ is degenerate. (Take $\beta = -T_1(x|x)/T_2(x|x)$ for some $x \in E$.) Its kernel is a non-trivial invariant subspace. Hence $f_1 + \beta f_2 = 0$, and we are done. □

**I.5.2. Orthogonality relations for simple characters.** Define the inner product on $\mathbb{C}[G]$ by the formula

$$(f|g) = \frac{1}{\#G} \sum_{\sigma \in G} f(\sigma)\overline{g(\sigma)}\ . \tag{I.5.2}$$

As is easily seen, this inner product respects both $L$ and $R$-structure in $\mathbb{C}[G]$. That is, this inner product is $G \times G$-invariant. Indeed,

$$(LR(\sigma_1, \sigma_2)f|LR(\sigma_1, \sigma_2)g) = \frac{1}{\#G} \sum_{\sigma \in G} f(\sigma_2\sigma\sigma_1^{-1})\overline{g(\sigma_2\sigma\sigma_1^{-1})}.$$

Since the mapping $(\sigma \in G) \mapsto (\sigma_2\sigma\sigma_1^{-1} \in G)$ is one-to-one, the last sum differs from the sum in Eq. (I.5.2) only in the order of terms. This proves the invariance.

We would like to describe orthogonal bases for $\mathbb{C}[G]$ and $\mathbb{C}[G]^{\#}$.

**Proposition I.5.2.** *For $i \neq j$, the subspaces $M(\rho_i)$ and $M(\rho_j)$ are orthogonal.*

*Proof.* These subspaces afford non-equivalent irreducible representations of $G \times G$. Therefore the following general assertion applies. □

**Lemma I.5.3.** *Let $E$ be a $G$-module and $U, V$ are minimal invariant subspaces of $E$. If $U$ and $V$ afford non-equivalent representations of $G$, then they are orthogonal with respect to any invariant inner product on $E$.*

*Proof.* Let $T$ be a $G$-invariant inner product on $E$. Consider the invariant projection $p : E \to U$ whose kernel is $U^{\perp_T}$. Then the $G$-homomorphism $p|_V : V \to U$ is zero in virtue of Schur's lemma. That is, $V \subset U^{\perp_T}$. □

**Theorem I.5.4** (Orthogonality relations for characters). *The simple characters form an orthonormal basis in $\mathbb{C}[G]^{\#}$.*

*Proof.* Since $\chi_i \in M(\rho_i)$, the orthogonality of $\chi_i$'s follows from Proposition I.5.2. To compute the norm of a simple character, we use the decomposition of the right regular representation: $R \simeq \sum_i n_i\rho_i$ and an explicit expression for $\chi_R$. Notice that $\mathbb{C}[G]$ has a basis consisting of $\delta$-functions $\{h^\sigma \mid \sigma \in G\}$, where $h^\sigma(\sigma') = \delta_{\sigma,\sigma'}$. Since $G$ acts via permutations in this basis, one readily obtains

$$\chi_R(\sigma) = \begin{cases} 0, & \sigma \neq \mathbb{1}, \\ \#G, & \sigma = \mathbb{1}. \end{cases}$$

Therefore $n_i = (\chi_R|\chi_i) = n_i(\chi_i|\chi_i)$, and we are done. □

**Corollary I.5.5.** *The norm of a complex character is a non-negative integer. A complex character of G is irreducible if and only if its norm equals 1.*

**I.5.3. The isotypic decomposition of a $G$-module.** Let $(G, \psi, E)$ be an arbitrary representation and $\psi \simeq \sum_{i=1}^m k_i\rho_i$. As we know, the multiplicities $k_i$ are well-defined. Choosing somehow a decomposition of $E$ into a direct sum of minimal invariant subspaces, we may construct for each $i$ the subspace $E[i] \subset E$ that affords the representation $k_i\rho_i$. Our goal is to prove that the subspaces $\{E[i]\}$, $i = 1, \dots, m$, do not depend on the choice of minimal invariant subspaces. To this end, it is enough to construct the canonical $G$-equivariant projection $E \to E[i]$ for each $i$.

**Proposition I.5.6.** *The operator* $\mathsf{P}_j = \dfrac{\deg\rho_j}{\#G}\displaystyle\sum_{\sigma\in G}\psi(\sigma)\overline{\chi_j(\sigma)} \in \mathrm{End}\,(E)$ *is the $G$-equivariant projection to $E[j]$.*

*Proof.* It follows from the definition that $\mathsf{P}_j$ is a $G$-equivariant operator. Therefore its restriction to any minimal invariant subspace is a scalar operator. Computing the trace of $\mathsf{P}_j$ on minimal invariant subspaces of all types, we obtain

$$\mathrm{tr}\,(\mathsf{P}_j|_{E_i}) = \frac{\deg\rho_j}{\#G}\sum_{\sigma\in G}\chi_i(\sigma)\overline{\chi_j(\sigma)} = \deg\rho_j(\chi_i|\chi_j) = \delta_{i,j}\deg\rho_j.$$

Hence $\mathsf{P}_j$ vanishes on $E_i$ if $i \neq j$ and is the identity operator on $E_j$. Since the definition of $\mathsf{P}_j$ does not depend on the choice of a decomposition, we see that $E[j]$ is canonically defined as the image of $\mathsf{P}_j$. □

In this way, one obtains the canonical decomposition of a representation space that is called the *isotypic decomposition*. Notice that $E^G$ is the isotypic component corresponding to the trivial representation. However, if $k_i > 1$ then the further splitting of $E[i]$ is not unique.

**Remark.** One can establish the orthogonality relations for characters over "any" field. Let us just set

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{\#G} \sum_{\sigma \in G} \chi_1(\sigma)\chi_2(\sigma^{-1}). \tag{I.5.3}$$

If $\Bbbk = \mathbb{C}$, then $\chi(\sigma^{-1}) = \overline{\chi(\sigma)}$. Hence Eq. (I.5.2) and (I.5.3) coincide whenever we only consider the characters of representations, i.e., actually the functions in $\mathbb{C}[G]^{\#}$.

**I.5.4. Orthogonality for matrix coefficients.** Here we obtain a refinement of Theorem I.5.4, which is, however, not quite canonical. Fix an invariant inner product in each $E_l$, $l = 1, \ldots, m$. By Proposition I.5.1, such a product is essentially unique. Choose an orthonormal basis for $E_l$, and let $\rho_{l,ij}$ be the matrix coefficients of $\rho_l$ with respect to this basis.

**Theorem I.5.7.** *The matrix coefficients $\rho_{l,ij}$ form an orthogonal basis for $\mathbb{C}[G]$. Furthermore, $(\rho_{l,ij}|\rho_{l,ij}) = 1/\deg \rho_l$.*

*Proof.* In view of Proposition I.5.2, we may restrict ourselves with considering the matrix elements of a single representation.

Using the $G \times G$-isomorphism $\mu : \operatorname{End}_{\Bbbk}(E_l) \xrightarrow{\sim} M(\rho_l)$, we reduce the problem to linear operators on $E_l$. We define the inner product on $\operatorname{End}_{\Bbbk}(E_l)$ by $(\xi, \eta) \mapsto \langle \xi, \eta \rangle := \operatorname{tr}(\xi\eta^*)$, where $\eta^*$ stands for the adjoint operator[1] of $\eta$ with respect to the fixed inner product on $E_l$. This inner product is $G \times G$-invariant. Indeed,

$$\langle \rho(g_1)\xi\rho(g_2)^{-1}, \rho(g_1)\eta\rho(g_2)^{-1} \rangle = \operatorname{tr}(\rho(g_1)\xi\rho(g_2)^{-1}\rho(g_2)^{*-1}\eta^*\rho(g_1)^*) = \\ = \operatorname{tr}(\rho(g_1)\xi\eta^*\rho(g_1)^*) = \operatorname{tr}(\xi\eta^*).$$

Here we used the fact that $\rho_i(\xi)$ and $\rho_i(\eta)$ are unitary operators and therefore their adjoint are equal to their inverses. It follows form Proposition I.5.1 that pushing forward this inner product to $M(\rho_l)$, we obtain, up to a scalar (real) multiple, the restriction of the inner product defined by Eq. (I.5.2).

It is easily seen that the matrix elements $\rho_{l,ij}$ corresponds to the matrix units $e_{ij} \in \operatorname{End}_{\Bbbk}(E_l)$ with respect to the fixed orthonormal basis of $E_i$, and that the matrix units form an *orthonormal* basis in $\operatorname{End}_{\Bbbk}(E_l)$ with respect to the Hermitian form $\operatorname{tr}(\xi\eta^*)$. Hence the matrix coefficients are pairwise orthogonal, and have the same norm.

It remains to compute the norms of matrix elements. Since the matrices $\rho_l(\sigma)$ are unitary, we have

$$\sum_j \rho_{l,ij}(\sigma)\overline{\rho_{l,ij}(\sigma)} = 1$$

[1] The adjoint operator of $A : E_l \to E_l$ is the operator $A^*$ such that $\langle Ax, y \rangle = \langle x, A^*y \rangle$ for all $x, y \in E_l$.

for each $\sigma$. Taking the sum over all $\sigma \in G$ and dividing by $\#G$, we obtain

$$\sum_j (\rho_{l,ij} | \rho_{l,ij}) = 1.$$

Hence $(\rho_{l,ij}|\rho_{l,ij}) = 1/\dim E_l$, as required. □

**I.5.5. The index of an irreducible representation.** Let $\chi_\rho$ be the character of an non-trivial irreducible representation $\rho$ in $E$. Then $\sum_{\sigma\in G} \chi_\rho(\sigma) = 0$. Indeed, up to a scalar multiple, it is the inner product of $\chi_\rho$ and the character of the trivial representation. It turns out that the sum of $\chi_\rho(\sigma^2)$ also has an interesting description. Recall that $\rho$ is said to be *self-dual*, if $\rho \simeq \rho^*$. In this case, $E_\rho$ has a $G$-invariant non-degenerate bilinear form. If $\rho$ is irreducible and self-dual, then such a form is unique up to a scalar multiple (cf. Proposition I.5.1). Therefore a $G$-invariant bilinear form is either symmetric or alternate.

**Theorem I.5.8.** *For any irreducible representation, we have* $\dfrac{1}{\#G}\displaystyle\sum_{\sigma\in G} \chi_\rho(\sigma^2) \in \{-1, 0, 1\}$. *These cases correspond to the following situations:*

$0$: $\rho \not\simeq \rho^*$;

$+1$: $\rho \simeq \rho^*$ *and a* $G$*-invariant bilinear form on* $E_\rho$ *is symmetric;*

$-1$: $\rho \simeq \rho^*$ *and a* $G$*-invariant bilinear form on* $E_\rho$ *is alternate.*

*Proof.* Let $S^2\rho$ and $\wedge^2\rho$ denote the second symmetric and exterior power of $\rho$, respectively. Then an easy calculation with the eigenvalues shows that

$$\chi_\rho(\sigma^2) = \chi_{S^2\rho}(\sigma) - \chi_{\wedge^2\rho}(\sigma).$$

Therefore the sum in question equals $\dim(S^2E)^G - \dim(\wedge^2E)^G$. On the other hand, $S^2\rho + \wedge^2\rho \simeq \rho\otimes\rho$ and it follows from Schur's lemma that $\dim(E\otimes E)^G = \dim \mathrm{Hom}_G(E, E^*) \leqslant 1$. In other words, $\dim(S^2E)^G + \dim(\wedge^2E)^G \leqslant 1$ and it is equal to 1 if and only if $\rho \simeq \rho^*$. The rest is clear. □

**Definition 9.** The integer considered in Theorem I.5.8 is called the *index* of $\rho$, denoted $\mathrm{ind}\,(\rho)$.

**Remark.** If $\mathrm{ind}\,(\rho) = 1$, then there is a basis for $E_\rho$ such that all matrices $\rho(\sigma)$ are real and orthogonal. Therefore such representations are said to be *of real type*. The representations with $\mathrm{ind}\,(\rho) = -1$ are also said to be *of quaternion type*.

Consider the function $\sigma \mapsto Q(\sigma) = \#\{x \in G \mid x^2 = \sigma\}$. Obviously, $Q \in \Bbbk[G]$ is a central function, hence it is a linear combination of simple characters. What are the coefficients?

**Exercise 5.** *Prove that* $Q = \sum_{\rho\in\widehat{G}} \mathrm{ind}\,(\rho)\chi_\rho$.
[Hint: compute the inner product $\langle Q, \chi_\rho\rangle$ and use the equality $Q(\sigma) = Q(\sigma^{-1})$.]

Let $\mathrm{inv}(G)$ denote the set of involutions of $G$. Taking the value of $Q$ at $\mathbb{1}$, we obtain

$$\#\mathrm{inv}(G) = \sum_{\rho \in \widehat{G}} \mathrm{ind}\,(\rho) \deg \rho.$$

### I.5.6. Some miscellaneous results.

1. One-dimensional representations and representations of abelian groups.

**Proposition I.5.9.** *All irreducible representations of $G$ are 1-dimensional if and only if $G$ is Abelian. In general, the number of the irreducible 1-dimensional representations equals $G/(G,G)$.*

2. Irreducible representations of $G_1 \times G_2$.

**Proposition I.5.10.** *Let $\{\rho_i\}_{i \in I}$ (resp. $\{\mu_j\}_{j \in J}$) be a full set of pairwise non-equivalent irreducible representations of $G_1$ (resp. $G_2$). Then $\{\rho_i \otimes \mu_j\}_{i \in I, j \in J}$ is a full set of pairwise non-equivalent irreducible representations of $G_1 \times G_2$.*

*Proof.* By Theorem I.2.8, all the representations $\rho_i \otimes \mu_j$ are irreducible. On the other hand, $\#\mathrm{conj}(G_1 \times G_2) = \#\mathrm{conj}(G) {\cdot} \#\mathrm{conj}(G_2)$. Hence $G_1 \times G_2$ has $\#(I \times J)$ irreducible representations. □

3. Burnside's Theorem.

**Theorem I.5.11.** *If $\rho \in \widehat{G}$, then the span of all operators $\rho(\sigma)$, $\sigma \in G$, equals* $\mathrm{End}\,(E_\rho)$.

## I.6. The group algebra of $G$ and its properties

The vector space $\Bbbk[G] = \{f : G \to \Bbbk\}$ has a natural structure of associative algebra. Every function $f \in \Bbbk[G]$ can be written as a formal linear combination $f = \sum_{\sigma \in G} f_\sigma \sigma$, where $f_\sigma = f(\sigma) \in \Bbbk$. In the last form, the multiplication in $\Bbbk[G]$ is given by the formula

$$(\sum_{\sigma \in G} f_\sigma \sigma)(\sum_{\tau \in G} g_\tau \tau) = \sum_{\sigma, \tau \in G} f_\sigma g_\tau (\sigma\tau).$$

In the former "functional" realisation, the multiplication of $f, g \in \Bbbk[G]$ is the *convolution*. That is,

$$(f * g)(\sigma) = \sum_{\tau \in G} f(\tau) g(\tau^{-1}\sigma).$$

**Exercise 6.** *Convince yourself that the above two formulae define the same product in* $\Bbbk[G]$.

The vector space $\Bbbk[G]$ equipped with this product is said to be the *group algebra of $G$*. The two realisations of $\Bbbk[G]$ will be referred to as "functional" and "formal", respectively. We will use both realisations. Sometimes the formal realisation is more convenient, because then $G$ can naturally be regarded as a subset of $\Bbbk[G]$. Whenever we regard $\sigma \in G$ as a function, we write $h^\sigma$ for it (the delta-function supported at $\sigma$). For instance, $h^{\mathbb{I}}$ is the multiplicative unit of $\Bbbk[G]$.

