Centrum voor Wiskunde en Informatica
Centre for Mathematics and Computer Science

M. Hazewinkel

Three lectures on formal groups

Department of Pure Mathematics Report PM-R8505 July

The Centre for Mathematics and Computer Science is a research institute of the Stichting Mathematisch Centrum, which was founded on February 11, 1946, as a nonprofit institution aiming at the promotion of mathematics, computer science, and their applications. It is sponsored by the Dutch Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O.).

MSC 85 : 1405

Three Lectures on Formal Groups

Michiel Hazewinkel
Centre for Mathematic and Computer Science, Amsterdam

This paper is the written version of a series of three lectures given in Windsor at the occasion of the Canadian Mathematical Society's summer school in Lie algebras and related topics in July 1984. They were antended as in introduction to the subject for an algebraically oriented audience with special emphasis on the kind of phenomena that appear when dealing with commutative formal groups over rings (rather than fields). Proofs and more details of most everything can be found in [9]. I am (and was) most grateful for the opportunity to speak on this topic and heartily thank the organising committee, notably Bob Moody, and the local organizers, the two friendly giants Dan Britten and Frank Lemire, for the opportunity. The phenomena are extraordinary rich in the commutative case-privately I suspect (with admittedly little grounds) especially in the commutative case - and much work remains to be done to get even a first idea of what the noncommutative theory has in store.

These written notes follow the original lectures in structure but contain rather more. The contents are: 0) Introduction; 1) Two classes of examples of formal groups from other parts of mathematics; 2) Generalities and bialgebras; 3) The Lie algebra of a formal group. Characteristic zero formal Lie theory; 4) The commutativity theorem; 5) Logarithms; 6) The functional equation lemma. Examples of formal groups; 7) Universal formal groups. Generalities; 8) p-typical formal groups; 9) A universal p-typical formal group and a formal group universal over $\mathbf{Z}_{(p)}$-algebras; 10) Construction of a universal formal group; 11) Application to algebraic topology; 12) Atkin-Swinnerton Dyer congruences for elliptic curves; 13) Witt vectors; 14) Curves, Frobenius and Verschiebung; 15) Cart(A); 16) Cartier-Dieudonné classification theory; 17) p-typification; 18) Other classification results; 19) Universality of the formal group of the Witt vectors; 20) $U(\hat{W})$; 21) Remarks on noncommutative formal group theory.

0. Introduction.

Consider a Lie group G over $\mathbf{R}$ or $\mathbf{C}$. Let $e \in G$ be the identity element and consider coordinates on a neighborhood U of e, such that the coordinates of e are (0,0,...,0). Let $x,y \in U$ be such that $xy \in U$. Let the coordinates of x,y and xy be respectively $(x_1,...,x_n);(y_1,...,y_n);(f_1, \ldots, f_n)$. Then because G is analytic the f_i are power series in the x_k and y_l

$$f = (f_i), \quad f_i = f_i(x_1,...,x_n;y_1,...,y_n)$$

and this n-tuple of power series f satisfies

$$f(x, 0) = x, \quad f(0,y) = y \tag{0.1}$$

$$f(f(x,y),z) = f(x,f(y,z)) \tag{0.2}$$

The first relation comes from $xe = x$ and $ey = y$; the second one from $(xy)z = x(yz)$.

Now consider $f(x,y)$ simply as an n-tuple of power series (forgetting about convergence). Then we have an infinitesimal object attached to G that is intermediate between the Lie algebra of G and the group G itself. Indeed the Lie algebra of G can be recovered from the n-tuple of power series $f(x;y)$ as follows. Let

$$f(x;y) = x + y + B(x,y) + (\text{terms of degree} \geqslant 3) \tag{0.3}$$

Report PM-R8505
Centre for Mathematics and Computer Science
P.O. Box 4079, 1009 AB Amsterdam, The Netherlands

Then by (0.1) $B(x,y)$ is bilinear. The Lie algebra g is now the n-dimensional vector space $V = \bigoplus_{i=1}^{n} \mathbf{R}e_i$ (in the real case) with the commutator defined by

$$[\,\sum a_i e_i, \sum b_i e_i\,] = \sum B(a,b)_k e_k - \sum B(b,a)_k e_k \tag{0.4}$$

where $B(a,b)_k$ is the k-th component of $B(a,b)$. The Jacobi identity of course follows from considering (0.2) mod degree 4. (Non trivial exercise).

For (sufficiently nice) group schemes G over an arbitrary commutative ring with $1 \in A$ there exists an entirely analogous construction: the fornal completion $\hat{G}$ of G along the identity resulting this time in an n-tuple of fornal power series over A also satisfying (0.1) and (0.2).

It is now easy to abstract from these considerations. Let A be any commentative ring, $1 \in A$. Then an n-dimensional *formal group law* over A is an n-tuple of power series

$$F(X,Y) \in A[[X_1,\ldots,X_n;Y_1,\ldots,Y_n]] = A[[X;Y]]$$

such that

$$F(X,0) = X, \quad F(0,Y) = Y \tag{0.5}$$

$$F(F(X,Y),Z) = F(X,F(Y,Z)). \tag{0.6}$$

Note that (0.6) makes sense (if $n < \infty$; for $n = \infty$ $F(X,Y)$ has to satisfy certain support conditions or, more generally, a topological condition with respect to a topology on A). It follows from (0.5), (0.6) that there exists an n-tuple of power series $\iota(X)$ such that

$$F(X,\iota(X)) = 0 \tag{0.7}$$

If the formal group law $F(X,Y)$ satisfies in addition

$$F(X,Y) = F(Y,X) \tag{0.8}$$

it is called a commutative formal group law.

Formal group laws over $\mathbf{R}$ or $\mathbf{C}$ naturally arose from classical Lie theory when BOCHNER [2] in 1946 separated Lie theory into a formal part (constructing the formal group law from the Lie algebra) and an analytic part (showing convergence to obtain a Lie group germ). The formal part of course amounts to the Baker-Campbell-Hausdorff formula

$$exp(x)exp(y) = exp(z),\ z = x+y+\tfrac{1}{2}[x,y]+\frac{1}{12}([x,[x,y]+[y,[y,x]])+\ldots$$

Over fields of characteristic p the familiar dictionary between Lie-algebras and Lie-groups breaks down completely as discovered by CHEVALLEY [6] in the early 1950's and thus the search was on for a suitable infinitesimal object that could replace the Lie algebra. The latter simply carried not nearly enough information. This was the direct inspiration for the researches of Dieudonné in the 1950's and his long series of papers on formal groups over fields of characteristic p.

Indeed, to illustrate the point consider the two one dimensional formal groups

$$\hat{\mathbf{G}}_a(X,Y) = X+Y \tag{0.9}$$

$$\hat{\mathbf{G}}_m(X,Y) = X+Y+XY \tag{0.10}$$

over, say, $\mathbf{F}_p$, the field of p-elements. An homomorphism $\alpha: F \to G$ between two formal groups of dimensions n and m respectively would of course be an m-tuple of power series $\alpha(X)$ in $X_1,\ldots,X_n$ such that $\alpha(F(X,Y)) = G(\alpha(X),\alpha(Y))$ and an isomorphism is a homomorphism such that $\alpha^{-1}(X)$ exists (where $\alpha^{-1}(\alpha(X)) = X$); then of course we must have $m = dimG = dimF = n$)

0.11. Exercise.
Show that $\hat{\mathbf{G}}_a$ and $\hat{\mathbf{G}}_m$ are not isomorphic over $\mathbf{F}_p$ or indeed over any characteristic p field.

But of course $\hat{\mathbf{G}}_a$ and $\hat{\mathbf{G}}_m$ have the same Lie algebra.

As a matter of fact it has turned out that the phenomena are very rich even just for one dimensional commutative formal groups. For example over $\mathbf{F}_p$ there are uncountably many nonisomorphic formal groups. One classification result puts them into a bijective correspondence with all maps $\mathbf{N} \to \mathbf{F}_p$; another classification results sets up a bijective correspondence with Eisenstein polynomials over $W_{p^\infty}(\mathbf{F}_p) = \mathbf{Z}_p$, the p-adic integers. Still another classification results describes them in terms of conjugacy classes of elements in E_h, the ring of integers in D_h the division algebra of rank h^2 and invariant h^{-1} over $\mathbf{Q}_p$ (for varying $h \in \mathbf{N} = \{1,2,3,...\}$).

And even over $\mathbf{F}_{p^\infty}$ the algebraic closure of $\mathbf{F}_p$ it turns out that there are countably many nonisomorphic one dimensional commutative formal groups. (This holds for every algebraically closed field of char $p > 0$). Later in these lectures they will all be constructed.

This enormous richness and the fact that commutative formal group laws occur naturally in several parts of mathematics certainly has steered the theory of formal group laws away from topics traditionally met in the neighborhood of Lie groups and Lie algebras such as representation theory. At least for the moment.

Still it seems quite likely that they can play a significant role especially there where the group cannot be recovered from the algebra (characteristic p) or where the group is difficult (perhaps impossible) to construct (infinite dimensional Lie algebras). Especially since various applications areas (Kac-Moody Lie algebras in completely integrable systems, differential galois theory) seem to have a large and growing formal part to them.

