Topology Vol. 14. pp. 173-177. Pergamon Press. 1975. Printed in Great Britain

ON A THEOREM OF PITTIE

ROBERT STEINBERG

(*Received* 1 *October* 1974)

§1. INTRODUCTION

HARSH V. PITTIE[3] has proved the following result:

THEOREM 1.1. *Let G be a connected compact Lie group with $\pi_1 G$ free and G' a (closed) connected subgroup of maximal rank. Then $R(G')$ is free (as a module) over $R(G)$ (by restriction).*

Here $R(G)$ denotes the complex representation ring of G. For the bearing of (1.1) on the K-theory of G the reader may consult [3]. Pittie's proof actually omits a few cases, which can however be checked out by hand. Here we present an elementary proof which yields an explicit basis for $R(G')$ over $R(G)$ (see (2.2) and (2.3(a)) below) and then a converse after suitably weakening the assumption on $\pi_1 G$.

THEOREM 1.2. *Let G be a connected compact Lie group and S its semisimple component. Then the following conditions are equivalent.*

(a) *$R(G')$ is free over $R(G)$ for every connected subgroup G' of maximal rank.*

(b) *$R(T)$ is free over $R(G)$ for some maximal torus T.*

(c) *$R(G)$ is the tensor product of a polynomial algebra and a Laurent algebra.*

(d) *$R(S)$ is a polynomial algebra.*

(e) *S is a direct product of simple groups, each simply connected or of type SO_{2r+1}.*

Since $\pi_1 G$ is free if and only if S is simply connected, because G is the product of S and a central torus, the equivalence of (a) and (e) provides the just-mentioned extension and converse of (1.1).

As a result of our development we also obtain:

THEOREM 1.3. *Theorems 1.1 and 1.2 are true for linear algebraic groups over algebraically closed fields (instead of compact Lie groups) and their rational representations.*

§2. PROOF OF (1.1)

We may, and shall, assume that G is semisimple, hence simply connected since $\pi_1 G$ is free, as is indicated in [3]. Let T be a maximal torus of G', hence also of G, and W' and W the corresponding Weyl groups, and X the character group (lattice) of T. As is known (see [1]), $R(G)$ may be identified with $Z[X]^W$ via restriction to T, even if G is not semisimple, and similarly for $R(G')$. To prove (1.1), therefore, we need only produce a free basis for $Z[X]^{W'}$ over $Z[X]^W$. This puts us in the realm of weights, roots and reflection groups, for which we use [2] as a general reference. Let $\Sigma \subseteq X$ be the root system of G relative to T, Σ^+ the set of positive roots and Π the corresponding basis of simple roots relative to some, fixed, ordering. The condition that G be simply connected is:

2.1. The fundamental weights $\{\lambda_a\}$, defined by $(\lambda_a, b^*) = \delta_{ab}$ $(a, b \in \Pi)$ with $b^* = 2b/(b, b)$, form a basis for X.

We generalize our problem slightly by allowing W' to be any reflection subgroup of W. Let Σ' be the corresponding root system, consisting of the roots orthogonal to the reflecting hyperplanes for W', and W'' the subset of W keeping Σ'^+ positive. Finally, for $v \in W''$ let λ_v denote the product in X of those λ_a for which $a \in \Pi$ and $v^{-1}a < 0$, and $e_v = \Sigma x^{-1} v^{-1} \lambda_v \in Z[X]$, the sum over $x \in W'(v)\backslash W'$ with $W'(v)$ denoting the stabilizer of $v^{-1}\lambda_v$ in W'.

THEOREM 2.2. *Assume G simply connected and the other notations as above. Then $Z[X]^{W'}$ is free over $Z[X]^W$ with $\{e_v | v \in W''\}$ as a basis.*

Remarks 2.3. (a) Observe that each $v^{-1}\lambda_v$ is dominant for Σ'. For $(v^{-1}\lambda_v, a) = (\lambda_v, va) \geq 0$ since $va > 0$ for all $a \in \Sigma'^+$. It follows from (2.2) and the above discussion that (1.1) holds with a basis consisting of those irreducible representations of G' for which the highest weights are $\{v^{-1}\lambda_v | v \in W''\}$. It also follows that the rank is $|W|/|W'|$, in (1.1) or in (2.2), either by Galois theory or by (2.5(a)) below. (b) In the principal case in which $W' = \{1\}$, in which G' is a torus in (1.1), we get $Z[X]$ free over $Z[X]^W$ with $\{w^{-1}\lambda_w | w \in W\}$ as a basis.

MAIN LEMMA 2.4. *Let $\{e_v\}$ be as above and $\{f_v\}$ ($v \in W''$) any collection of elements of $Z[X]^{W'}$. Set $D = \det ue_v$, $E = \det uf_v$ ($u, v \in W''$).*

(a) $D \neq 0$.

(b) *D divides E and the ratio is in $Z[X]^W$.*

Granted this lemma, we may prove (2.2) as follows. If $f \in Z[X]^{W'}$, then the system $\Sigma a_v ue_v = uf$ has a unique solution for $a_v \in Z[X]^W$, hence the equation $\Sigma a_v e_v = f$ does also, whence (2.2).

It remains to prove (2.4).

LEMMA 2.5. *Let everything be as above.*

(a) *W'' is a system of representatives for W/W'.*

(b) *If Σ' has a basis consisting of a subset of Π, then $\ell(ux) = \ell(u) + \ell(x)$ for $u \in W''$, $x \in W'$.*

Here $\ell(w)$ denotes the number of positive roots made negative by w. Fix $w \in W$. Then $w^{-1}\Sigma^+ \cap \Sigma'$ and $\Sigma'^+$are two positive systems for Σ', hence (*) they are congruent under a unique $x \in W'$. Then $u = wx^{-1} \in W''$ and $w = ux \in W'' \cdot W'$. Conversely, if w has this form, we may work backwards to conclude that x satisfies (*), hence is uniquely determined. This proves (a). The number of roots in Σ'^+ made negative by ux as in (b) is $\ell(x)$ since x fixes Σ' and u fixes the signs of the roots in Σ', while the number in $\Sigma^+ - \Sigma'^+$ is $\ell(u)$ since x fixes this set, whence (b).

LEMMA 2.6. *Assume as before and that $w \in W$ keeps $\Sigma^+ - \Sigma'^+$ positive. Then $w \in W'$, in fact w is in the subgroup generated by the simple reflections that W' contains.*

Assume w as given, $w \neq 1$. Then $wa < 0$ for some simple root a, so that $\ell(ww_a) < \ell(w)$. By our assumption $a \in \Sigma'^+$, so that w_a preserves $\Sigma^+ - \Sigma'^+$ and hence ww_a keeps it positive. By induction on $\ell(w)$ we conclude that ww_a is in the above subgroup, whence w is also.

LEMMA 2.7. *For $v \in W''$ we have $vW(v) \subseteq W''W'(v)$.*

Recall that $W(v)$, for example, denotes the stabilizer of $v^{-1}\lambda_v$ in W. As is known, this is a reflection group. Let $\Sigma(v)$ be the corresponding system of roots, those orthogonal to v. We have $v\Sigma'(v) = v\Sigma' \cap v\Sigma(v)$. Hence $v(\Sigma'^+ - \Sigma'^+(v))$ is disjoint from $(v\Sigma(v))^+$, and it is positive since $v \in W''$. Now if $w \in W(v)$, then $vwv^{-1} \in {}^vW(v)$, the group corresponding to the root system $v\Sigma(v)$, which is the subset of Σ orthogonal to λ_v and hence is like Σ' in (2.5(b)) since λ_v is dominant. By the above disjointness, $vwv^{-1} . v(\Sigma'^+ - \Sigma'^+(v)) > 0$. If we write $vw = ux$ as in (2.5(b)), this yields $x(\Sigma'^+ - \Sigma'^+(v)) > 0$ since u fixes signs on Σ'. Thus $x \in W'(v)$ by (2.6) with Σ, Σ' there replaced by Σ', $\Sigma'(v)$ here, whence (2.7).

LEMMA 2.8. *For each root a let n_a denote the number of pairs in W/W' interchanged by left multiplication by w_a.*

(a) *n_a is constant on W-conjugacy classes of roots.*

(b) *If a is simple then n_a is the number of v's in W'' such that $v^{-1}a < 0$.*

If a and b are conjugate, then so are w_a and w_b, hence also their left multiplications on W/W', whence (a). In (b) let w_a fix vW'. Then $v^{-1}w_a v \in W'$, whence $v^{-1}a \in \Sigma'$ and $v^{-1}a > 0$ since $v \in W''$. Now assume w_a does not fix vW', i.e. $v^{-1}a \notin \Sigma'$. Then $v\Sigma'^+$ is disjoint from a and positive, whence $w_a v\Sigma'^+$ is also positive and $w_a v \in W''$. Now just one of $v^{-1}a$, $(w_a v)^{-1}a$ is negative. Thus $v^{-1}a < 0$ for exactly n_a choices of $v \in W''$.

LEMMA 2.9. *If D is as in (2.4) and n_a as in (2.8) then D has $\Pi\lambda_a^{n_a}$ ($a \in \Pi$) as its unique highest term and $\pm\Pi\lambda_a^{-n_a}$ as its unique lowest term.*

This is relative to the usual partial order in which $\lambda > \mu$ denotes that $\lambda\mu^{-1}$ is a product of positive roots. Let A denote the matrix (ue_v). Recall that $ue_v = \Sigma ux^{-1}v^{-1}\lambda_v$, summed over $x \in W'(v)\backslash W'$. Consider the vth column of A. We have $\lambda_v \geq ux^{-1}v^{-1}\lambda_v$ for all terms there. We claim that equality can hold on or above the diagonal only for the term with $u = v$ and $x \in W'(v)$, if we order the rows so that u is above u' whenever $\ell(u) < \ell(u')$. Assume equality. Then $v^{-1}ux^{-1} \in W(v)$ by definition, so that $ux^{-1} \in W''W'(v)$ by (2.7), and $x \in W'(v)$ by (2.5(a)), so that $uv^{-1}\lambda_v = \lambda_v$. Thus uv^{-1}, hence also vu^{-1}, is in the group generated by the reflections for the simple roots orthogonal to λ_v, which are those kept positive by v^{-1} by the definitions. Applying (2.5(b)) to this situation we get $\ell(u^{-1}) = \ell(v^{-1}) + \ell(vu^{-1})$. On or above the diagonal where $\ell(u) \leq \ell(v)$ this can hold only if $\ell(vu^{-1}) = 0$, whence $u = v$ and our claim. It follows that $D = \det A$ has $\Pi\lambda_v$ as its unique highest term. Now λ_a ($a \in \Pi$) makes a contribution to λ_v just when $v^{-1}a<0$. Thus by (2.8(b)) the highest term is as in (2.9). Now each $w \in W$ permutes the rows of A by (2.5(a)) and the invariance of e_v under W', hence fixes D up to sign. It follows that there is a unique lowest term, $\pm w_0\Pi\lambda_a{}^{n_a}$, with w_0 the element of W that makes all positive roots negative. Now if $b = -w_0a$ then $n_a = n_b$ by (2.8(a)). Thus the lowest term is as in (2.9), as required.

