4. Finite groups.

4.1. Some general results.

4.1.1. In this chapter we discuss results about the invariant theory of finite groups. We assume that $k = \mathbb{C}$. Let V be a finite dimensional complex vector space, of dimension n. Put $S = S(V)$ and let K be the quotient field of S.

We denote by $G \subset GL(V)$ a finite group of linear transformations of V. Its order is denoted by $|G|$.

According to 2.3.2 and 2.4.9 or, more simply, to 2.4.4, the algebra S^G of G-invariants is of finite type over $\mathbb{C}$. The group G acts as a group of $\mathbb{C}$-linear automorphisms on K. Let K^G be the field of invariants.

4.1.2. Lemma. (i) S *is integral over* S^G;

(ii) K^G *is the quotient field of* S^G;

(iii) K *is a finite extension of* K^G, *of degree* $|G|$.

(i) follows from $\prod_{g \in G} (f - g \cdot f) = 0$, if $f \in S$. (ii) is already contained in 2.5.12 (a), and (iii) follows from well-known results in Galois theory (see e.g. [14,p.194]).

Write $P_G(T)$ for the Poincaré series $P_{S^G}(T)$, i.e.

$$P_G(T) = \sum_{d=0}^{\infty} (\dim_{\mathbb{C}} S_d^G) T^d.$$

In the case of finite groups, there is an explicit formula for the rational function represented by $P_G(T)$.

4.1.3. Proposition. *We have*

$$P_G(T) = |G|^{-1} \sum_{g \in G} \det(1 - gT)^{-1}.$$

This follows from 3.3.1 and the following lemma (applied to the image of G in the spaces S_d).

4.1.4. <u>Lemma</u>. $\dim V^G = |G|^{-1} \sum_{g\in G} \operatorname{tr}(g,V)$.

Here, as usual, V^G is the subspace of V whose elements are fixed by all $g \in G$. The proof of 4.1.4 follows by observing that the linear transformation

$$P = |G|^{-1} \sum_{g\in G} g$$

is a projection of V onto V^G (see 2.3.2), so that $\dim V^G = \operatorname{tr}(P,V)$.

Now let $f_1,\ldots,f_n$ be algebraically independent homogeneous elements of S^G such that S^G is integral over $\mathbb{C}[f_1,\ldots,f_n]$ (see 2.5.1). Notice that the number of these elements equals $n = \dim V$, because the transcendence degree of the quotient field of S^G equals that of S (according to 4.1.2). Let d_i be the degree of f_i, and let d be the degree of K^G over $\mathbb{C}(f_1,\ldots,f_n)$. We then have

$$P_G(T) = F(T) \prod_{i=1}^{n} (1 - T^{d_i})^{-1} ,$$

where $F(T) \in \mathbb{Z}[T]$ and $F(1) = d$ (see 2.5.6).

4.1.5. <u>Corollary</u>. $d^{-1} \prod_{i=1}^{n} d_i = |G|$. <u>In other words, the order of the graded $\mathbb{C}$-algebra</u> S^G (<u>see</u> 2.5.7)<u>equals the order of</u> G.

Since $d^{-1} \prod_{i=1}^{n} d_i$ equals the value of $(1 - T)^n P_G(T)$ at $T = 1$, this follows from 4.1.3.

We say that $g \in G$ is a *reflection* if $n-1$ of its eigenvalues are equal to 1 and if moreover V has a basis consisting of eigenvectors of g.

4.1.6. <u>Corollary</u>. <u>The number of reflections in</u> G <u>equals</u> $\sum_{i=1}^{n} (d_i-1) - 2F(1)^{-1}F'(1)$.

It follows from 2.5.9 (i) that $\sum_{i=1}^{n} (d_i-1) - 2F(1)^{-1}F'(1)$ equals the value at 1 of

$$2|G|(1-T)^{n-1}P_G(T) - 2(1-T)^{-1}.$$

By 4.1.3 this is the same as the value at 1 of

$$2 \sum_{\substack{g\in G \\ g \text{ reflection}}} (1-T)^{n-1} \det(1 - Tg)^{-1}.$$

Let g be a reflection of G, whose eigenvalue different from 1 is ζ. Then

$$(1-T)^{n-1}(\det(1-Tg)^{-1} + \det(1-Tg^{-1})^{-1}) = (1-\zeta T)^{-1} + (1-\zeta^{-1}T)^{-1}$$

which has the value 1 at $T = 1$. This implies the assertion.