However, that is for the future and the lectures shall mainly be about commutative finite dimensional formal groups, and their applications. Indeed apart from technicalities the one dimensional theory is as rich as the n-dimensional one, so I shall concentrate on that. Although even there it will be necessary to pay attention to one infinite dimensional formal group, the one of the (generalized) Witt vectors.

1. Two Classes of Examples of Formal Groups from other Parts of Mathematics

1.1. Dirichlet series over $\mathbf{Z}$.
Let

$$L(s) = \sum_{n \geq 1} a_n n^{-s}, \quad a_n \in \mathbf{Z} \tag{1.1.1}$$

be a Dirichlet series. Suppose $L(s)$ admits an Euler factorization

$$L(s) = \prod_p (1 - a_{p,1}p^{-s} - a_{p,2}p^{1-2s} - a_{p,3}p^{2-3s} - ...), \tag{1.1.2}$$

$$a_{p,i} \in \mathbf{Z}.$$

where the product is over all prime numbers. (Actually a weaker condition suffices). For example this is the case for the Artin L-series of an elliptic curve over $\mathbf{Q}$.

Construct (Mellin transform)

$$f(X) = \sum_{n \geq 1} n^{-1} a_n X^n, \quad F(X,Y) = f^{-1}(f(X)+f(Y)) \tag{1.1.3}$$

where $f^{-1}(X)$ is the inverse function power weries to $f(X)$, i.e. $f^{-1}(f(X)) = X = f(f^{-1}(X))$.

Theorem 1.1.4. *$F(X,Y)$ has its coefficients in $\mathbf{Z}[X,Y]$ and hence is a one-dimensional commutative formal group over $\mathbf{Z}$.*

A proof will be given later (meanwhile it is a nontrivial exercise) as well as an application (Atkin-Swinnerton Dyer congruences).

1.2. Complex oriented cohomology theories

Let h^* be a complex oriented (generalized) cohomology theory. Here generalized of course means that $h^*(pt)$ is not necessarily concentrated in degree 0. I do not want to define "complex oriented" but basically it means that there are Euler (characteristic) classes $e^h(E) \in h^*(M)$ for complex vector bundles E over M, which behave suitably.

Being complex oriented has certain (purely formal) consequences. It implies e.g. that

$$h^*(\mathbf{CP}^\infty) = h^*(pt)[[\xi]], \quad x = e^h(\xi) \tag{1.2.1}$$

where ξ is the canonical (classifying) complex line bundle over $\mathbf{CP}^\infty$. Also

$$h^*(\mathbf{CP}^\infty \times \mathbf{CP}^\infty) = h^*(pt)[[x,y]], \; x = e^h(\xi \otimes 1), \; y = e^h(1 \otimes \xi). \tag{1.2.2}$$

Now because ξ is classifying for line bundles, there must exist a universal formula which gives $e^h(L_1 \otimes L_2)$ in terms of $e^h(L_1)$ and $e^h(L_2)$ with coefficients in $h^*(pt)$. Indeed we must have

$$e^h(\xi \otimes \xi) = \sum_{i,j} a_{ij} x^i y^j, \quad a_{i,j} \in h^*(pt) \tag{1.2.3}$$

and hence

$$e^h(L_1 \otimes L_2) = \textstyle\sum_{i,j} a_{ij} e^h(L_1) e^h(L_2) \tag{1.2.3}$$

universally for line bundles L_1 and L_2 over a space M. Let

$$F_h(X,Y) = \textstyle\sum_{i,j} a_{i,j} X^i Y^j \tag{1.2.4}$$

Then because the tensor product of line bundles is associative and commutative and $L_1 \otimes$ trivial $\approx L_1$, e^h (trivial) $= 0$ it follows that $F_h(X,Y)$ as defined by (1.2.4) is a commutative one dimensional formal group law over $h^*(pt)$.

Examples of complex oriented cohomology theories are ordinary cohomology H^*, complex K-theory K^*, complex cobordism MU^* and Brown-Peterson cohomology BP^*.

For generalized cohomology theories the coefficient ring $h^*(pt)$ carries insufficient information for comparison purposes in that it is no longer necessarily true that if $\alpha: h_1^* \to h_2^*$ is a transformation of cohomology theories and $\alpha(pt)$ is an isomorphism then α is an isomorphism. However if the theories are complex oriented and $\alpha(pt)$ carries F_{h_1} into F_{h_2} (i.e. $F_{h_2}(X,Y) = \sum \alpha(pt)(a_{ij}) X^i Y^j$ if $F_{h_1}(X,Y) = \sum a_{ij} X^i Y^j$) then α is an isomorphism of cohomology theories.

2. Generalities and Bialgebras

Let $F(X,Y)$ be a formal group law over A. Then of course the $F_i(X,Y)$ define a homomorphism of topological algebras

$$A[[X_1,\ldots,X_n]] \to A[[X_1,\ldots,X_n]] \otimes A[[X_1,X_2,\ldots,X_n]] \tag{2.1}$$

$$X_i \mapsto F_i(X_1 \otimes 1,\ldots,X_n \otimes 1; 1 \otimes X_1,\ldots,1 \otimes X_n).$$

Together with the augmentation

$$\epsilon: A[[X_1,\ldots,X_n]] \to A, \quad X_i \mapsto 0 \tag{2.2}$$

this makes $A[[X]]$ a Hopf-algebra There is also an antipode $X \to \iota(X)$ which makes $A[[X]]$ into a cogroup object in the category of algebras. This object is denoted $R(F)$ and is called the *contra variant bialgebra of the formal group F.*

This also permits to define formal groups in a less pedestrian way as cogroup objects in a suitable category of algebras over A. There is no particular reason to limit oneself to formal power series algebras only (though these remain a most important kind). For many purposes the right category of algebras seems to be the category $AlgT_A$ of topological A algebras which are of the form $\Pi_{i\in I} A_i$, $A_i = A$ as A-modules, topologized by the product topology (discrete topology on the factors)

Finite etale group schemes and finite infinitesimal group schemes over A of suitable kinds are then also formal groups over A.

Given a formal group over A defined by its Bialgebra $R(F)$ one considers

$$U(F) = ModT_A(R(F),A) \tag{2.3}$$

the continuous linear dual of $R(F)$

The comultiplication (2.1) and the co-unit (or augmentation) (2.2) define a multiplication and identity element on $U(F)$ making $U(F)$ an A-algebra. The original multiplication and unit then make $U(F)$ also a Hopf algebra with an antipode defined by (the dual of) $\iota: R(F) \to R(F)$. The result is more precisely a group object in the category of co-algebras (but unless F is commutative not a cogroup object in the category of algebras).

$U(F)$ is called the covariant bialgebra of F and group objects in a suitable category of co-algebras provide another way to define formal groups. This is the approach favoured by Dieudonné [7].

The relation $R(F) <\!\!\to U(F)$ is of course a kind of duality (between, in the commutative case, very similar objects) and it can be souped-up and reinterpreted as a Pontryagin-like duality between commutative formal groups and commutative algebraic groups (Cartier duality [3]).

3. The Lie Algebra of a Formal Group. Characteristic Zero Formal Lie Theory

Let $R(F)$ be the covariant bialgebra of a formal group F over A. Let $\underline{\mathfrak{m}}(F)$ be the augmentation ideal; i.e. $\underline{\mathfrak{m}}(F) = Ker(\epsilon)$, c.. (2.2). Then the Lie algebra $L(F)$ of F can be identified with

$$L(F) = Mod_A(\underline{\mathfrak{m}}(F)/\underline{\mathfrak{m}}^2(F) \to A) \subset U(F) \tag{3.1}$$

and it coincides with the Lie-algebra of primitive elements of the Hopf-algebra $U(F)$. (An element c in a co-algebra μ: $C \to C\otimes C$ is primitive if $\mu(c) = c\otimes 1 + 1\otimes c$; these elements form a Lie algebra (under commutator difference) if C is a Hopf-algebra.

3.2. Exercise.
Check that the Lie-algebra thus defined is the same as the one prosaically defined in section 0 above for F a "power series formal group" as in section 0.

Now consider $L(F) \subset U(F)$. Because $U(F)$ is an associative algebra there is an induced homomorphism of associative algebras

$$UL(F) \to U(F) \tag{3.3}$$

where $UL(F)$ is the universal enveloping algebra of $L(F)$.

Theorem 3.4. (Formal Lie theory in char. 0) *If A is a $\mathbf{Q}$-algebra, then (3.3) is an isomorphism of associative algebras.*

In characteristic p however $L(F)$ (usually) generates only a tiny bit of $U(F)$ and this of course is the source of the break down of Lie-theory in characteristic p as discovered by Chevalley [6].

It is true though that the universal enveloping algebra (in characteristic zero) provided a great deal of inspiration for the development of bialgebra-type formal group theory.

4. The Commutativity Theorem

There are many nonisomorphic one dimensional formal groups over a ring A that is not a $\mathbf{Q}$-algebra. But one thing goes right

Theorem 4.1. (Lazard, [10], [9, §6]). *If A has no nilpotents, then every one-dimensional formal group over A is commutative.*

Actually it suffices that A have no elements which are simultaneously torsion and nilpotent (Connell). If A has such elements noncommutative formal groups of dim.1 over A exist.