Consider now (2.4). We show that $D_1 = \Pi(a^{1/2} - a^{-1/2})$ $(a \in \Sigma^+)$ divides E and that $D_1 = D$. Assume $a \in \Sigma^+$. As noted earlier there are n_a pairs of rows of (uf_v) which are interchanged by w_a. If we subtract row w_au from row u for such a pair then all entries of the result are divisible by $a-1$ since $w_a\lambda = \lambda a^n$, $n = -(\lambda, a^*)$, for $\lambda \in X$. Thus $(a-1)^{n_a}$ divides E, and since $\mathbf{Z}[X]$ is a u.f.d., so do $\Pi(a-1)^{n_a}$ and D_1. In particular D_1 divides D. To prove $D_1 = D$ we need only show that the highest and lowest terms match up, i.e. by (2.9), that $\Sigma n_a a$ $(a>0) = \Sigma n_a\lambda_a$ $(a \in \Pi)$, with the operation of X now written as addition. If s denotes the left side and b a simple root then w_b maps b on $-b$ and permutes the other positive roots. Thus $(1-w_b)s = 2n_bb$, and $(s, b^*) = 2n_b$ by the formula for a reflection, so that s equals the right side by (2.1). Finally, each $w \in W$ acts on the rows of (ue_v) and (uf_v) just as it does on W/W', hence fixes E/D. This proves (2.4), hence also (2.2) and (1.1).

§3. PROOF OF (1.2) AND (1.3)

In this section G is a simply connected group, T is a maximal torus, and the other notations of §2 are used. Further r_a $(a \in \Pi)$ denotes the irreducible representation of G with highest weight λ_a, so that $R(G)$ is a polynomial algebra in the r_a's. If z is in the center of G, then $r_a(z) = \lambda_a(z)$. id. Thus there is a natural action of z on $R(G)$ and $\mathbf{Z}[X]$ with their scalars extended from $\mathbf{Z}$ to $\mathbf{C}$ such that $zr_a = \lambda_a(z)r_a$ and $z\lambda_a = \lambda_a(z)\lambda_a$ for all a. Observe that z fixes roots and commutes with W. We call z a pseudoreflection if it is one on $\Sigma\, \mathbf{C}\, r_a$ or $\Sigma\, \mathbf{C}\, \lambda_a$, i.e. if $\lambda_a(z) = 1$ for every a but one.

Main Lemma 3.1. *Let G be simply connected and Z a subgroup of the center of G. Then the following conditions are equivalent.*

(a) *$R(G')^Z$ is free over $R(G)^Z$ for every connected subgroup G' of maximal rank.*

(b) *$R(T)^Z$ is free over $R(G)^Z$ for some maximal torus T.*

(c) *$R(G)^Z$ is a polynomial algebra over $\mathbf{Z}$.*

(d) *Z is a direct product of the centers of a number of the simple components of G of type* Spin_{2r+1}.

(e) *Z is generated by pseudoreflections.*

(f) *$R(G)^Z$ has a generating set of the form $\{r_a{}^{m_a} \mid a \in \Pi\}$.*

(g) *X^Z has a basis of the form $\{m_a\lambda_a\}$.*

(h) *(X^Z, W, Σ_1) is the data for a simply connected group for some choice of an abstract root system $\Sigma_1 \subseteq X^Z$.*

Consider now (1.2) in which, as noted earlier, G may be assumed semisimple. Since every semisimple group may be written G/Z with G and Z as in (3.1), and since $R(G)^Z, R(T)^Z, \ldots$ have the same significance for G/Z as $R(G), R(T), \ldots$ have for G, Theorem 1.2 follows from the equivalence of (a), (b), (c) and (d) of (3.1).

We first prove the equivalence of the last four parts of (3.1), which have been added mainly for convenience. If (e) holds and Z acts as a product of cyclic groups, the one on r_a being of order m_a, say, then $R(G)^Z = \mathbf{Z}[r_a\text{'s}]^Z = \mathbf{Z}[r_a{}^{m_a}\text{'s}]$, whence (f). Conversely, if this equation holds then Z is a subgroup of the above product, is the whole product in fact since otherwise some nontrivial character $\Pi\lambda_a{}^{d_a}$ $(0 \leq d_a < m_a)$ would vanish on Z and $\Pi r_a{}^{d_a}$ would contradict the last equation, whence (e). Since $\Pi r_a{}^{d_a}$ is in $R(G)^Z$ if and only if $\Sigma\, d_a\lambda_a \in X^Z$ (additive notation here), (f) and (g) are equivalent. Observe that in (h) the elements of Σ_1 are multiples of those of Σ since their directions are determined by the reflections of W. If (g) holds then $m_aa = (1-w_a)m_a\lambda_a \in X^Z$ and $(m_aa, (m_bb)^*)$ is always integral since $\{(m_bb)^*\}$ is a basis for the dual of X^Z. It readily follows that $\{m_aa \mid a \in \Pi\}$ is a basis for a root system Σ_1 for which (h) holds. Conversely, if (h) holds and $\{m_aa\}$ is a basis for Σ_1, then $\{m_a\lambda_a\}$ is the corresponding basis of X^Z (see 2.1), whence (g).

Next we prove that (e) $\Rightarrow$ (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (e). If (e) holds, so does (h) and then also (a) by (1.1) which in (2.2) has been reduced to a theorem about (X, W, Σ). Clearly (a) implies (b). Assume (b). Then $A = \mathbf{C}R(T)^Z$ is free, hence also integral, over $B = \mathbf{C}R(G)^Z$. Localize B at the point q of Spec B where all r_a's are 0 and A at a point p of Spec A above q. The first condition makes sense since each r_a has some power in B. We now invoke a result of Auslander–Buchsbaum–Serre.

3.2 A (commutative, Noetherian) local ring R is regular if and only if its cohomological dimension $d(R)$ is finite.

Now let $\{x_1, x_2, \dots, x_r\}$ with $r = |\Pi|$, the rank of G, be a basis for X^Z, imbedded in A in the natural way, and $x_i(p) = c_i$. Then A_p is the tensor product of r algebras, the ith equal to $\mathbf{C}[x_1, x_i^{-1}]$ localized at $x_i = c_i$, hence is regular, whence $(d(A_p) < \infty$ by (3.2). Since A_p is free over B_q (with basis any basis for $R(T)^Z$ over $R(G)^Z$), $d(B_q) \leq d(A_p)$, so that B_q is regular by (3.2). Thus $\dim_{\mathbf{C}} m/m^2 = r$, if m denotes the maximal ideal of B_q. The monomials $\Pi r_a^{d_a}$ that lie in m form a multiplicative semigroup. Let C be its minimal generating set, consisting of those elements that are not products of others. Clearly B is a basis for m/m^2 over $\mathbf{C}$ so that $|B| = r$. However for each $a \in \Pi$ some $r_a^{m_a}$ lies in B. Thus B consists of the $r_a^{m_a}$'s, and $R(G)^Z$ is a polynomial algebra on the $r_a^{m_a}$'s, whence (f) and also (c). Now assume (c). The free generating set for $R(G)^Z$ may be taken in the ideal m just considered. Then the proof just given shows that (f) holds, hence also (e).

It remains only to prove the equivalence of (d) and (e). For this we may assume that G is simple since if $z \in Z$ is a pseudoreflection it acts nontrivially on just one r_a, hence belongs to some simple component of G. Let V be the universal covering space for T, a real Euclidean space, and for convenience take the character values $\lambda(v)$ to be in $\mathbf{R}/\mathbf{Z}$ rather than in the complex numbers of norm 1. Then there is the famous fundamental simplex $S: \{v \in V \mid a(v) \geq 0\ (a \in \Pi)$, $h(v) \leq 1\}$. Here $h = \Sigma\, h_a a$ is the highest root. This sum is to be taken over Π and similarly for the sums on $a, b, \dots$ that follow. The center of G is represented in S by 0 and the vertices z_a of S corresponding to a's for which $h_a = 1$. For any such we have

$$b(z_a) = \delta_{ba} \qquad (b \in \Pi). \tag{3.3}$$

For a again arbitrary write

$$\lambda_a = \Sigma\, n_{ab} b \qquad (n_{ab} \in \mathbf{Q}). \tag{3.4}$$

We claim that for the dual root system Σ^*, in which a is replaced by $2a/(a, a)$ and similarly for λ_a, the corresponding equation reads

$$\lambda_a^* = \Sigma\, n_{ba} b^*. \tag{3.5}$$

For substituting the definitions into (3.4) we get (3.5) with the coefficient of b^* equal to $n_{ab}(b, b)/(a, a)$. But $(\lambda_a, \lambda_c) = n_{ac}(c, c)/2$ by (3.4) and (2.1), whence $n_{ac}(c, c) = n_{ca}(a, a)$ by symmetry. The coefficient of b^* thus becomes n_{ba}, whence (3.5). Now assume that $z_a \in Z$ acts as a pseudoreflection on $\mathbf{C}R(G) = \mathbf{C}[r_a\text{'s}]$. Then $\lambda_c(z_a)$ is integral with just one exception, say for $c = b$. But $\lambda_c(z_a) = n_{ca}$ by (3.4). Thus (by (3.5)) $n_{ba} b^*$, hence also some submultiple of b^*, is a weight. This implies that Σ^* is of type C_r and b^* is the unique long simple root, as is well known and proved thus: in any other case there is a simple root c^* such that $(b^*, c^{**}) = -1$, so that b^* is primitive as a weight. Then Σ is of type B_r (and $G = \mathrm{Spin}_{2r+1}$), and a is the long root at the end of the Dynkin diagram and $\{1, z_a\}$ is the center of G since this a is the only simple root for which $h_a = 1$. Conversely, if Σ and a are as just mentioned it can be verified that λ_a^* in (3.5) has exactly one nonintegral coefficient so that z_a is a pseudoreflection. Thus (d) and (e) are equivalent, and (3.1) is completely proved.