4.1.7. Exercises.

(1) Let $n = 1$. Then G is a cyclic group. Determine S^G and P^G.

(2) Let G be the group of order 2, generated by scalar multiplication by -1. Determine S^G and P^G. If d is as above, show that $d \geq 2^{n-1}$.

4.2. Invariant theory of finite reflection groups.

4.2.1. Definition. G *is a reflection group if it is generated by the reflections which it contains*.

The next exercises give a few examples of reflection groups. In the course of this chapter more examples will appear.

4.2.2. Exercises.

(1) If $n = 1$ then G is a reflection group.

(2) Let $V = \mathbb{C}^n$, let G be the subgroup whose elements permute the elements of the canonical basis of $\mathbb{C}^n$. Then G is isomorphic to the symmetric group $\mathcal{T}_n$. Show that G is a reflection group.

Let $W \subset \mathbb{C}^n$ be the subspace of the vectors with coordinate sum 0. Then G stabilizes W, and induces a reflection group in W.

4.2.3. We first give a few simple properties of reflections, to be used hereafter. The proofs are left to the reader.

Let $s \in G$ be a reflection. The elements of V which are fixed by s form a hyperplane (= $(n-1)$-dimensional subspace) H_s. Fix $\ell_s \in S_1$, a linear function on V such that H_s is the set of zeros of ℓ_s. Such an ℓ_s is unique up to a scalar factor. Let ε_s be the eigenvalue of s different from 1. Then there is an eigenvector a_s for this eigenvalue, such that

$$sv = v + \ell_s(v)a_s ,$$

and that $\ell_s(a_s) = \varepsilon_s - 1$. We then have

$$s^{-1}v = v - \varepsilon_s^{-1}\ell_s(v)a_s.$$

It follows that for any $f \in S$ we have that $s \cdot f - f$ is divisible by ℓ_s, Write

(1) $$sf = f + \ell_s(\Delta_s f).$$

Then Δ_s maps S_d into S_{d-1} , and

$$\Delta_s(fg) = f(\Delta_s g) + (\Delta_s f)g + \ell_s(\Delta_s f)(\Delta_s g),$$

for $f,g \in S$.

4.2.4. Lemma. Let ℓ be a nonzero linear function on V such that $s\ell = c\ell$ ($c \in \mathbb{C}^*$). Then either $c = 1$ or $c = \varepsilon_s^{-1}$ and ℓ is a multiple of ℓ_s.

$\Delta_s\ell$ is a constant. If $c \neq 1$, (1) shows that ℓ is a multiple of ℓ_s. The assertion then follows by observing that $s\ell_s = \varepsilon_s^{-1}\ell_s$.

The main results about the invariant theory of finite reflection groups are contained in the following theorem.

4.2.5. Theorem. The following properties of the finite group G are equivalent:

(1) G is a finite reflection group;

(2) S is a free graded module over S^G with a finite basis;

(3) S^G is generated by n algebraically independent homogeneous elements[(1)].

We shall prove the implications (1) ⇒ (2) ⇒ (3) ⇒ (1). To do this, a number of lemmas is needed. In the first one k may be any field.

4.2.6. Lemma. Let S be a graded k-algebra with $S_0=k$, let R be a graded subalgebra. Denote by I the homogeneous ideal of S generated by the homogeneous elements of R of strictly positive degree. Let $(e_\alpha)_{\alpha\in A}$ be

<u>a set of homogeneous elements of</u> S <u>such that</u> $(e_\alpha+I)_{\alpha\in A}$ <u>is a basis of the vector space</u> S/I. <u>Then the</u> e_α <u>span the</u> R-<u>module</u> S.