Notice that the algebra $\Bbbk[G]$ is commutative if and only if $G$ is commutative. Let $\operatorname{conj}(G)$ denote the set of conjugacy classes in $G$. For $C \in \operatorname{conj}(G)$, set $\sigma_C := \sum\limits_{\sigma \in C} \sigma$. That is, $\sigma_C \in \Bbbk[G]$ is the characteristic function of the subset $C \subset G$.

**Proposition I.6.1.** *The elements $\sigma_C$, $C \in \operatorname{conj}(G)$ form a basis for the centre of $\Bbbk[G]$.*

*Proof.* Let $f = \sum f_\sigma \sigma$ and assume that $f\tau = \tau f$ for any $\tau \in G$. Then

$$\sum_{\sigma \in G} f_\sigma \tau^{-1} \sigma \tau = \sum_{\sigma \in G} f_\sigma \sigma.$$

Therefore $f_\nu = f_\sigma$ whenever $\nu$ and $\sigma$ are conjugate. The rest is clear. □

It follows that the centre of $\Bbbk[G]$ coincides with the space of central functions. Thus, we have two bases for $\Bbbk[G]^\#$: $\{\chi_\rho\}_{\rho \in \widehat{G}}$ and $\{\sigma_C\}_{C \in \operatorname{conj}(G)}$.

**Exercise 7.** *Let $\chi_1, \dots, \chi_m$ and $C_1, \dots, C_m$ be all the simple characters and conjugacy classes of $G$, respectively. Consider the $m \times m$ matrix $\mathcal{M} = (\chi_i(C_j))$. Prove that*
$|\det \mathcal{M}|^2 = \prod\limits_{i=1}^{m} \dfrac{\#G}{\#C_i}$.

The matrix $\mathcal{M}$ is called the *character table* of $G$. The $i$-th row of $\mathcal{M}$ contains all values of $\chi_i$.

If $\rho$ is a representation of $G$, then it naturally extends to the homomorphism of associative algebras $\Bbbk[G] \to \operatorname{End}_{\Bbbk}(E_\rho)$, which we denote by $\rho_a$. Recall from Theorem I.3.3 the $G \times G$-module decomposition $\Bbbk[G] = \oplus_{\rho \in \widehat{G}} M(\rho)$. Now we are in a position to relate this decomposition with the algebra structure of $\Bbbk[G]$.

**Theorem I.6.2.** *The group algebra $\Bbbk[G]$ is isomorphic to the direct sum of the matrix algebras $\operatorname{End}(E_\rho)$, $\rho \in \widehat{G}$.*

*Proof.* Consider $\rho_a : \Bbbk[G] \to \operatorname{End}_{\Bbbk}(E_\rho)$. It is an associative algebra homomorphism and a $G \times G$-homomorphism. Furthermore, $\rho_a$ is onto, since $\operatorname{End}(E_\rho)$ is a simple $G \times G$-module. It follows that $\ker(\rho_a) = \bigoplus\limits_{\rho' \in \widehat{G} \setminus \{\rho\}} M(\rho')$ and it is a subalgebra. Varying $\rho$, we conclude that each $M(\rho)$ is a subalgebra of $\Bbbk[G]$ that is isomorphic to $\operatorname{End}(E_\rho)$. □

**Corollary I.6.3.** *If $\chi_\rho$ is a simple character of $G$, then $\chi_\rho * \chi_\rho = \frac{\#G}{\deg \rho} \chi_\rho$.*

*Proof.* Since $\chi_\rho \in \operatorname{End}(E_\rho)$, we have $\chi_\rho * \chi_\rho \in \operatorname{End}(E_\rho)$ and it is still a central element of $\Bbbk[G]$. Hence $\chi_\rho * \chi_\rho$ is proportional to $\chi_\rho$. The corresponding coefficient is determined by comparing the values at $\mathbb{1}$. By definition, we have

$$\chi_\rho * \chi_\rho(\mathbb{1}) = \sum_{\tau \in G} \chi_\rho(\tau) \chi_\rho(\tau^{-1}) = \#G \langle \chi_\rho, \chi_\rho \rangle = \#G,$$

while $\chi_\rho(\mathbb{1}) = \deg \rho$. □

For any $\rho \in \widehat{G}$, let $e(\rho)$ denote the component of $h^{\mathbb{1}}$ in $M(\rho) \simeq \operatorname{End}(E_\rho)$.

**Proposition I.6.4.** $e(\rho) = \dfrac{\deg \rho}{\#G} \chi_\rho$.

*Proof.* Clearly, each $e(\rho)$ is a central element of $\Bbbk[G]$, hence $e(\rho) = \alpha \chi_\rho$ for some $\alpha \in \Bbbk$. As $e(\rho) * e(\rho) = e(\rho)$, $\alpha$ can be determined using Corollary I.6.3. □

As a consequence of Proposition, one obtains the identity in $\Bbbk[G]$

$$\sum_{\rho \in \widehat{G}} \frac{\deg \rho}{\#G} \chi_\rho = h^{\mathbb{1}}. \tag{I.6.4}$$

In particular, computing the values at $\mathbb{1}$ yields the known identity

$$\sum_{\rho \in \widehat{G}} (\deg \rho)^2 = \#G.$$

Using multiplicative properties of characters, we prove below an important property of representations.

**Theorem I.6.5.** *Suppose* $\operatorname{char} \Bbbk = 0$. *Then* $\deg \rho$ *divides the order of G for any* $\rho \in \widehat{G}$.

*Proof.* It follows from Corollary I.6.3 that $\chi_\rho^{n+1} = \left(\dfrac{\#G}{\deg \rho}\right)^n \chi_\rho$ and hence

$$\chi_\rho^{n+1}(\mathbb{1}) = \frac{(\#G)^n}{(\deg \rho)^{n-1}}.$$

In this formula, $n$ can be an arbitrary positive integer. The right-hand side is a rational number, while the left-hand side is written out as $\sum \chi_\rho(\sigma_1)\chi_\rho(\sigma_2)\ldots\chi_\rho(\sigma_{n+1})$, where the sum is taken over all $(n+1)$-tuples $(\sigma_1, \ldots, \sigma_{n+1}) \in G^{n+1}$ such that $\sigma_1 \cdots \sigma_{n+1} = \mathbb{1}$.

Below, we use some simple properties of algebraic numbers. By definition, $\alpha \in \Bbbk$ is an *algebraic number*, if it is a root of a monic polynomial with integral coefficients. Since we are in the characteristic zero case, $\mathbb{Q} \subset \Bbbk$. The following is true:

- the set of algebraic numbers is a subring of $\Bbbk$;
- if $\alpha \in \mathbb{Q}$ is algebraic, then actually $\alpha \in \mathbb{Z}$.

Being sums of roots of unity, the values of characters of finite groups are algebraic numbers. It follows the above description that $\chi_\rho^{n+1}(\mathbb{1})$ is also an algebraic number, which belongs to $\mathbb{Q}$. Hence $\dfrac{(\#G)^n}{(\deg \rho)^{n-1}} \in \mathbb{N}$ for any $n$, which is only possible if $\#G/\deg \rho \in \mathbb{N}$. □

## I.7. On finite $\mathbb{R}$-groups

In this section $\Bbbk = \mathbb{C}$.

**Definition 10.** A finite group $G$ is called an $\mathbb{R}$-*group*, if all irreducible characters of $G$ are real-valued.

Since the function $\sigma \mapsto \overline{\chi_\rho(\sigma)}$ is the character of the dual representation $\rho^*$, all irreducible representations of an $\mathbb{R}$-groups are self-dual, and vice versa. In view of Theorem I.5.8, this means that $G$ is an $\mathbb{R}$-group if and only if $\mathrm{ind}\,(\rho) \neq 0$ for any $\rho \in \widehat{G}$.

**Example I.7.1.** If $G$ is a cyclic group of order $m$, then it is an $\mathbb{R}$-group if and only if $m = 2$. The dihedral group of order $2n$ is an $\mathbb{R}$-group (see Exercise 4).

**Example I.7.2.** The symmetric group $\Sigma_3$ is an $\mathbb{R}$-group. Indeed, its character table is as follows:

| Conj. class | $\mathbb{I}$ | $(ij)$ | $(ijk)$ |
|---|---|---|---|
| $\chi_1$ $(triv)$ | 1 | 1 | 1 |
| $\chi_2$ $(sign)$ | 1 | -1 | 1 |
| $\chi_3$ (2-dim) | 2 | 0 | -1 |

Actually, $\Sigma_n$ is an $\mathbb{R}$-group for any $n$. It is a special case of a general fact that all irreducible representations of Weyl groups are defined over $\mathbb{Q}$.

Define the linear operator $\mathcal{A} : \mathbb{C}[G] \to \mathbb{C}[G]$ by the formula $(\mathcal{A}f)(\sigma) = f(\sigma^{-1})$. In the formal realisation, we just have $\mathcal{A}(\sum f_\sigma \sigma) = \sum f_\sigma \sigma^{-1}$. Clearly, $\mathcal{A}^2 = id$ and it is easily seen that $\mathcal{A}(f * g) = \mathcal{A}g * \mathcal{A}f$. For this reason, $\mathcal{A}$ is called the *anti-involution* of $\mathbb{C}[G]$.

Below we provide some other characterisations of $\mathbb{R}$-groups.

**Theorem I.7.3.** *The following properties of G are equivalent:*

(i) *$G$ is an $\mathbb{R}$-group;*
(ii) *Any $\sigma \in G$ is conjugate to $\sigma^{-1}$;*
(iii) *The function $\sigma \mapsto Q(\sigma) = \#\{x \in G \mid x^2 = \sigma\}$ is invertible with respect to convolution; i.e., there is a function $Q' \in \mathbb{C}[G]$ such that $Q * Q' = h^{\mathbb{I}}$.*
(iv) *The anti-involution $\mathcal{A} : \mathbb{C}[G] \to \mathbb{C}[G]$ commutes with the convolutions with all elements of the center of $\mathbb{C}[G]$.*

*Proof.* (i)$\Longleftrightarrow$(ii). If $G$ is an $\mathbb{R}$-group, then the characters do not distinguish $\sigma$ and $\sigma^{-1}$, since $\chi(\sigma^{-1}) = \overline{\chi(\sigma)}$. As the characters form a basis for the space of central functions, $\sigma$ and $\sigma^{-1}$ belong to the same conjugacy class.

This argument can be reversed.

(i)$\Longleftrightarrow$(iii). According to Exercise 5, $Q = \sum \mathrm{ind}\,(\rho)\chi_\rho$. Comparing with Eq. (I.6.4) shows that $Q$ is invertible if and only if its component in each $M(\rho)$ is non-trivial, i.e., $\mathrm{ind}\,(\rho) \neq 0$.

(i)$\Longleftrightarrow$(iv). Because the centre of $\Bbbk[G]$ is spanned by the simple characters, we have to compare the functions $\mathcal{A}(\chi_\rho * f)$ and $\chi_\rho * \mathcal{A}f$ for an arbitrary $\rho \in \widehat{G}$ and $f \in \mathbb{C}[G]$. Take $f = h^\sigma$, the delta-function corresponding to $\sigma \in G$ (in the functional interpretation), and compute the value of both functions at $\tau \in G$. We obtain:

$$\mathcal{A}(\chi_\rho * h^\sigma)(\tau) = \chi_\rho(\tau^{-1}\sigma^{-1}) = \overline{\chi_\rho(\sigma\tau)} \text{ and } (\chi_\rho * \mathcal{A}(h^\sigma))(\tau) = \chi_\rho(\sigma\tau). \qquad \square$$

The proof of equivalence of (i) and (iii) shows that the inverse of $Q$ is equal to $Q' = \sum_\rho \frac{1}{\operatorname{ind}(\rho)} \left(\frac{\deg\rho}{\#G}\right)^2 \chi_\rho$.

**Example I.7.4.** For $G = \Sigma_3$, we have

$$Q = \chi_{triv} + \chi_{sign} + \chi_{2dim} = 4\mathbb{1} + (123) + (132),$$
$$Q' = \frac{1}{36}\chi_{triv} + \frac{1}{36}\chi_{sign} + \frac{1}{9}\chi_{2dim} = \frac{5}{18}\mathbb{1} - \frac{1}{18}(123) - \frac{1}{18}(132).$$

**Exercise 8.** *The group of quaternion units* $\mathsf{Q}$ *is determined by generators and relations as follows:* $\mathsf{Q} = \langle a, b \mid a^4 = b^4 = \mathbb{1},\ bab^{-1} = a^{-1},\ a^2 = b^2\rangle$. *Determine the conjugacy classes and irreducible representations of* $\mathsf{Q}$*, fill in the character table, and compute the indices.*

[*Answer*: the 1-dimensional representations have index 1 and the unique 2-dimensional representation has index $-1$.]

**Exercise 9.** *Prove the identity*

$$\sum_{\rho\in\widehat{G}} \operatorname{ind}(\rho)^m (\deg\rho)^{2-m} = (\#G)^{1-m} Q^m(\mathbb{1}), \quad m \geqslant 0.$$

*Derive from this that the number of the self-dual irreducible representations of $G$ is equal to $Q^2(\mathbb{1})/\#G$.*

CHAPTER II

# Invariant theory of finite groups

In this chapter, $\Bbbk$ is an algebraically closed field of characteristic zero.

## II.1. Generalities on invariants of finite groups

Let $\rho : G \to GL(E)$ be a finite-dimensional representation of a finite group $G$. According to a general principle, this yields a representation (action) of $G$ in the space of functions on $E$. In the context of invariant theory, we restrict ourselves to the polynomial functions on $E$. In what follows, $\Bbbk[E]$ stands for the algebra of polynomials on $E$, which is identified with $\mathcal{S}^\bullet E^*$, the symmetric algebra (over $\Bbbk$) of the dual space $E^*$.

**II.1.1. Noether's bound for invariants.** As was proved earlier (Theorem I.2.5), any representation of $G$ is completely reducible. In invariant-theoretic terminology, this means that finite groups are *linearly-reductive*. By a general result of Invariant Theory, the algebra $\Bbbk[E]^G$ is finitely generated for any linearly-reductive group $G$. But in case of finite groups a more precise result is available. We will need the following auxiliary result:

**Lemma II.1.1.** *The polynomial algebra $\Bbbk[E]$ is generated, as vector space, by the powers of linear forms (i.e., polynomials of degree 1).*

**Theorem II.1.2** (E. Noether, 1916)**.** *The algebra of invariants $\Bbbk[E]^G$ is generated by polynomials of degree at most $\#G$. That is, the number of generators is at most $\binom{\#G+n}{n}$, where $\dim E = n$.*

*Proof.* $1^o$. Set $N = \#G$ and $\Bbbk[E]_{<N} = \{f \in \Bbbk[E] \mid \deg f \leqslant N-1\}$. Let $A$ be the subalgebra of $\Bbbk[E]^G$ generated by invariants of degree $\leqslant N$. Our goal is to prove that $A = \Bbbk[E]^G$.

