Astérisque

JEAN DIEUDONNÉ

Schur functions and group representations

Astérisque, tome 87-88 (1981), p. 7-19

<http://www.numdam.org/item?id=AST_1981__87-88__7_0>

SCHUR FUNCTIONS AND GROUP REPRESENTATIONS

by

J.Dieudonné

I have been asked to present a report on the history of the Schur calculus. It would have been nice if I had been able to give a complete bird's eye view of all its facets, stemming from a unified conception from which all its properties could be derived in a natural and logical way. However, extensive reading of the litterature has convinced me that no such presentation exists today ; perhaps after all it is fortunate for the younger generation that such a challenge remains and may lead to new unsuspected viewpoints on algebra and combinatorics.

I have the feeling that we don't understand at all the extraordinary interplay of combinatorics and what I would call "conceptual" mathematics. I think the renewed interest in these problems should be warmly welcomed, but I feel I am far too ignorant to talk at length on the combinatorial aspects, of which so many specialists in this meeting are very well aware. It is therefore the aspects of the Schur calculus in algebra and analysis which I will try to describe in this talk. What I would like to emphasize is the variety of seemingly unrelated contexts in which the Schur calculus comes up, standing so to speak at the confluence of very different types of theories. If we are some day to reach a unified conception, I believe it will be by a study in depth of the relations between these various theories ; to concentrate on a single aspect and deliberately neglect the others is probably a bad policy only likely to lead to dead ends.

1. The classical period (up to 1900) .

One may characterize that period as an era of manipulation of algebraïc formulas, generally without any external motivation, the only exception being the relations with the enumerative problems of the theory of partitions.

Beginning in the first half of the XVIIIth century, several algebraic themes have constantly been interwoven with one another, and still are inextricably bound together : enumerations problems, symmetric functions, determinants and generating series.

The fact that symmetric polynomials in n indeterminates $x_1, x_2, \ldots, x_n$ could be expressed as polynomials in the "elementary" symmetric functions

$$\begin{cases} e_1 = x_1 + x_2 + \ldots + x_n \\ e_2 = \Sigma_{i<j}\ x_i\, x_j \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ e_n = x_1\, x_2 \ldots x_n \end{cases}$$

was known at the end of the XVIIIth century. In modern terms :

A) At the end of the XVIIIth century, one has for the ring

$$(2)\quad \Lambda_n = \underline{Z}[x_1, x_2, \ldots, x_n]^{\underline{S}_n}$$

of polynomial symmetric functions, <u>three bases</u> for Λ_n as a $\underline{Z}$-module :

a) For each sequence λ : $\lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_n \geqslant 0$ of integers, the polynomials m_λ defined as the sum of all monomials in the orbit of the monomial $x_1^{\lambda_1} \ldots x_n^{\lambda_n}$ under the action of $\underline{S}_n$;

b) the polynomials $e_\lambda = e_{\lambda_1}\, e_{\lambda_2} \ldots e_{\lambda_n}$

c) if one writes

$$(3)\quad h_r = \Sigma_{|\lambda|=r}\, m_\lambda$$

the polynomials

$$h_\lambda = h_{\lambda_1}\, h_{\lambda_2} \ldots h_{\lambda_n}$$

B) It is also known in 1800 (the first proof being apparently due to Ruffini) that $e_1, e_2, \ldots, e_n$ are algebraically independent over $\underline{Q}$, and the same is true for $h_1, h_2, \ldots, h_n$.

C) One has generating series

$$E(T) = \Sigma_{r=0}^{\infty} e_r\, T^r = \prod_{i=1}^{n} (1 + x_i\, T)$$

$$H(T) = \Sigma_{r=0}^{\infty} h_r\, T^r = \prod_{i=1}^{n} (1 - x_i\, T)^{-1}$$

for the e_r and h_r ; one has

$$(4)\qquad H(T)\, E(-T) = 1$$

D) The power sums

$$(5)\qquad p_r = x_1^r + x_2^r + \ldots + x_n^r$$

were particularly studied ever since A.Girard at the beginning of the XVIIth century. Newton gave recurrence relations for their computation, and Waring gave an explicit expression of the p_r as functions of the e_j ; both stem from the fact that the generating series

$$P(T) = \Sigma_{r=0}^{\infty} p_r\, T^r$$

is given by

$$(6)\qquad P(-T) = E'(T) / E(T) .$$

E) New formulas appeared with the development of the theory of determinants, mainly due to Cauchy and Jacobi. Cauchy attributed the name of Vandermonde to the determinant

$$\Delta(x) = \det(x_i^{j-1})_{i,j=1,2,..,n} = \prod_{i<j} (x_i - x_j)$$

although Vandermonde apparently never wrote such a determinant. Cauchy also gave the formula expressing the "Cauchy determinant"

$$(7) \qquad \det\left((1-x_i y_j)^{-1}\right)_{i,j=1,2,..,n} = \Delta(x)\,\Delta(y)\,\Pi_{i,j}\,(1-x_i y_j)^{-1}$$