Let M be the graded R-submodule of S spanned by the e_α. We prove by induction on d that $M_d = S_d$. This is so for $d = 0$. Let $d > 0$ and assume it for degrees smaller than d. Then if $f \in S_d$ we can write f as a finite linear combination

$$f = \sum_\alpha c_\alpha e_\alpha + \sum_\beta f_\beta r_\beta,$$

with $c_\alpha \in k$, $r_\beta \in R$ and f_β homogeneous of degree less than d. By induction we have $f_\beta \in M$. It follows that $f \in M$.

Now let G be a finite reflection group, as before. Let I be the homogeneous ideal in S generated by the homogeneous elements of S^G of strictly positive degree. So we are in the situation of 4.2.6, with $R = S^G$.

4.2.7. <u>Lemma</u>. <u>Let</u> $x_i \in S^G$, $y_i \in S$ $(1 \leqslant i \leqslant m)$ <u>be homogeneous elements. such that</u> $x_1y_1 + \ldots + x_my_m = 0$. <u>If</u> $x_1 \notin S^Gx_2 + \ldots + S^Gx_m$ <u>then</u> $y_1 \in I$.

We put $P = |G|^{-1} \sum_{g\in G} g$ (acting on S). This is an S^G-linear map $S \to S^G$ which is the identity on S^G (see the proof of 4.1.4). We prove the lemma by induction on the degree d of y_1. If $d = 0$ then there are $z_2,\ldots,z_m \in S$ such that

$$x_1 = z_2x_2 + \ldots + z_mx_m,$$

and we arrive at the contradiction

$$x_1 = (Pz_2)x_2 + \ldots + (Pz_m)x_m \in S^Gx_2 + \ldots + S^Gx_m.$$

Assume that $d > 0$ and that the assertion is true for lower degrees. Let $s \in G$ be a reflection. Δ_s being as in 4.2.3, we have

$$x_1\Delta_s(y_2) + \ldots + x_m\Delta_s(y_m) = 0.$$

By induction it follows that $\Delta_s y_1 \in I$, whence $sy_1 - y_1 \in I$, for any reflection s in G. Since G is a reflection group it follows that $gy_1 - y_1 \in I$ for all $g \in G$ (check this), whence $y_1 - Py_1 \in I$. This implies $y_1 \in I$.

4.2.8. <u>Lemma</u>. <u>Let</u> $y_1,\dots,y_m$ <u>be homogeneous elements of</u> S <u>such that their classes modulo</u> I <u>are linearly independent in the vector space</u> S/I. <u>Then</u> $y_1,\dots,y_m$ <u>are linearly independent over</u> S^G.
Assume that $x_1y_1 +\dots+ x_my_m = 0$, with $x_i \in S^G$. By 4.2.7 we can write $x_1 = z_2x_2 +\dots+ z_mx_m$, with $z_i \in S^G$, whence

$$x_2(y_2+z_2y_1) +\dots+ x_m(y_m+z_my_1) = 0.$$

By an induction on m we may assume $x_2 = \dots = x_m = 0$, which implies the assertion of the lemma.

4.2.9. We can now prove the implication (1) ⇒ (2) of 4.2.5. With the previous notations, choose homogeneous elements $(e_\alpha)_{\alpha\in A}$ of S such that $(e_\alpha+I)_{\alpha\in A}$ is a basis of S/I. It follows from 4.2.6 and 4.2.8 that S is a free module over S^G, with basis (e_α). It remains to see that this basis is finite. Now it is clear that (e_α) is also a basis of K, the quotient field of S, over the quotient field of S^G. The finiteness now follows from 4.1.2. In fact, the basis has $|G|$ elements.