$2^o$. Consider the vector space $B = A \cdot \Bbbk[E]_{<N} \subset \Bbbk[E]$. Let $\xi \in E^* = \Bbbk[E]_1$. Let us prove that $\xi^m \in B$ for any $m \in \mathbb{N}$. If $m < N$, then this follows from the definition of $B$. Next, consider the polynomial $\prod_{\sigma\in G}(t-\sigma\xi) = t^N + a_1t^{N-1} + \ldots + a_N$, where $a_i \in \Bbbk[E]^G$ and $\deg a_i = i$. Hence $a_i \in A$ for all $i$. Substituting $t = \xi$, we obtain

$$\xi^N \in A + \xi A + \ldots + \xi^{N-1}A.$$

By induction, we then obtain

$$\xi^m \in A + \xi A + \ldots + \xi^{N-1}A \quad \text{for any} \quad m \geqslant N.$$

Using Lemma II.1.1, we conclude that $B = \Bbbk[E]$.

$3^o$. Take an arbitrary $f \in \Bbbk[E]^G$. By virtue of part $2^o$, it can be written $f = \sum a_i f_i$, where $a_i \in A$ and $f_i \in \Bbbk[E]_{<N}$.

Let $f \mapsto f^\#$ denote the (degree-preserving) projection to $G$-invariants. Then

$$f = f^\# = \sum a_i f_i^\#,$$

where $f_i^\#$ is an invariant of degree $< N$. Hence $f \in A$, and we are done. □

There is a relative version of Noether's theorem concerning a "group–subgroup" pair $G \supset H$, see [2, Theorem 1.5.2].

**II.1.2. The isotypic decomposition and modules of covariants.** In Chapter I, we have defined the isotypic decomposition for any finite-dimensional $G$-module. Since $\Bbbk[E]$ is a direct sum of finite-dimensional $G$-modules, one can consider the isotypic components for $\Bbbk[E]$ as well. Hence, $\Bbbk[E] = \oplus_{\nu\in\hat G}\Bbbk[E]_{(\nu)}$. If $(G, \nu, \mathfrak{S})$ is an irreducible representation, then the corresponding isotypic component is denoted by either $\Bbbk[E]_{(\nu)}$ or $\Bbbk[E]_{(\mathfrak{S})}$. Clearly, $\Bbbk[E]^G$ is one of the isotypic components and each $\Bbbk[E]_{(\nu)}$ is a $\Bbbk[E]^G$-module.

**Proposition II.1.3.** *Each $\Bbbk[E]_{(\nu)}$ is a finitely generated $\Bbbk[E]^G$-module. More precisely, if $\nu$ is non-trivial, then $\Bbbk[E]_{(\nu)}$ is generated by elements of degree at most $\#G - 1$.*

**Exercise 10.** *Prove the proposition, using an adaptation of the previous proof.*

Let $\mathfrak{S}$ be a simple $G$-module and $\Bbbk[E]_{(\mathfrak{S})}$ the isotypic component of type $\mathfrak{S}$ in $\Bbbk[E]$. There is a natural isomorphism

$$\Bbbk[E]_{(\mathfrak{S})} \simeq \mathfrak{S} \otimes \mathrm{Hom}_G(\mathfrak{S}, \Bbbk[E])$$

and $\mathrm{Hom}_G(\mathfrak{S}, \Bbbk[E]) \simeq (\Bbbk[E] \otimes \mathfrak{S}^*)^G$. The latter is naturally a $\Bbbk[E]^G$-module. Let $\mathrm{Mor}_G(E, \mathfrak{S})$ be the vector space of all $G$-equivariant polynomial mappings $\alpha : E \to \mathfrak{S}$. The $\Bbbk[E]^G$-module structure on $\mathrm{Mor}_G(E, \mathfrak{S})$ is defined by

$$(f{\cdot}\alpha)(v) = f(v)\alpha(v), \quad \text{where } v \in E, f \in \Bbbk[E]^G, \text{and } \alpha \in \mathrm{Mor}_G(E, \mathfrak{S}).$$

**Lemma II.1.4.** *The $\Bbbk[E]^G$-modules $\mathrm{Mor}_G(E, \mathfrak{S})$ and $(\Bbbk[E] \otimes \mathfrak{S})^G$ are naturally isomorphic.*

*Proof.* Suppose $c = \sum f_i \otimes v_i \in (\Bbbk[E] \otimes \mathfrak{S})^G$, where $f_i \in \Bbbk[E]$ and $v_i \in \mathfrak{S}$. The corresponding mapping $\alpha_c : E \to \mathfrak{S}^*$ is defined by $\alpha_C(y) = \sum f_i(y)v_i$. Conversely, given a polynomial mapping $\alpha : E \to \mathfrak{S}$, we can write $\alpha(y) = \sum g_i(y)e_i$, where $(e_i)$ is a basis for $\mathfrak{S}$ and the $(g_i)$'s are polynomials on $E$. Then we associate to $\alpha$ the element $c_\alpha = \sum g_i \otimes e_i$. It is easily seen that the $G$-equivariance of $\alpha$ exactly means that $c_\alpha$ is a $G$-invariant element of the tensor product $\Bbbk[E] \otimes \mathfrak{S}$. □

In view of the lemma, $(\Bbbk[E]\otimes\mathfrak{S})^G$ is called *the module of covariants (of type* $\mathfrak{S}$). The previous discussion shows that the isotypic component of type $\mathfrak{S}$ gives rise to the module of covariants of type $\mathfrak{S}^*$, and vice versa.

**II.1.3. The ring extension $\Bbbk[E]\supset\Bbbk[E]^G$ and quotient variety.** Set $S=\Bbbk[E]$, $R=\Bbbk[E]^G$, and $R_+=\oplus_{i\geqslant 1}R_i$. Let $I$ be the ideal of $S$ generated by $R_+$, i.e., $I=SR_+$.

$1^o$. *Each element of* $\Bbbk[E]$ *is integral over* $\Bbbk[E]^G$.
Indeed, for any $f\in S$, $\prod_{\sigma\in G}(t-\sigma{\cdot}f)$ is a monic polynomial in $t$ with coefficients in $R$.

By a standard fact from Commutative algebra (see [1]), this property is equivalent to that $S$ is a finite $R$-module.

$2^o$. *$R$ is integrally closed in its field of fractions, $Q(R)$.*
For, if $g\in Q(R)$ is integral over $R$, then it is also integral over $S$. Being a polynomial algebra, $S$ is a unique factorisation domain. This easily implies that $g\in S$. Thus, $g\in S\cap Q(R)=R$.

$3^o$. $Q(R)=Q(S)^G$.
Clearly, there is an embedding $Q(R)\subset Q(S)^G$. Conversely, if $f=f_1/f_2\in Q(S)^G$, then one can also write

$$\frac{f_1}{f_2}=\frac{f_1\prod_{\sigma\ne 1\!\!1}\sigma{\cdot}f_2}{\prod_{\sigma\in G}\sigma{\cdot}f_2}\in Q(R)\ .$$

$4^o$. *The ideal $I$ is of finite codimension in $S$.*
This is just another way to say that $S$ is a finite $R$-module. More precisely, let $H$ be a subspace of $S$ such that $H\oplus I=S$. Then an easy argument shows that $H$ spans $S$ as $R$-module and that it is a minimal subspace having such property.

$5^o$. *If $v,v'\in E$ and $G{\cdot}v\ne G{\cdot}v'$, then there is an $f\in\Bbbk[E]^G$ such that $f(v)\ne f(v')$.*
Take any polynomial $p$ such that $p|_{G\cdot v}\equiv 1$ and $p|_{G\cdot v'}\equiv 0$. then $p^{\#}=(\sum_{\sigma\in G}\sigma{\cdot}p)/\#G$ is an invariant polynomial, which still has the same property.

Let $E/G$ denote the affine variety corresponding to $R$. The embedding $R\hookrightarrow S$ gives rise to a morphism $\pi: E\to E/G$. The above properties $1^o$, $2^o$, $5^o$ have the following geometric counterparts:

- $\pi$ is a finite morphism;
- $E/G$ is a normal variety;
- each fibre of $\pi$ consists of a single $G$-orbit; in particular, $\pi^{-1}(\pi(0))=\{0\}$.

## II.2. Graded algebras and graded modules

In order to deal with the algebra of invariants and isotypic components/modules of covariants, we have to discuss some general notions of Commutative algebra.

**II.2.1. Systems of parameters and regular sequences.** Let $\mathcal{A} = \bigoplus_{i\geqslant 0}\mathcal{A}_i$ be a commutative noetherian graded $\Bbbk$-algebra such that $\mathcal{A}_0 = \Bbbk$. In this case, each homogeneous space $\mathcal{A}_i$ is finite-dimensional over $\Bbbk$ and $\mathcal{A}_+ := \underset{i\geqslant 1}{\oplus}\mathcal{A}_i$ is a maximal ideal of $\mathcal{A}$. Let $\mathcal{M} = \oplus_{i\in\mathbb{Z}}\mathcal{M}_i$ be a $\mathbb{Z}$-graded noetherian $\mathcal{A}$-module. Then $\mathcal{M}_i = 0$ for $i \ll 0$ and $\dim\mathcal{M}_i < +\infty$ for all $i$. For brevity, we then say that $\mathcal{A}$ is a graded $\Bbbk$-algebra and $\mathcal{M}$ is a graded $\mathcal{A}$-module. The *annihilator* of $\mathcal{M}$ is $\mathrm{Ann}_{\mathcal{A}}\mathcal{M} = \{a \in \mathcal{A} \mid am = 0 \text{ for any } m \in \mathcal{M}\}$. Clearly, it is an ideal of $\mathcal{A}$, and $\mathcal{A}/\mathrm{Ann}_{\mathcal{A}}\mathcal{M}$ is again a graded $\Bbbk$-algebra.

There are homogeneous algebraically independent elements $f_1, \dots, f_r \in \mathcal{A}$ such that $\mathcal{A}$ is a finite $\Bbbk[f_1, \dots, f_r]$-module, see e.g. [2]. The family $\{f_1, \dots, f_r\}$ is called a *homogeneous system of parameters* (h.s.o.p.) (in $\mathcal{A}$). Then $r$ is necessarily the Krull dimension of $\mathcal{A}$, denoted $K\!\dim\mathcal{A}$.

**Definition 11.** A graded $\mathcal{A}$-module $\mathcal{M}$ is called *Cohen-Macaulay* (CM for short) if $\mathcal{M}$ is a free $\Bbbk[f_1, \dots, f_r]$-module for $\underline{\text{some}}$ h.s.o.p. $f_1, \dots, f_r \in \mathcal{A}/\mathrm{Ann}_{\mathcal{A}}\mathcal{M}$. An algebra $\mathcal{A}$ is called a Cohen-Macaulay (CM) algebra if it is a CM $\mathcal{A}$-module.

Notice that $\mathrm{Ann}_{\mathcal{A}}\mathcal{A} = 0$, so that a h.s.o.p. for $\mathcal{A}$ is a sequence in $\mathcal{A}$. A key result from Commutative Algebra asserts that the property of being CM does not depend on h.s.o.p., that is, if $\mathcal{M}$ is a CM $\mathcal{A}$-module, then $\mathcal{M}$ is a free $\Bbbk[g_1, \dots, g_r]$-module for $\underline{\text{any}}$ h.s.o.p. $\{g_1, \dots, g_r\}$ in $\mathcal{A}/\mathrm{Ann}_{\mathcal{A}}\mathcal{M}$.

Obviously, Definition 11 shows that a polynomial algebra is Cohen-Macaulay. But the passage from "some h.s.o.p." to "any h.s.o.p." is non-trivial even in this case. This fact for polynomial algebras was essentially proved by Macaulay in 1916.

**Definition 12.** Let $f_1, \dots, f_l$ be a sequence of homogeneous elements of $\mathcal{A}_+$. Then $(f_1, \dots, f_l)$ is called a *regular sequence* (for $\mathcal{A}$) if $f_i$ is not a zero-divisor in $\mathcal{A}/(f_1, \dots, f_{i-1})$ for each $i$. The integer $l$ is called the *length* of a regular sequence.

It can be shown that the elements of a regular sequence are algebraically independent (try to prove this!); in particular, $l \leqslant K\!\dim\mathcal{A}$.

**Proposition II.2.1.** (i) *A sequence $(f_1, \dots, f_l)$ is regular if and only if $\mathcal{A}$ is a free $\Bbbk[f_1, \dots, f_l]$-module (not necessarily of finite rank);* (ii) *Suppose that $\mathcal{A}$ has a regular sequence $f_1, \dots, f_r$, where $r = K\!\dim\mathcal{A}$. Then $f_1, \dots, f_r$ is a h.s.o.p. and $\mathcal{A}$ is a free $\Bbbk[f_1, \dots, f_r]$-module.*

This shows that for graded algebras the property of being CM can also be stated as follows: *A graded algebra $\mathcal{A}$ is CM if and only if it has a regular sequence of length $K\!\dim A$.*

**II.2.2. The Poincaré series of a graded module.**
Since $\dim\mathcal{M}_i < \infty$ for all $i$, the formal power series

$$F(\mathcal{M};t) = \sum_{i\geqslant 0}(\dim\mathcal{M}_i)t^i \in \mathbb{Z}[[t]]$$

is well-defined. We say that $F(\mathcal{M};t)$ is the *Poincaré series* of $\mathcal{M}$. In particular, we may take $\mathcal{M}=\mathcal{A}$.

**Theorem II.2.2** (Hilbert-Serre). *The Poincaré series $F(\mathcal{M};t)$ is (the Taylor expansion of) a rational function. More precisely, if $a_1,\dots,a_n$ are homogeneous generators of $\mathcal{A}$ and $\deg a_i=d_i$, then there is a polynomial $p(t)\in\mathbb{Z}[t]$ such that*

$$F(\mathcal{M};t)=\frac{p(t)}{\prod_{i=1}^{n}(1-t^{d_i})}\ . \tag{II.2.1}$$

*Proof.* We argue by induction on $n$. If $n=0$, then $\mathcal{M}$ is finite-dimensional over $\mathcal{A}=\Bbbk$ and $F(\mathcal{M};t)$ is a polynomial. Assume that $n>0$ and the assertion is true for algebras with fewer than $n$ generators. Let $\phi:\mathcal{M}\to\mathcal{M}$ be the endomorphism defined by $\phi(m)=a_nm$. This yields two exact sequences of graded $\mathcal{A}$-modules:

$$0\to\ker\phi\to\mathcal{M}\to\mathcal{M}/\ker\phi\to 0,$$
$$0\to\operatorname{Im}\phi\to\mathcal{M}\to\mathcal{M}/\operatorname{Im}\phi\to 0\ .$$

Then we have $(\mathcal{M}/\ker\phi)_d\simeq(\operatorname{Im}\phi)_{d+d_n}$. Using the fact that the Poincare series is additive for short exact sequences of graded $\mathcal{A}$-modules, we deduce from this that

$$F(\mathcal{M};t)=F(\ker\phi;t)+t^{-d_n}F(\operatorname{Im}\phi;t),$$
$$F(\mathcal{M};t)=F(\mathcal{M}/\operatorname{Im}\phi;t)+F(\operatorname{Im}\phi;t)\ .$$

It follows that $(1-t^{d_n})F(\mathcal{M};t)=F(\mathcal{M}/\operatorname{Im}\phi;t)-t^{d_n}F(\ker\phi;t)$. Now $\mathcal{M}/\operatorname{Im}\phi$ and $\ker\phi$ are modules over the graded algebra $\mathcal{A}/a_n\mathcal{A}$ that is generated by $n-1$ elements. The assertion now follows by induction. □

If $\mathcal{M}$ is a CM $\mathcal{A}$-module, then the rational function $F(\mathcal{M};t)$ can be written such that the numerator $p(t)$ is a polynomial with *nonnegative* coefficients. Indeed, if $f_1,\dots,f_n$ is h.s.o.p. for $\mathcal{M}$, with $\deg f_i=d_i$, and $\eta_1,\dots,\eta_l$ is a homogeneous basis for the free $\Bbbk[f_1,\dots,f_n]$-module $\mathcal{M}$ with $\deg\eta_j=e_j$, then

$$F(\mathcal{M};t)=\frac{t^{e_1}+\ldots+t^{e_l}}{\prod_{i=1}^{n}(1-t^{d_i})}\ .$$

A connection between regular sequences and Poincaré series is revealed in the following assertion.