From now on all formal groups will be pedestrian power series groups as in section 0 and all will be commutative (unless it is explicitly stated otherwise).

5. Logarithms.

Theorem 3.4 shows that over a $\mathbf{Q}$-algebra all n-dimensional commutative formal group laws are isomorphic.

More precisely it is true that if A is a $\mathbf{Q}$-algebra, then for a formal group F over A there exists a unique n-tuple of power series $f(x) = X + \ldots$ such that

$$F(X,Y) = f^{-1}(f(X)+f(Y)). \tag{5.1}$$

$f(X)$ is called the logarithm of F and is occasionally denoted $\log_F(X)$. The name derives from the example

$$\hat{\mathbf{G}}_m(X,Y) = X+Y+XY$$

Indeed if $g(X) = log(1+X)$, then $g(\hat{\mathbf{G}}_m(X,Y)) = log(1+X+Y+XY) = log(1+X)+log(1+Y) = g(X)+g(Y)$ so that

$$\log_{\hat{\mathbf{G}}_m}(X) = log(1+X).$$

More generally if A is torsion free, so that $A \hookrightarrow A\otimes\mathbf{Q}$ is injective, the logarithm of a formal group over A exists over $A\otimes\mathbf{Q}$. Thus the study of formal groups over A becomes the study of power series $f(X)$ over $A\otimes\mathbf{Q}$ with the peculiar property that

$$f^{-1}(f(X)+f(Y)) \in A[[X,Y]],\ f(X) \in A\otimes\mathbf{Q}[[X]] \tag{5.2}$$

and the study of "equivalence classes" of such power series under the relation $f \sim f'$ if $f' = f(a(X))$, $a(X) \in A[[X]]$.

As it turns out even for fields of characteristic p and more generally arbitrary rings A with torsion much information can be gained by studying the logarithms of lifts (to torsion free base rings) of formal groups over A.

Theorem 3.4 (applied to commutative formal groups) does not quite prove the "existence of logarithm theorem", but almost. Thus this section mainly serves as motivation only. The existence and uniqueness of logarithms will be an easy corollary of later results.

6. The Functional Equation Lemma

The main and really only tool for constructing formal groups from scratch is the functional equation lemma. Honda's twisted power series method is a special case, and there is (of course) also a step by step (never ending) procedure of writing down the right kind of power series. Other methods to obtain formal groups are "formal completion along the identity of a group scheme" (cf. §1.1 above) and the construction which attaches a formal group to a complex oriented cohomology theory (cf. §1.2 above), and that is about all.

The functional equation lemma more or less gives necessary and sufficient conditions on a power series $f(X) \in A \otimes \mathbf{Q}[[X]]^n$ to satisfy the peculiar integrality property $f^{-1}(f(X)+f(Y)) \in A[[X,Y]]^n$. Here A is assumed to be a torsion free ring so that $A \hookrightarrow A \otimes \mathbf{Q}$ is injective. In a certain sense to be explained below this statement holds even for all A.

The functional equation lemma needs the following setting (ingredients) for its statement.

$$A \subset K, \quad \sigma: K \to K, \quad \mathfrak{o} \subset A, \quad p, q, s_1, s_2, \ldots \tag{6.1}$$

Here A and K are commutative rings, $\mathfrak{o}$ is an ideal of A, σ is a ring endomorphism, p is a prime number, q is a power of p and $s_1, s_2, \ldots$ are $n \times n$ matrices with coefficients in $K, s_k = (s_k(i,j))$. These ingredients are supposed to satisfy the conditions

$$\sigma(a) \equiv a^q \bmod \mathfrak{o} \text{ for all } a \in A; \sigma^l(s_k(i,j))\mathfrak{o} \subset A \text{ all } l,k,i,j. \tag{6.2}$$

Now let $g(x)$ be an n-tuple of power series in $X_1, \ldots, X_m$ with coefficients in A and such that $g(0) = 0$. Then a new n-tuple of power series $f_g(X)$ is constructed by

$$f_g(X) = g(X) + \sum_{i=1}^{\infty} s_i \sigma^i_* f_g(X^{q^i}). \tag{6.3}$$

Here X^{q^i} is short for $(X_1^{q^i}, \ldots, X_m^{q^i})$ and $\sigma^i_* \alpha(X)$ for a power series $\alpha(X)$ over K is the result of applying σ^i to each of the coefficients of $\alpha(X)$.

EXERCISE 6.4. Note that (6.3) in fact gives a recursive formula for the coefficients of $f_g(X)$. Note also that a power series $f(X)$ (with $f(0) = 0$) is of the form $f_g(X)$ for some $g(X) \in A[[X]]^n$ iff $f(X) - \sum_i s_i \sigma^i_* f(X^{q^i}) \in A[[X]]^n$.

EXAMPLE 6.5. $\mathbf{Z} \subset \mathbf{Q}$, $\sigma = id$, $m = p\mathbf{Z}$, $p^h = q$, $s_1 = p^{-1}$, $s_2 = s_3 = \cdots = 0$; $n = m = 1$, $g(X) = X$, $f_g(X) = X + p^{-1}X^p + p^{-2}X^{p^2} + p^{-3}X^{p^3} + \ldots$.

Now let $A, K, \mathfrak{o}, \sigma, p, q, s_1, s_2, \ldots$ be as above and let $g(X), \bar{g}(\bar{X})$ be two n-tuples of power series in respectively n variables $X_1, \ldots X_n$ and m variables $\bar{X}_1, \ldots, \bar{X}_m$, such that $g(0) = 0$, $\bar{g}(0) = 0$. Suppose moreover that the Jacobian matrix of $g(X)$ (at 0) is invertible, i.e. $g(X) = MX$ mod(degree 2) with $M \in GL_n(A)$. Then one has

THEOREM 6.6. (The functional equation lemma).

(i) *the n-tuple of power series $F_g(X;Y) = f_g^{-1}(f_g(X)+f_g(Y))$ in $X_1, \ldots, X_n, Y_1, \ldots, Y_n$ has its coefficients in A.*

(ii) *the n-tuple of power series $f_{\bar{g}}^{-1}(f_{\bar{g}}(\bar{X}))$ in $\bar{X}_1, \ldots, \bar{X}_m$ has its coefficients in A.*

(iii) *let $h(\hat{X})$ be an n-tuple of power series over A with $h(0) = 0$.*

Then $f_g(h(\hat{X})) - \sum_i s_i \sigma^i_* f_g(h(\hat{X}^{q^i})) \in A[[\hat{X}]]^r$, i.e. $f_g(h(\hat{X}))$ is of the form (6.3) (for some $\hat{h}(\hat{X})$ instead of g in (6.3)).

(iv) *Iff $\alpha(\hat{X})$, $\beta(\hat{X})$ are n-tuples of power series in $\hat{X}_1, \ldots, \hat{X}_r$ with coefficients in A and K respectively, then for all $l = 1,2,3,\ldots$*

$$\alpha(\hat{X}) \equiv \beta(\hat{X}) \bmod \mathfrak{o}^l \Leftrightarrow f_g(\alpha(\hat{X})) \equiv f_g(\beta(\hat{X})) \bmod \mathfrak{o}^l.$$

Application 6.7.
Let $f_h(X) = X + p^{-1}X^{p^h} + p^{-2}X^{p^{2h}} + \ldots$, cf. (6.5) above. Then $F_h(X,Y) = f_h^{-1}(f_h(X)+f_h(Y))$ is a formal group over $\mathbf{Z}$.

DEFINITION 6.8. Let $F(X,Y), G(X,Y)$ be two formal groups over A of dimensions n and m respectively. A *homomorphism* $\alpha: F \to G$ is an m-tuple of power series in n-variables with $\alpha(0) = 0$ such that $\alpha(F(X,Y)) = G(\alpha(X),\alpha(Y))$. A formula which is easy to remember if one writes the "product" $F(X,Y)$ of the "elements" X, Y as $X *_F Y$. This gives $\alpha(X * Y) = \alpha(X) * \alpha(Y)$. The homomorphism α is an *isomorphism* if α is invertible i.e. if $n = m$ and $\alpha(X) \equiv MX$ mod degree 2 with $M \in GL_n(A)$, and α is a *strict isomorphism* if $\alpha(X) \equiv X$ mod degree 2.

Exercise 6.9.
The one dimensional formal groups $F_{h_1}(X,Y), F_{h_2}(X,Y)$ over $\mathbf{Z}$ or $\mathbf{Z}_p$ are isomorphic iff $h_1 = h_2$. Hint: let $\alpha(X)$ be the isomorphism. Let $h_1 < h_2$. Calculate $\alpha(F_{h_1}(X,Y)$ and $F_{h_2}(\alpha(X),\alpha(Y))$ mod degree $(p^{h_1}+1)$. Alternative: apply part (iii) of the functional equation lemma.