F) It was quite natural to consider generalizations of the Vandermonde determinant in which an arbitrary sequence of distinct integers replaces the sequence δ : $n-1, n-2, \ldots, 0$ of exponents. They were first considered by Jacobi ; up to sign, they may be written

$$(8) \qquad a_{\lambda+\delta} = \det\left(x_i^{\lambda_j+n-j}\right)_{i,j=1,2,..,n}$$

for a descending sequence $\lambda : \lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_n \geqslant 0$

and Jacobi showed that

$$(9) \qquad t_\lambda = a_{\lambda+\delta} \,/\, a_\delta = \Sigma_{w \in S_n}\, \epsilon(w)\, h_{\lambda+\delta-w.\lambda}$$

($\epsilon(w)$ being the signature of the permutation w)

and also

$$(10) \qquad t_\lambda = \det\left(h_{\lambda_i-i+j}\right)_{i,j=1,2,..,n}$$

the so-called Jacobi-Trudi identity. These symmetric functions are those which later will be called Schur functions.

II. Schur's dissertation and semi-simple algebras.

The concept of linear representation of finite groups was created and studied by Frobenius in the years 1896-1900. The problem is to determine for a given finite group G , all group homomorphisms $\rho : G \longrightarrow GL(N,\mathbb{C})$ for arbitrary integers N. Very soon Frobenius realized that this was equivalent to the study of the group algebra $\mathbb{C}[G]$. In present day terminology, a group homomorphism $\rho : G \longrightarrow GL(E)$ extends uniquely to an algebra homomorphism $\mathbb{C}[G] \longrightarrow End(E)$, and therefore defines the vector space E as a left $\mathbb{C}[G]$-module ; the converse being obvious, there is a one-to-one correspondence between left $\mathbb{C}[G]$-modules of finite type and linear representations. A linear representation is called irreducible if the corresponding module is simple, completely reducible if the corresponding module is semi-simple ; two representations are equivalent if the corresponding modules are isomorphic.

Now $\mathbb{C}[G]$ may be identified with the vector space of all functions $f : G \longrightarrow \mathbb{C}$, with the multiplication known as the convolution

$$(11) \qquad (f \star g)(s) = \Sigma_{t \in G}\, f(t)\, g(t^{-1}s) \,/\, Card(G) \ .$$

Its center Z consists of all functions which are constant on each conjugacy class. If h is the number of these classes, there is a basis of Z consisting of h central idempotents $u_1, u_2, \ldots, u_h$, verifying $u_i \star u_j = 0$ if $i \neq j$ and $1 = u_1 + u_2 + \ldots + u_h$. One has then a direct decomposition

(12) $$\mathbb{C}[G] = \oplus_{1 \leqslant j \leqslant h} \underline{a}_j$$

where each $\underline{a}_j = u_j\,\mathbb{C}[G]$ is a minimal two-sided ideal ; as an algebra, $\underline{a}_j$ is isomorphic to a (simple) matrix algebra $M_{n_j}(\mathbb{C})$; one has $\underline{a}_i\,\underline{a}_j = 0$ for $i \neq j$, so that $\mathbb{C}[G]$ is a semi-simple algebra ; $g = \sum_{j=1}^{h} n_j^2$ is the order of G .

Every left $\mathbb{C}[G]$-module is a direct sum of minimal (or simple) ones, each of which is isomorphic to a minimal left ideal of one of the algebras $\underline{a}_j$. Such an ideal is isomorphic to $\mathbb{C}^{n_j}$ on which $\underline{a}_j \cong M_{n_j}(\mathbb{C})$ operates in the natural way, and the other $\underline{a}_i$ annihilate the ideal.

The characters of G are the h central functions

(13) $$s \longrightarrow \chi_j(s) = n_j^{-1}\, u_j(s)$$

on G . If $s \to \underline{M}_j(s)$ is the irreducible representation of G corresponding to a minimal left ideal of $\underline{a}_j$, one has $\chi_j(s) = \mathrm{Tr}(\underline{M}_j(s))$. A linear representation $s \longrightarrow \rho(s)$ is entirely determined, up to equivalence, by the scalar function $s \longrightarrow \mathrm{Tr}(\rho(s))$, which has the form $s \longrightarrow \sum_{j=1}^{h} d_j \chi_j(s)$, with integers $d_j \geqslant 0$; one says that ρ contains d_j times the irreducible representation $s \longrightarrow \underline{M}_j(s)$.