**Proposition II.2.3.**
(i) *Suppose $f\in\mathcal{A}_d$ is not a zero-divisor. Then $F(\mathcal{A}/(f);t)=F(\mathcal{A};t)(1-t^d)$;*
(ii) *If $f_1,\dots,f_m$ is a regular sequence in $\mathcal{A}$ and $\deg f_i=d_i$, then $F(\mathcal{A}/(f_1,\dots,f_m);t)=F(\mathcal{A};t)\prod_{i=1}^{m}(1-t^{d_i})$.*

*Proof.* Part (ii) follows from (i) by induction. Part (i) follows from the equality $\dim(\mathcal{A}/(f))_m = \dim \mathcal{A}_m - \dim(f\mathcal{A})_m = \dim \mathcal{A}_m - \dim(\mathcal{A})_{m-d}$. □

This proposition has a natural extension to graded $\mathcal{A}$-modules, which is left to the reader.

**II.2.3. Some formulae for rational functions.** Let $F(t)$ be a rational function of the form

$$F(t) = \frac{p(t)}{\prod_{i=1}^{n}(1-t^{d_i})}, \text{ where } p(t) \in \mathbb{Z}[t] \text{ and } d_i \in \mathbb{N}.$$

We wish to have explicit formulae for the first two terms of the Laurent expansion of $F(t)$ about $t = 1$. If $p(1) \neq 0$, then $F(t)$ has the pole of order $n$ at $t = 1$ and the Laurent expansion starts as $F(t) = \dfrac{\gamma}{(1-t)^n} + \dfrac{\tau}{(1-t)^{n-1}} + \dots$
Then the direct computation shows that

$$\text{(II.2.2)} \qquad \gamma = \frac{p(1)}{\prod_{i=1}^{n} d_i} \text{ and } \frac{2\tau}{\gamma} = \sum_{i=1}^{n}(d_i - 1) - 2\frac{p'(1)}{p(1)} .$$

(Here $p'$ denotes the derivative.) Suppose that $p(t)$ has non-negative coefficients. This condition is satisfied in the invariant-theoretic situation that is of interest for us. Then we can write $p(t) = t^{e_1} + \dots + t^{e_l}$, where $e_1 \leqslant \dots \leqslant e_l$. Then $p(1) = l$ and $p'(1) = \sum_{i=1}^{l} e_i$.

The *degree* of $F$ is the integer $\deg F = \deg p - \sum d_i = e_l - \sum d_i$. If $p(t)$ is a reciprocal polynomial, that is to say, $e_i + e_{l+1-i}$ does not depend on $i$, then $\frac{2}{l}\sum e_i = e_1 + e_l$. Hence

$$2\tau/\gamma = \text{(degree of denominator)} - \text{(degree of numerator)} - n - e_1.$$

In particular, if $p(t)$ is reciprocal and $e_1 = 0$, then

$$2\tau/\gamma = -\deg F - n.$$

In case $p(t)$ is reciprocal, we have a simple relation between the rational functions $F(t)$ and $F(t^{-1})$:

$$F(t^{-1}) = (-1)^n t^{\sum d_i - (e_1+e_l)} F(t) = (-1)^n t^{\frac{2\tau}{\gamma} - n} F(t).$$

**II.2.4. Applications to isotypic components.**

**Theorem II.2.4.** *Let $(G, \rho, E)$ be a finite-dimensional representation of a finite group. Then each isotypic component $\Bbbk[E]_{(\nu)}$ is a Cohen-Macaulay $\Bbbk[E]^G$-module. In particular, the algebra of invariants $\Bbbk[E]^G$ is Cohen-Macaulay.*

*Proof.* Since $\Bbbk[E]$ is a finite $\Bbbk[E]^G$-module, the Krull dimension of $\Bbbk[E]^G$ equals that of $\Bbbk[E]$, i.e., $n = \dim E$. Therefore, if $\{f_1, \dots, f_n\}$ is a h.s.o.p. in $\Bbbk[E]^G$, then it is also a h.s.o.p. in $\Bbbk[E]$. Since $\Bbbk[E]$ is CM, it is a free $\Bbbk[f_1, \dots, f_n]$-module. Hence each isotypic component is also a free module. (For, in the graded situation, a direct summand of a free finitely-generated module is again free.) □

Since $\Bbbk[E]$ is a domain, the annihilator (in $\Bbbk[E]^G$) of each isotypic component is trivial.

As a consequence of this theorem and the previous theory, we see that if $f_1, \dots, f_n \in \Bbbk[E]^G$ is h.s.o.p., then it is a regular sequence in $\Bbbk[E]$ and $\Bbbk[E]/(f_1, \dots, f_n)$ is finite-dimensional.

**Remark.** An anologue of Theorem II.2.4 is not true in case of infinite reductive groups. If $H$ is a connected reductive groups, then the number of isotypic components is infinite for any non-trivial irreducible representation $\rho : H \to GL(V)$. However, for all but finitely many irreducible representations, the number of CM isotypic components $\Bbbk[V]_{(\nu)}$ is finite.

## II.3. Molien's formula and symmetries of Poincaré series

**II.3.1. Molien's formula.** Let $G$ be a finite subgroup of $GL(E)$. Since the algebra of invariants $\Bbbk[E]^G$ is graded, one may consider the corresponding Poincaré series. An explicit form of it is given by *Molien's formula*.

**Theorem II.3.1** (T. Molien, 1897).

$$F(\Bbbk[E]^G; t) = \frac{1}{\#G} \sum_{\sigma \in G} \frac{1}{\det(id_E - \sigma t)}. \tag{II.3.3}$$

*Proof.* Since $\dim V^G = \dim(V^*)^G$ for any $G$-module $V$, we may compute the Poincaré series for $\mathcal{S}^\bullet E = \oplus_{m \geqslant 0} \mathcal{S}^m E$, the symmetric algebra of $E$.

Recall that the averaging operator $T_G = \frac{1}{\#G} \sum_{\sigma \in G} \sigma$ yields the projection to the subspace of fixed elements in any $G$-module. Therefore $\operatorname{tr}(T_G)$ equals the dimension of the fixed-point subspace. Applying this to the symmetric powers of $E$, we obtain

$$\dim(\mathcal{S}^m E)^G = \frac{1}{\#G} \sum_{\sigma \in G} \chi_{\mathcal{S}^m E}(\sigma).$$

Hence

$$F(\Bbbk[E]^G; t) = F(\mathcal{S}^\bullet E; t) = \frac{1}{\#G} \sum_{\sigma \in G} \sum_{m \geqslant 0} \chi_{\mathcal{S}^m E}(\sigma) t^m. \tag{II.3.4}$$

Let us compute the contribution of each $\sigma$ to this expression. Suppose $\dim E = n$ and $\gamma_1, \dots, \gamma_n$ are the eigenvalues of $\sigma$ in $E$. Then

$$\chi_{\mathcal{S}^m E}(\sigma) = \sum_{k_1 + \dots + k_n = m} \gamma_1^{k_1} \dots \gamma_n^{k_n}$$

and hence

$$\sum_{m \geqslant 0} \chi_{\mathcal{S}^m E}(\sigma) t^m = \sum_{m \geqslant 0} \sum_{k_1 + \dots + k_n = m} \gamma_1^{k_1} \dots \gamma_n^{k_n} t^m = \prod_{j=1}^n \sum_{k_j \geqslant 0} (\gamma_j t)^{k_j} = \prod_{j=1}^n \frac{1}{1 - \gamma_j t} = \frac{1}{\det(id_E - \sigma t)}.$$

Substituting this to Eq. (II.3.4), we obtain Molien's formula. □

**Exercise 11.** *Prove an "exterior" analogue of Molien's formula:*

$$F((\wedge^\bullet E)^G;t)=\sum_{m=0}^{\dim E}(\wedge^m E)^G t^m=\frac{1}{\#G}\sum_{\sigma\in G}\det(id_E+\sigma t).$$

Recall that an element of finite order $\sigma\in GL(E)$ is called a *reflection* if $\mathrm{rk}\,(id_E-\sigma)=1$. This means that $\sigma$ has precisely one eigenvalue not equal to 1.[1] Write $\varepsilon_\sigma$ for this eigenvalue. Let $\mathcal{R}(G)$ denote the set of all reflection in $G$. Set $r(G)=\#\mathcal{R}(G)$. If $\sigma\in\mathcal{R}(G)$, then the hyperplane $E^\sigma$ is called a *reflecting hyperplane* of $G$. The set of all reflecting hyperplanes is denoted by $\mathcal{H}(G)$.

**Theorem II.3.2.** *The Laurent expansion of $F(\Bbbk[E]^G;t)$ about $t=1$ starts as follows:*

$$F(\Bbbk[E]^G;t)=\frac{1}{\#G}\left(\frac{1}{(1-t)^n}+\frac{r(G)/2}{(1-t)^{n-1}}+\dots\right)$$

*That is,* $\gamma(\Bbbk[E]^G)=\dfrac{1}{\#G}$ *and* $\tau(\Bbbk[E]^G)=\dfrac{r(G)}{2{\cdot}\#G}$.

*Proof.* Let us look at the contribution of various $\sigma\in G$ to Molien's formula. If $\sigma=\mathbb{1}$, then $\det(id_E-\sigma t)=(1-t)^n$. In general, if $\nu_1,\dots,\nu_n$ are the eigenvalues of $\sigma$, then $\det(id_E-\sigma t)=\prod_i(1-\nu_i t)$. It follows that if $\dim E^\sigma=k\leqslant n$, then the term $1/\det(id_E-\sigma t)$ does not affect the summands $\frac{a_{-n}}{(1-t)^n}+\frac{a_{-n+1}}{(1-t)^{n-1}}+\dots+\frac{a_{-k-1}}{(1-t)^{k+1}}$ of the Laurent series. This already proves the formula for $a_{-n}=\gamma(\Bbbk[E]^G)$ and shows that $\tau(\Bbbk[E]^G)$ depends only on terms $\dfrac{1}{\det(id_E-\sigma t)}$ with $\sigma\in\mathcal{R}(G)$. Then

$$\sum_{\sigma\in\mathcal{R}(G)}\frac{1}{\det(id_E-\sigma t)}=\frac{1}{(1-t)^{n-1}}\sum_{\sigma\in\mathcal{R}(G)}\frac{1}{1-\varepsilon_\sigma t}. \tag{II.3.5}$$

If $\sigma\in\mathcal{R}(G)$, then $\sigma^{-1}\in\mathcal{R}(G)$ as well. Therefore for any $\varepsilon_\sigma$ the inverse $\varepsilon_\sigma^{-1}$ also occurs in this set of eigenvalues. Since $\left(\dfrac{1}{1-\varepsilon t}+\dfrac{1}{1-\varepsilon^{-1}t}\right)|_{t=1}=1$, the Taylor expansion of $\displaystyle\sum_{\sigma\in\mathcal{R}(G)}\frac{1}{1-\varepsilon_\sigma t}$ about $t=1$ starts with the term $r(G)/2$. □

[1] Sometimes, especially in old literature, the reflections in our sense are called *pseudoreflections*, while the word "reflection" is reserved for pseudoreflections of order two.

**II.3.2. Molien's formula for isotypic components and modules of covariants.** Recall that the algebra of invariants is just one of many isotypic components sitting in $\Bbbk[E]$.

**Theorem II.3.3.** *Let $\Bbbk[E]_{(\mathfrak{S})}$ be the isotypic component corresponding to a a simple $G$-module $\mathfrak{S}$. Then its Poincaré series is given by the formula* [the Molien formula]

$$F(\Bbbk[E]_{(\mathfrak{S})};t)=\frac{\dim\mathfrak{S}}{\#G}\sum_{\sigma\in G}\frac{\mathrm{tr}\,(\sigma,\mathfrak{S})}{\det(id_E-\sigma t)}.$$

*Proof.* The proof is very similar to that of Theorem II.3.1. For each $S^m(E^*)$, one should use the projection onto the $\mathfrak{S}$-isotypic component (see Proposition I.5.6) in place of the averaging operator. □

This formula has some easy but still useful consequences. Recall that we assume that $G$ is a subgroup of $GL(E)$. In other words, we deal with a faithful representation of $G$.

**Corollary II.3.4.**
1. $\lim_{t\to 1}F(\Bbbk[E]_{(\mathfrak{S})};t)(1-t)^n=(\dim\mathfrak{S})^2/(\#G)$;
2. $\Bbbk[E]_{(\mathfrak{S})}\neq\varnothing$ *for any* $\mathfrak{S}$.

*Proof.* The second assertion follows from the first. To prove the first assertion, one should notice that only the summand corresponding to $\sigma=1\!\!1$ in the Molien formula contributes to the above limit. □

The second assertion can be stated as follows: *every simple $G$-module $\mathfrak{S}$ occurs in a suitable symmetric power of a faithful $G$-module.*

**Remark.** The above relations shows that $\Bbbk[E]_{(\mathfrak{S})}\simeq\mathfrak{S}\otimes(\Bbbk[E]\otimes\mathfrak{S}^*)^G$, hence $\dim\Bbbk[E]_{(\mathfrak{S}),n}=\dim\mathfrak{S}\cdot\dim(\Bbbk[E]_n\otimes\mathfrak{S}^*)^G$. Because $\mathrm{tr}\,(\sigma,\mathfrak{S}^*)=\mathrm{tr}\,(\sigma^{-1},\mathfrak{S})$, the Molien formula for modules of covariants can be written in the equivalent form

$$F((\Bbbk[E]\otimes\mathfrak{S})^G;t)=\frac{1}{\#G}\sum_{\sigma\in G}\frac{\mathrm{tr}\,(\sigma^{-1},\mathfrak{S})}{\det(id_E-\sigma t)}. \tag{II.3.6}$$

If $\mathfrak{S}$ is a one-dimensional $G$-module, then it corresponds to a linear character of $G$, $\mu: G\to\Bbbk^\times$. In this case, we write $\mathfrak{S}=\Bbbk_\mu$ and denote by $\Bbbk[E]_\mu$ the respective isotypic component. That is,

$$\Bbbk[E]_\mu=\{f\in\Bbbk[E]\mid\sigma{\cdot}f=\mu(\sigma)f\quad\forall\sigma\in G\}.$$

We also say that $\Bbbk[E]_\mu$ is the module of *semi-invariants* (= relative invariants) of weight $\mu$. For such modules of covariants, the formula of Theorem II.3.3 reads

$$F(\Bbbk[E]_\mu;t)=\frac{1}{\#G}\sum_{\sigma\in G}\frac{\mu(\sigma)}{\det(id_E-\sigma t)}\ . \tag{II.3.7}$$

Given a simple $G$-module $E$, there are several natural choices of modules of covariants, e.g., $\mathfrak{S} = \Bbbk$, $E$, $E^*$, and $\Bbbk_{\det}$, where $\det = \det_E$ is the linear character assigning the determinant $\det \rho_E(\sigma)$ to any $\sigma \in G$. The first choice gives us the algebra of invariants $\Bbbk[E]^G$. Our next goal is to look at the Laurent expansions of the Poincaré series in the other cases.