Remarks 3.6. (a) For a proof of the equivalence of (b), (c) and (e) in a more general setting see [4], from which our proof that (b) implies (c) is taken. We could avoid the other heavy commutative algebra used there because of the simple action of Z in our case. (b) The geometric essence of the equivalence of (c) and (e) in its general form is that, in an algebraic or analytic variety acted on by a finite group Z of order not divisible by the characteristic a nonsingular point p remains nonsingular in the quotient space if and only if Z^p acting on the tangent space at p is generated by pseudoreflections.

Finally, we consider (1.3). Since every irreducible representation of G is trivial on the unipotent radical of G, we may assume G reductive. Then we may reduce (1.3) to properties of abstract root systems and reflection groups, as we reduce (1.1) to (2.2), properties which have been proved above.

REFERENCES

1. J. F. ADAMS: *Lectures on Lie Groups.* Benjamin, New York (1969).
2. N. BOURBAKI: *Groupes et algèbres de Lie,* Chapters IV, V and VI. Hermann, Paris (1968).
3. H. V. PITTIE: Homogeneous vector bundles on homogeneous spaces, *Topology* **11** (1972) 199–203.
4. J.-P. SERRE: *Colloque d'algèbre,* no. 8. Ecole Normale Supérieure de Jeunes Filles, Paris (1967).

University of California, Los Angeles

Ecole Normale Supérieure de Jeunes Filles
Colloque d'Algèbre [1967. Paris], n° 8, 11 p.

GROUPES FINIS D'AUTOMORPHISMES D'ANNEAUX LOCAUX RÉGULIERS

par Jean-Pierre SERRE

Exposé rédigé par Marie-José BERTIN

1. Introduction.

Il s'agit de regarder l'action de certains groupes finis d'automorphismes sur des anneaux locaux réguliers ou sur des algèbres graduées de polynômes sur un corps (i. e. sur $k[X_1 , \ldots , X_n]$), G agissant linéairement.

On a souvent, en effet, une correspondance entre les théorèmes sur les anneaux locaux réguliers et ceux sur les anneaux gradués de type fini sur un corps. Le passage "local -> gradué" est généralement aisé ; quant au passage "gradué -> local", moins aisé, il se fait au moyen du "gradué associé".

Situation : On se donne un anneau local régulier S , et un groupe fini d'automorphismes G , agissant sur S . On désigne par $R = S^G$ le sous-anneau de S formé des éléments invariants par G . Le problème est de savoir sous quelles hypothèses l'anneau R est régulier.

– Dans le cas où $S = k[X_1 , \ldots , X_n]$, il s'agit donc de savoir dans quels cas $R = k[X_1 , \ldots , X_n]^G$ est une algèbre de polynômes.

– En langage des schémas, le problème se formule ainsi : Etant donnés un schéma affine Spec S , régulier sur Spec k (S étant un anneau local de corps résiduel k), et G un groupe fini d'automorphismes opérant sur Spec S , dans quels cas Spec$(S)/G$ est-il un schéma régulier ?

Le passage d'une traduction à l'autre est donné par le lemme suivant :

LEMME. – Soit R une algèbre graduée de type fini sur un corps k . Les trois assertions suivantes sont équivalentes :

1° Spec R est régulier (en tant que schéma sur Spec k) ;

2° $R_{\mathfrak{m}}$ est régulier ($\mathfrak{m}$ désignant l'idéal maximal formé par les éléments homogènes de degré positif) ;

3° R est une algèbre graduée de polynômes.

2. Enoncé et principe de démonstration des théorèmes dans le cas gradué (cas historiquement le premier résolu).

"Cas gradué" signifie : S , algèbre graduée de polynômes sur un corps k ; $S = k[X_1 , \dots , X_n]$.

Définition. - Soit G un groupe fini, $G \subset G\ell(n , k)$. G opère sur $(k)^n$. Supposons $(\operatorname{card} G , p) = 1$, où p désigne l'exposant caractéristique de k . On dit qu'un élément g de G est une pseudo-réflexion, si $\operatorname{Im}(1 - g)$ est de rang inférieur ou égal à 1 (i. e. si $g(x) = x + \lambda(x)e$, $\forall\ x \in (k)^n$, où e désigne un vecteur fixe et λ une forme linéaire sur k^n).

Exemple de pseudo-réflexion :

(1)
$$g = \begin{pmatrix} 1 & & & & 0 \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ 0 & & & & \mu \end{pmatrix} .$$

Si $(\operatorname{card} G , p) = 1$, alors toute pseudo-réflexion $g \in G$ se met sous la forme (1) où μ est une racine de l'unité.

THÉORÈME 1. - Soient $S = k[X_1 , \dots , X_n]$, et G un groupe fini d'automorphismes de S tel que $(\operatorname{card} G , p) = 1$, où p désigne l'exposant caractéristique de k . Les assertions suivantes sont équivalentes :

(a) $R = S^G$ algèbre de polynômes ;

(b) G est engendré par des pseudo-réflexions.

Ce théorème a été démontré par SHEPHARD-TODD, en [6], dans le cas $k = \underset{\sim}{C}$.

Dans le sens (a) $\Longrightarrow$ (b) , leur démonstration est applicable à un corps quelconque de caractéristique $p \neq 0$.

Dans le sens (b) $\Longrightarrow$ (a) , leur démonstration est la suivante : ils font la liste de tous les groupes ayant cette propriété, et ils vérifient que R est bien une algèbre de polynômes.

En 1955, CHEVALLEY a donné une démonstration a priori de ce théorème.

THÉORÈME 2. - Soient $S = k[X_1 , \dots , X_n]$, et G un groupe fini d'automorphismes de S ; alors :

($R = S^G$ algèbre de polynômes) implique (G est engendré par des pseudo-réflexions).

La réciproque est fausse à partir du cas $n = 4$, pour $k = \underset{\sim}{F}_q$, et G groupe orthogonal pour la forme quadratique $2X_1 X_2 + 2X_3 X_4$.

Principe de démonstration de SHEPHARD-TODD. - Les théorèmes de Shepherd-Todd sur $\underset{\sim}{C}$ passent à la caractéristique 0 , sinon à la caractéristique p telle que $(\text{card } G , p) = 1$.

Donc, soit $G \subset G\ell(n , \underset{\sim}{C})$.

1er cas : Il existe une structure réelle sur $\underset{\sim}{C}^n$, invariante par G (i. e. G se plonge dans $G\ell(n , \underset{\sim}{R})$, et les éléments de G peuvent s'écrire par des matrices à coefficients réels).

On avait vu que, si G était une pseudo-réflexion, dans le cas $(\text{card } G , p) = 1$ (or ici $p = 0$, c'est donc toujours le cas), g se mettait sous la forme

$$\begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ 0 & & 1 & \\ & & & \mu \end{pmatrix} ,$$

où μ était une racine de l'unité. Comme $G \subset G\ell(n , \underset{\sim}{R})$, on a donc ici forcément $\mu = \pm 1$.

Donc les éléments de G sont dans ce cas des réflexions (une réflexion est une pseudo-réflexion d'ordre 2).

Ces groupes sont les groupes étudiés dans les travaux d'Elie CARTAN, et ce sont, à quelques exceptions près, les groupes de Weyl des groupes de Lie semi-simples.

Lorsque G est irréductible, il se représente par un schéma de Coxeter ; or la liste des schémas possibles est bien connue.

2e cas : G est vraiment un groupe "complexe".

SHEPHARD et TODD dressent alors la liste des divers groupes G possibles.

Pour cela, ils envoient $G\ell(n , \underset{\sim}{C})$ dans $PGL(n , \underset{\sim}{C})$. Dans $PG\ell(n , \underset{\sim}{C})$, ces transformations correspondent aux "homologies".

Or MITCHELL, en 1914, avait fait la liste des groupes finis engendrés par les homologies. Pour obtenir les groupes finis de $G\ell(n , \underset{\sim}{C})$, engendrés par des pseudo-réflexions, il suffit donc de relever ces groupes dans $G\ell(n , \underset{\sim}{C})$.

Parmi les groupes G irréductibles, on en trouve de deux sortes :

1° Les imprimitifs : Ce sont les groupes $G(m , p , n)$, où $n =$ dimension de l'espace vectoriel, et m est un entier tel que p divise m . Ces groupes sont des variantes du groupe symétrique $\mathfrak{S}_n$. En effet, ils agissent ainsi :

$$g(x_i) = x_i' = \theta^{\nu_i} x_{\sigma(i)} , \qquad \text{où} \quad \sigma \in \mathfrak{S}_n ,$$

θ est une racine primitive m-ième de l'unité, et $\sum \nu_i \equiv 0 \quad (p)$.

2° Les primitifs :

(a) En dimension 2 , il y en a un grand nombre, 12 environ.

(b) En dimension $n > 2$, on en trouve seulement un nombre fini.

- En dimension 3 , on trouve :

$G_{168} \times \{\pm 1\}$, où $G_{168} = S\ell_3(\underset{\sim}{F}_2)$;
Deux groupes d'ordre 648 et 1296 qui correspondent au même groupe projectif ;
Un groupe d'ordre 2160 (qui revêt 6 fois son groupe projectif qui, lui, est isomorphe à GL_6).

- En dimension $n = 4$, on trouve deux groupes d'ordres 46080 et 7680 , et un groupe d'ordre 25920 .

- En dimension $n = 5$, on trouve un groupe d'ordre 72×6 !

- En dimension $n = 6$, un groupe d'ordre 108×9 !

3. Enoncé et démonstration des théorèmes dans le cas local régulier.

Dans toute la suite, on fait les hypothèses suivantes :

S est un anneau local, régulier, d'idéal maximal $\mathfrak{m}_S$; G un sous-groupe fini de $\mathrm{Aut}(S)$. R désigne le sous-anneau S^G des invariants de S par G (on sait que R est local), et on suppose en outre :

(1) R noethérien ;
(2) S de type fini sur R ;
(3) R et S de même corps résiduel k de caractéristique p (cas totalement ramifié).