Frobenius paid special attention to relations between linear representations of a finite group G and of a subgroup H . If E is a finitely generated $\mathbb{C}[G]$-module, one may consider it as a $\mathbb{C}[H]$-module by restriction of the scalars ; for the corresponding representation $\rho : G \longrightarrow GL(E)$, this corresponds to the restriction $\rho|H$ of ρ to H , and one writes $\rho|H = \mathrm{Res}_H^G \rho$. Conversely, for any finitely generated left $\mathbb{C}[H]$-module F , one may consider the $\mathbb{C}[G]$-module obtained by extension to $\mathbb{C}[G]$ of the scalars, namely $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} F$ (where $\mathbb{C}[G]$ is considered as a right $\mathbb{C}[H]$-module) ; for the corresponding representation $\sigma : H \to GL(F)$, this module corresponds to what Frobenius calls the induced representation $\mathrm{Ind}_H^G \sigma$ of G . If $\rho : G \longrightarrow GL(E)$ is irreducible, in general $\mathrm{Res}_H^G \rho$ will not be irreducible ; if it contains d times an irreducible representation σ of H , then $\mathrm{Ind}_H^G \sigma$ contains d times the irreducible representation ρ ; this the reciprocity theorem of Frobenius.

Around 1900, Frobenius suggested to his student I.Schur to examine the linear representations of the infinite group $GL(n,\mathbb{C})$. This was the subject of Schur's dissertation of 1901, a landmark in Algebra, second only to Frobenius 's own papers. Schur limits himself to rational representations, i.e. homomorphisms $GL(n) \longrightarrow GL(N)$ of the form $\underline{X} \to \underline{F}(\underline{X})$ where each entry of the matrix $\underline{F}(\underline{X})$ is a rational function of the entries of the matrix $\underline{X}$. Elementary argument show that one can write

$$\underline{F}(\underline{X}) = p(\underline{X})\, q(\underline{X})^{-1}\, \underline{G}(\underline{X}) \quad .$$

Here $X \to p(X)$ and $X \to q(X)$ are homomorphisms $GL(n) \longrightarrow \mathbb{C}^*$ for which $p(\underline{X})$ and $q(\underline{X})$ are polynomials in the entries of $\underline{X}$, and the entries of the matrix $\underline{G}(\underline{X})$ are polynomials in the entries of $\underline{X}$. Another elementary argument proves that,

after a change of bases, one may write

$$\underline{G}(\underline{X}) = \begin{pmatrix} \underline{G}_1(\underline{X}) & 0 & \dots & 0 \\ 0 & \underline{G}_2(\underline{X}) & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \underline{G}_m(\underline{X}) \end{pmatrix}$$

where each representation $\underline{X} \to \underline{G}_j(\underline{X})$ is such that the entries of $\underline{G}_j(\underline{X})$ are all homogeneous polynomials of the same degree in the entries of $\underline{X}$. One is reduced to considering only this type of representation. Here comes Schur's discovery of the commutation theorem. If the entries of $\underline{X} \to \underline{F}(\underline{X})$ are homogeneous polynomials of given degree f in the entries of $\underline{X}$, this theorem establishes a one-to-one relation between these representations and the linear representations of the symmetric group $\underline{S}_f$. Following H.Weyl's presentation of Schur's arguments, one may write $\underline{F}(X) = (F_{hk}(\underline{X}))$, where each $F_{hk}(\underline{X})$ is a homogeneous polynomial of degree f; one may thus write it in a redundant form

$$F_{hk}(\underline{X}) = \Sigma_{\alpha,\beta}\ a_{hk\alpha\beta}\ X_{\alpha\beta} \tag{14}$$

where α and β run independently through the set $\{1,2,..,n\}^f$, and

$$X_{\alpha\beta} = x_{\alpha_1\beta_1}\, x_{\alpha_2\beta_2} \cdots x_{\alpha_f\beta_f} \quad . \tag{15}$$

Of course the coefficients $a_{hk\alpha\beta}$ in (14) are not unique; but the group $\underline{S}_f$ acts on $\{1,2,..,n\}^f$ by permuting the factors, and the expression (14) becomes unique if one imposes on the coefficients the conditions

$$a_{hk,\pi(\alpha),\pi(\beta)} = a_{hk\alpha\beta} \quad \text{for all } \pi \in \underline{S}_f \quad . \tag{16}$$

The matrix $(X_{\alpha\beta})$ of order n^f is the tensor product $\underline{X}^{\otimes f}$. Let A_n^f be the subalgebra of $\mathrm{End}((\underline{C}^n)^{\otimes f})$ generated by the matrices $\underline{X}^{\otimes f}$. Then one may write $\underline{F}(\underline{X}) = \underline{G}(\underline{X}^{\otimes f})$ where, for any matrix $\underline{U} = (u_{\alpha\beta}) \in A_n^f$,

$$\underline{G}(\underline{U}) = (G_{hk}(\underline{U}))_{h,k=1,2,..,N} \tag{17}$$

with

$$G_{hk}(\underline{U}) = \Sigma_{\alpha,\beta}\ a_{hk\alpha\beta}\ u_{\alpha\beta} \tag{18}$$