**Theorem II.3.5.** *The Laurent expansion of $F(\Bbbk[E]_{\det_E}; t)$ about $t = 1$ starts as follows:*

$$F(\Bbbk[E]_{\det_E}; t) = \frac{1}{\#G}\left(\frac{1}{(1-t)^n} - \frac{r(G)/2}{(1-t)^{n-1}} + \dots\right)$$

*Proof.* As in the proof of Theorem II.3.2, it is enough to calculate the contribution to Eq. (II.3.7) of the neutral element and all reflection in $G$.

For $\sigma = \mathbb{I}$, we obtain the term $\dfrac{1}{\#G}\dfrac{n}{(1-t)^n}$. If $\sigma \in \mathcal{R}(G)$, then

$$\frac{\det_E(\sigma)}{\det(id_E - \sigma t)} = \frac{\varepsilon_\sigma}{(1-t)^{n-1}(1-\varepsilon_\sigma t)}.$$

Therefore the coefficient of $1/(1-t)^{n-1}$ equals

$$\sum_{\sigma\in\mathcal{R}(G)} \frac{\varepsilon_\sigma}{1-\varepsilon_\sigma} = \sum_{\sigma\in\mathcal{R}(G)} (\frac{1}{1-\varepsilon_\sigma} - 1) = \frac{r(G)}{2} - \sum_{\sigma\in\mathcal{R}(G)} 1 = -\frac{r(G)}{2}.$$

□

**Theorem II.3.6.** *The Laurent expansion of $F((\Bbbk[E] \otimes E^*)^G; t)$ about $t = 1$ starts as follows:*

$$F((\Bbbk[E] \otimes E^*)^G; t) = \frac{1}{\#G}\left(\frac{n}{(1-t)^n} + \frac{r(G)(n/2-1)}{(1-t)^{n-1}} + \dots\right)$$

*Proof.* As in the proof of Theorem II.3.2, it is enough to calculate the contribution to Eq. (II.3.6) of the neutral element and all reflection in $G$.

If $\sigma \in \mathcal{R}(G)$, then

$$\frac{\operatorname{tr}(\sigma, E)}{\det(id_E - \sigma t)} = \frac{n - 1 + \varepsilon_\sigma}{(1-t)^{n-1}(1-\varepsilon_\sigma t)}.$$

Therefore the coefficient of $1/(1-t)^{n-1}$ equals

$$\sum_{\sigma\in\mathcal{R}(G)} \frac{n-1+\varepsilon_\sigma}{1-\varepsilon_\sigma} = n\sum_{\sigma\in\mathcal{R}(G)} \frac{1}{1-\varepsilon_\sigma} - \sum_{\sigma\in\mathcal{R}(G)} 1 = \frac{n}{2}r(G) - r(G).$$

□

Recall that $\mathcal{H}(G)$ is the set of all reflecting hyperplanes (in $E$) of $G$.

**Theorem II.3.7.** *The Laurent expansion of $F((\Bbbk[E] \otimes E)^G; t)$ about $t = 1$ starts as follows:*

$$F((\Bbbk[E] \otimes E)^G; t) = \frac{1}{\#G}\left(\frac{n}{(1-t)^n} + \frac{\frac{n}{2}r(G) - \#\mathcal{H}(G)}{(1-t)^{n-1}} + \dots\right)$$

*Proof.* As in the proof of Theorem II.3.2, it is enough to calculate the contribution to Eq. (II.3.6) of the neutral element and all reflection in $G$.

If $\sigma \in \mathcal{R}(G)$, then

$$\frac{\operatorname{tr}(\sigma, E^*)}{\det(id_E - \sigma t)} = \frac{n-1+\varepsilon_\sigma^{-1}}{(1-t)^{n-1}(1-\varepsilon_\sigma t)}.$$

Therefore the coefficient of $1/(1-t)^{n-1}$ equals

$$\sum_{\sigma\in\mathcal{R}(G)} \frac{n-1+\varepsilon_\sigma^{-1}}{1-\varepsilon_\sigma} = n\sum_{\sigma\in\mathcal{R}(G)} \frac{1}{1-\varepsilon_\sigma} + \sum_{\sigma\in\mathcal{R}(G)} \varepsilon_\sigma^{-1} = \frac{n}{2}r(G) - \#\mathcal{H}(G).$$

In the last equality, we use the fact that all the reflections with the same reflecting hyperplane, together with $1\!\!1$, form a cyclic group, see Lemma II.3.8 below. Assume that this group is of order $m$. Gathering together all such reflection, we obtain the sum $\varepsilon + \varepsilon^2 + \ldots + \varepsilon^{m-1}$, where $\varepsilon$ is a primitive root of unity of order $m$. Since the last sum equals $-1$, we conclude that $\sum_{\sigma\in\mathcal{R}(G)} \varepsilon_\sigma^{-1} = -\#\mathcal{H}(G)$. □

**Lemma II.3.8.**
*1. Suppose $\sigma, \sigma' \in r(G)$ and $E^\sigma = E^{\sigma'}$. If $v \in E$ is a non-trivial eigenvector of $\sigma$ (i.e., $\sigma v = \varepsilon_\sigma v$), then $v$ is also an eigenvector of $\sigma'$.*

*2. For any $H \in \mathcal{H}(G)$, the set $\{\sigma \in \mathcal{R}(G) \mid E^\sigma = H\} \cup 1\!\!1$ is a cyclic subgroup of $G$.*

*Proof.* 1. Let $v'$ be a non-trivial eigenvector of $\sigma'$. Then $v' = v + x$ for some $x \in E^\sigma$. Assume that $x \neq 0$. Then the 2-dimensional plane $\Bbbk v \oplus \Bbbk x$ is invariant with respect to the subgroup generated by $\sigma$ and $\sigma'$. Computing the matrix of $[\sigma, \sigma'] = \sigma\sigma'\sigma^{-1}\sigma'^{-1}$ with the respect of the basis $(v, x)$, we obtain $\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}$, where $z = \dfrac{(1-\varepsilon_\sigma)(1-\varepsilon_{\sigma'})}{\varepsilon_\sigma \varepsilon_{\sigma'}}$. Hence $[\sigma, \sigma']$ has infinite order, which contradicts the finiteness of $G$. Thus, $x$ must be $0$.

2. By virtue of part 1, these elements form a subgroup of $G$, say $\Gamma$. The mapping $(\sigma \in \Gamma) \mapsto \varepsilon_\sigma$ is an injective homomorphism $\Gamma \to \Bbbk^\times$, and it is well known that any subgroup of $\Bbbk^\times$ is cyclic. □

The number of the reflecting hyperplanes can be strictly less than that of reflections.

**Exercise 12.** *Prove that $\#\mathcal{R}(G) = \#\mathcal{H}(G)$ if and only if all reflections are of order two.*

**II.3.3. Symmetries of Poincaré series.** As $F(\Bbbk[E]_{(\nu)}; t)$ is a rational function in $t$, it is conceivable to make the substitution $t \mapsto t^{-1}$. In the context of power series, this means that we wish to compare the expansions of $F(\Bbbk[E]_{(\nu)}; t)$ at the origin and infinity.

The following is a straightforward consequence of the Molien formula (Theorem II.3.3).

**Proposition II.3.9.** *For any simple $G$-module $\mathfrak{S}$, we have*

$$F(\Bbbk[E]_{(\mathfrak{S})};t^{-1}) = (-t)^{\dim E} F(\Bbbk[E]_{(\mathfrak{S}^*\otimes \det_E)};t)\ .$$

*In particular,*

$$F(\Bbbk[E]^G;t^{-1}) = (-t)^{\dim E} F(\Bbbk[E]_{\det_E};t)\ .$$

This yields the following symmetry properties of Poincare series of algebras of invariants.

**Corollary II.3.10.**

(i) *If $G\subset SL(E)$, then $F(\Bbbk[E]^G;t^{-1}) = (-t)^{\dim E}F(\Bbbk[E]^G;t)$;*

(ii) *If the equality $F(\Bbbk[E]^G;t^{-1}) = (-1)^s t^q F(\Bbbk[E]^G;t)$ holds for some $s,q\in\mathbb{Z}$ and $G$ contains no reflections, then $G\subset SL(E)$.*

*Proof.* (i) is obvious.
(ii) Consider the equality of rational functions

$$(-1)^s t^q \frac{1}{\#G}\sum_{\sigma\in G}\frac{1}{\det(id_E-\sigma t)} = (-1)^{\dim E}t^{\dim E}\frac{1}{\#G}\sum_{\sigma\in G}\frac{\det\sigma}{\det(id_E-\sigma t)}\ .$$

Comparing the Laurent expansion about $t=1$ for both parts, we obtain $s\equiv \dim E \pmod 2$ and $q=\dim E + r(G)$. This shows that

$$t^{r(G)}\sum_{\sigma\in G}\frac{1}{\det(id_E-\sigma t)} = \sum_{\sigma\in G}\frac{\det\sigma}{\det(id_E-\sigma t)}\ .$$

By the hypothesis, $r(G)=0$. Then setting $t=0$, we obtain $\#G=\sum_{\sigma\in G}\det\sigma$. Since each $\det\sigma$ is a root of unity, we must have $\det\sigma=1$ for all $\sigma\in G$. □

These properties have a homological interpretation, which we discuss below (may be). Namely, if $G\subset SL(V)$, then $\Bbbk[E]^G$ is a *Gorenstein algebra*. Conversely, if $\Bbbk[E]^G$ is Gorenstein and $r(G)=0$, then $G\subset SL(E)$.

By virtue of Proposition II.3.9, one obtains a natural duality on the set of all isotypic components (or modules of covariants): $\mathfrak{S}\leftrightarrow\mathfrak{S}^*\otimes\det_E$.

**Exercise 13.** *Using the ideas from the proof of Theorems II.3.5–II.3.7, prove that the Laurent expansions of $F(\Bbbk[E]_{(\mathfrak{S})};t)$ and $F(\Bbbk[E]_{(\mathfrak{S}^*\otimes\det_E)};t)$ about $t=1$ have the following properties: the coefficients of $1/(1-t)^n$ are equal and the coefficients of $1/(1-t)^{n-1}$ are opposite.*

## II.4. A reciprocity for invariants of cyclic groups

In this section, we consider a curious example related to the algebra of invariants of a cyclic group.

Let us begin with an observation concerning the invariants of a regular representation of *any* finite group. Let $R$ be the space of the (left) regular representation of $G$. It turns out that Molien's formula for $\Bbbk[R]^G$ admits a simplification. Let $\varphi_G(d)$ denote the number of elements of order $d$ in $G$.

**Theorem II.4.1** (Almkvist-Fossum, 1978). $F(\Bbbk[R]^G;t) = \sum_{d\geqslant 1} \frac{\varphi_G(d)}{(1-t^d)^{\#G/d}}$.

*Proof.* Using Molien's formula, it suffices to show that if $\gamma \in G$ is of order $d$, then $\frac{1}{\det(id_R - \gamma t)} = \frac{1}{(1-t^d)^{\#G/d}}$. Indeed, each coset of $\langle\gamma\rangle\backslash G$ is a cycle of length $d$ with respect to the action of $\gamma$. Hence the matrix of $\gamma$ is the direct sum of the diagonal $d$-blocks of the form $\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \ddots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}$. Since $\det \begin{bmatrix} 1 & -t & 0 & \dots & 0 \\ 0 & 1 & -t & \dots & 0 \\ 0 & 0 & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \ddots & -t \\ -t & 0 & 0 & \dots & 1 \end{bmatrix} = 1 - t^d$, and the number of such diagonal blocks equals $(\#G)/d$, we are done. □

Now, we consider the case $G = \mathcal{C}_n$, the cyclic group of order $n$. Then $\varphi_{\mathcal{C}_n}(d) =: \varphi_n(d)$ is almost the usual Euler function. That is, $\varphi_n(d) = \begin{cases} 0, & \text{if } d \nmid n \\ \varphi(d), & \text{if } d | n \end{cases}$. Here $\varphi(d)$ is the number of integers $s$ less than or equal to $d$ such that $\gcd(s,d) = 1$.

**Theorem II.4.2** (Elashvili-Jibladze, 1998). *Let $R_n$ be the space of the regular representation of $\mathcal{C}_n$. Then $F(\Bbbk[R_n]^{\mathcal{C}_n};t) = \sum a(\mathcal{C}_n,m)t^m$, where*

$$a(\mathcal{C}_n,m) = \frac{1}{n+m} \sum_{d|\gcd(n,m)} \varphi(d) \binom{n/d + m/d}{n/d} . \tag{II.4.8}$$

*Proof.* Left to the reader (exercise!). □

It follows that $a(\mathcal{C}_n,m) = a(\mathcal{C}_m,n)$ for all $n,m \in \mathbb{N}$. This curious equality is obtained via formal manipulations with power series. It would be interesting to find a more conceptual explanation of it. One might suggest that this has something to do with the classical "Hermite reciprocity" for $SL_2$-modules.

**Remark.** From Eq. (II.4.8) one easily derives the equality of formal power series

$$\sum_{n,m} a(\mathcal{C}_n,m)x^n y^m = -\sum_{k=1}^{\infty} \frac{\varphi(k)}{k} \log(1 - x^k - y^k) .$$

## II.5. Finite reflection groups: basic properties

**Definition 13.** Let $G \subset GL(E)$ be a finite group. We say that $G$ is a *finite reflection group* or *finite group generated by reflections* (= f.g.g.r.) if the set of reflections, $\mathcal{R}(G)$, generates $G$ as group.

*Notation.* If $\sigma \in \mathcal{R}(G)$, then $l_\sigma \in E^*$ is a linear form defining the hyperplane $E^\sigma$.

The following is the main result on f.g.g.r.

**Theorem II.5.1** (Shephard-Todd,1954). *For a linear group $G \subset GL(E)$, the following conditions are equivalent:*

(i) *$G$ is a f.g.g.r.*

(ii) *$\Bbbk[E]$ is a free $\Bbbk[E]^G$-module of finite rank;*

(iii) *$\Bbbk[E]^G$ is a polynomial algebra.*

*Proof.* Set $S = \Bbbk[E]$, $R = \Bbbk[E]^G$, $R_+ = \oplus_{i\geqslant 1} R_i$, and $I = SR_+ \lhd S$.

(i)⇒ (ii) We proceed with a series of assertions. For any $p \in S$, its image in $S/I$ is denoted by $\bar{p}$.