Exercise 6.10.
(Integrality of the addition polynomials of the big Witt vectors). Define the polynomials $w_i(X)$ in $X_1, X_2, X_3, \ldots$ over $\mathbf{Z}$, $i = 1,2,3,\ldots$ by the formula

$$w_n(X) = \sum_{d|n} dX_d^{n/d} \tag{6.11}$$

Thus $w_1(X) = X_1$, $w_4(X) = 4X_4 + 2X_2^2 + X_1^4$, $w_6(X) = 6X_6 + 2X_2^3 + 3X_3^2 + X_1^6$. Let $\Sigma_1, \Sigma_2, \ldots$ be the polynomials in $X_1; Y_1$, resp. $X_1, X_2; Y_1, Y_2$, resp... defined by

$$w_n(\Sigma_1, \ldots, \Sigma_n) = w_n(X) + w_n(Y). \tag{6.12}$$

Then the $\Sigma_1, \Sigma_2, \ldots$ have their coefficients in $\mathbf{Z}$. Hint: consider $\overline{w}_n = n^{-1}w_n$ and $\overline{w} = (\overline{w}_1, \overline{w}_2, \ldots)$, and for each p the functional equation lemma situation $\mathbf{Z}_{(p)} \subset \mathbf{Q}$, $\sigma = id$, $q = p$, $\mathfrak{o} = p\mathbf{Z}_{(p)}$, $\sigma_1 = S_p$, $\sigma_2 = \sigma_3 = \cdots = 0$, where S_p is the $\infty \times \infty$ matrix defined by $S_p(a_1, a_2, a_3, \ldots) = (b_1, b_2, \ldots)$ with $b_{pi} = p^{-1}a_i$ and $b_j = 0$ if $p \nmid j$. Now observe that $\overline{w}(X)$ satisfies (6.3) and apply the functional equation lemma. In this form this requires an infinite dimensional version of theorem 6.3. Such a version exists provided the $f_g(X)$ satisfy certain support conditions (which are automatic in the case of finitely many variables and which are satisfied for $\overline{w}(X)$). In this case because the Σ_n depend only an $X_1, \ldots, X_n; Y_1, \ldots, Y_n$ it suffices to consider the n-tuple of power series $(\overline{w}_1(X), \ldots, \overline{w}_n(X))$ in n variables for all n.

The infinite dimensional formal group defined by the power series $\Sigma_1(X;Y), \Sigma_2(X;Y), \ldots$ in $X_1, X_2, \ldots; Y_1, Y_2, \ldots$ is called the *formal group of the big Witt vectors* and denoted W.

7. UNIVERSAL FORMAL GROUPS. GENERATIES

An n-dimensional formal group law $F(X,Y)$ over a ring L is universal (resp. a universal abelian formal group law) if for every n-dimensional formal group (resp. abelian formal group) $G(X,Y)$ over a ring A there is a unique homomorphism of rings $\phi: L \to A$, such that

$$\phi_* F(X,Y) = G(X,Y). \tag{7.1}$$

Here, as usual, ϕ_* means "apply ϕ to the coefficients of the power series involved".

It is easy to see that universal formal group laws exist. To this end for the case $n = 1$ consider the ring $\tilde{L} = \mathbf{Z}[c_{ij}]$, where the c_{ij} are indeterminates and $i,j = 1,2,,\ldots$. Write $F(X,Y) = X + Y + \Sigma_{i,j \geq 1} c_{ij} X^i Y^j$. In order for the associativity relation

$F(F(X,Y),Z) = F(X,F(Y,Z))$ to hold certain relations must hold between the c_{ij}. Let I be the ideal generated by these relations and $\pi:\tilde{L} \to \tilde{L}/I$ the projection. Then $\pi_* F(X,Y)$ over $\tilde{L}/I$ is a universal formal group law. Clearly for $n>1$ a similar construction works. For abelian universal group laws one adds of course the relations $c_{ij} = c_{ji}$.

It is also easy to see that the underlying ring L is unique (up to isomorphism). Exercise: show that this follows directly from the definition of universality. It is a totally different matter to calculate L. This was first done for abelian group laws by Lazard (whence the letter L to denote it). The result is that L is a ring of polynomials.

Lazard's proof of this fact is an ingenious step by step argument, requires lots of hard calculations and gives little insight in the nature of the universal formal group itself.

8. p-TYPICAL FORMAL GROUPS

First let us deal with the case that there is so to speak only are prime number involved. A commutative formal group $F(X,Y)$ over a torsion free ring A is called *p-typical* if it is of the form $F(X,Y) = f^{-1}(f(X)+f(Y))$ with

$$f(X) = X + a_1 X^p + a_2 X^{p^2} + \dots \quad a_i \in (A \otimes \mathbf{Q})^{n\times n} \tag{8.1}$$

where as usual X^j is short for $(X_1^j,\dots,X_n^j)$. A formal group $F(X,Y)$ over an arbitrary ring A is p-typical iff there exists a torsion free ring A' with a homomorphism $\pi:A' \to A$ and a p-typical formal group $F'(X,Y)$ over A' such that $\pi_* F'(X,Y) = F(X,Y)$. There exists a better, more intrinsic definition. What a universal p-typical commutative formal group would be is clear. Though now is *not* obvious that such animals exist. They do, however.

The following fact sort of shows that one can deal with formal groups "one prime at a time" so to speak.

THEOREM 8.2. [9, Thm 20.5.1] *Let A be a torsion free ring and let $\mathbf{Z}_{(p)}$ be the ring of integers localized at the prime p. Then two commutative formal groups $F(X,Y)$, $G(X,Y)$ over A are strictly isomorphic iff they are strictly isomorphic isomorphic over $A \otimes \mathbf{Z}_{(p)}$ for all p. Also if for each p there is given an n-dimensional commutative formal group $F_{(p)}(X,Y)$ over $A \otimes \mathbf{Z}_{(p)}$ then there exist a unique (up to strict isomorphism) formal group law $F(X,Y)$ over A which for each p is strictly isomorphic to $F_{(p)}(X,Y)$ over $A \otimes \mathbf{Z}_{(p)}$.*

Also over $\mathbf{Z}_{(p)}$-algebras A (where therefore all primes except possibly p are invertible) every commutative formal group law is strictly isomorphism to a p-typical one. Proof later.

9. A UNIVERSAL p-TYPICAL FORMAL GROUP AND A FORMAL GROUP UNIVERSAL OVER $\mathbf{Z}_{(p)}$-ALGEBRAS

For simplicity let the dimension n of the formal groups in this section be $n=1$. Consider $\mathbf{Z}[V_1,V_2,V_3,\dots] = \mathbf{Z}[V] \subset \mathbf{Q}[V]$. Let $p=q$, $s_i = p^{-1}V_i$, and $\sigma:\mathbf{Q}[V] \to \mathbf{Q}[V]$ be given by $\sigma(V) = V_i^p$ and let $\mathfrak{o} = p\mathbf{Z}[V]$. Then we are in a functional equation type situation, cf. §6 above. Now let $G(X) = X$ so that $f_V(X) = f_g(X)$ is given by

$$f_V(X) = X + \sum_{i=1}^{\infty} \frac{V_i}{p^{\sigma}} \sigma^{*i} f_V(X^{p^i}) = X + a_1 X^p + a_2 X^{p^2} + \dots \tag{9.1}$$

where

$$a_1 = \frac{V_1}{p},\ a_2 = \frac{V_1 V_1^p}{p^2} + \frac{V_2}{p},\ a_3 = \frac{V_1 V_1^p V_1^{p^2}}{p^3} + \frac{V_1 V_2^p}{p^2} + \frac{V_2 V_1^{p^2}}{p^2} + \frac{V_3}{p},\dots$$

The general formula for the a_i is

$$a_m = \sum_{\substack{i_1,\dots,i_r \in \mathbf{N} \\ i_1+\dots+i_r=m}} \frac{V_{i_1} V_{i_2}^{p^{i_1}} \cdots V_{i_r}^{p^{i_1+\dots+i_{r-1}}}}{p^r} \tag{9.2}$$

and it is also not hard to prove the recursion formula

$$pa_m = V_1^{p^{m-1}} a_{m-1} + V_2^{p^{m-2}} a_{m-2} + \ldots + V_{m-1} a_1^p + V_m \tag{9.3}$$

which will be useful later.

By the functional equation lemma

$$F_V(X,Y) = f_V^{-1}(f_V(X) + f_V(Y)) \tag{9.4}$$

is a formal group law over $\mathbf{Z}[V]$. It is certainly p-typical and in fact it is a universal p-typical formal group law.

Now consider $\mathbf{Z}[T_2,T_3,\ldots] = \mathbf{Z}[T] \subset \mathbf{Q}[T]$, $p=q$, $V_i = T_{p^i}$, $s_i = p^{-1}V_i$, $\sigma(T_j) = T_j^p$, $\mathfrak{o} = p\mathbf{Z}[T]$, which is again a functional equation type situation. Also $\mathbf{Z}[V]$ above is a subring of $\mathbf{Z}[T]$ and this embedding is compatible with everything in sight. Now take

$$G(X) = \sum_{j \text{ not a power of } p} T_j X^j, \quad f_T(X) = f_g(X) = g(X) + \sum_{i=1}^{\infty} \frac{V_i}{p} \sigma^{*i} f_T(X^{p^i}) \tag{9.5}$$

Let

$$F_T(X,Y) = f_T^{-1}(f_T(X)+f_T(Y)). \tag{9.6}$$

Then, by the functional equation lemma $F_T(X,Y)$ is a formal group over $\mathbf{Z}[T]$.