The next lemma will take care of the implication (2) ⇒ (3) of the theorem.
In this lemma k is an arbitrary field of characteristic 0 and S = $= k[T_1,\dots,T_n]$ a graded polynomial algebra over k.
4.2.10. <u>Lemma</u>. <u>Let</u> R <u>be a graded subalgebra of</u> S <u>such that the</u> R-<u>module</u> S <u>has a finite basis consisting of homogeneous elements. Then there exist elements</u> $f_1,\dots,f_n$ <u>in</u> R <u>which are homogeneous and algebraically independent over</u> k <u>such that</u> $R = k[f_1,\dots,f_n]$.
S is integral over R (see e.g.[14,p.238]). It follows from 2.4.3 that R is of finite type over k. In particular, R is a noetherian ring. Let R^+ be the ideal of R generated by the homogeneous elements of strictly positive degree. Choose homogeneous elements $f_1,\dots,f_m$ in R such that $R^+ =$ $= Rf_1 +\dots+ Rf_m$ and let the set $\{f_1,\dots,f_m\}$ be minimal for this property, i.e. no element can be omitted. As in the proof of 2.4.5 one sees that $R = k[f_1,\dots,f_m]$. To establish 4.2.10 we shall prove

that $f_1,\dots,f_m$ are algebraically independent.
Assume that this is not the case. Then there is a nonzero $h \in k[X_1,\dots,X_m]$ such that $h(f_1,\dots,f_m) = 0$. Assume that h has minimum possible degree. Put $g_i = \frac{\partial h}{\partial X_i}(f_1,\dots,f_m)$, then not all g_i are 0. We may assume the g_i to be homogeneous elements of R (check this). Let J be the ideal in R generated by $g_1,\dots,g_m$ and assume that $\{g_1,\dots,g_s\}$ is a minimal set of generators of J occurring among the subsets of $\{g_1,\dots,g_m\}$. So there are homogeneous elements $r_{ij} \in R$ $(s+1 \leqslant i \leqslant m,\ \ 1 \leqslant j \leqslant s)$, such that

$$g_j = \sum_{i=1}^{s} r_{ij} g_i \ .$$

Let $h_{i\ell} = \frac{\partial f_i}{\partial T_\ell}$ $(1 \leqslant i \leqslant m,\ \ 1 \leqslant \ell \leqslant n)$. Then

$$0 = \frac{\partial h}{\partial T_\ell}\ (f_1,\dots,f_m) = \sum_{i=1}^{m} g_i h_{i\ell} = \sum_{i=1}^{s} g_i (h_{i\ell} + \sum_{j=s+1}^{m} r_{ij} h_{j\ell}).$$

Put

(2) $$u_{i\ell} = h_{i\ell} + \sum_{j=s+1}^{m} r_{ij} h_{j\ell} \qquad (1 \leqslant i \leqslant s,\ \ 1 \leqslant \ell \leqslant n).$$

Let $(e_\alpha)_{1 \leqslant \alpha \leqslant t}$ be a homogeneous basis of S over R and write

$$u_{i\ell} = \sum_\alpha r_{i\ell\alpha} e_\alpha.$$

Then

$$\sum_{i=1}^{s} g_i r_{i\ell\alpha} = 0,$$

and by the choice of $g_1,\dots,g_s$ we have that the nonzero elements $r_{i\ell\alpha}$ must have constant term zero. Hence we can write

$$u_{i\ell} = \sum_{h=1}^{m} u_{i\ell h}\, f_h.$$

Let d_i be the degree of f_i. Since f_i is homogeneous we have

$$d_i f_i = \sum_{\ell=1}^{n} T_\ell h_{i\ell}.$$

If $1 \leqslant i \leqslant s$ it follows from (2) that

$$\sum_{h=1}^{m} \sum_{\ell=1}^{n} u_{i\ell h}\, T_\ell f_h = d_i f_i + \sum_{j=s+1}^{m} d_j r_{ij} f_j \ .$$

Taking homogeneous components of degree d_i, we see that f_i is a linear combination with coefficients in S of the f_j with $j \neq i$. Because S has a basis over R it then follows that f_i is such a combination with coefficients in R (check this). This is a contradiction. The lemma follows.