On désigne par $V = \mathfrak{m}_S/\mathfrak{m}_S^2$ l'espace tangent de Zariski relativement à S . Alors G opère linéairement sur V , et on désigne par ε l'application $\varepsilon :\ G \to \mathrm{Aut}(V)$

THÉORÈME 1'. - Si (card G , p) = 1 , alors :

(R régulier) $\Longleftrightarrow$ ($\varepsilon(G)$ est engendré par des pseudo-réflexions) .

THÉORÈME 2'. – (R *régulier*) *implique* ($\varepsilon(G)$ *engendré par des pseudo-réflexions*

Démonstration du théorème 2'. – Soit H le sous-groupe de G, engendré par les éléments $g \in G$ tels que $\varepsilon(g)$ soit une pseudo-réflexion. Soit $R' = S^H$; on a donc les inclusions suivantes :

$$S \supset R' \supset R \ .$$

On va démontrer que $R' = R$, ce qui entraînera, par la théorie de Galois, que $G = H$, et par suite le théorème 2'.

LEMME. – R' *est non ramifié sur* R *en codimension* **1** (i. e. divisoriellement non ramifié).

Autrement dit : Après localisation par des idéaux premiers de hauteur 1, l'extension est non ramifiée.

Autrement dit encore : Le lieu de ramification du revêtement est de codimension $\geqslant 2$.

On montre que le *groupe d'inertie* $I_{G/H}$ *de tout idéal premier* q' *de hauteur* 1 *de* R' *est nul* (G/H est le groupe de Galois de l'extension R' sur R). Pour cela, on démontre que, pour tout $\mathfrak{P}$, idéal premier de hauteur 1 de S, tel que $q' = \mathfrak{P} \cap R'$ (q' est un idéal premier de hauteur 1 de R', car S est intègre, entier sur R', et R' intégralement clos), on a $I_G = I_H$, ce qui entraînera bien le résultat voulu.

Or I_G, groupe d'inertie de $\mathfrak{P}$ dans G, est formé des éléments $g \in G$ tels que $g(\mathfrak{P}) = \mathfrak{P}$ et que g opère trivialement sur $S/\mathfrak{P}$ (même définition pour I_H). On a évidemment l'inclusion $I_H \subset I_G$.

Il nous reste donc à montrer l'inclusion inverse. Donc, soit $g \in I_G$, alors $g(x) \equiv x \ (\mathfrak{P})$, $\forall\, x \in S$, et g opère trivialement sur $S/\mathfrak{P}$.

Soit $x \in \mathfrak{M}_S$,

$$g(x) = x + y \ , \qquad \text{où } y \in \mathfrak{M}_S \cap \mathfrak{P} = \mathfrak{P} \ . \tag{2}$$

Or l'image de $\mathfrak{P}$ dans $\mathfrak{M}_S/\mathfrak{M}_S^2$ (i. e. $(\mathfrak{P} + \mathfrak{M}_S^2)/\mathfrak{M}_S^2$) est un *k-espace vectoriel de dimension* 0 *ou* 1. Car si $\dim_k((\mathfrak{P} + \mathfrak{M}_S^2)/\mathfrak{M}_S^2) \neq 0$, il existe $\bar{x} \neq 0$, $\bar{x} \in (\mathfrak{P} + \mathfrak{M}_S^2)/\mathfrak{M}_S^2$; ou encore, il existe $x \in \mathfrak{P}$, $x \notin \mathfrak{M}_S^2$, tel que l'idéal Sx soit premier.

(En effet, S étant de type fini sur R noethérien, est lui-même noethérien ; S étant local, noethérien, régulier, et $x \neq 0$, $x \in \mathfrak{M}_S$ et $x \notin \mathfrak{M}_S^2$, alors S/xS est régulier, donc intègre, et xS est un idéal premier.)

Or $Sx \subset \wp$. Comme $\wp$ est un idéal premier de hauteur 1 , cela entraîne $\wp = Sx$. D'où $k\bar{x} = (\wp + \mathfrak{M}_S^2)/\mathfrak{M}_S^2$ (en prenant les images dans $\mathfrak{M}_S/\mathfrak{M}_S^2$), et par suite $\dim_k((\wp + \mathfrak{M}_S^2)/\mathfrak{M}_S^2) = 1$. En réduisant la relation (2) modulo $\mathfrak{M}_S^2$, on obtient

$$g(\bar{x}) - \bar{x} \in (\wp + \mathfrak{M}_S^2)/\mathfrak{M}_S^2 , \qquad \forall\ \bar{x} \in \mathfrak{M}_S/\mathfrak{M}_S^2 .$$

Donc $\mathrm{Im}(\varepsilon(g) - 1)$ est de dimension $\leqslant 1$, et $\varepsilon(g)$ est une pseudo-réflexion. Par suite $g \in I_H$.

C. Q. F. D.

Ce lemme étant démontré, d'après le théorème de pureté de "Nagata-Auslander" ([1]), comme R' est normal (car c'est un anneau d'invariants), et R régulier par hypothèse, la non-ramification de R' sur R en codimension 1 entraîne la non-ramification de R' sur R . Comme R et R' sont deux anneaux locaux ayant même corps résiduel (car par hypothèse S et R avaient même corps résiduel), cela entraîne que $R = R'$. Par suite $G = H$, et $\varepsilon(G)$ est bien engendré par des pseudo-réflexions.

Démonstration du théorème 1'.

Remarque : Le problème se pose également quand on considère le quotient d'un domaine borné D par un sous-groupe discret Γ . Si l'on désigne par x un point de D , et par Γ_x son stabilisateur (c'est un groupe fini), alors :

(D/Γ , variété analytique complexe sans singularités) $\Longleftrightarrow$ (Les Γ_x sont engendrés par des pseudo-réflexions) .

Exemple de cas singulier : Soit le point (x , y) . Si Γ est engendré par les symétries $\left\{\begin{matrix} x \longmapsto -x \\ y \longmapsto -y \end{matrix}\right\}$, Γ n'est pas engendré par des pseudo-réflexions, et l'espace quotient est un cône quadratique, qui a donc une singularité à l'origine.

Il s'agit donc de démontrer que, si $(\mathrm{card}\ G , p) = 1$, et si $\varepsilon(G)$ est engendré par des pseudo-réflexions, alors R est régulier (l'autre implication étant donnée par le théorème 2').

LEMME. - Soient R et S deux anneaux locaux tels que R soit contenu dans S S soit de type fini sur R et entier sur R , R soit noethérien et S régulier alors les assertions suivantes sont équivalentes :

(a) R régulier ;

(b) S est un R-module libre.

(a) $\Longrightarrow$ (b) . Comme R est un anneau local régulier, et S un R-module de type fini, on a :

$$\operatorname{prof}_R S + \dim \operatorname{proj}_R S = \dim R = \dim S \tag{3}$$

(car S est entier sur R). Or, l'on est dans la situation suivante : $R \subset S$, R et S locaux noethériens, S entier sur R , l'homomorphisme injection $R \to$ est un homomorphisme local ; donc, comme S est un R-module de type fini, on a

$$\operatorname{prof}_R S = \operatorname{prof}_S S \quad .$$

De plus, S étant local régulier, est un anneau de Macaulay, d'où

$$\operatorname{prof}_S S = \dim S \quad . \tag{4}$$

En comparant les relations (3) et (4), on trouve :

$$\dim \operatorname{proj}_R S = 0 \quad .$$

Par suite, S est un R-module projectif ; comme, par hypothèse, S est un R-module de type fini et que R est un anneau local noethérien, cela entraîne que S est un R-module libre.

(b) $\Longrightarrow$ (a) . Supposons S un R-module libre. On va montrer que R est régulier, et pour cela que $\dim \operatorname{coh} R$ est finie. Or, S étant libre sur R , est pla sur R , d'où

$$\dim \operatorname{coh}(R) \leqslant \dim \operatorname{coh}(S) \quad .$$

S , étant régulier, a une dimension cohomologique finie, d'où R également.

<u>Il reste donc à démontrer que</u> S <u>est un</u> R-<u>module libre</u>, et le théorème 1' sera démontré.

Pour cela, il suffit de montrer que $T = \operatorname{Tor}_1^R(S\ , k)$ est nul (car S est de type fini sur R). Or T est un S-module. Donc G opère dessus. De plus, T est un S-module de type fini (car c'est un espace vectoriel de dimension finie sur k). Donc, si l'on montre que $T' = T/(\mathfrak{m}_S T) = 0$, d'après le lemme de Nakayama, cela entraînera que $T = 0$. Mais si :

(a) Tout élément de T' invariant par G est nul, et

(b) G opère trivialement sur T' (i. e. toute pseudo-réflexion de G opère trivialement sur T' , puisque G est engendré par des pseudo-réflexions),

alors, on aura bien $T' = 0$.

(a) Puisque $(\operatorname{card} G\ , p) = 1$, $\operatorname{card} G$ est inversible dans R . Ceci rend alor le foncteur "invariants" exact, c'est-à-dire que la suite exacte de G-homomorphismes :

$$(5) \qquad 0 \longrightarrow \mathfrak{M}_S T \longrightarrow T \xrightarrow{u} T' \longrightarrow 0$$

donne naissance à la suite exacte :

$$(6) \qquad 0 \longrightarrow (\mathfrak{M}_S T)^G \longrightarrow T^G \xrightarrow{u} (T')^G \longrightarrow 0 \ .$$

(En effet, le seul point à montrer est la surjectivité de u . Donc, soit $y \in (T')^G$. Puisque $y \in T'$, il existe $x \in T$ tel que $u(x) = y$ (suite exacte (5)). Si l'on considère alors

$$x_1 = \frac{1}{\text{card } G} \sum_{s \in G} s(x) \quad ,$$

$x_1 \in T^G$ et $u(x_1) = y$, car $s(y) = y$, $\forall\, s \in G$.)

C. Q. F. D.

D'où

$$T^G = (\mathrm{Tor}_1^R(S\ ,\ k))^G = \mathrm{Tor}_1^R(S^G\ ,\ k) = \mathrm{Tor}_1^R(R\ ,\ k) = 0$$

(car R est libre sur lui-même). Par suite, $T^G = 0$, et grâce à la suite exacte (6), $(T')^G = 0$.

(b) On peut <u>se ramener au cas où</u> R <u>et</u> S <u>sont complets</u>. (En effet, pour un anneau local noethérien S , on a l'équivalence : S noethérien $\Longleftrightarrow$ $\hat{S}$ noethérien .