THEOREM 9.7. *$F_T(X,Y)$ is universal for formal groups over $\mathbf{Z}_{(p)}$-algebras. I.e. if $F(X,Y)$ is a one dimensional commutative formal group over a $\mathbf{Z}_{(p)}$-algebra A, then there is a unique homomorphism of rings $\phi:\mathbf{Z}[T] \to A$ such that $\phi_* F_T(X,Y) = F(X,Y)$.*

Also the functional equation lemma (part (ii)) says that $F_V(X,Y)$ and $F_T(X,Y)$ are strictly isomorphic over $\mathbf{Z}[T]$ and combined with theorem 9.7 this shows that over $\mathbf{Z}_{(p)}$-algebras every formal group is isomorphic to a p-typical one (as promised).

10. CONSTRUCTION OF A UNIVERSAL FORMAL GROUP LAW

Again let us take $n=1$. Theorem (8.2), so far unproved, suggest that to find a universal formal group over a ring L one should look for a power series $f_U(X)$ which is like $f_T(X)$ for every prime p simultaneously. This turns out to be possible basically as a result of the Chinese remainder theorem. Explicitly one can proceed as follows.

10.1. For each sequence $(i_1,\ldots,i_s)$ with $i_j \in \mathbf{N} \setminus \{1\}$ choose an integer $n(i_1,\ldots,i_s)$ such that the following conditions are satisfied

(10.2) $n(i_1,\ldots,i_s) = 1$ if $s=1$

(10.3) $n(i_1,\ldots,i_s) \equiv 1 \bmod p^r$ if $i_1,\ldots,i_r$ are powers of the prime p and i_{r+1} is not a power of p $(r \leqslant s)$.

(10.4) $n(i_1,\ldots,i_s) \equiv 0 \bmod p^{r-1}$ if $i_2,\ldots,i_r$ are powers of the prime p and i_1 and i_{r+1} are not powers of the prime p.

Now define $f_U(X) \in Q[U_2,U_3,\ldots][[X]]$ by

$$f_U(X) = \sum_{n=1}^{\infty} m_n(U) X^n, \quad m_1(U) = 1, \tag{10.5}$$

$$m_n(U) = \sum_{(i_1,\ldots,i_s)} \frac{n(i_1,\ldots,i_s)}{\nu(i_1)} \frac{n(i_2,\ldots,i_s)}{\nu(i_2)} \cdots \frac{n(i_s)}{\nu(i_s)} U_{i_1} U_{i_2}^{i_1} \cdots U_{i_s}^{i_1 \cdots i_{s-1}}$$

where $\nu(j) = p$ if j is a power of the prime p and $\nu(j) = 1$ otherwise, and where the sum is over all factorizations $(i_1,\ldots,i_s)$, $i_j \in \mathbf{N} \setminus \{1\}$, $i_1 \cdots i_s = n$.

Note the family relationship with formula (9.2)

Now consider for each prime number p the functional equation situation $\mathbf{Z}_{(p)}[U] \subset \mathbf{Q}[U]$, $\mathfrak{o} = p\mathbf{Z}_{(p)}[U]$, $p=q$, $s_i = p^{-1}U_{p^i}$, $\sigma(U_j) = U_j^p$. It is not hard to check that

$$f_U(X) - \sum_{i=1}^{\infty} \frac{U_{p^i}}{p} \sigma^{*i} f_U(X^{p^i}) \in \mathbf{Z}_{(p)}[U][[X]] \tag{10.7}$$

and it follows that if

$$F_U(X,Y) = f_U^{-1}(f_U(X) + f_U(Y)) \tag{10.8}$$

then $F_U(X,Y) \in \mathbf{Z}_{(p)}[U][[X,Y]]$. This holds for all p, so that $F_U(X,Y)$ has in fact its coefficients in $\mathbf{Z}[U]$. An elegant argument due to Buhstaber and Novikov now permits to conclude that $F_U(X,Y)$ is universal as follows. Let

$$F_U(X,Y) = X+Y+\sum e_{i,j}X^iY^j,\ e_{i,j} \in \mathbf{Z}[U]. \tag{10.9}$$

For each n choose integers $\lambda_1^{(n)}, \ldots, \lambda_{n-1}^{(n)}$ such that $\lambda_1^{(n)} \begin{bmatrix} n \\ 1 \end{bmatrix} + \ldots + \lambda_{(n-1)}^{(n)} \begin{bmatrix} n \\ n-1 \end{bmatrix} = \nu(n)$. Define

$$y_n = \sum_{i=1}^{n-1} \lambda_i^{(n)} e_{i,n-1} \tag{10.10}$$

Observe that $y_n \equiv U_n \mod(U_2,\ldots,U_{n-1})$ so that the $y_2,y_3,\ldots$ form a free polynomial basis of $\mathbf{Z}[U]$. Now let $G(X,Y)$ over A be any one-dimensional commutative formal group.

$$G(X,Y) = X+Y+\sum a_{ij}X^iY^j. \tag{10.11}$$

Define $\phi:\mathbf{Z}[U] \to A$ by requiring that

$$\phi(y_n) = \sum_{i=1}^{n-1} \lambda_i^{(n)} a_{i,n-1}. \tag{10.12}$$

This is well defined because the $y_2,y_3,\ldots$ form a free polynomial basis for $\mathbf{Z}[U]$. We now claim that $\phi(e_{i,j}) = a_{i,j}$ for all $i,j \geqslant 1$. This is proved by induction starting with the case $i=j=1$ which is trivial because $y_2 = e_{1,1}$. Now suppose that $\phi(e_{i,j}) = a_{i,j}$ for all $i,j \geqslant 1, i+j < n$. Now because $F(X,Y), G(X,Y)$ are commutative formal group laws the coefficients $e_{i,j}$ and $a_{i,j}$ must satisfy certain conditions, viz.

$$a_{i,j} = a_{j,i},\ e_{i,j} = e_{j,1} \tag{10.13}$$

$$p_{ijk}(e_{l,m}) = 0,\ p_{ijk}(a_{l,m}) = 0 \tag{10.14}$$

where the p_{ijk} are certain universal polynomials expressing associativity. There is one such polynomial for each triple (i,j,k), $i,j,k \in \mathbf{N}$. And of course $p_{ijk} = 0$ expresses the equality of the coefficients of $X^iY^jZ^k$ on both sides of the identity $F(F(X,Y),Z) = F(X,F(Y,Z))$. It follows that these polynomials (in the indeterminates $C_{l,m}$) are of the form

$$\begin{bmatrix} i+j \\ i \end{bmatrix} C_{i+j,k} - \begin{bmatrix} j+k \\ j \end{bmatrix} C_{i,j+k} - q_{ijk}(C_{l,m}) \tag{10.15}$$

with q_{ijk} a polynomial involving only $C_{l,m}$ with $l+m < i+j+k$. We now need the nontrivial

Binomial coefficient lemma 10.16.
Each $C_{r,s} = C_{s,r}$, $r+s = n$ can be written as an integral linear combination of the expressions

$$\lambda_1^{(n)} C_{1,n-1} + \ldots + \lambda_{n-1}^{(n)} C_{n-1,1}$$

$$\begin{bmatrix} i+j \\ i \end{bmatrix} C_{i+j,k} - \begin{bmatrix} k+j \\ j \end{bmatrix} C_{k+j,i},\ i,j,k \geqslant 1,\ i+j+k = n.$$

Now by induction $\phi(Q_{ijk}(e_{l,m})) = Q_{ijk}(a_{l,m})$. Also $\phi(\lambda_1^{(n)} e_{1,n-1} + \ldots + \lambda_{n-1}^{(n)} e_{n-1,1}) =$

$\lambda_1^{(n)}a_{1,n-1}+\ldots+\lambda_{n-1}^{(n)}a_{n-1,1}$ by definition. Thus by (10.14) and 10.16 $\phi(e_{i,j}) = a_{i,j}$ for all $i+j = n$. This concludes the proof of the universality of $F_U(X,Y)$.

This is quite considerably easier than Lazard's original arguments. Especially in the more dimensional case where in this approach the generalizations are easy while Lazard's method becomes almost impossible to handle [11]. On the other hand I think it quite unlikely that I would have been able to guess at the form of $F_U(X,Y)$ without Lazard's original work. And of course it is crucial to this approach to have a (reasonably explicit) candidate universal formal group law available.

As constructed the universal formal group law $F_U(X,Y)$ has a logarithm, viz $f_U(X)$. It follows, because $F_U(X,Y)$ is universal, that logarithms exist for all formal groups defined over torsion free rings.

Also $f_U(X)$ is of functional equation type. Thus every logarithm has this sort of structure. That is it looks as if it were constructed by means of a functional equation type recursion scheme. Though, of course, the construction itself often does not apply simply because, e.g., there may very well be no endomorphism σ satisfying $\sigma(a) \equiv a^q$ mod a suitable ideal.