Claim 1. *Suppose the elements $\{e_\alpha\}_{\alpha\in\mathfrak{J}}$ in $S$ satisfy the property that $\{\bar{e}_\alpha = e_\alpha + I \mid \alpha \in \mathfrak{J}\}$ form a basis for $S/I$. Then $\{e_\alpha\}_{\alpha\in\mathfrak{J}}$ generate the $R$-module $S$.*

Set $M = \sum_{\alpha\in\mathfrak{J}} Re_\alpha$. It is a graded $R$-submodule of $S$. Arguing by induction on degree, we prove that $M = S$. Suppose that $M_i = S_i$ for all $i < i_0$. Take any $f \in S_{i_0}$. Then $\bar{f} = \sum_{\alpha\in\mathfrak{J}} k_\alpha \bar{e}_\alpha$ for some $k_\alpha \in \Bbbk$. Therefore $f = \sum_{\alpha\in\mathfrak{J}} k_\alpha e_\alpha + \sum f_\beta r_\beta$, where $r_\beta \in R_+$ and $\deg f_\beta < i_0$. It follows that $f \in M$, and we are done. □

Claim 2. *Let $x_i \in R$, $y_i \in S$ $(1 \leqslant i \leqslant m)$ be homogeneous elements such that $(*)$ $\sum_i x_i y_i = 0$. If $x_1 \notin Rx_2 + \cdots + Rx_m$, then $y_1 \in I$.*

For any $s \in \mathcal{R}(G)$, we define the linear operator $\Delta_s : S \to S$ by the formula $s{\cdot}f - f = l_s \Delta_s(f)$. Obviously, $\Delta_s$ decrease the degree by one. That is, either $\deg \Delta_s(f) = \deg f - 1$ or $\Delta_s(f) = 0$.

To prove Claim 2, we argue by induction on $d = \deg y_1$.
– If $d = 0$, then $x_1 = -\sum_{i\geqslant 2} x_i y_i = -\sum_{i\geqslant 2} x_i y_i^{\#}$, which contradicts the assumption.
– Suppose $d > 0$ and the claim is true for elements of degree smaller than $d$. Applying $\Delta_s$ to $(*)$, we obtain $\sum_i x_i \Delta_s(y_i) = 0$. By the induction hypothesis, $\Delta_s(y_1) \in I$. Hence $s{\cdot}y_1 - y_1 \in I$ for any $s \in \mathcal{R}(G)$. Since $G$ is a f.g.g.r., one easily verifies that $\sigma{\cdot}y_1 - y_1 \in I$ for any $\sigma \in G$. Taking the average yields $y_1^{\#} - y_1 \in I$ and hence $y_1 \in I$. □

Claim 3. *Suppose $y_1, \dots, y_m \in S$ satisfy the property that $\bar{y}_i \in S/I$ are linearly independent over $\Bbbk$. Then $y_1, \dots, y_m$ are linearly independent over $R$.*

Assume that $\sum_i x_i y_i = 0$, $x_i \in R$. We perform a decreasing induction on the number summands in such a relation. In virtue of Claim 2, we have $x_1 \in Rx_2 + \ldots + Rx_m$, i.e., $x_1 = \sum_{i\geqslant 2} x_i z_i$ $(z_i \in R)$. Then $x_2(y_2 + z_2 y_1) + \ldots + x_m(y_m + z_m y_1) = 0$. Since $\overline{y_i + z_i y_1} = \overline{y_i}$ and these elements are linearly-independent, we have $x_2 = \ldots = x_m = 0$. Hence $x_1$ as well, and we are done. □

Now, we can complete the first part of the proof. Take elements $\{e_\alpha\}_{\alpha\in\mathfrak{J}}$ in $S$ such that $\{\bar{e}_\alpha\}$ form a basis for $S/I$. Then they span the $R$-module $S$ (Claim 1) and are linearly independent over $R$ (Claim 3). Hence $S$ is a free $R$-module. It remains to observe that $\mathfrak{J}$ is finite, since $S$ is a finite $R$-module in case of finite group invariants.

(ii)⇒(iii) Since this part has no relation to invariant theory, we omit the proof. Actually, $\Bbbk[E]^G$ can be replaced with an arbitrary homogeneous finitely generated subalgebra of $\Bbbk[E]$.

(iii)⇒(i) First, we prove that $G$ contains some reflections. Let $d_1, \dots, d_n$ be the degree of basic invariants in $R$. Then

$$F(R;t) = \prod_{i=1}^{n} \frac{1}{1-t^{d_i}} = \frac{1}{\prod_{i=1}^n d_i} \left( \frac{1}{(1-t)^n} + \frac{\sum_{i=1}^n (d_1-1)/2}{(1-t)^{n-1}} + \dots \right)$$

On the other hand, by Theorem II.3.2, the Laurent expansion of the algebra of invariants about $t = 1$ begins with

$$F(R;t) = \frac{1}{\#G} \left( \frac{1}{(1-t)^n} + \frac{r(G)/2}{(1-t)^{n-1}} + \dots \right).$$

Comparing the two expressions, we obtain $\#G = \prod_i d_i$ and $r(G) = \sum_i (d_i - 1)$. Because there is an $i$ such that $d_i \geqslant 2$, we see that $r(G) \neq 0$. Let $U$ be the (normal) subgroup of $G$ generated by all reflections. Then $U \neq \mathbb{1}$, and according to the first two parts of the proof, $\Bbbk[E]^U$ is a polynomial algebra. Let $\psi_1, \dots, \psi_n$ be basic $U$-invariants, with $\deg \psi_i = l_i$. The preceding argument also works for $U$ and shows that $\#U = \prod_i l_i$ and $r(U) = \sum_i (l_i - 1)$.

Since $\Bbbk[E]^G \subset \Bbbk[E]^U$, each $f_i$ is a polynomial in $\psi_j$'s. W.l.o.g., we may assume that $d_1 \leqslant d_2 \leqslant \dots \leqslant d_n$ and $l_1 \leqslant l_2 \leqslant \dots \leqslant l_n$. Then we claim that $l_i \leqslant d_i$ for all $i$. Assume not, and let $i_0$ be the minimal index with the property that $l_{i_0} > d_{i_0}$. Then the dimension argument shows that $f_1, \dots, f_{i_0}$ are polynomials in $\psi_1, \dots, \psi_{i_0 - 1}$. This contradicts, however, the fact that $f_1, \dots, f_{i_0}$ are algebraically independent. Thus, $l_i \leqslant d_i$ for all $i$, and hence $r(U) = \sum_i (l_i - 1) \leqslant \sum_i (d_i - 1) = r(G)$. But $G$ and $U$ have the same reflections. Hence $l_i = d_i$ for all $i$, and therefore $\#U = \prod_i l_i = \prod_i d_i = \#G$. This means that $U = G$. □

As a by-product of this proof, we obtain

**Corollary II.5.2.** *Let $G$ be a f.g.g.r. and $\Bbbk[E]^G = \Bbbk[f_1, \dots, f_n]$, where $\deg f_i = d_i$. Then $\#G = \prod_{i=1}^n d_i$ and $r(G) = \sum_{i=1}^n (d_i - 1)$.*

We know that $\Bbbk[E]$ is a free graded $\Bbbk[E]^G$-module of finite rank and $\Bbbk[E] = \oplus_{\nu \in \hat{G}} \Bbbk[E]_{(\nu)}$ is the direct sum of $\Bbbk[E]^G$-modules. Therefore each isotypic component $\Bbbk[E]_{(\nu)}$ is a free $\Bbbk[E]^G$-module as well.

**Proposition II.5.3.** *For any $\nu \in \hat{G}$, the rank of the free $\Bbbk[E]^G$-module $\Bbbk[E]_{(\nu)}$ equals $(\deg \nu)^2$. Equivalently, for any simple $G$-module $\mathfrak{S}$, the rank of the module of covariants $\mathrm{Mor}_G(V, \mathfrak{S})$ equals $\dim \mathfrak{S}$.*

*Proof.* Suppose $\operatorname{rk}\Bbbk[E]_{(\nu)} = m$. Then

$$F(\Bbbk[E]_{(\nu)};t) = \frac{\sum_{i=1}^m t^{k_i}}{\prod_{i=1}^n (1-t^{d_i})},$$

where $k_1,\dots,k_m$ are the degrees of the elements of a basis for this module. It follows that $\lim_{t\to 1} F(\Bbbk[E]_{(\nu)};t)(1-t)^n = m/\prod_i d_i = m/(\#G)$. On the other hand, Corollary II.3.4(1) shows that this limit equals $(\deg\nu)^2/(\#G)$. Hence the assertion. □

### II.5.1. The coinvariant algebra.

**Definition 14.** The algebra $\Bbbk[E]/(f_1,\dots,f_n)$ is called the *coinvariant algebra* of $G$. It is denoted by $\Bbbk[E]_G$.

Since the ideal $(f_1,\dots,f_n)$ is $G$-stable, $\Bbbk[E]_G$ is a $G$-module.

**Theorem II.5.4.** *$\Bbbk[E]_G$ affords the regular representation of $G$.*

*Proof.* Being a $G$-module, the coinvariant algebra has the isotypic decomposition $\Bbbk[E]_G = \oplus_{\nu\in\hat G}\Bbbk[E]_{G,(\nu)} = \oplus_{\nu\in\hat G} m_\nu E_\nu$. To compute the multiplicities $m_\nu$, we use the fact that $f_1,\dots,f_n$ is a regular sequence. Therefore

$$\dim\Bbbk[E]_{G,(\nu)} = F(\Bbbk[E]_{G,(\nu)},t)|_{t=1} = F(\Bbbk[E]_\nu,t)\prod_{i=1}^n(1-t^{d_i})|_{t=1} =$$

$$\frac{(\deg\nu)^2}{\#G}\cdot\frac{\prod_{i=1}^n(1-t^{d_i})}{(1-t)^n} = (\deg\nu)^2\ .$$

Hence $m_\nu = \deg\nu$, and the assertion follows from Corollary I.3.5. □

**Remark.** 1. Although $\Bbbk[E]_G$ and $\Bbbk[G]$ are isomorphic as $G$-modules, they are quite different as algebras.

2. Suppose that $\Bbbk = \mathbb{C}$, $E = \mathfrak{h}$ is a Cartan subalgebra of semisimple Lie algebra $\mathfrak{l}$, and $G = W$ is the the corresponding Weyl group. Then a famous result of A. Borel (1953) asserts that $\Bbbk[\mathfrak{h}]_W$ is isomorphic to the cohomology ring of the flag variety of $L$.

## II.6. Semi-invariants of finite reflection groups

Throughout this section, $G \subset GL(E)$ is a f.g.g.r and $f_1,\dots,f_n \in \Bbbk[E]^G$ are basic invariants, $\deg f_i = d_i$.

As was already noticed, each isotypic component is a free $\Bbbk[E]^G$-module. In particular, if $\mu$ is a linear character of $G$, then $\Bbbk[E]_\mu$ is generated by a single homogeneous polynomial. Such a polynomial is said to be a *basic semi-invariant* (of weight $\mu$). Our goal in this section is to describe basic semi-invariants for all linear characters of $G$. We begin with describing a distinguished isotypic component.

**Definition 15.** A polynoimal $f \in \Bbbk[E]$ is said to be *anti-invariant* or *skew-invariant* (w.r.t. $G$) if $\sigma{\cdot}f = \det_E(\sigma)f$ for any $\sigma \in G$.

Hence the set of all anti-invariant polynomials is the isotypic component corresponding to the linear character $\sigma \mapsto \det_E(\sigma)$. For the next theorem, we need some notation. Recall that, for $\sigma \in \mathcal{R}(G)$, $\varepsilon_\sigma$ is the only non-unit eigenvalue of $\sigma$ and $l_\sigma$ is a non-zero linear form determining the hyperplane $E^\sigma$. There is the natural mapping $p : \mathcal{R}(G) \to \mathcal{H}(G)$, $\sigma \mapsto E^\sigma$. By Lemma II.3.8, $p^{-1}(H) \cup \{1\!\!1\}$ is a cyclic group. The order of this group is denoted by $c_H$. Without loss of generality, we may assume that, for all elements of $p^{-1}(H)$, we have chosen one and the same linear form, which is denoted by $l_H$.

**Theorem II.6.1.**

(i) $J = \det\left(\dfrac{\partial f_i}{\partial x_j}\right)$ *is a semi-invariant of weight* $\det_E$*;*

(ii) $J = \alpha \displaystyle\prod_{\sigma\in\mathcal{R}(G)} l_\sigma = \alpha \prod_{H\in\mathcal{H}(G)} l_H^{c_H-1}$ *for some* $\alpha \in \Bbbk^\times$*;*

(iii) $\Bbbk[E]_{\det_E} = \Bbbk[E]^G J$.

*Proof.* (i) If $f \in \Bbbk[E]^G$, then s$pan\{\partial f/\partial x_j \mid j = 1,\dots,n\}$ is a $G$-stable subspace which affords the representation $\rho$. Hence if $M = \left(\frac{\partial f_i}{\partial x_j}\right)$, then $\sigma{\cdot}M = \rho(\sigma)M$. Therefore $\sigma{\cdot}J = \det(\sigma{\cdot}M) = \det\rho(\sigma)\det M = \det_E(\sigma)J$. Since $f_1,\dots,f_n$ are algebraically independent, we also have $J \neq 0$.

(ii) For $\sigma \in \mathcal{R}(G)$, we have $\det(\sigma) = \varepsilon_\sigma$. Hence $\sigma{\cdot}J = \varepsilon_\sigma J$. Since $(\varepsilon_\sigma - 1)J = \sigma{\cdot}J - J = l_\sigma \Delta_\sigma(J) \neq 0$, we see that $l_\sigma$ divides $J$. Write $J = l_\sigma^a K$, where $K$ and $l_\sigma$ are relatively prime. Then $\sigma{\cdot}K = K$. (Otherwise, we would obtain that $l_\sigma$ still divides $K$.) Notice that $\sigma{\cdot}l_\sigma = \varepsilon_\sigma^{-1} l_\sigma$. Hence

$$\varepsilon_\sigma J = \sigma{\cdot}J = \sigma{\cdot}(l_\sigma^a K) = \varepsilon_\sigma^{-a} l_\sigma^a K = \varepsilon_\sigma^{-a} J\ .$$

Without loss of generality, we may assume that $\sigma$ is a generator of the cyclic group associated with the hyperplane $H = E^\sigma$. It then follows that $c_H$ divides $a+1$, and therefore $a \geqslant c_H - 1$. Repreating this argument for each $H \in \mathcal{H}(G)$, we obtain, in view of the fact that different linear forms are mutually prime in $\Bbbk[E]$, that $\prod_{H\in\mathcal{H}(G)} l_H^{c_H-1}$ divides $J$. As $\deg J = r(G) = \sum_{H\in\mathcal{H}(G)} c_H - 1$, the two polynomials are equal, up to a scalar multiple.

(iii) Let $F$ be an arbitrary semi-invariant of weight $\det_E$. Then the very same argument shows that $J = \prod_{H\in\mathcal{H}(G)} l_H^{c_H-1}$ divides $F$. Hence $F = J{\cdot}Q$ for some $Q \in \Bbbk[E]^G$. □

Similar ideas are being used in the proof of the general description of "basic" semi-invariants.

The group $G$ permutes the elements of $\mathcal{H} = \mathcal{H}(G)$. For any $G$-orbit $\mathcal{O} \in \mathcal{H}/G$, set $f_{\mathcal{O}} = \prod_{H\in\mathcal{O}} l_H$. It is a polynomial of degree $\#\mathcal{O}$.