Alors, si un élément g de G est une pseudo-réflexion, $\exists\ \xi_1^1 , \dots , \xi_n^1$ éléments de $\mathfrak{M}_S/\mathfrak{M}_S^2$ tels que

$$\begin{aligned} g(\xi_1^1) &= \xi_1^1 \\ &\vdots \\ g(\xi_{n-1}^1) &= \xi_{n-1}^1 \\ g(\xi_n^1) &= w\xi_n^1 \qquad , \end{aligned}$$

où w est une racine de l'unité de k . Et ces n éléments forment une base du k-espace vectoriel $\mathfrak{M}_S/\mathfrak{M}_S^2$ (voir la définition d'une pseudo-réflexion).

On peut relever les (ξ_i^1) en des éléments (ξ_i^2) de $\mathfrak{M}_S/\mathfrak{M}_S^3$, puis de proche en proche, en des éléments $(\xi_i^{\ell-1})$ de $\mathfrak{M}_S/\mathfrak{M}_S^{\ell}$ vérifiant :

$$g(\xi_i^{\ell-1}) = \xi_i^{\ell-1} \ , \qquad \forall\ 1 \leqslant i \leqslant n-1 \quad ,$$

$$g(\xi_n^{\ell-1}) = w(\xi_n^{\ell-1}) \quad ,$$

et ceci, quel que soit ℓ entier positif $\geqslant 3$.

En effet, par exemple, montrons comment s'effectue le relèvement de $\mathfrak{M}_S/\mathfrak{M}_S^2$ à $\mathfrak{M}_S/\mathfrak{M}_S^3$.

Considérons le diagramme suivant où N est le noyau de l'application $g - 1$ suivante :

$$\mathfrak{M}_S/\mathfrak{M}_S^3 \xrightarrow{g-1} \mathrm{Im}(\mathfrak{M}_S/\mathfrak{M}_S^3) \longrightarrow 0 \quad .$$

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & N' = (\mathfrak{M}_S^2/\mathfrak{M}_S^3) \cap N \arrow[r] \arrow[d] & \mathfrak{M}_S^2/\mathfrak{M}_S^3 \arrow[r, "g-1"] \arrow[d] & \mathrm{Im}(\mathfrak{M}_S^2/\mathfrak{M}_S^3) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & N \arrow[r] \arrow[d] & \mathfrak{M}_S/\mathfrak{M}_S^3 \arrow[r, "g-1"] \arrow[d] & \mathrm{Im}(\mathfrak{M}_S/\mathfrak{M}_S^3) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & N'' = N/((\mathfrak{M}_S^2/\mathfrak{M}_S^3) \cap N) \arrow[r] \arrow[d] & \mathfrak{M}_S/\mathfrak{M}_S^2 \arrow[r, "g-1"] \arrow[d] & \mathrm{Im}(\mathfrak{M}_S/\mathfrak{M}_S^2) \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Ce diagramme est formé de lignes et de colonnes exactes, car

$$(g - 1)(\mathfrak{M}_S/\mathfrak{M}_S^2) \simeq (\mathfrak{M}_S/\mathfrak{M}_S^3)/[N + (\mathfrak{M}_S^2/\mathfrak{M}_S^3)] \quad ,$$

et c'est ainsi le même diagramme que dans Cartan-Eilenberg ([3], exercice 1, chap. I), où $A = \mathfrak{M}_S/\mathfrak{M}_S^3$, $A_1 = \mathfrak{M}_S^2/\mathfrak{M}_S^3$, et $A_2 = N$.

Par suite, les éléments (ξ_j^1) , $1 \leqslant j \leqslant n - 1$, qui appartiennent en fait à N", peuvent se relever en des éléments (ξ_j^2) $(1 \leqslant j \leqslant n - 1)$ de N , donc de $\mathfrak{M}_S/\mathfrak{M}_S^3$, vérifiant

$$g(\xi_j^2) = \xi_j^2 \quad .$$

On peut effectuer la même opération pour l'élément ξ_n^1 , en remplaçant $g - 1$ par l'application $g - w.\mathrm{Id}$, et en écrivant un diagramme analogue.

Finalement, comme S est complet, ceci nous prouve qu'il existe des éléments $x_1 , \ldots , x_{n-1} \in \mathfrak{M}_S$ tels que

$$\begin{gathered} g(x_1) = x_1 \\ \vdots \\ g(x_{n-1}) = x_{n-1} \quad . \end{gathered}$$

Comme, de plus, $S/\mathfrak{M}_S = R/\mathfrak{m}_R = k$, on peut relever w , racine de l'unité de k , en un élément ω de R . Il existe donc $x_n \in \mathfrak{M}_S$ et $\omega \in R$ tels que

$$g(x_n) = \omega x_n \quad .$$

On voit alors que $S = R[x_1 , \dots , x_n]$. En effet, soit $x \in S$. Si $x \notin \mathfrak{m}_S$, soit $\bar{x}$ sa classe dans $S/\mathfrak{m}_S = k = R/(\mathfrak{m}_S \cap R)$. $\bar{x} \neq 0$, donc il existe $y \in R \subset$ tel que $\bar{y} = \bar{x}$. Par suite $x - y \in \mathfrak{m}_S$, et $x = y + z$ où $z \in \mathfrak{m}_S$. On est donc amené à étudier le cas où $x \in \mathfrak{m}_S$.

Le cas $x \in \mathfrak{m}_S$, $x \notin \mathfrak{m}_S^2$, peut se traiter ainsi : Comme S est complet : $x = (\overline{x_1} , \overline{\xi_2} , \dots , \overline{\xi_n} , \dots)$, où $\overline{\xi_n} = \mathrm{cl}\ x \pmod{\mathfrak{m}_S^{n+1}}$. Posons

$$y = (\overline{x_1} , \bar{x}_2 , \dots) \quad ,$$

où $\overline{x_1}$ est la classe de x dans $\mathfrak{m}_S/\mathfrak{m}_S^2$ (par suite $\overline{x_1} = \sum_{j=1}^{n} \xi_j^1 \alpha_j$, où $\alpha_j \in k$ et $\overline{x_2}$ le relèvement de $\overline{x_1}$, obtenu en relevant les (ξ_j^1) , etc.

Ceci nous montre, d'après la complétion de S et le fait que S et R ont mêm corps résiduel, que

$$y = \sum_{j=1}^{n} r_j x_j \ , \qquad \text{où } r_j \in R \quad .$$

Or $y - x \in \mathfrak{m}_S^2$; ceci nous amène donc à étudier le cas $x \in \mathfrak{m}_S^2$. Or, de toutes façons, si $x \in \mathfrak{m}_S$, on a

$$x = \sum_{\text{fini}} y_1^j \dots y_{q(j)}^j \ , \qquad \text{où les } y_{q(j)}^j \begin{cases} \in \mathfrak{m}_S \ , \\ \notin \mathfrak{m}_S^2 \ . \end{cases}$$

Par suite, pour tout j , x se met sous la forme

$$x = y_j + t_j \ , \qquad \text{où } y_j \in R[x_1 , \dots , x_n] \quad \text{et} \quad t_j \in \mathfrak{m}_S^{j+1} \quad .$$

En passant à la limite, comme S est complet, on voit donc que x s'exprime comm une série formelle en $x_1 , \dots , x_n$ à coefficients dans R . Mais R étant complet et les x_i entiers sur R , x appartient donc en fait à $R[x_1 , \dots , x_n]$ Par suite, on a bien $S = R[x_1 , \dots , x_n]$.

Considérons maintenant $S' = S/(x_n S)$. g opère trivialement sur S' (d'après la construction des x_i). Autrement dit : $\mathrm{Im}(g - 1) \subset x_n S$, et l'application $g - 1 : S \to S$ se factorise :

$$\begin{tikzcd} S \arrow[rr, "g-1"] \arrow[dr, "\varphi"'] & & S \\ & S \arrow[ur, "(x_n)"'] & \end{tikzcd} ,$$

où (x_n) désigne la multiplication par x_n dans S . Or ces applications, $g - 1$ φ , (x_n) sont des applications R-linéaires qui opèrent sur $T = \mathrm{Tor}_1^R(S , k)$, et l'on a également le diagramme suivant :

$$\begin{tikzcd}
T \arrow[rr, "g-1"] \arrow[dr, "\varphi"'] & & T \\
& T \arrow[ur, "(x_n)"'] &
\end{tikzcd}.$$

D'où les inclusicns $(g - 1)(T) \subset x_n T \subset \mathfrak{m}_S T$. Comme $T' = T/(\mathfrak{m}_S T)$, l'image de $g - 1$ opérant sur T' est nulle, c'est-à-dire, g opère trivialement sur T' . (b) est ainsi prouvé, ce qui permet de conclure à la nullité de T' , puis de T , et achève la démonstration.

BIBLIOGRAPHIE

[1] AUSLANDER (Maurice). - On the purity of the branch locus, Amer. J. of Math., t. 84, 1962, p. 116-125.

[2] BOURBAKI (Nicolas). - Algèbre commutative. Chapitre 2 : Localisation. - Paris, Hermann, 1961 (Act. scient. et ind., 1290 ; Bourbaki, 27).

[3] CARTAN (Henri) and EILENBERG (Samuel). - Homological algebra. - Princeton, Princeton University Press, 1956 (Princeton mathematical Series, 19).

[4] GROTHENDIECK (Alexander) et DIEUDONNÉ (Jean). - Eléments de géométrie algébrique. Chapitre 4 : Etude locale des schémas et des morphismes de schémas. - Paris, Presses Universitaires de France, 1964 (Institut des hautes Etudes scientifiques, Publications mathématiques, 20).

[5] JACOBSON (Nathan). - Lie algebras. - New York, Interscience Publishers, 1962 (Interscience Tracts in pure and applied Mathematics, 10).

[6] SHEPHARD (G. C.) and TODD (J. A.). - Finite unitary reflection groups, Canad. J. of Math., t. 6, 1954, p. 274-304.

INVARIANTS OF FINITE GROUPS GENERATED BY REFLECTIONS.*

By Claude Chevalley.