11. Applications to algebraic topology

Let MU^* be the generalized cohomology theory defined by the complex cobordism spectrum MU. This theory is complex oriented (i.e. has Chern classes) and hence gives rise to a formal group over $MU^*(pt)$.

Theorem 11.1. (Quillen). *The formal group law $F_{MU}(X,Y)$ of complex cobordism is universal.*

Theorem *11.2.* (Miscenko). *The logarithm, cf. §5, of the formal group law of complex cobordism is equal to*

$$\log F_{MU}(X) = \sum_{n=0}^{\infty} \frac{[\mathbf{CP}^n]}{n+1} X^{n+1} \tag{11.3}$$

where $[\mathbf{CP}^n]$ is the complex cobordism class of complex projective n-space.

We now have two universal formal groups laws, $F_{MU}(X,Y)$ and the one just constructed above. It follows that there are mutually inverse ring isomorphisms $\phi:\mathbf{Z}[U] \to MU^*(pt), \psi:MU^*(pt), \to \mathbf{Z}[U]$ taking these formal group laws into each other. In particular the $\phi(U_2),\phi(U_3),\ldots$ form a polynomial basis of $MU^*(pt)$ which can be calculated in terms of the $[\mathbf{CP}^n]$ because we know $\log F_{MU}(X)$ and the relations between the $U_2, U_3,\ldots$ and the coefficients of $f_U(X)$.

The resulting formulas become especially nice is we concentrate on one prime only (because the structure of the particular p-typical universal group $F_V(X,Y)$ is so especially pleasant). Topologically this is done as follows. By smashing the spectrum MU with a suitable Moore space all primes except p are inverted yielding the cohomology theory $MU^* \otimes \mathbf{Z}_{(p)}$. The spectrum $MU \otimes \mathbf{Z}_{(p)}$ splits as a wedge sum of suspensions of the socalled Brown-Peterson spectrum BP. This one, "therefore", defines a complex oriented cohomology theory BP^* whose associated formal group is the p-typification of $F_{MU}(X,Y)$ which means that the logarithm of $F_{BP}(X,Y)$ is obtained from $\log F_{MU}(X)$ by simply removing all terms not involving X to the power a power of p. (The functional equation lemma says that this procedure again yields a formal group). Also it follows that $F_{BP}(X,Y)$ must be a universal p-typical formal group.

Thus

$$\log F_{BP}(X) = \sum_{n=0}^{\infty} m_n X^{p^n}, \; m_n = p^{-n}[\mathbf{CP}^{p^n-1}]. \tag{11.4}$$

Both F_{BP} and F_V of §10 above are p-typically universal. So, again, there is a ring isomorphism $\phi:\mathbf{Z}[V] \to BP^*(pt)$ taking $f_V(X)$ into $\log F_{BP}(X)$. And, again there result formulas for a set of free

polynomial generators for $BP^*(pt)$, the $\phi(V_i) = v_i$, in terms of the known elements $m_i \in BP^*(pt)$. The result is that

$$BP^*(pt) = \mathbf{Z}_{(p)}[v_1, v_2, \ldots], \; pm_n = v_1^{p^{n-1}} m_{n-1} + v_2^{p^{n-2}} m_{n-2} + \ldots + v_{n-1} m_1^p + v_n \tag{11.5}$$

cf. formula (9.3). Because $F_V(X,Y)$ is in fact defined over $\mathbf{Z}[V]$, not just $\mathbf{Z}_{(p)}[V]$ (though the p-typification isomorphism $F_U \approx F_V$ is of course only defined over $\mathbf{Z}_{(p)}[U]$, $V_i = U_{p^i}$) there is the added bonus that the v_i are in fact integral, i.e. in $MU^*(pt)$, i.e. real cobordism classes of manifolds (not just element of $MU^*(pt) \otimes \mathbf{Z}_{(p)}$).

The generators $v_1, v_2, \ldots$ of $BP^*(pt)$ have found numerous applications in algebraic topology in the hands of S. Araki, W. Steven Wilson, Douglas Ravenel, Haynes Miller, P. Landweber, J. Morava, D.C. Johnson, Larry Smith, R. Zahler, Z. Yoshimura, M. Kamata, K. Shimakawa, N. Yagita, H. Yasumasa, K. Shibata, N. Shimada, P.B. Shay, U. Würgler a.o.; they permit one, so to speak, to calculate with BP-cohomologY.

There are also other ways (than constructing an explicit universal formal group law) to obtain the generators due to S. Araki and J. Kozma. The first one to guess at a formula like (11.5) for the generators (but different) for the prime 2 was A. Liulevicius. Formal groups are now a most useful and well-established tool in algebraic topology. The papers of the authors already quoted and the lecture notes by Adams or Araki and the Helsinki lecture of D.C. Ravenel are good starting points.

12. Atkin-Swinnerton Dyer congruences

Let E be an elliptic curve over $\mathbf{Q}$. There then exist an essentially unique minimal model of E over $\mathbf{Z}$ (i.e. an equation with coefficients in $\mathbf{Z}$ defining E) of the form $Y^2 + c_1XY + c_3Y = X^3 + c_2X^2 + c_4X + c_6$. For this model one can reduce modulo p to obtain curves over $\mathbf{F}_p$ for each p. One defines the global Artin L-series of E by the formula

$$L(s,E) = \prod_p L_p(s) = \sum_n c_n n^{-s} \tag{12.1}$$

where

(i) If $E \otimes \mathbf{F}_p$ is nonsingular, $L_p(s) = (1 - a_p p^{-s} + p^{1-2s})^{-1}$ where $1 - a_pX + pX^2$ is the numerator of the zeta function of $E \otimes \mathbf{F}_p$.

(ii) If $E \otimes \mathbf{F}_p$ has an ordinary double point, $L_p(s) = (1 - \epsilon_p p^{-s})^{-1}$ with $\epsilon_p = +1$ or -1 depending on whether the tangent at the double point are rational over $\mathbf{F}_p$ or not.

(iii) If $E \otimes \mathbf{F}_p$ has a cusp, $L_p(s) = 1$.

To E one now associates a commutative one-dimensional formal group F_E with logarithm

$$f_E(X) = \sum_{n=1}^{\infty} n^{-1} c_n X^n. \tag{12.2}$$

It is an immediate consequence of the functional equation lemma that F_E has its coefficients in $\mathbf{Z}$.

There is a second formal group attached to E viz. the formal completion along the identity (cf. §0 above) of its minimal model over $\mathbf{Z}$. This one can be explicity described as follows. Lert $z = X/Y$ be a local parameter at the zero element. Now $\omega = dY/2Y + c_1X + c_3$ is the invariant differential on E. Develop ω locally around the zero element in powers of z to find an expression

$$\omega = \sum_{n=1}^{\infty} \beta_n z^{n-1} dz, \quad \beta_1 = 1. \tag{12.3}$$

The logarithm of the formal completion G_E along the identity of E is now equal to

$$G_E(X) = \sum_{n=1}^{\infty} n^{-1} \beta_n X^n. \tag{12.4}$$

THEOREM 12.5. (Honda). *The formal groups $F_E(X,Y)$ and $G_E(X,Y)$ over* $\mathbf{Z}$ *are strictly isomorphic over* $\mathbf{Z}$.

However $F_E(X,Y)$ is a functional equation type formal group. Any strictly isomorphic formal group must therefore, according to part (iii) of the functional equation lemma, satisfy the same functional equation type integrality relations. This yields

$$\beta_{np} - a_p\beta_n + pb_p\beta_{n\|p} \equiv 0 \mod p^s \text{ if } n \equiv 0 \mod p^{s-1} \tag{12.6}$$

where $\beta_{n\|p} = 0$ if $(p,n) = 1$ and $\beta_{n\|p} = \beta_{n/p}$ if $p \mid n$, and where a_p, b_p are defined by $1 - a_p p^{-s} + b_p p^{1-2s} = L_p(s)^{-1}$, cf. just below (12.1) and above. These are the Atkin-Swinnerton Dyer congruences (originally the Atkin- Swinnterton Dyer conjectures) which were originally discovered numerically.

13. THE WITT VECTORS

For each $n = 1,2,\ldots$ let $w_n(X_1,\ldots,X_n)$ be the polynomial

$$w_n(X) = \sum_{d \mid n} dX_d^{n/d}. \tag{13.1}$$

THEOREM 13.2. *There is a unique functor W:Ring $\to$ Ring which satisfies the following properties:*

(i) *As a functor* **Ring** $\to$ **Set**, $W(A) = \{(a_1,a_2,a_3,\ldots): a_i \in A\}$ *and* $W(\phi)(a_1,a_2,\ldots) = (\phi(a_1),\phi(a_2),\ldots)$ *for* $\phi: A \to B$ *in* **Ring**.

(ii) $w_{n,A}: W(A) \to A$, $w_{n,A}(a_1,a_2,\ldots,) = w_n(a_1,\ldots,a_n)$ *is a functorial ring homomorphism for every* $n = 1,2,\ldots$.