where the coefficients satisfy (16). It is then easy to see that $\underline{G}$ is an algebra homomorphism of A_n^f into $M_N(\underline{C})$, and finding the representations $\underline{F}$ is thus equivalent to finding the left A_n^f-modules; the algebras A_n^f are thus seen to play the role held by $\underline{C}[G]$ for finite groups. Now $\underline{S}_f$ also acts on $\mathrm{End}((\underline{C}^n)^{\otimes f})$ by permuting the factors; one immediately sees that A_n^f consists of the matrices $\underline{U}$ such that $\pi.\underline{U} = \underline{U}.\pi$ for all $\pi \in \underline{S}_f$. Let B be the image of $\underline{C}[\underline{S}_f]$ in $M_{n^f}(\underline{C}) = \mathrm{End}((\underline{C}^n)^{\otimes f})$ for that action; then A_n^f is the commutant in the simple algebra $M_{n^f}(\underline{C})$ of the subalgebra B.

A theorem proved much later by E.Noether says that in any semi-simple ring R, the commutant of any semi-simple subring B (containing 1) is a semi-simple ring

B' , and that $B'' = B$. In Schur's case, an elementary proof (essentially Schur's own proof) shows that if

$$B \cong \oplus_i (M_{n_i}(\underline{C}))^{m_i}$$

then

$$B' \cong \oplus_i (M_{m_i}(\underline{C}))^{n_i} .$$

Furthermore, every finitely generated B'-module is a direct sum of simple modules ; in Schur's case, any simple A_n^f-module can be written $b.(\underline{C}^n)^{\otimes f}$, where b is a generator of a minimal left ideal of B and it is independent of that generator. As the minimal left ideals of B are isomorphic to some of those of $\underline{C}[\underline{S}_f]$, all rational irreducible representations of the groups $GL(n,\underline{C})$ can thus be derived from those of the symmetric groups $\underline{S}_f$, and the latter had been explicitly determined by Frobenius and A.Young.

This was not, however, the way in which Schur proceeded to determine the characters $\underline{X} \longrightarrow \mathrm{Tr}(\underline{F}(\underline{X}))$ (which he called "characteristics") of these representations. He used a tacit "irrelevance" argument to restrict himself to finding these characters as symmetric functions of the eigenvalues of $\underline{X}$ (he says that this is possible "because the elements of $\underline{X}$ are variables"!). Knowing, by the commutation theorem and by the results of Frobenius-Young, that the characters are in one-to-one correspondence with the finite partitions of f , he orders the partitions, and determines the characters of $GL(n,\underline{C})$ by induction on this ordering, obtaining as the end result the Jacobi expressions (9). From this result he then shows how one may rederive the explicit formula of Frobenius for the characters of $\underline{S}_f$.

III. The general theory of linear representations of semi-simple Lie groups.

After many years, I.Schur returned in 1924 to the question of linear representations of infinite groups, this time those of the orthogonal groups $O(n)$; he had the idea of replacing the discrete sums which define the group algebra $\underline{C}[G]$ for a finite group, by integration over the compact group $O(n)$, a device which had already been used in invariant theory by Hurwitz in 1898 ; he thus was able to generalize a substantial part of the Frobenius theory. But almost immediately, H. Weyl realized the power of this new idea, and was able to extend it to all compact connected Lie groups, a theory with which Schur was not familiar.

The two main concepts for a general (not necessarily Lie) compact group G are :
1) Integration with respect to a (right and left) invariant measure dx on G , normalized so that G has measure 1 .
2) The convolution of any two L^1-functions f,g , defined by

(19) $$(f \star g)(s) = \int_G f(x)\, g(x^{-1}s)\, dx$$

which reduces to (11) when G is finite ; it is always a L^1 function.

What replaces $\underline{C}[G]$ is the Banach algebra $L^2_{\underline{C}}(G)$, for which one has

$$N_2(f\star g) \leqslant N_2(f)\, N_2(g) \quad .$$

Its <u>center</u> Z is the closure of the set of continuous <u>central functions</u>, i.e. those such that $f(sts^{-1}) = f(t)$ for all s,t in G. The generalization of Frobenius's results is the <u>Peter-Weyl theorem</u>, which one can express in the following way : there is a decomposition of $L^2_{\underline{C}}(G)$ as a <u>Hilbert sum</u>

$$L^2_{\underline{C}}(G) = \oplus_\rho \underline{a}_\rho \tag{20}$$

where each $\underline{a}_\rho$ is a <u>minimal two-sided ideal</u>, consisting of <u>continuous</u> functions ; as an algebra, $\underline{a}_\rho$ is again isomorphic to an <u>algebra of matrices</u> $M_{n_\rho}(\underline{C})$. Its unit element u_ρ is a central function, such that $\check{u}_\rho = u_\rho$, and the orthogonal projection of $L^2_{\underline{C}}(G)$ onto $\underline{a}_\rho$ is given by $f \longrightarrow f\star u_\rho = u_\rho \star f$. The irreducible representations of G are then defined as in the finite case, replacing the $\underline{a}_j$ of the decomposition (12) by the $\underline{a}_\rho$; the <u>characters</u> of G are again the central functions

$$s \longrightarrow \chi_\rho(s) = n_\rho^{-1}\, u_\rho(s) \quad . \tag{21}$$

Now, when one specializes G to <u>compact connected Lie groups</u>, it is amazing to see how Schur had put his finger on the important general ideas, in the special cases he was considering, and how H.Weyl was able to give them their full meaning :