1. An invertible linear transformation of a finite dimensional vector space V over a field K will be called a *reflection* if it is of order two and leaves a hyperplane pointwise fixed. A group G of linear transformations of V is a *finite reflection group* if it is a finite group generated by reflections. The operations of G extend to automorphisms of the symmetric algebra S of V by the rule $g(P)(x) = P(g^{-1}(x))$, $(P \in S, x \in V)$, and an element $P \in S$ such that $g(P) = P$ for all $g \in G$ is said to be *an invariant of* G. Our main purpose in this note is to prove the theorem:

(A) *Let G be a finite reflection group in a n-dimensional vector-space V over a field K of characteristic zero. Then the K-algebra J of invariants of G is generated by n algebraically independent homogeneous elements (and the unit).*

A vector space A is *graded* by subspaces A^i, (i positive integer), if it is the direct sum of the A^i. The degree d^0P of $P \in A$ is the smallest integer j such that $P \in \sum_{i \leqq j} A^i$; the elements of A^i are the homogeneous elements of degree i. When the A^i are finite dimensional, the Poincaré series of A in the indeterminate t is defined as

$$P_t(A) = \sum_{i \geqq 0} \dim. A^i \cdot t^i.$$

In particular S is graded in the obvious way and $P_t(S) = (1-t)^{-n}$. Let F be the ideal generated by the homogeneous elements of strictly positive degrees in J. Then the grading of S induces a grading of the quotient space S/F. Since F is invariant under G, the operations of G in S induce automorphisms of S/F. We shall also prove:

(B) *Let $I_1, \cdots, I_n$ be a minimal system of homogeneous generators of J and let m_i be the degree of I_i, $(1 \leqq i \leqq n)$. Then*

$$P_t(S/F) = (1-t)^{-n} \cdot \prod_{i=1}^{i=n} (1-t^{m_i}).$$

* Received June 9, 1955.

The product of the m_i is equal to the order of G and to the dimension of S/F. The natural representation of G in S/F is equivalent to the regular representation.

2. Two lemmas. In this paragraph, the characteristic p of the infinite groundfield K is allowed to be $\neq 0$ and G denotes a finite reflection group in V whose order N is prime to p.[1] To any element $P \varepsilon S$ we can then associate its average over G:

$$M(P) = 1/N \sum_{g \varepsilon G} g(P).$$

LEMMA 1. *Let $U_1, \cdots, U_m$ be invariants of G such that U_1 does not belong to the ideal generated in J by $U_2, \cdots, U_m$. Let P_i, $(1 \leqq i \leqq m)$, be homogeneous elements of S satisfying a relation $\sum_1^m P_i \cdot U_i = 0$. Then $P_1 \varepsilon F$.*

If $d^0 P_1 = 0$, then it follows from the assumption and from the relation

$$M(P_1) \cdot U_1 + \cdots + M(P_m) \cdot U_m = 0$$

that $P_1 = M(P_1) = 0$. Assume now $d^0 P_1 > 0$ and the lemma to be true for all relations $\sum_1^m Q_i \cdot U_i = 0$ with homogeneous Q_i and $d^0 Q_1 < d^0 P_1$. Let s be a reflection of G leaving pointwise fixed a hyperplane with equation $L = 0$. Then $s(P_i) - P_i = L \cdot Q_i$, $(Q_i \varepsilon S,\ i = 1, \cdots, m)$, and

$$Q_1 \cdot U_1 + \cdots + Q_m \cdot U_m = 0$$

whence, by induction, $Q_1 \varepsilon F$ or, otherwise said, $s(P_1) \equiv P_1 \operatorname{mod.} F$; the group G being generated by reflections, we have then $g(P_1) \equiv P_1 \operatorname{mod.} F$ for any $g \varepsilon G$, whence $P_1 \equiv M(P_1) \operatorname{mod.} F$; since P_1 is homogeneous of strictly positive degree, the same is true for $M(P_1)$; therefore $M(P_1) \varepsilon F$ and $P_1 \varepsilon F$.

LEMMA 2. *Assume K to be a perfect field. Let I_i, $(1 \leqq i \leqq m)$, be homogeneous invariants which form an ideal basis of F,[2] with $m_i = d^0 I_i$ prime to p for $i \leqq r$. Then $I_1, \cdots, I_r$ are algebraically independent.*

Let us suppose the lemma to be false and let $H(I_1, \cdots, I_r) = 0$ be a non trivial relation of minimal degree between $I_1, \cdots, I_r$ where $H(y_1, \cdots, y_r)$

[1] In this paper, we are primarily interested in the case $p = 0$, but Lemma 2 will be used in a forthcoming paper of A. Borel, to appear in Jour. Math. Pur. Appl.

[2] This always exists since by the classical theorem for invariants of a finite group, J is a finitely generated K-algebra.

is a polynomial in r letters y_i. We may assume that there exists an integer h such that for any monomial $y_1^{k_1} \cdot \cdots \cdot y_r^{k_r}$ of H we have

$$k_1 \cdot m_1 + \cdots + k_r \cdot m_r = h.$$

The partial derivatives $\partial H/\partial y_i$ are not all zero, because otherwise (for $p \neq 0$, the only case for which it is not obvious), K being perfect, H would be the p-th power of a polynomial H^*, and $H^*(I_1, \cdots, I_r) = 0$ would be a non trivial relation of strictly smaller degree. Set

$$H_i = \partial H/\partial y_i \, (I_1, \cdots, I_r), \qquad (1 \leqq i \leqq r);$$

then $H_1, \cdots, H_r$ are in J and not all zero; after a possible permutation of indices, we may assume that they belong to the ideal generated in J by the first s of them, but that none of $H_1, \cdots, H_s$ belongs to the ideal generated by the other ones in J. Set

$$H_{s+j} = \sum_{j=1}^{i=s} V_{j,i} H_i.$$

Let x_k, $(1 \leqq k \leqq n)$, be coordinates in V. Since

$$\sum_{i=1}^{i=r} H_i \cdot (\partial I_i/\partial x_k) = 0, \qquad (1 \leqq k \leqq n),$$

we have by Lemma 1

$$\partial I_i/\partial x_k + \sum_{j=1}^{j=r-s} V_{j,i}(\partial I_{s+j}/\partial x_k) \, \varepsilon \, F, \qquad (1 \leqq i \leqq s; 1 \leqq k \leqq n)$$

(the left hand sides are homogeneous in the x_k by the above remark on the monomials of H). Multiplying this relation by x_k and adding the relations thus obtained, we get

$$m_i I_i + \sum_{j=1}^{j=r-s} V_{j,i} m_{s+j} I_{s+j} = \sum_{l=1}^{l=m} A_{i,l} I_l, \qquad (1 \leqq i \leqq s).$$

where the $A_{i,l}$ are forms belonging to the ideal generated by $x_1, \cdots, x_n$. For reasons of homogeneity, we have $A_{i,l} = 0$ if I_l is not of strictly lower degree than I_i; m_i being prime to p for $i \leqq r$, we see that I_i belongs to the ideal generated by the other I_j, which is a contradiction. Thus $I_1, \cdots, I_r$ are algebraically independent.

3. Proofs of Theorems (A) and (B). We assume again the groundfield to be of characteristic zero and denote as in Lemma 2 by $I_1, \cdots, I_m$ homogeneous invariants of G forming an ideal basis of F. By Lemma 2 they are algebraically independent, whence also $m \leqq n$. Using averages over G, it is readily seen by induction on the degree that the unit and the I_i generate J and thus, to finish the proof of (A), there remains to show that $m \geqq n$.

Let $x_1, \cdots, x_n$ be coordinates in V and let $K(x)$ be the field of rational functions in the x_i. It is acted upon in a natural way by G and we denote by L the subfield of elements invariant under G. Then $K(x)$ is a Galois extension of L, with Galois group G and L has also transcendence degree n over K. On the other hand, G being *finite*, every invariant in $K(x)$ is classically the quotient of two invariant polynomials; thus $L = K(J)$ is generated by the I_i, and $m \geqq n$.

LEMMA 3. *Let $P_1, \cdots, P_s$ be homogeneous elements of S whose residue classes* mod F *are linearly independent over K in S/F. Then $P_1, \cdots, P_s$ are linearly independent over $K(J)$.*

Let $V_1 \cdot P_1 + \cdots + V_s \cdot P_s = 0$ be a relation with $V_i \varepsilon K(J)$, $(1 \leqq i \leqq s)$. We have to prove that $V_i = 0$ for all i and it is enough to consider the case where the V_i are homogeneous elements of J such that $d^0V_i + d^0P_i$ is equal to a constant h independent of i.

By the degree of the monomial $I_1^{k_1} \cdot \cdots \cdot I_n^{k_n}$ we mean its degree as element of S, i.e. $k_1m_1 + \cdots + k_nm_n$. Let S_j, $(j = 1, 2, \cdots)$, be the different monomials in the I_i arranged by increasing degrees, with $S_1 = 1$. We have

$$V_i = \sum_{j \geqq 0} k_{ij} S_j, \qquad (k_{ij} \varepsilon K, k_{ij} = 0 \text{ for } d^0V_i \neq d^0S_j,\ (1 \leqq i \leqq n)),$$

and our relation may be written

$$\sum_{j \geqq 0} W_j \cdot S_j = 0, \qquad (W_j = \sum_{i=1}^{i=s} k_{ij} P_i),$$

where W_j is homogeneous, of degree equal to $h - d^0S_j$. Assume that $k_{ij} = 0$ for $1 \leqq i \leqq s$ and $j < t$. Since by Theorem A the monomial S_t does not belong to the ideal generated in J by the S_j with $j > t$, we have by Lemma 1 $W_t \varepsilon F$ and the hypothesis gives then $k_{it} = 0$ for $i = 1, \cdots, s$. This proves by induction on j that $k_{ij} = 0$ for all i, j, and the lemma.

We now come to the proof of (B). The field $K(x)$ being a normal extension of $K(J)$ with Galois group G, has degree N over $K(J)$, hence the dimension of S/F over K is finite. Let $A_1, \cdots, A_q$ be homogeneous polynomials whose residue classes mod F form a basis of S/F. By induction on the degree we see that every $P \varepsilon S$ may be expressed as linear combination of the A_i with coefficients in J, and this expression is unique in view of Lemma 3. Hence

$$P_t(S) = P_t(S/F) \cdot P_t(J);$$

but $P_t(S) = (1 - t)^{-n}$ and Theorem A gives $P_t(J) = \prod_1^n (1 - t^{m_i})^{-1}$, whence the first assertion of (B). We may also write

$$P_t(S/F) = \prod_{i=1}^{i=n} (1 + t + t^2 + \cdots + t^{m_i-1})$$

and, setting $t = 1$, we get $\dim. S/F = m_1 \cdot \cdots \cdot m_n$. Since every element of $K(x)$ may be written as the quotient of a polynomial by an invariant polynomial, it also follows from the above and Lemma 3 that the A_i form a basis of $K(x)$ over $K(J)$, whence $N = \dim. S/F$.