Moreover

(iii) *The functor W admits functorial ring homomorphisms* $\mathbf{f}_n: W(A) \to W(A)$ *which are uniquely characterized by* $w_m\mathbf{f}_n = w_{nm}$, $n,m \in \mathbf{N}$

(iv) *There is a functdorial homomorphism of rings* $\Delta: W(-) \to W(W(-))$ *characterized uniquely by* $w_{n,W(A)}\Delta_A = \mathbf{f}_{n,A}$ *for all n and* $A \in$ **Ring**

(v) *There are functorial endomorphisms of abelian groups* $\mathbf{V}_n: W(-) \to W(-)$ *characterized by* $w_n V_m = w_{n\,|\,m}$ *if* $m \mid n$ *and* $w_n V_m = 0$ *if* $m \nmid n$.

This is probably the most efficient way to introduce the Witt vectors, especially if the proofs of these statements are omitted. As a matter of fact the first thing to prove is that the polynomials defining the addition in $W(A)$: $(a_1,a_2,\ldots)+(b_1,b_2,\ldots) = (\Sigma_1(a,b),\Sigma_2(a,b),\ldots)$ which means $W_n(\Delta_1,\Delta_2,\ldots) = w_n(X)+w_n(Y)$ (by (iii)), have coefficients in $\mathbf{Z}$. This we have already done in §6 above. The other statements of 13.2 above (which basically are all integrality statements concerning various polynomials) can also be dealt with using various functional equation lemma tricks (cf. [9,Ch.III].

Anotherd good way (and more "classical") to get at W is as follows. Define $\Lambda(A) = \{1+a_1t+a_2t^2+\ldots: a_i \in A\}$. Multiplication of these formal power series with constant term 1 defines a functorial abelian group structure on $\Lambda(A)$. Now write formally $a(t) = 1+a_1t+\ldots = \Pi_i(1-\xi_i t)$. A multiplication on $\Lambda(A)$ is now defined by $a(t)*b(t) = \Pi_{i,j}(1-\xi_i\eta_j t)$ if $b(t) = \Pi_j(1-\eta_j t)$. When this product is written out the coefficients of the t^n are symmetric in the ξ's and η's and therefore can be written as polynomials in the a_i and b_j. This defines a functorial ring structure on $\Lambda(A)$. The endomorphisms $\mathbf{f}_n$ and $\mathbf{V}_n$ are defined by

$$\mathbf{f}_n(\prod_i(1-\xi_i t) = \prod_i(1-\xi_i^n t), \quad \mathbf{V}_n a(t) = a(t^n). \tag{13.3}$$

Define $s_n: \Lambda(A) \to A$ by the formula

$$\sum_{n=1}^{\infty} s_n(a(t))t^n = -t\frac{d}{dt}\log a(t) \tag{13.4}$$

so that e.g. $s_n(\prod_i(1-\xi_i t)) = \sum_i \xi_i^n$. It is now easy to check that the functor Λ:**Ring** $\to$ **Ring** together with the functor morphisms $s_n:\Lambda(A) \to A$ satisfies properties completely analogous to those claimed for $(W, w_1, w_2, \ldots)$ in Theorem 13.2 parts (i),(ii),(iii),(v). (Part (iv), (souped-up Hasse-Witt exponential) is more difficult to get at).

The connection between Λ and W is given by the functorial isomorphism $E: W(A) \to \Lambda(A), (a_1, a_2, \ldots) \mapsto \prod_i(1-a_i t^i)$

Indeed,

$$-t\frac{d}{dt}\log\prod_i(1-a_i t^i) = -t\frac{d}{dt}\sum log(1-a_i t^i) =$$

$$= -t\sum_i \frac{-ia_i t^{i-1}}{1-a_i t^i} = \sum_i ia_i t^i(1+a_i t^i + a_i^2 t^{2i} + \ldots) = \sum_{i,j} ia_i^j t^{ji}$$

$$= \sum_n \sum_{i|n} ia_i^{n/i} t^n = \sum_n w_n(a) t^n.$$

Exercise 13.5.
Check everything that needs checking to prove theorem 13.2 minus part (iv).

14. Curves, Frobenius and Verschiebung

Now let again $F(X, Y)$ be an n-dimensional commutative formal group over a ring A. By definition the group of curves $C(F)$ of F is as a set equal to the set of all n-tuples of power series $\lambda(t)$ with coefficients in A with zero constant term. Two curves are added by the formula

$$\gamma(t) +_F \delta(t) = F(\gamma(t), \delta(t)) \tag{14.1}$$

which makes perfect sense. This turns $C(F)$ into a group. There is a topology of $C(F)$ defined by the subgroups $C_m(F)$ consisting of all curves $\gamma(t) = (\gamma_1(t), \ldots, \gamma_n(t))$ such that the first m coefficients of each of the $\gamma_j(t)$ are zero. With this topology $C(F)$ is a complete topological group.

There are a number of operators defined on $C(F)$. The first two kinds are

$$\text{(homotheties) } <a>\gamma(t) = \gamma(at) \tag{14.2}$$

$$\text{(Verschiebung) } \mathbf{V}_n\gamma(t) = \gamma(t^n). \tag{14.3}$$

The group $C(F)$ also has a sort of topological freeness property. The precise statement is that there are elements $\epsilon_1(t), \ldots, \epsilon_n(t) \in C(F)$, e.g. $\epsilon_1(t) = (t, 0, \ldots, 0), \ldots, \epsilon_n(t) = (0, \ldots, 0, t)$ such that each element of $C(F)$ can be uniquely written as a convergent series

$$\sum_{i,j} \mathbf{V}_i <a_{ij}> \epsilon_j(t).$$

Such a basis $\epsilon_1(t), \ldots, \epsilon_n(t)$ is called a Vbasis. All this is perfectly simple and uses little more than that $F(X, Y) = X + Y +$ (higher degree) (and the group property).

The third kind of operator is

$$\text{(Frobenius) } \mathbf{f}_n\gamma(t) = \gamma(\zeta_n t^{1/n}) +_F \cdots +_F \gamma(\zeta_n^n t^{1/n}) \tag{14.4}$$

where ζ_n is a primitive n-th root of unity. This is then (symmetric functions!) a power series in t (not just one in $t^{1/n}$). A little care must be taken in interpreting this formula as roots of unity do not always make sense in the right way over all rings A. But things can be made precise fairly simply (in various ways).

Of course the $\mathbf{V}_m, \mathbf{f}_n$ are rather different things then the $\mathbf{V}_m, \mathbf{f}_n$ of §13 just above. However

14.5. Exercise. Show that the abelian groups with operators $(W(A), \mathbf{V}_m, \mathbf{f}_n)$ *and* $C(\mathbf{G}_m), \mathbf{F}_m, \mathbf{f}_n)$ *are isomorphic, where* $\mathbf{G}_m$ *is the one-dimensional formal group* $X + Y + XY$ *over* A.

Still, it would have been better, logically speaking, not to use the same symbols, and machines would certainly object. Humans however are able to live with such ambiguities and seem even to thrive on them.

There are a rather large number of relations between the various operators on $C(F)$:

$$<a><a'> = <aa'> \tag{14.6}$$

$$<1> = \mathbf{V}_1 = \mathbf{f}_1 = id \tag{14.7}$$

$$\mathbf{V}_m\mathbf{V}_n = \mathbf{V}_{mn} \tag{14.8}$$

$$\mathbf{f}_m\mathbf{f}_n = \mathbf{f}_{mn} \tag{14.9}$$

$$<a>\mathbf{V}_m = \mathbf{V}_m<a^m> \tag{14.10}$$

$$\mathbf{f}_m<a> = <a^m>\mathbf{f}_m \tag{14.11}$$

$$\text{if } (n,m) = 1,\ \mathbf{f}_n\mathbf{V}_m = \mathbf{V}_m\mathbf{f}_n \tag{14.12}$$

$$\mathbf{f}_n\mathbf{V}_n = [n] \tag{14.13}$$

$$<a>+<b> = \sum_{n=1}^{\infty} \mathbf{V}_n<r_n(a,b)>\mathbf{f}_n. \tag{14.14}$$

Here $[n]$ stands for the operator $\gamma(t) \mapsto \gamma(t) +_F \gamma(t) +_F \ldots +_F \gamma(t)$ (n summands) and the $r_n(Z_1, Z_2)$ are certain universal polynomials in two variables Z_1, Z_2 defined by

$$Z_1^n + Z_2^n = \sum_{d \mid n} d r_d(Z_1, Z_2)^{n/d}. \tag{14.15}$$

(Note that the right hand side of (14.15) is equal to $w_n(r_1, \ldots, r_n)$. Now $w_n(\Sigma_1, \ldots, \Sigma_n) = w_n(X) + w_n(Y)$ where the $\Sigma_1, \ldots, \Sigma_n$ are the addition polynomials of the Witt vectors; thus $r_d(Z_1, Z_2) = y\Sigma_d(Z_1, 0, \ldots, 0; Z_2, 0, \ldots, 0)$ and hence has integral coefficients).