A) The "irrelevance" argument in Schur's dissertation amounted to restricting the representations of $GL(n,\underline{C})$ to the subgroup D_C of complex <u>diagonal matrices</u>, which is isomorphic to $(\underline{C}^\star)^n \cong \underline{R}^n \times \underline{T}^n$. Now, in any compact connected Lie group G, there are subgroups isomorphic to groups $\underline{T}^k$, and which one calls the <u>tori</u> of the compact group G ; the <u>maximal tori</u> of G generalize the subgroup $D = D_C \cap U(n)$ of diagonal matrices in the unitary group $U(n)$; all maximal tori in G are <u>conjugate</u> subgroups.

B) In $U(n)$, D is its own centralizer, and its normalizer $N(D)$ is such that $N(D)\,/\,D$ is isomorphic to the symmetric group $\underline{S}_n$. In a general compact connected Lie group G, a maximal torus T is its own centralizer, and its normalizer $N(T)$ is such that $N(T)/T$ is a <u>finite</u> group, called the <u>Weyl group</u> W of G. Although this reminds one of the intervention of the symmetric groups in the representations of $GL(n,\underline{C})$, here the Weyl group is independent of the representations of G, whereas for $GL(n,\underline{C})$ the symmetric groups $\underline{S}_f$ are related to degree f of the entries of the polynomial representations.

C) It is in the computations of the <u>characters</u> of G that Schur's results generalize. The classical fact that all unitary matrices are similar to matrices of D generalizes to the theorem that a connected compact Lie group is the <u>union</u> of its maximal tori ; as they all are conjugate to one of them T, a character χ_ρ is known once one knows its <u>restriction</u> $\chi_\rho | T$; Weyl's main result is a marvelous extension of the Jacobi-Schur formula (9)

(22) $\chi_\rho | T = J(e^{p+\delta})/J(e^{\delta})$

with

(23) $J(e^p) = \Sigma_{w \in W} \det(w)\, e^{w \cdot p}$.

In these formulas, the e^p are the characters of T, defined by

(24) $\exp u \longrightarrow e^{p(u)}$

where u is in the Lie algebra $\underline{t}$ of T, $u \longrightarrow \exp(u)$ is the exponential mapping of $\underline{t}$ into T, and p is a weight of T, i.e. a linear map $\underline{t} \longrightarrow i\underline{R}$ such that $p(u) \in 2\pi i\underline{Z}$ when $\exp(u) = e$; δ is the half sum of the "positive roots", which are certain weights corresponding to the restriction to T of the adjoint representation $Ad : G \longrightarrow Aut(g)$ in its Lie algebra. The Weyl group W acts on $\underline{t}$ as a group of linear maps of determinants ± 1, and leaves invariant the lattice of the weights. In (22), p is a well-determined weight of T, called the dominant weight of the representation ρ.

D) How is it that the representations of $U(n)$ determine those of $GL(n,\underline{C})$ obtained by Schur, in other words, how does one justify the "irrelevance" argument ? The answer is again given by H.Weyl, it is what he calls the unitarian trick : if $\underline{g}_u$ is the Lie algebra of a compact connected group, its complexified Lie algebra $\underline{g} = \underline{g}_u \otimes_{\underline{R}} \underline{C}$ is in the Lie algebra of a reductive complex Lie group ; if $\widetilde{G}$ and $\widetilde{G}_u$ are the simply connected groups having $\underline{g}$ and $\underline{g}_u$ as Lie algebras, the linear representations of $\widetilde{G}$ and $\widetilde{G}_u$ are in one-to-one correspondence, through the derived respective representations of $\underline{g}$ and $\underline{g}_u$ in a $gl(N,\underline{C})$, which are linked to each other by the complexification process.

E) How can Schur's restriction to rational representations be justified in general? It is easy to prove that any compact connected Lie group G is an algebraic subgroup of some $GL(N,\underline{R})$; but for any torus T contained in $GL(N,\underline{R})$, all representations of T are rational. Therefore Schur would not have obtained additional representations of $GL(n,\underline{C})$ if he had more generally considered representations which were only supposed to be continuous.

IV. Witt vectors and λ-rings

We now turn to questions which at first glance do not seem to have anything to do with symmetric functions. In 1936, a group of bright young German specialists in Algebra and Number theory, around H.Hasse, made a deep study of local fields and of applications of the theory of those fields to various problems in the theory of algebraic numbers and of algebraic curves. One of their problems was to study the structure of complete discrete valuation rings A of characteristic 0, in which the prime number p is a uniformizing element (i.e. its normalized valuation is 1); the residual field has characteristic p and is supposed to be perfect ; a typical

example is the ring $\underline{Z}_p$ of p-adic integers, where $k = \underline{Z}/p\underline{Z}$.