We have for $g \varepsilon G$

$$g(A_i) = \sum_{j=1}^{j=N} a_{ij}(g) A_j, \qquad (i = 1, \cdots, N),$$

where the $a_{ij}(g)$ are homogeneous elements of J and where $a_{ii}(g) \varepsilon K$ by homogeneity. The matrices $(a_{ij}(g))$ describe the natural representation of G in $K(x)$, considered as vector space over $K(J)$. If we reduce the coefficients mod F we get the natural representation of G in S/F, considered as vector space over K; this reduction does not affect the diagonal coefficients, hence both representations have the same character and are equivalent. But G is the Galois group of the normal extension $K(x)$ of $K(J)$, so that the former representation is equivalent to the regular representation, which proves the last statement of (B).

COLUMBIA UNIVERSITY.

Theorem [Bou, Lie, Ch. V §5 no. 2 Theorem 1] Let

$\mathfrak{h}_{\mathbb{C}}^*$ be a finite dimensional $\mathbb{C}$-vector space

W_0 a finite subgroup of $GL(\mathfrak{h}_{\mathbb{C}}^*)$.

Let $\varepsilon : S(\mathfrak{h}_{\mathbb{C}}^*) \to \mathbb{C}$ be the $\mathbb{C}$-algebra homomorphism given by

$$\varepsilon(x) = 0, \quad \text{for } x \in \mathfrak{h}_{\mathbb{C}}^*.$$

Let

$J = \langle f - \varepsilon(f) \mid f \in S(\mathfrak{h}_{\mathbb{C}}^*)^{W_0} \rangle$ an ideal of $S(\mathfrak{h}_{\mathbb{C}}^*)^{W_0}$,

$\gamma_1, \ldots, \gamma_d$, a $\mathbb{C}$-basis of $S(\mathfrak{h}_{\mathbb{C}}^*)/J$, and

$h_1, \ldots, h_d \in S(\mathfrak{h}_{\mathbb{C}}^*)$ such that $\gamma_j = h_j + J$.

If W_0 is generated by reflections then

$h_1, \ldots, h_d$ is an $S(\mathfrak{h}_{\mathbb{C}}^*)^{W_0}$-basis of $S(\mathfrak{h}_{\mathbb{C}}^*)$.

Proof

To show: (a) $h_1, \ldots, h_d$ are $S(\mathfrak{h}_{\mathbb{C}}^*)^{W_0}$-linearly independent,

(b) The $S(\mathfrak{h}_{\mathbb{C}}^*)^{W_0}$-span of $h_1, \ldots, h_d$ is $S(\mathfrak{h}_{\mathbb{C}}^*)$.

(a) For each reflection s_β in W_0 define

$$\partial_\beta : S(\mathfrak{h}_{\mathbb{C}}^*) \to S(\mathfrak{h}_{\mathbb{C}}^*) \quad \text{by} \quad \partial_\beta f = \frac{1}{\beta}(s_\beta - 1) f$$

where $\beta \in \mathfrak{h}_{\mathbb{C}}^*$ is such that $\mathfrak{h}_{\mathbb{C}}^* = (\mathfrak{h}_{\mathbb{C}}^*)^{s_\beta} \oplus \mathbb{C}\beta$.

Assume that $g_1, \dots, g_d \in S(\mathfrak{h}^*_{\mathbb{C}})^{W_0}$ and

$$g_1h_1 + \cdots + g_dh_d = 0.$$

To show: $g_1 = g_2 = \cdots = g_d = 0$.

Assume $\deg(h_1) \geq \deg(h_j)$ and let $r = \deg(h_1)$.

Find $\beta_1, \dots, \beta_r$ so that ~~$\partial_{\beta_1, \dots,} \partial_{\beta_r}$~~ $\partial_{\beta_1} \cdots \partial_{\beta_r} h_1 \neq 0$.

Then

$$\begin{aligned} 0 &= \partial_{\beta_1} \cdots \partial_{\beta_r}(g_1h_1 + \cdots + g_dh_d) \\ &= g_1 \partial_{\beta_1} \cdots \partial_{\beta_r}(h_1) + \cdots + g_d \partial_{\beta_1} \cdots \partial_{\beta_r}(h_d) \\ &= g_1\lambda_1 + \cdots + g_d\lambda_d, \end{aligned}$$

with $\lambda_1, \dots, \lambda_d \in \mathbb{C}$ and $\lambda_j = 0$ if $\deg(h_1) > \deg(h_j)$

and $\lambda_1 \neq 0$.

So, letting $\mu_j = -\lambda_1^{-1}\lambda_j$,

$$g_1 - \mu_2 g_2 - \cdots - \mu_d g_d = 0$$

and

$$g_1 = \mu_2 g_2 + \cdots + \mu_d g_d.$$

So

$$\begin{aligned} 0 &= g_1h_1 + \cdots + g_dh_d \\ &= (\mu_2g_2 + \cdots + \mu_dg_d)h_1 + g_2h_2 + \cdots + g_dh_d \\ &= g_2(h_2 + \mu_2h_1) + g_3(h_3 + \mu_3h_1) + \cdots + g_d(h_d + \mu_dh_1). \end{aligned}$$

Note that

$$h_j + \mu_jh_1 = \begin{cases} h_j, & \text{if } \deg(h_1) > \deg(h_j), \\ h_j + \mu_jh_1, & \text{if } \deg(h_j) = \deg(h_j), \end{cases}$$

so that ~~deg~~ $h_j + \mu_jh_1$ is homogeneous.

Iterate this process to get

$$0 = g_K \Big(\sum_j v_j \cdot h_j \Big),$$

where the sum is over j such that $\deg(h_j) = \deg(h_1)$.

Since $\deg\big(\sum_j h_j\big) = r$, it follows that $g_K = 0$.

(b) To show: The $S(\mathfrak{h}_{\mathbb{C}}^*)^{W_0}$-span of $h_1, \dots, h_d$ is $S(\mathfrak{h}_{\mathbb{C}}^*)$.

Lemma 1 [Bou, Ch V §5 No. 3 Lemma 1]

Let $S = \mathbb{C}[x_1, \dots, x_r]$ with $\deg(x_i) = m_i$,

S^{W_0} a $\mathbb{Z}_{\geq 0}$ graded subalgebra of S.

C1) Let $e_1, \dots, e_s \in S^{W_0}$ be a minimal generating set of

$$J = \langle f \mid f \in S^{W_0}_{>0} \rangle \text{ as an ideal of } S.$$

Let

$$\varphi : \mathbb{C}[z_1, \dots, z_s] \longrightarrow S^{W_0}$$
$$z_j \longmapsto e_j, \quad \text{and}$$

C2) let $H(z_1, \dots, z_s) \in \ker\varphi$ of minimal degree.

Let

$$p_i = \deg(e_i) \frac{\partial H}{\partial z_i}(e_1, \dots, e_s), \quad \text{and} \quad d_{ik} = \frac{1}{\deg(e_i)} \frac{\partial e_i}{\partial x_k},$$

for $i = 1, 2, \dots, s$ and $k = 1, 2, \dots, r$. Let

$$\mathfrak{b} = \langle p_1, \dots, \beta_s \rangle \text{ as an ideal in } S^{W_0}.$$

C3) Let $J \subseteq \{1, 2, \dots, s\}$ be minimal such that

$$\langle p_j \mid j \in J \rangle = \mathfrak{b}.$$

Let $h_1, \dots, h_d \in S$ be an S^{W_0}-spanning set of S.

If $H(z_1, \dots, z_s) \neq 0$ then $h_1, \dots, h_d$ are not S^{W_0} linearly independent.

Proof Since $H(e_1,\dots,e_s)=0$,

$$0=\frac{\partial H}{\partial x_i}=\sum_{i=1}^{s}\deg(e_i)\frac{\partial H}{\partial z_i}\frac{1}{\deg(e_i)}\frac{\partial e_i}{\partial x_k}=\sum_{i=1}^{s}p_i d_{ik}.$$

By C3 there exist homogeneous $\gamma_{ji}\in S^{W_0}$ such that $p_j=\sum_{i\in J}\gamma_{ji}p_i$, for $j\in I-J$.

where $I=\{1,2,\dots,s\}$. Let

$$u_{ik}=d_{ik}+\sum_{j\in I-J}\gamma_{ji}d_{jk}=\sum_{\ell=1}^{d}c_{ik\ell}h_\ell,\ \text{for } i\in J,\ k=1,2,\dots,r$$

with $c_{ik\ell}\in S^{W_0}$. Then

$$0=\sum_{i=1}^{s}p_i d_{ik}=\sum_{i\in J}p_i\Big(d_{ik}+\sum_{j\in I-J}\gamma_{ji}d_{jk}\Big)$$

$$=\sum_{i\in J}p_i u_{ik}=\sum_{i\in J}p_i\sum_{\ell=1}^{d}c_{ik\ell}h_\ell$$

$$=\sum_{\ell=1}^{d}h_\ell\Big(\sum_{i\in J}p_i c_{ik\ell}\Big),\ \text{for } k=1,2,\dots,r.$$

If $\deg(c_{ik\ell})=0$, then $c_{ik\ell}$ is a constant and the equation $\sum_{i\in J}p_i\sum_{\ell=1}^{d}c_{ik\ell}h_\ell$ violates (C3).

So $\deg(c_{ik\ell})>0$ and so $c_{ik\ell}\in S^{W_0}_{>0}$ and $u_{ik}\in S^{W_0}_{>0}S=\mathcal{J}$, for $i=1,2,\dots,s$ and $k=1,2,\dots,r$.

So

$$u_{ik} = \sum_{h=1}^{s} u_{ikh} e_h, \text{ with } u_{ikh} \in S.$$

So

$$\sum_{h=1}^{s} \sum_{k=1}^{r} u_{ikh} y_k e_h = \sum_{k=1}^{r} u_{ik} y_k$$

$$= \sum_{k=1}^{r} y_k \Big(d_{ik} + \sum_{j \in I-J} \gamma_{ji} d_{jk} \Big) = e_i + \sum_{j \in I-J} \gamma_{ji} e_j .$$

where the last equality follows from Euler's formula

$$\sum_{k=1}^{r} d_{ik} y_k = \sum_{k=1}^{r} \frac{1}{\deg(e_i)} \frac{\partial e_i}{\partial x_k} \deg(x_k) x_k = e_i .$$

Since $\deg(y_k) > 0$, comparing these two sides in degree $\deg(e_i)$ gives

e_i is an S-linear combination of $\{e_j \mid j \neq i\}$.