4.2.11. We finally prove the implication (3) ⇒ (1) of 4.2.5. Assume that $S^G = \mathbb{C}[f_1,\dots,f_n]$, where f_i is homogeneous of degree d_i. (Since the transcendence degree of the quotient field of S^G equals n, by 4.1.2, this already implies that the f_i are algebraically independent.) Then the Poincaré series $P_G(T)$ equals $\prod_{i=1}^{n}(1-T^{d_i})^{-1}$ (2.5.5). It follows, using 4.1.5 and 4.1.6, that if $G \neq \{1\}$ (which we may assume) there are refections in G. Let G' be the subgroup of G generated by them. By the implication (1) ⇒ (3) of 4.2.5 (which was already established) we know that there are homogeneous elements $h_1,\dots,h_n$ in $S^{G'}$ which generate this algebra. Let e_i be the degree of h_i.
We may assume that $d_1 \leqslant d_2 \leqslant \dots \leqslant d_n$, $e_1 \leqslant e_2 \leqslant \dots \leqslant e_n$. Since $S^G \subset S^{G'}$ there exists for $i = 1,\dots,n$ a (unique) polynomial $P_i \in \mathbb{C}[T_1,\dots,T_n]$ such that $f_i = P_i(h_1,\dots,h_n)$. Fix an i. Since $f_1,\dots,f_i$ are algebraically independent the polynomials $P_1,\dots,P_i$ cannot be built up only from $T_1,\dots,T_{i-1}$. Hence there is $j \geqslant i$ and $\ell \leqslant i$ such that T_j occurs in P_ℓ. It follows that

$$d_i \geqslant d_\ell \geqslant e_j \geqslant e_i.$$

Since $\sum_{i=1}^{n} d_i \leqslant \sum_{i=1}^{n} e_i$ (as follows from 4.1.6) we have $d_i = e_i$. Then, by 4.1.5, it follows that $G' = G$. This shows that G is a reflection group, which had to be proved.

4.2.12. <u>Corollary</u>. *Let G be a reflection group. Let $S^G = \mathbb{C}[f_1,\dots,f_n]$, where f_i is homogeneous of degree d_i. The integers d_i are uniquely determined by G, up to order. The order of G is $\prod_{i=1}^{n} d_i$ and the number of reflections in G equals $\sum_{i=1}^{n}(d_i-1)$.*

This follows from 2.5.5, 4.1.5 and 4.1.6. We call the integers d_i the degrees of the reflection group G.

4.2.13. Exercises.

(1) Show, in the examples of 4.2.2 (2) that the degrees of the reflection groups are $1,2,\dots,n$ and $2,\dots,n$, respectively.
Determine the reflections in these groups.

(2) Let G be a reflection group, let $h_1,\dots,h_n$ be n algebraically independent homogeneous elements of S^G, let e_i be the degree of h_i. Then $\prod_{i=1}^{n} e_i \geq |G|$ and if equality holds then $S^G = k[h_1,\dots,h_n]$.
(Hint: use 4.1.5.)

4.2.14. The finite reflection groups can be classified. The classification can be reduced to that of the irreducible ones (see exercise 4.2.16 (1) below). We shall not go into the classification here. Some examples of irreducible finite reflection groups can be found in the exercises below.
The subgroup $G \subset GL(V)$ is called *real* if there is a G-stable subset V_0 of V which is a vector space over $\mathbb{R}$ (the vector space operations being induced by those of V), such that $\dim_{\mathbb{R}} V_0 = \dim_{\mathbb{C}} V$. The classification of reflection groups decomposes in two cases: that of the real ones and that of the others. The classification of real finite reflection groups (also called finite Coxeter groups) can be found in [1, Ch.VI,§4]. For the other ones see [4].

We insert a lemma, to be used occasionally. Assume $V = \mathbb{C}^n$ and denote by $(\ ,\ )$ the standard positive definite hermitian form on V with

$$\left(\sum_{i=1}^{n} x_i e_i,\ \sum_{i=1}^{n} y_i e_i\right) = \sum_{i=1}^{n} x_i \overline{y_i}\ ,$$

(e_i) denoting the canonical basis of $\mathbb{C}^n$. Recall that a linear transformation a of $\mathbb{C}^n$ is called hermitian if $(ax,y) = (x,ay)$ and unitary if $(ax,ay) = (x,y)$ (for all $x,y \in \mathbb{C}^n$). The unitary transformations form a subgroup $U_n(\mathbb{C})$ of $GL_n(\mathbb{C})$. The hermitian a is called positive definite if $(ax,x) > 0$ for $x \neq 0$.