**Lemma II.6.2.** *Each $f_{\mathcal{O}}$ is a semi-invariant of $G$. More precisely, for $\sigma \in \mathcal{R}(G)$, we have*
$$\begin{cases} \text{if } E^\sigma \in \mathcal{O}, \text{ then } \sigma{\cdot}f_{\mathcal{O}} = \varepsilon_\sigma^{-1} f_{\mathcal{O}}, \\ \text{if } E^\sigma \notin \mathcal{O}, \text{ then } \sigma{\cdot}f_{\mathcal{O}} = f_{\mathcal{O}}. \end{cases}$$

*Proof.* The first claim follows from the fact that $\mathcal{O}$ is a $G$-orbit. Indeed, each $g \in G$ preserves the set of reflecting hyperplanes in $\mathcal{O}$. Hence $g{\cdot}f_{\mathcal{O}}$ has the same divisor of zeros as $f_{\mathcal{O}}$. That is, $g{\cdot}f_{\mathcal{O}} = \alpha_g f_{\mathcal{O}}$ for some $\alpha_g \in \Bbbk^\times$. The second claim follows from the following two facts (both are already used above):

(1) $\sigma{\cdot}l_\sigma = \varepsilon_\sigma^{-1} l_\sigma$;

(2) if $\sigma \in \mathcal{R}(G)$, $F \in \Bbbk[E]$, and $\sigma{\cdot}F = \alpha F$ with $\alpha \neq 1$, then $l_\sigma$ divides $F$. □

Obviously, the cyclic subgroups associated with different hyperplanes in the orbit $\mathcal{O}$ have the same order. Therefore we can write $c_{\mathcal{O}}$ for $c_H$, where $H \in \mathcal{O}$.

**Theorem II.6.3.** *(1) Any homogeneous semi-invariant of G is of the form $\prod_{\mathcal{O}\subset\mathcal{H}} f_{\mathcal{O}}^{a_{\mathcal{O}}}{\cdot}f_1$, where $0 \leqslant a_{\mathcal{O}} \leqslant c_{\mathcal{O}} - 1$ and $f_1 \in \Bbbk[E]^G$; (2) The semi-invariants corresponding to different strings of numbers $\{a_{\mathcal{O}} \mid \mathcal{O} \in \mathcal{H}/G\}$ have different weights.*

*Proof.* 1. It follows from Lemma II.6.2 that each such polynomial is a semi-invariant. Furthermore, since $f_{\mathcal{O}}^{c_{\mathcal{O}}}$ is invariant, it is enough to assume that $a_{\mathcal{O}} \leqslant c_{\mathcal{O}} - 1$.

Suppose that $F$ is a homogeneous semi-invariant, which is not an invariant. Then there is a $\sigma \in \mathcal{R}(G)$ such that $\Delta_\sigma(F) \neq 0$. Hence $F$ has a factor $l_\sigma$ and therefore $f_{\mathcal{O}}$, where $\mathcal{O}$ is the orbit containing $E^\sigma$, divides $F$. Then the induction on the degree shows that each homogeneous semi-invariant is of the required form.

2. This follows from Lemma II.6.2. □

It follows from Theorem II.6.3 that the polynomials $\prod_{\mathcal{O}\in\mathcal{H}/G} f_{\mathcal{O}}^{a_{\mathcal{O}}}$, where $0 \leqslant a_{\mathcal{O}} \leqslant c_{\mathcal{O}} - 1$, form a full set of basic semi-invariants for all linear characters of $G$. In particular, the total number of nontrivial linear characters of $G$ equals $(\prod_{\mathcal{O}\in\mathcal{H}/G} c_{\mathcal{O}}) - 1$.

**Example II.6.4.** $\prod_{\sigma\in\mathcal{R}(G)} l_\sigma = \prod_{\mathcal{O}\in\mathcal{H}/G} f_{\mathcal{O}}$ is a basic semi-invariant of weight $\det_E^{-1}$.

## II.7. Miscellaneous results on f.g.g.r.: Shchvartsman, Solomon, Steinberg, etc.

In this section, we prove some important miscellaneous results related to finite reflection groups.

**II.7.1. Shchvartsman: invariant differential 1-forms.** Theorem II.5.1 asserts, in particular, that $G$ is a f.g.g.r. if and only if all isotypic components are free $\Bbbk[E]^G$-modules. Shchvartsman's theorem strengthens one of the implications. It says that it suffices to verify the freeness for one specific isotypic component.

**Theorem II.7.1** (Shchvartsman, 1982)**.** *Suppose $E$ is a simple $G$-module. Then $G$ is a f.g.g.r. if and only if $\mathrm{Mor}_G(E, E^*)$ is a free $\Bbbk[E]^G$-module.*

We need some preparations for the proof. We use the notation $S$, $R$, $I = SR_+$, as above. Set $M = \mathrm{Mor}_G(E, E^*)$. There are some well-known connections between $R$ and the $R$-module $M$.

$1^o$. If $f \in R$, then the differential of $f$, $\boldsymbol{d}f$, can be regarded as a $G$-equivariant mapping from $E$ to $E^*$, i.e., an element of $M$. Recall that $\boldsymbol{d}f(v)$, $v \in E$, is an element of $E^*$ that is defined as follows. If $u \in E$ and $\langle\ ,\ \rangle$ denotes the natural pairing between $E$ and $E^*$, then $\langle \boldsymbol{d}f(v), u\rangle$ is the coefficient of $t$ in the Taylor expansion of $f(v + tu)$.

$2^o$. There is a mapping called "restitution" $\mathrm{rt} : M \to R_+$, which is defined by $\mathrm{rt}(F)(v) := \langle F(v), v\rangle$, where $v \in E$.

$3^o$. Euler's formula: $\mathrm{rt}(\boldsymbol{d}f) = (\deg f)f$.
Indeed, the definition of $\boldsymbol{d}f$ shows that

$$\mathrm{rt}(\boldsymbol{d}f)(v) = \langle \boldsymbol{d}f(v), v\rangle = \{\text{coefficient of } t \text{ in the expansion of } f(v + tv) = (1 + t)^{\deg f} f(v)\}\ .$$

*Proof of Shchvartsman's theorem.* Let $f_1, \dots, f_p$ be a minimal generating system of $R$. Without loss of generality, we assume that $\deg f_1 \leqslant \dots \leqslant \deg f_p$ and $f_i$ is an invariant of minimal degree that is not contained in the ideal $Sf_1 + \dots + Sf_{i-1}$.

*Claim 1. The images of $\boldsymbol{d}f_i$ in $M/R_+M$ are linearly independent over $\Bbbk$.*
Assume not, and $\sum \alpha_i \boldsymbol{d}f_i \in R_+M$ for some $\alpha_i \in \Bbbk$. Then taking the restitution, we obtain $\sum \alpha_i(\deg f_i)f_i \in (R_+)^2$. This contradicts however the construction of the $f_i$'s. [This argument does not use the fact that $M$ is a free $R$-module.]

*Claim 2. Suppose $M'$ is a free graded $R'$-module of finite rank ($R'$ is a noetherian graded $\Bbbk$-algebra) and $q_1, \dots, q_p \in M'$ satisfy the property that the images of $q_i$'s in $M'/R'_+M'$ are linearly independent over $R'/R'_+ = \Bbbk$. Then $q_1, \dots, q_p$ are linearly independent over $R'$.*
This is a standard and easy fact on free modules.

Now, if $M$ is a free $R$-module, then combining Claims 1 and 2 shows that the $\boldsymbol{d}f_i$'s are linearly independent over $R$. It follows that $f_1, \dots, f_p$ are algebraically independent. (For, differentiating a polynomial relation between $f_1, \dots, f_p$ would yield a non-trivial linear dependence between the $\boldsymbol{d}f_i$ with coefficients in $R$.) □

Using the previous results, we can describe a natural basis for the free $R$-module $M = \mathrm{Mor}_G(E, E^*)$.

**Theorem II.7.2.** *If $G$ is a f.g.g.r., then $\mathrm{Mor}_G(E, E^*)$ is a free $\Bbbk[E]^G$-module generated by $df_1, \dots, df_n$, where $f_1, \dots, f_n$ are basic invariants.*

*Proof.* We already know that $M$ is a free $R$-module, its rank equals $n = \dim E$, and $df_1, \dots, df_n$ are linearly independent over $R$. That is, $\oplus_i R(df_i)$ is a submodule of $M$ of the same rank.

To prove that these elements do form a basis, we use the Poincaré series techniques. By Theorem II.3.6, we have

$$F(M,t) = \frac{1}{\#G}\left(\frac{n}{(1-t)^n} + \frac{r(G)(n/2-1)}{(1-t)^{n-1}} + \dots\right)$$

On the other hand, if the degrees of the elements of a basis of $M$ are equal to $l_1, \dots, l_n$, then

$$F(M,t) = \frac{\sum_{j=1}^n t^{l_j}}{\prod_{i=1}^n (1-t^{d_i})} \ .$$

Using formulae from subsection II.2.3 and comparing the coefficient of $1/(1-t)^{n-1}$ in the two Laurent expansions of $F(M,t)$, we obtain $\sum_{i=1}^n l_i = r(G)$. Since $\deg(df_i) = d_i - 1$ and $\sum_i (d_i - 1) = r(G)$, one must have $\{d_i - 1 \mid i = 1, \dots, n\} = \{l_i \mid i = 1, \dots, n\}$. Hence $M = \oplus_i R(df_i)$. □

In particular, we proved that the sum of degrees of the elements of a homogeneous basis of the free $R$-module $M = \mathrm{Mor}_G(E, E^*)$ equals $\#\mathcal{R}(G)$.

**Exercise 14.** *Let $l'_1, \dots, l'_n$ be the degrees of the elements of a homogeneous basis of the free $R$-module $M' = \mathrm{Mor}_G(E, E)$. Prove that $\sum_i l'_i = \#\mathcal{H}(G)$.* [Hint: Use Theorem II.3.7.]

**II.7.2. Solomon: polynomial tensor exterior algebra.** Let $\wedge^\bullet(E^*)$ denote the exterior algebra of $E^*$ over $\Bbbk$. Then the $\Bbbk$-algebra $\Bbbk[E] \otimes \wedge^\bullet(E^*)$ can be regarded as the algebra of polynomial differential forms on $E$. Our goal is to describe $G$-invariant differential forms if $G$ is a f.g.g.r.

**Theorem II.7.3** (Solomon, 1963). *Suppose $G \subset GL(E)$ is a f.g.g.r. and $f_1, \dots, f_n$ are basic invariants in $\Bbbk[E]^G$. Then $(\Bbbk[E] \otimes \wedge^\bullet(E^*))^G = \Bbbk[f_1, \dots, f_n] \otimes \wedge^\bullet(df_1, \dots, df_n)$.*

*Proof.* The following proof is essentially based on the equality $\Bbbk[E]_{\det_E} = \Bbbk[E]^G J$ and the description of $J$ obtained in Theorem II.6.1.

$1^o$. First, we prove that $\binom{n}{j}$ differential forms $df_{i_1} \wedge \dots \wedge df_{i_j}$, $\{i_1, \dots, i_j\} \in [n]$, are linearly independent over $\Bbbk(E)$. Assume that

$$\sum_{i_1,\dots,i_j} a_{i_1,\dots,i_j} df_{i_1} \wedge \dots \wedge df_{i_j} = 0$$

is a linear relation with coefficients in $\Bbbk(E)$. For each subset $\{i_1,\dots,i_j\}$, we multiply this relation with the remaining $df_k$, $k\not\in\{i_1,\dots,i_j\}$. Then

$$0=\pm a_{i_1,\dots,i_j}df_1\wedge\ldots\wedge df_n=\pm a_{i_1,\dots,i_j}J dx_1\wedge\ldots\wedge dx_n\ .$$

This shows that $a_{i_1,\dots,i_j}=0$.

$2^o$. It follows that, for a fixed $j$, the $df_{i_1}\wedge\ldots\wedge df_{i_j}$'s form a basis for the $\Bbbk(E)$-vector space $\Bbbk(E)\otimes\wedge^j(E^*)$. In particular, for any $\omega\in(\Bbbk[E]\otimes\wedge^j(E^*))^G$, we can write

$$\omega=\sum_{i_1,\dots,i_j} a_{i_1,\dots,i_j}df_{i_1}\wedge\ldots\wedge df_{i_j}\ ,$$

where $a_{i_1,\dots,i_j}\in\Bbbk(E)$. Since the forms $df_{i_1}\wedge\ldots\wedge df_{i_j}$ are $G$-invariant, each coefficient is a $G$-invariant rational function. Multiplying $\omega$ with the remaining $df_k$, $k\not\in\{i_1,\dots,i_j\}$, as before, we see that

$$a_{i_1,\dots,i_j}df_1\wedge\ldots\wedge df_n=a_{i_1,\dots,i_j}J dx_1\wedge\ldots\wedge dx_n$$

is also a $G$-invariant polynomial differential $n$-form. Therefore $a_{i_1,\dots,i_j}J\in\Bbbk[E]_{\det_E}$. Using the relation $\Bbbk[E]_{\det_E}=\Bbbk[E]^G J$, we conclude that $a_{i_1,\dots,i_j}\in\Bbbk[E]$ (and is $G$-invariant!). Thus, each coefficient $a_{i_1,\dots,i_j}$ is actually a polynomial in $f_1,\dots,f_n$. □

### II.7.3. Steinberg: stabilisers for f.g.g.r.

**Theorem II.7.4** (R. Steinberg, 1964). *If $G$ is a f.g.g.r., then $G_v$ is a f.g.g.r. for any $v\in E$.*

*Proof.* We give a sketch of the proof that is based on Luna's slice theorem.

Consider the quotient mappings $\pi: E\to E/G$ and $\pi_v: E\to E/G_v$. Since the orbit $G{\cdot}v$ is finite and therefore closed, Luna's theorem applies to it. In particular, it says that there is a morphism $E/G_v\to E/G$, which takes $\pi_v(v)$ to $\pi(0)$, and this morphism is étale in a Zariski neighbourhood of $\pi_v(v)$. Since $G$ is a f.g.g.r. $E/G\simeq\Bbbk^n$. Hence $p_v(v)$ is a smooth point of $E/G_v$. Write $E=E'\oplus E^{G_v}$, where $E'$ is a $G_v$-module. Then $E/G_v\simeq(E'/G_v)\times E^{G_v}$. As $v\in E^{G_v}$, the above property of $p_v(v)$ implies that

$(*)$ the image of $0\in E'$ in $E'/G_v$ is a smooth point.

Let $R'$ denote the algebra $\Bbbk[E']^{G_v}$. The property $(*)$ means that $\dim_{\Bbbk}(R'_+/R'^2_+)=K\text{dim}\,R'$. But it is well-known that the left-hand side gives the number of elements in a minimal generating system of a graded $\Bbbk$-algebra $R'$. □

The original proof of Steinberg involved holomorphic functions on $E$ and a subtle characterisation of reflection groups. An elementary proof of Steinberg's theorem is found by G. Lehrer (see Intern. Math. Res. Notices (2004), no. 28, 1407–1411).

**Corollary II.7.5.** *For any $v\in E$, the stabiliser $G_v$ is generated by the reflection $\sigma$ such that $v\in E^\sigma$. In particular, $G_v=\{\mathbb{1}\}$ if and only if $v\in E\setminus\cup_{H\in\mathcal{H}}H$.*

## II.8. A return to general theory

Many assertions on f.g.g.r. can be carried over to arbitrary finite linear groups due to the fact that $\Bbbk[E]^G$ is always a CM algebra. As a sample, we mention a generalisation of Theorem II.5.4.