Since S is a free S^{W_0}-module and $e_1, \dots, e_s \in S^{W_0}$ it follows (Alg. Comm. Chap I §3, no 5, prop 9d)

e_i is an S^{W_0}-linear combination of $\{e_j \mid j \neq i\}$.

This contradicts (C1). //.

Elliptic Functions sn, cn, dn, as Trigonometry

W. Schwalm, Physics, Univ. N. Dakota

Background: Jacobi discovered that rather than studying elliptic integrals themselves, it is simpler to think of them as inverses for some functions like trig functions. For instance, recall that

$$\sin^{-1}(x) = \int_0^x \frac{dx}{\sqrt{1-x^2}},$$

but that it is easier to study $\sin(x)$ than the inverse sine. The resulting elliptic functions satisfy non-linear DEs that arise in many applications.

Here we develop the Jacobi elliptic functions as a form of trigonometric functions, but using an ellipse rather than a circle. These notes evolved from a lecture by William M. Kinnersley, circa 1975. The approach ought to be in some classic text, but I have not found it.

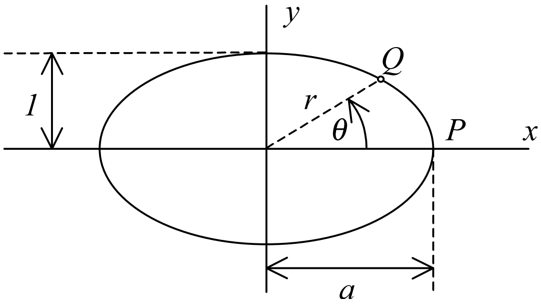

Figure 1: ellipse featured in construction.

Trigonometry of the ellipse: The ellipse equation is

$$\left(\frac{x}{a}\right)^2 + \left(\frac{y}{b}\right)^2 = 1,$$

but we normalize the ellipse by choosing $b = 1$ so that,

$$\left(\frac{x}{a}\right)^2 + y^2 = 1. \tag{1}$$

Also of course,

$$x^2 + y^2 \; = \; r^2. \tag{2}$$

The eccentricity of an ellipse with general a, b is

$$\frac{b^2}{a^2} \; = \; 1 \; - \; \epsilon^2, \qquad \text{or} \qquad \epsilon \; = \; \sqrt{1 - \frac{b^2}{a^2}},$$

so that $\epsilon = 0$ for a circle, $\epsilon = 1$ for a parabola. Since $b = 1$, the eccentricity is

$$\epsilon \; \equiv \; k \; = \; \sqrt{1 - \frac{1}{a^2}},$$

which is the *modulus* of the corresponding elliptic functions. Thus $0 \leq k \leq 1$, and $k = 1$ should give ordinary trigonometry.

The next and very important thing to define is the *argument* u of the elliptic functions. The u is the thing the elliptic functions are functions of. In the case of trig functions, the argument would be the angle θ, but here u is a bit more complicated.

$$u \; \equiv \; \int_P^Q \; r \, d\theta, \tag{3}$$

where P and Q are as shown in Fig. 1. Notice that u is not an angle. It is not arc length and it is not area either. However, u becomes the angle θ or arc length in the limit $a \to 1$, or $k \to 0$ when the ellipse becomes a circle.

With the argument and modulus of the elliptic functions defined, the functions themselves are just ratios, just as in the case of trigonometry.

$$\begin{aligned} \operatorname{sn}(u, k) \; &= \; y, && (4) \\ \operatorname{cn}(u, k) \; &= \; x/a, && (5) \\ \operatorname{dn}(u, k) \; &= \; r/a. && (6) \end{aligned}$$

The first two generalize the sine and cosine, and the third comes about because the radius is not constant on an ellipse. When $k \to 0$, so that $a = 1$, these become just y, x, and $+1$, since $r \to 1$ also. This connects the elliptic functions to $\sin\theta$, $\cos\theta$ and $+1$.

There are several notational points to mention here. First, one often omits the modulus k in writing the elliptic functions and just writes

$$\operatorname{sn} u \; = \; \operatorname{sn}(u, k), \qquad \text{and so on.}$$

Corresponding to a given modulus k there is a *complementary modulus* k' such that

$$k' = \sqrt{1-k^2}.$$

There are also other notations. For example, a modern invention is to use $m = k^2$ so that fewer square roots appear. Then one defines

$$\mathrm{sn}(u|m) \equiv \mathrm{sn}(u,k), \qquad \text{where } m = k^2.$$

In fact there are twelve Jacobi elliptic functions, defined using a simple convention

$$\begin{array}{lll} \mathrm{ns}\,u = \frac{1}{\mathrm{sn}\,u} & \mathrm{nc}\,u = \frac{1}{\mathrm{cn}\,u} & \mathrm{nd}\,u = \frac{1}{\mathrm{dn}\,u} \\ \mathrm{sc}\,u = \frac{\mathrm{sn}\,u}{\mathrm{cn}\,u} & \mathrm{dc}\,u = \frac{\mathrm{dn}\,u}{\mathrm{cn}\,u} & \mathrm{cs}\,u = \frac{\mathrm{cn}\,u}{\mathrm{sn}\,u} \\ \mathrm{ds}\,u = \frac{\mathrm{dn}\,u}{\mathrm{sn}\,u} & \mathrm{sd}\,u = \frac{\mathrm{sn}\,u}{\mathrm{dn}\,u} & \mathrm{cd}\,u = \frac{\mathrm{cn}\,u}{\mathrm{dn}\,u} \end{array}$$

and these all satisfy certain nonlinear differential equations, as we shall see.

From Eq.(1) we have

$$\mathrm{cn}^2\,u + \mathrm{sn}^2\,u = 1, \tag{7}$$

which generalizes $\cos^2\theta + \sin^2\theta = 1$. An then from Eq.(2),

$$\mathrm{dn}^2\,u + k^2\,\mathrm{sn}^2\,u = 1. \tag{8}$$

The differential relations now follow essentially from Eqs(1) and (2), just as the differentials of the sine and cosine follow from the Pytagorean formula. From

$$\theta = \tan^{-1}\left(\frac{y}{x}\right),$$

one has

$$d\,\theta = \frac{1}{r^2}(x\,dy - y\,dx).$$

But

$$du = r\,d\theta = \frac{1}{r}(x\,dy - y\,dx).$$

Also, from Eq.(1),

$$\frac{x\,dx}{a^2} + y\,dy = 0,$$

so one can replace either

$$dy = -\frac{x}{a^2\,y}\,dx,$$

or

$$dx = -\frac{a^2\,y}{x}\,dy.$$

The corresponding substitutions for du are therefore

$$du = \frac{1}{r}\left(-\frac{x^2}{a^2\,y} - y\right)\,dx,$$

or

$$du = \frac{1}{r}\left(x + \frac{a^2\,y^2}{x}\right)\,dy.$$

With these substitutions we get the following formulas for differentiating elliptic functions (with respect to the argument u, not k),

$$\frac{d}{du}\operatorname{sn} u = \operatorname{cn} u\operatorname{dn} u, \tag{9}$$

$$\frac{d}{du}\operatorname{cn} u = -\operatorname{sn} u\operatorname{dn} u, \tag{10}$$

$$\frac{d}{du}\operatorname{dn} u = -\,k^2\operatorname{sn} u\operatorname{cn} u. \tag{11}$$

Equations (9) and (10) relate in obvious ways to the trigonometric limit, while Eq.(11) is new. It reduces to an identity when $k \to 0$.

The elliptic functions satisfy differential equations that we find by starting with a solution and working backward. Apparently the modulus k should enter the DE as a parameter.

$$\frac{d}{du}\operatorname{sn} u = \operatorname{cn} u\operatorname{dn} u = \sqrt{1-\operatorname{sn}^2 u}\sqrt{1-k^2\operatorname{sn}^2 u},$$

so if $y(u) = \operatorname{sn} u$, then

$$\left(\frac{dy}{du}\right)^2 = (1-y^2)(1-k^2\,y^2). \tag{12}$$

If I solve for $u(y)$,

$$u = c + \int\frac{dy}{\sqrt{1-y^2}\sqrt{1-k^2\,y^2}},$$

which I recognize as an elliptic integral of the first kind, $F(y,k)$. Thus, as I mentioned earlier, the elliptic functions are the inverse functions for the elliptic integrals. On the other hand, If I differentiate Eq.(12) again with respect to u I get

$$y'' + (1+k^2)\,y - 2\,k^2\,y^3 = 0. \tag{13}$$

This relates to a nonlinear duffing-type oscillator. In fact, all twelve of the Jacobi elliptic functions satisfy nonlinear first order DEs like Eq.(12), and also nonlinear second order DEs like Eq.(13). Moreover, you will find that the squares of the elliptic functions satisfy equations of the form

$$(y')^2 + \alpha\,y^2 + \beta\,y^3 = 0,$$

and of the form

$$y'' + \gamma\,y + \delta\,y^2 = 0.$$

One can thus solve all such equations exactly, in closed form, in terms of elliptic functions. Different functions cover different parameter ranges.

Elliptic functions open up a window of solvable nonlinear (polynomial) DEs, all of which relate to physical problems and physical phenomena. I do not know of other types of solutions of this quality for any nonlinear dynamical problems.

Homework: Perform the same construction starting from a hyperbola,

$$\frac{x^2}{a^2} - y^2 = 1$$

rather than from the ellipse in Fig.(1). Thus define the “Jacobi hyperbolic functions,” $\mathrm{sn}(u,k)$, $=\ y$, $\mathrm{ch}(u,k)\ =\ x/a$ and $\mathrm{dh}(u,k)\ =\ r/a$ and derive their properties. You should find that,

$$\mathrm{ch}^2\,u - \mathrm{sh}^2\,u = 1$$

and

$$\frac{d}{du}\,\mathrm{sh}\,u = \mathrm{ch}\,u\,\mathrm{dh}\,u$$

and then compute all the other properties, including the first and second order DEs these functions satisfy. (By the way, these functions are not discussed in the literature, since they are related to elliptic functions with complex arguments, just as hyperbolic sines and cosines relate to sines and cosines of complex argument. Using the DEs, can you show this relationship?)