Each $x \in A$ can be written in at least one way as a convergent series

(25) $$x = a_0 + a_1 p + \ldots + a_n p^n + \ldots \quad , \quad a_n \in A \ ,$$

but obviously such a series is not uniquely determined by x . Now O.Teichmüller discovered that there is a unique map $f : A/pA \to A$ such that : 1° for $\xi \in k$, $f(\xi)$ belongs to the class ξ ; 2° f is multiplicative, i.e. $f(\xi\eta) = f(\xi)f(\eta)$ (the $f(\xi)$ are the elements of A which are p^n-th powers for all n). Using the fact that k is perfect, Teichmüller could then represent elements of A by canonical series (25) :

(26) $$x = \Sigma_{n=0}^{\infty} f(\xi_n^{p^{-n}})p^n \quad , \quad y = \Sigma_{n=0}^{\infty} f(\eta_n^{p^{-n}})p^n \ .$$

Hence, one can write

(27) $$x+y = \Sigma_{n=0}^{\infty} f(\zeta_n^{p^{-n}})p^n \quad , \quad xy = \Sigma_{n=0}^{\infty} f(\theta_n^{p^{-n}})p^n$$

with well determined ζ_n and θ_n , and immediately the problem arose of how to express these elements of k as functions of the ξ_n and η_n ? The solution was very soon found by E.Witt ; he showed that there are polynomials

(28) $$S_n(X_0,..,X_n;Y_0,..,Y_n) \quad , \quad P_n(X_0,..,X_n;Y_0,..,Y_n)$$

with coefficients in $\underline{Z}$, explicitely computable and universal (i.e. independent of k) such that

(29) $$\zeta_n = S_n(\xi_0,..,\xi_n;\eta_0,..,\eta_n) \quad , \quad \theta_n = P_n(\xi_0,..\xi_n;\eta_0,..,\eta_n) \ .$$

Witt arrived at this result by a very remarkable construction ; he considers an infinite sequence of indeterminates $X_0, X_1, \ldots, X_n, \ldots$, and the sequence of Witt polynomials, with coefficents in Z :

(30)
$$\begin{cases} W_0 = X_0 \\ W_1 = X_0^p + pX_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ W_n = X_0^p + pX_1^{p^{n-1}} + p^2X_2^{p^{n-2}} + \ldots + p^nX_n \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

It is clear that from these relations one deduces, conversely,

$$X_0 = W_0 \ , \ X_1 = p^{-1}(W_1 - W_0^p) \ , \ \ldots \ , \ X_n = \varphi_n(W_0,W_1,..,W_n) \ , \ \ldots$$

polynomials in the W_n with coefficients in $\underline{Z}[1/p]$. Suppose now we have two systems of indeterminates , $X'_0,..,X'_n,..$ and $X''_0,..,X''_n,..$, and let W'_n and W''_n be the corresponding Witt polynomials. If we write

$$Y_n = \varphi_n(W'_0+W''_0,..,W'_n+W''_n) \quad , \quad Z_n = \varphi_n(W'_0W''_0,..,W'_nW''_n)$$

and then replace in these formulas the W'_j and W''_j by their expressions, one obtains polynomials

$$Y_n = S_n(X'_0,..,X'_n;X''_0,..,X''_n) \quad , \quad Z_n = P_n(X'_0,..,X'_n;X''_0,..,X''_n) \ .$$

But then a miracle happens : the coefficients of these polynomials are integers (when one only expected them to be in $\mathbb{Z}[1/p]$) ; for instance

$$S_1(X'_0,X'_1;X''_0,X''_1) = X'_1 + X''_1 - p^{-1}\left(\binom{p}{1}X'^{p-1}_0X''_0 + \ldots + \binom{p}{p-1}X'_0X''^{p-1}_0\right) .$$

One can thus substitute in these polynomials elements of arbitrary rings ; it turns out that it is these polynomials which give formulas (29) .

The polynomials S_n for $n \leqslant N$ define a structure of affine commutative algebraic group over the prime field $\mathbb{F}_p$, called the Witt group of dimension $N+1$. During the period 1950-1970, it transpired that these groups played a role of "universal models" in the theory of commutative algebraic groups over a perfect field of characteristic $p>0$ and in the theory of formal groups over such fields .

Around 1965, in a private letter to S.Lang, Witt observed that his construction can be generalized : for a sequence of indeterminates $U_1,U_2,..,U_n,..$, one considers the sequence of polynomials

$$R_n = \sum_{d|n} d.U_d^{n/d} \qquad n = 1,2,... \tag{31}$$

This time, one has $U_n = f_n(R_1,..,R_n)$ for $n \geqslant 1$ with coefficients in $\mathbb{Q}$, but the same miracle occurs : when one replaces R_n by $R'_n+R''_n$ or $R'_nR''_n$, one gets polynomials with coefficients in $\mathbb{Z}$. To get the previous polynomials, for a prime number p , one has to replace U_{p^m} by X_m , U_n by 0 if n is not divisible by p , and similarly R_{p^m} is replaced by 0 if n is not divisible by p .