**Theorem II.8.1.** *Let $G \subset GL(E)$ be an arbitrary linear group and $f_1, \dots, f_n$ a h.s.o.p. in $\Bbbk[E]^G$. Suppose the rank of the $\Bbbk[f_1, \dots, f_n]$-module $\Bbbk[E]^G$ equals $m$. Then $\Bbbk[E]/(f_1, \dots, f_n)$ is isomorphic to $\Bbbk[G]^m$ as $G$-module.*

*Proof.* Left to the reader. □

Next result provides an estimate of the degree of the numerator for the Poincaré series for $\Bbbk[E]^G$.

**Proposition II.8.2.** *Suppose $f_1, \dots, f_n$ is a h.s.o.p. for $\Bbbk[E]^G$, with $\deg f_i = d_i$, and $\eta_1, \dots, \eta_l$ is a homogeneous basis for the free $\Bbbk[f_1, \dots, f_n]$-module $\Bbbk[E]^G$ with $\deg \eta_j = e_j$; that is, $\Bbbk[E]^G = \oplus_{i=1}^l \Bbbk[f_1, \dots, f_n]\eta_i$. Assume that $e_1 \leqslant \dots \leqslant e_l$. Then $\sum_i (d_i - 1) - e_l$ is the least degree of a semi-invariant of weight $\det_E$.*

*Proof.* Recall that $F(\Bbbk[E]^G; t^{-1}) = (-t)^n F(\Bbbk[E]_{\det_E}; t)$ (Proposition II.3.9). On the other hand,

$$F(\Bbbk[E]^G; t) = \frac{t^{e_1} + \dots + t^{e_l}}{\prod_{i=1}^n (1 - t^{d_i})} .$$

Commining these equalities, we obtain

$$(-1)^n \frac{\sum_j t^{d_1 + \dots + d_n - e_j}}{\prod_{i=1}^n (1 - t^{d_i})} = (-t)^n F(\Bbbk[E]_{\det_E}; t) .$$

Now equating the initial degrees of the Taylor expansions, we get

$$d_1 + \dots + d_n - e_l = n + \min\{\text{degrees of semi-invariants of weight } \det_E\}.$$

□

This result has an interesting consequence. Recall that the degree of a rational function is defined in Subsection II.2.3. From the last formulae in the proof, it follows that

$$\deg F(\Bbbk[E]^G; t) = -n - \min\{\text{degrees of semi-invariants of weight } \det_E\}.$$

In particular, $\deg F(\Bbbk[E]^G; t) \leqslant -\dim E$, and $\deg(\Bbbk[E]^G; t)F = -\dim E$ if and only if $G \subset SL(E)$.

Again, we wish to point out that some aspects of invariant theory of finite and connected reductive groups are quite different. Suppose that $H$ is connected and semismple, and $V$ is an $H$-module. The degree of $F(\Bbbk[V]^H; t)$ is well-defined. But in contrast to the finite group case, one always has $\deg F(\Bbbk[V]^H; t) \geqslant -\dim V$. (A criterion for the equality is also known.)

### II.8.1. A lower bound for degrees of algebraically independent invariants.

**Theorem II.8.3.** *Let $U \subset GL(E)$ be a finite group and $q_1, \dots, q_n$ are algerbaically independent homogeneous polynomials in $\Bbbk[E]^U$ with $\deg q_i = d_i$. Then*

(i) *$\#U \leqslant d_1 \cdots d_n$;*
(ii) *If $\#U = d_1 \cdots d_n$, then $U$ is a f.g.g.r. and $\Bbbk[E]^U = \Bbbk[q_1, \dots, q_n]$.*

*Proof.* Our proof applies if $\Bbbk = \mathbb{C}$.
(i) Consider two Poincaré series: $F_1(t) = F(\mathbb{C}[q_1, \dots, q_n]; t)$ and $F_2(t) = F(\mathbb{C}[E]^U; t)$. Considering $t$ as a complex variable, we see that these two series converge if $|t| \leqslant 1$. Since $\mathbb{C}[q_1, \dots, q_n]$ is a subalgebra of $\mathbb{C}[E]^U$, we have the coefficient-wise inequality $F_1 \preccurlyeq F_2$. It follows that $F_1(t) \leqslant F_2(t)$ for any real $t$ in the interval $(0, 1)$. Hence

$$\frac{1}{d_1 \cdots d_n} = \lim_{t\to 1}(1-t)^n F_1(t) \leqslant \lim_{t\to 1}(1-t)^n F_2(t) = \frac{1}{\#U} \ .$$

(ii) If $\#U = d_1 \cdots d_n$, then $F_2(t) - F_1(t)$ has the pole of order $\leqslant n-1$ at $t = 1$ and, by the same argument, the coefficient of $1/(1-t)^{n-1}$ is nonnegative. Using the Equation (II.2.2) and Theorem II.3.2, this nonnegativity translates into the condition

$$\frac{\#\mathcal{R}(U)}{2\#U} \geqslant \frac{1}{d_1 \cdots d_n} \cdot \frac{\sum_{i=1}^n (d_i - 1)}{2} \ ,$$

i.e., $\#\mathcal{R}(U) \geqslant \sum_{i=1}^n (d_i - 1)$. Then one can repeat the argument used in the proof of (iii)⇒(i) in Theorem II.5.1, which shows that the subgroup of $U$ generated by all reflections coincides with $U$. The rest is clear. □

## II.9. Complete intersections

Let $\mathcal{A}$ be a finitely generated graded $\Bbbk$-algebra. Then $\mathcal{A}$ is a quotient of a graded polynomial ring, i.e., $\mathcal{A} = \Bbbk[X_1, \cdots, X_N]/I$, where $\deg X_i = d_i$ and $I$ is a homogeneous ideal.

**Definition 16.** The algebra $\mathcal{A}$ is called a *complete intersection*, if $I$ is generated by a regular sequence. (Equivalently, if $I$ is generated by $N - K\dim \mathcal{A}$ elements.). If $I$ is generated by a sole polynomial, then $\mathcal{A}$ is called a *hypersurface*. The same terminology applies to the corresponding affine variety $\operatorname{Spec} \mathcal{A}$.

If $I$ is generated by polynomials of degree $m_1, \dots, m_l$, then the Poincaré series of $\mathcal{A}$ is of the form

$$(\diamond) \qquad F(\mathcal{A}; t) = \textstyle\prod_{i=1}^l (1 - t^{m_i}) / \prod_{i=1}^N (1 - t^{d_i}).$$

This already shows that $F(\mathcal{A}; t)$ has a rather specific property: it can be written such that all the roots of the numerator and denominator are roots of unity.

**Warning.** If $F(\mathcal{A}; t)$ can be written in form $(\diamond)$, then this does not imply that $\mathcal{A}$ is a complete intersection. Furthermore, if $F(\mathcal{A}; t) = 1/\prod_{i=1}^N (1 - t^{d_i})$, then it is not necessarily true that $\mathcal{A}$ is a graded polynomial algebra. An example of such phenomenon is found by R. Stanley in 1978. It is especially instructive for us, since $\mathcal{A}$ in Stanley's example is the algebra of invariants of a finite group.

**Example II.9.1** (Stanley)**.** Suppose $E = \Bbbk^3$ and $G$ is generated by two diagonal matrices with diagonals $(-1, -1, 1)$ and $(1, 1, \sqrt{-1})$. If $\Bbbk[E] = \Bbbk[x, y, z]$, then $\Bbbk[E]^G$ is generated by monomials $x^2$, $xy$, $y^2$, $z^4$. It follows that $\Bbbk[E]^G$ is a hypersurface, and the unique relation is $(x^2)(y^2) = (xy)^2$. Assuming that $\deg x = \deg y = \deg z = 1$, we see that the relation is of degree 4. Therefore $F(\Bbbk[E]^G; t) = (1 - t^4)/(1 - t^2)^3(1 - t^4) = 1/(1 - t^2)^3$.

Below, we consider the following

**Question.** When is the algebra of invariants of a finite group a complete intersection?

We begin with two simple observation.

$1^o$. If one is only interested in possible algebras of invariants, then it suffices to consider linear groups without reflections.

Indeed, if $G_r$ is the (normal) subgroup of $G$ generated by all reflections, then $E/G_r$ is an affine space, and the induced action of $G/G_r$ on $E/G_r$ is linear with respect to any system of algebraically independent homogeneous generators of $\Bbbk[E]^{G_r}$. That is, we obtain $G/G_r \subset GL(E/G_r)$. The key fact is that the linear group $G/G_r$ has no reflections at all. However, $E/G \simeq (E/G_r)/(G/G_r)$.

$2^o$. If $E/G$ is a complete intersection and $\mathcal{R}(G) = \varnothing$, then $G \subset SL(E)$.
Formula $(\diamond)$ for $\mathcal{A} = \Bbbk[E]^G$ shows that in this case $F(\Bbbk[E]^G; t)$ satisfies the equation $F(\Bbbk[E]^G; t^{-1}) = (-t)^{\dim E} F(\Bbbk[E]^G; t)$. Then one can refer to Corollary II.3.10(ii).

The following theorem of Kac and Watanabe gives a strong necessary condition for $E/G$ to be a complete intersection. No reasonable sufficient condition is known.

**Theorem II.9.2** (Kac-Watanabe, 1982)**.** *If $E/G$ is a complete intersection, then $E$ is generated by elements $\sigma$ such that $\mathrm{rk}\,(\sigma - id) \leqslant 2$.*

*Proof.* Let $G_{ci}$ be the subgroup of $G$ generated by the elements described in the formulation. It is a normal subgroup, and we obtain the commutative diagram

$$\begin{tikzcd}
E \arrow[d] \arrow[dr, bend left] & \\
E/G_{ci} \arrow[r] & E/G
\end{tikzcd}$$

Let us slightly modify the varieties occurring in this diagram. Set $G_{(3)} = \{\sigma \in G \mid \mathrm{codim}_E E^\sigma \geqslant 3\}$ and $Y = E \setminus \bigcup_{\sigma \in G_{(3)}} E^\sigma$. Then $Y$ is an open $G$-stable subset of $E$, and we obtain the modified diagram

$$\begin{tikzcd} Y \arrow[d] \arrow[rd, bend left] & \\ Y/G_{ci} \arrow[r, "\varphi"] & Y/G \end{tikzcd}$$

The advantage of this new diagram is that the action of $G/G_{ci}$ on $Y/G_{ci}$ is *free*, that is, the stabiliser of each point in $Y/G_{ci}$ is trivial. The reason is that all points having non-trivial stabilisers belong to the closed subvariety $(E/G_{ci}) \setminus (Y/G_{ci})$. Hence $\varphi$ is an unramified Galois covering, with the Galois group $G/G_{ci}$.

Now, we can use the result of Grothendieck which says that if $X$ is an irreducible complete intersection and $Z$ is a closed subvariety of codimension $\geqslant 3$, then $\pi_1(X) = \pi_1(X \setminus Z)$. Here $\pi_1(\cdot)$ denotes the algebraic fundamental group of $X$. We apply it to $X = E/G$. Since $E/G$ is contractible and therefore simply-connected, $Y/G$ is also simply-connected. The simply-connectedness means that any unramified Galois covering of $Y/G$ must be trivial. Thus, $Y/G_{ci} = Y/G$ and $G = G_{ci}$. □

**Remarks.** 1. The condition of the theorem is not sufficient. Already for $n = 3$, there are finite subgroups $G$ of $SL_3$ generated by elements $\sigma$ such that $\mathrm{rk}\,(\sigma - id) = 2$, but $E/G$ is not a complete intersection.

2. The same type of argument proves the implication (iii)⇒(i) in Theorem II.5.1. In place of Grothendieck's result, one has to use the Zariski-Nagata theorem which says that if $X$ is smooth and $\mathrm{codim}_X Z \geqslant 2$, then $\pi_1(X) = \pi_1(X \setminus Z)$.

**Example II.9.3.** Suppose $G \subset GL(E)$ is a f.g.g.r. having the property that $\mathcal{H}(G)/G = \{pt\}$; i.e., all reflecting hyperplanes are $G$-conjugate. (This happens, for instance, if $G$ is the Weyl group of a simply-laced irreducible root system.) Then all the reflections are of order two and $\det_E$ is the only linear character of $G$. Set $G' = G \cap SL(E)$. Then $|G : G'| = 2$ and $\Bbbk[E]^{G'}$ is a hypersurface. Indeed, if $\Bbbk[E]^G$ is freely generated by $f_1, \dots, f_n$, then $\Bbbk[E]^{G'}$ is generated by $f_1, \dots, f_n$, and $J$. The unique relation between these polynomials is of the form $J^2 = F(f_1, \dots, f_n)$. Here $F$ is certain polynomial, which is called the *discriminant* of $G$.

Motivated by similar examples for other reflection groups, R. Stanley [5] conjectured that if $E/G$ is a c.i., then there is a f.g.g.r. $G^* \subset GL(E)$ such that $[G^*, G^*] \subset G \subset G^*$. Then it was understood that there are counterexamples in dimension 3, but the conjecture holds if $\dim E$ is sufficiently large. A complete classification of finite linear groups whose algebra of invariants is a complete intersection is obtained by H. Nakajima and N. Gordeev (independently) in the mid-eighties.

**Example II.9.4.** If $\dim E = 2$ and $G \subset SL(E)$, then $E/G$ is a hypersurface. Since $E/G$ is normal, conical, and 2-dimensional, it has a unique singular point; namely, the image of the origin in $E$. The corresponding singularity is well-known. It has many names (Kleinian singularity, simple singularity, platonic singularity, rational double point, simple critical point) and even more characterisations, see [3]. Recall that the finite subgroups of $SL(2)$ are the following: $C_n$ – the cyclic group of order $n$; $D_n$ – the binary dihedral group of order $4n$; $T$ – the binary tetrahedral group of order 24; $O$ – the binary octahedral group of order 48; $I$ – the binary icosahedral group of order 120. The equations of the corresponding hypersurfaces are given below.

| | |
|---|---|
| $C_n$ | $X^n + YZ = 0$ |
| $D_n$ | $X^{n+1} + XY^2 + Z^2 = 0$ |
| $T$ | $X^4 + Y^3 + Z^2 = 0$ |
| $O$ | $X^3 + XY^3 + Z^2 = 0$ |
| $I$ | $X^5 + Y^3 + Z^2 = 0$ |

# Bibliography

[1] M. ATYAH and I. MACDONALD. ”Introduction to commutative algebra”, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969, ix+128 pp.

[2] D. BENSON. “Polynomial invariants of finite groups”, Cambridge University Press, 1994.

[3] ALAN H. DURFEE. Fifteen characterizations of rational double points and simple critical points, *Enseign. Math.* (2) **25**(1979), no. 1-2, 131–163.

[4] J.-P. SERRE. “Représentations linéaires des groupes finis”, Hermann, Paris, 1967.

[5] R.P. STANLEY. Invariants of finite groups and their applications to combinatorics, *Bull. Amer. Math. Soc.*(New Ser.) **1**(1979), 475–511.

[6] E.B. VINBERG. “Linear representations of groups”, Birkhäuser, Basel, 1989.