There is thus the possibility, for an arbitrary commutative ring with unit A , to define on the set $A^{\mathbb{N}}$ of all sequences $(a_n)_{n \geqslant 1}$ of elements of A the structure of a ring $R(A)$, using the generalized Witt polynomials for definition of sum and product, or, for each prime number p , a ring $W^{(p)}(A)$ using instead the Witt polynomials.

Furthermore, the additive law on $R(A)$ can be interpreted in a different way : consider, in the ring $A[[T]]$ of formal power series, the multiplicative group $\Lambda(A)$ of all series $1 + x_1T + .. + x_nT^n + ..$ with first coefficient 1 . Then, for any sequence $(a_n) \in A^{\mathbb{N}}$, let

$$E((a_n)) = \prod_{n=1}^{\infty}(1-a_nT^n)^{-1} = 1 + E_1(a_1)T + \ldots + E_n(a_1,..,a_n)T^n + .. \in \Lambda(A) \tag{32}$$

One easily shows that

$$E((a_n) + (b_n)) = E((a_n))\,E((b_n)) \tag{33}$$

where the "sum" in the left-hand side is addition in $R(A)$. Each E_n is a polynomial with coefficients in $\mathbb{Z}$, of the form $a_n + \Phi_n(a_1,..,a_{n-1})$, so that E is a bijection of $R(A)$ onto $\Lambda(A)$, the inverse E^{-1} being given by polynomials with coefficients in $\mathbb{Z}$. (There is a similar "exponential mapping" $E^{(p)}$ for the additive groups $W^{(p)}(A)$, the so-called "Artin-Hasse exponentials", but this time the polynomials which intervene only have their coefficients in the local

ring $\underline{Z}_{(p)}$, rational numbers with denominator prime to p) .

The bijection $E : R(A) \xrightarrow{\sim} \Lambda(A)$ enables one to "transfer" to $\Lambda(A)$ the ring structure of $R(A)$, by defining, for two elements f,g of $\Lambda(A)$

$$f.g = E(E^{-1}(f)E^{-1}(g)) \quad .$$

This may seem artificial, but here another miracle occurs. It turns out that this ring structure on $\Lambda(A)$ had been introduced around 1956 in a completely different context, the theory of characteristic classes in algebraic topology, and by a totally different formalism, the Hirzebruch-Grothendieck algorithm. One may say (with Witt) that the laws of composition in the rings $R(A)$ and $W^{(p)}(A)$ are obtained by computing with "phantom components" of elements in $A^{\underline{N}}$, namely the $R_n(a)$ and $W_n(a)$; the laws of composition defined by Hirzebruch and Grothendieck are similarly obtained by computing also with "phantom components" but of a totally different kind.

In his famous work on the Riemann-Roch theorem, Hirzebruch was led in 1953 to express in a convenient way the Chern classes of the complex vector bundles $E \oplus F$, $E \otimes F$ and $\Lambda^d E$, knowing the Chern classes of E and F (complex vector bundles over a compact space X). This time one introduces a sequence of indeterminates $\xi_1,\xi_2,..,\xi_n,..$, and one associates to that sequence the sequence of their "formal elementary symmetric functions" $e_1,...,e_n,..,$ defined by

$$(34) \qquad 1 + e_1T + .. + e_nT^n + .. = \prod_{i=1}^{\infty}(1+\xi_iT)$$

(the e_n are formal power series in the ξ_i). If then one writes

$$1 + c_1(E)T + .. + c_n(E)T^n + .. = \prod_{i=1}^{\infty}(1+\xi_iT)$$

$$1 + c_1(F)T + .. + c_n(F)T^n + .. = \prod_{i=1}^{\infty}(1+\eta_iT)$$

for two sequences of indeterminates (ξ_i) , (η_i) , the $c_n(E)$ and $c_n(F)$ being the Chern classes of E and F , one has

$$(35) \qquad 1 + c_1(E\oplus F)T + .. + c_n(E\oplus F)T^n + .. = \prod_{i=1}^{\infty}(1+\xi_iT)\prod(1+\eta_iT)$$

$$(36) \qquad 1 + c_1(E\otimes F)T + .. + c_n(E\otimes F)T^n + .. = \prod_{j,k}(1+(\xi_j+\eta_k)T)$$

$$(37) \qquad 1 + c_1(\Lambda^dE)T + .. + c_n(\Lambda^dE)T^n + .. = \prod_{i_1<i_2<..<i_d}(1+(\xi_{i_1} + .. + \xi_{i_d})T)$$

All these formulas make sense, for on the right hand sides one always has symmetric functions of the ξ_i and η_i in finite number, since the Chern classes, for a compact space X , are 0 after a certain dimension.

When in 1956 Grothendieck introduced the ring $K(X)$ of classes of complex vector bundles over X , he modified Hirzebruch's formalism in order to get operations in $\Lambda(A)$ for any commutative ring A ; as "additive law" he kept the usual multiplication in $A[[T]]$, but in (36) and (37) he replaced addition of the "phantom" components by their multiplication, so that "multiplication" of $\prod_{i=1}^{\infty}(1+\xi_iT)$ and $\prod_{i=1}^{\infty}(1+\eta_iT)$ is given by $\prod_{j,k}(1+\xi_j\eta_kT)$. The miracle is that the ring structure

obtained on $\Lambda(A)$ is the same as the one transferred from the Witt structure on $R(A)$.

Similarly, Grothendieck defined, for an element $x = 1 + x_1T + .. + x_nT^n + ..$ of $\Lambda(A)$, the element $\lambda^d x$ by taking, for $x = \prod_{i=1}^{\infty}(1+\xi_i T)$,

$$\lambda^d x = \prod_{i_1<i_2<..<i_d} (1+\xi_{i_1}\xi_{i_2}..\xi_{i_d}T) \quad ; \tag{38}$$

the coefficient of T^n on the right-hand side is $P_{nd}(x_1,x_2,..,x_{nd})$, where P_{nd} is a universal polynomial with coefficients in $\underline{Z}$; one thus arrives at the definition of what Grothendieck called a λ-ring.

In the hand of Atiyah, Hirzebruch and J.F.Adams, this "K-theory" became a wonderfully powerful tool in algebraic topology. But Adams was led to work with a system of "operations" in $\Lambda(A)$ which have better properties than the λ^d, because in particular they are ring homomorphisms, whereas the λ^d are only homomorphisms for the multiplication.

In general, any symmetric function, written as a polynomial $F(e_1,e_2,...)$ in the elementary symmetric functions, defines an operation in $\Lambda(A)$ by the assignment $x \longrightarrow F(x,\lambda^2x,\lambda^3x,..)$; for instance λ^d corresponds to $F = e_d$. The Adams operation Ψ^d corresponds to the "power sum" p_d (5). When one transfers back that operation to $R(A)$ by the isomorphism E, Ψ^d takes the very simple form

$$(a_n) \longrightarrow F_d((a_n))$$

where, for the "phantom" components,

$$R_N(F_D(a)) = R_{dn}(a) \quad \text{for all} \quad n \geqslant 1 \quad . \tag{39}$$

It would be surprising if these operations had not been considered for Witt vectors; and indeed, if, for a prime number p, one considers the operation F_p restricted to $W^{(p)}(A)$, one discovers that when A is a field of characteristic p, F_p is the well-known Frobenius morphism

$$(a_o,a_1,..,a_n,..) \longrightarrow (a_o^p,a_1^p,..,a_n^p,..)$$

which plays a fundamental part in the theory of commutative algebraic and formal groups, and in the theory of local fields.

To crown this series of miracles, we finally have the Atiyah isomorphism. For each finite group G, let $R(G)$ be the $\underline{Z}$-module consisting of formal linear combinations (with coefficients in $\underline{Z}$) of equivalence classes of the irreducible representations of G; the class of any linear representation ρ of G may be identified with the element of $R(G)$ such that the coefficient of any irreducible representation is the multiplicity of that representation in ρ. One may also identify $R(G)$ with the additive group generated by the characters of G.

Now Atiyah considers the direct sum

$$R(\underline{S}) = \oplus_{f=0}^{\infty} R(\underline{S}_f)$$

and introduces on the $\underline{Z}$-module $R(\underline{S})$ a <u>multiplication</u> in the following way . Let ρ_m , ρ_n be linear representations of $\underline{S}_m$ and $\underline{S}_n$ respectively. There are natural injective homomorphisms $\underline{S}_m \times \underline{S}_n \to \underline{S}_{m+n}$, any two of which are conjugate. One then considers the representation $\rho_m \times \rho_n$ of the group $\underline{S}_m \times \underline{S}_n$, and the <u>induced</u> representation

$$\mathrm{Ind}_{\underline{S}_m \times \underline{S}_n}^{\underline{S}_{m+n}} (\rho_m \times \rho_n)$$

of $\underline{S}_{m+n}$; its class does not depend on the embedding of $\underline{S}_m \times \underline{S}_n$, and that class is taken as the product of the classes of ρ_m and ρ_n in $R(\underline{S})$.

The fundamental result of Atiyah is then that there is a natural ring isomorphism $R(\underline{S}) \to \Lambda(\underline{Z})$: it associates to each irreducible representation of an $\underline{S}_f$ the "formal" Schur function which is the character of the corresponding representation (by matrix polynomials of degree f) of $GL(n,\underline{C})$ for n large enough .