15. CART(A)

Basically the Cartier-Dieudonné classification theorem for commutative formal groups laws over a ring A states that $F \mapsto C(F)$ is an equivalence of categories between formal groups over A and filtered complete topological groups with operators $<a>, \mathbf{V}_n, \mathbf{f}_n$ satisfying all the relations (14.6)-(14.14) and such that $C(F)$ is "topologically free" in the sense that it admits a V-basis in the sense of §14 above. This theorem extends to include infinite dimensional commutative formal groups.

It is more elegant to collect all the operators in one ring, first described by LAZARD [12] and called *Cart*(A) by him after Cartier. This is the ring of all formal expressions of the form

$$\sum_{m,n=1}^{\infty} \mathbf{V}_m<a_{mn}>\mathbf{f}_n, \quad a_{m,n} \in A \tag{15.1}$$

with the support condition: for all $m \in \mathbf{N}$ there are only finitely $a_{m,n} \neq 0$. The "calculation rules" (14.6)-(14.14) now describe *Cart* (A) completely as a topological ring with the topology defined by the ideals M_l consisting of all expressions (15.1) for with $a_{m,n} = 0$ for all $m \leqslant l$.

16. CARTIER-DIEUDONNEO' CLASSIFICATION THEORY

The topological group of curves $C(F)$ of a formal group over A can now by means of the operations $<a>, \mathbf{f}_n, \mathbf{V}_m$ be seen as a topological module over the (noncommutative topological ring *Cart*(A). They have special properties as *Cart*(A) modules, viz. the following

(16.1)If $(X_i)_{i\in I}$ is a set of elements in *Cart*(A) converging to zero for the filter of finite subsets of I and $(\gamma_i)_i \in I$ is any set of elements of the *Cart*(A)-module C then $(X_i\gamma_i)_{i\in I}$ converges in C.

(16.2)For each $n \in \mathbf{N}$ let C^n be the closure of the sum of all subgroups $\mathbf{V}_i C$ for $i \geqslant n$. Then the C^n define the topology of C.

(16.3)$\mathbf{V}_m : C = C^1 \to C^m$ induces a bijection $C^1 / C^2 \xrightarrow{\sim} C^m / C^{m+1}$

(16.4)C^1 / C^2 is a free A-module (for the operators induced by the $<a>$)

Let us call such *Cart*(A)-modules *reduced.* The Cartier-Dieudonné classification theory as formulated by Lazard now is summed up in

THEOREM 16.5. *The functor $F \mapsto C(F)$ of commutative formal groups over A to reduced Cart(A) modules (with continuous Cart(A)-module morphisms as morphisms), is an equivalence of categories.*

17. P-TYPIFICATION

The ring Cart(A) is a complicated object and so is a reduced *Cart*(A)-module. So there is lots of room for special cases and easier to use classification results. A first substantial simplification occurs if one limits oneself to "one prime at a time", i.e. formal groups over rings A which are $\mathbf{Z}_{(p)}$-algebras. Then $C(F)$ splits as a direct sum of copies of the group of socalled p-typical curves $C_p(F)$. For a torsion free $\mathbf{Z}_{(p)}$-algebra A these are the curves such that $\log_F(\gamma(t))$ is of the form $\sum c_i t^{p^i}$; for arbitrary $\mathbf{Z}_{(p)}$-algebras A a definition similar to the one used in §8 works. The topological group $C_p(F)$ is a module over a ring $Cart_p(A)$ which is just like *Cart*(A) except that only the $\mathbf{V}_p^m = \mathbf{V}_{p^m}$ and $\mathbf{f}_p^m = \mathbf{f}_{p^m}$ occur. *Cart*(A) is a ring of infinite matrices over $Cart_p(A)$ in this case. The rules of calculation of $Cart_p(A)$ are obtained from those of *Cart*(A) by setting $\mathbf{V}_n = \mathbf{f}_n = 0$ if n is not a power of p.

Now let $A = k$ be an algebraically closed field of characteristic $p > 0$. Let $R = W_{p^\infty}(k)$ be the unramified discrete valuation ring with residue field k. The ring $W_{p^\infty}(k)$ is the quotient of $W(k)$ by the ideal of all $(b_1, b_2, b_3, \ldots) \in W(k)$ such that $b_i = 0$ if i is not a power of p. It follows that as a set $W_{p^\infty}(k) = \{(a_0, a_1, \ldots) : a_i \in k\}$ (with so to speak $a_i = b_{p^i}$) and its ring structure is given by the polynomials $w_{p,n} = w_{p^n}$ in $X_{p^0}, X_{p^1}, \ldots, X_{p^n}$ in the same way as the ring structure of $W(-)$ is determined by the w_n. The quotient $W_{p^\infty}(-)$ admits the endomorphisms $\mathbf{f}_p$ and $\mathbf{V}_p$ here denoted σ and ρ in order not to confuse them with the operators $\mathbf{f}_p$ and $\mathbf{V}_p$ on $C_p(F)$. (The other Frobenius and Verschiebung morphisms of $W(-)$ do not descend).

The map

$$(a_0, a_1, a_2, \ldots) \mapsto \sum \mathbf{V}_p^i <a_i> \mathbf{f}_p^i \tag{17.1}$$

defines an embedding (of topological rings), $W_{p^\infty}(k) \hookrightarrow Cart_p(k)$. Now define the Dieudonné ring $D(k)$ as the ring $W_{p^\infty}(k)[\mathbf{f}, \mathbf{V}]$ of twisted polynomials in $\mathbf{f}$ and $\mathbf{V}$ over $W_{p^\infty}(k)$ subject to the relations

$$\mathbf{fV} = \mathbf{Vf} = p, \quad x\mathbf{V} = \mathbf{V}x^\sigma, \quad \mathbf{f}x = x^\sigma \mathbf{f} \tag{17.2}$$

where σ is the Frobenius endomorphism of $W_{p^\infty}(k)$. Under the identification $\mathbf{f} \mapsto \mathbf{f}_p$ and $\mathbf{V} \mapsto \mathbf{V}_p$, $D(k)$ becomes a dense subring of $Cart_p(k)$ and in this way one recovers a version (a covariant one) of Dieudonnés original classification of commutative formal groups over algebraically closed fields of characteristic $p > 0$, by means of certain modules over $D(k)$.

Localization with respect to $\mathbf{V}$ turns $D(k)$ into a ring of twisted Laurent series in $\mathbf{V}$ with coefficients in $W_{p^\infty}(k)$ and isomorphism classes of finitely generated torsion modules over this ring turn out to correspond to isogeny classes of formal groups over k. These torsion modules can be classified and there results the classification theorem that every formal group over k is isogeneous to an up to isogeny unique direct sum of explicitly given formal groups $G_{n,m}(X, Y)$,

$1 \leqslant n \leqslant \infty$, $0 \leqslant m \leqslant \infty$,$(n,m) = 1$. (A homorphism $\alpha: F \to G$ between formal groups over k of the same dimension with finite kernel is called an isogeny. And isogeny is the weakest equivalent relation with identifies F and G in such a case).

18. Other classification results

Classification by means of $Cart_p(A)$ modules still leaves plenty of room for interesting and useful special cases, and so does classification by means of $D(k)$ modules (i.e. Dieudonné modules) for k an algebraically closed field of characteristic $p > 0$.

Let k be a field of characteristic $p > 0$, and F a commutative formal group over k. Consider the ring homomorphism $[p]_F: k[[X]] \to k[[X]]$, $X \mapsto [p]_F(X)$, where $[1]_F(X) = X$, $[n]_F(X) = F(X, [n-1]_F(X))$. The formal group F is said to be a finite height if $[p]_F$ makes $k[[X]]$ a finite rank module over itself. This rank is then necessarily a power p^h of the prime p and h is called the height of F.

Exercise 18.1.
If F is one dimensional the height of F is equal to h iff $F(X,Y) \equiv X + Y + aC_{p^h}(X,Y)$ mod degree $p^h + 1$ for some $a \neq 0$ in k. Thus the formal groups $F_h(X < Y)$ over $\mathbf{F}_p$ described in §6 above are of height h.

Theorem 18.2.
(Lazard [10]). *Let k be an algebraically closed field of characteristic $p > 0$. Then the one dimensional formal groups laws over k are classified by their heights h, $1 \leqslant h \leqslant \infty$ ($h = \infty$ corresponds to $F \approx \mathbf{G}_a$).*

Now let k be a finite field, say $\mathbf{F}_q$. The first result is that over $\bar{k} = \mathbf{F}_{p^\infty}$, the algebraic closure of $k = \mathbf{F}_q$ the ring of endomorphisms is E_h the ring of integers of the division algebra D_h over $\mathbf{Q}_p$ of rank h^2 and invariant h^{-1}.

A very special endomorphism of each F over $\mathbf{F}_q$ is $\xi_F(X) = X^q$, the "Frobenius endomorphism". $End_k(F)$ consists of those elements in E_h which commute with ξ_F and it results that $End_k(F)$ is the ring of integers of a central division algebra of rank h^2/m^2 and invariant m/h over $\mathbf{Q}_p(\xi_F)$ with $m = [\mathbf{Q}_p(\xi_F):\mathbf{Q}_p]$. The "Frobenius endomorphism" ξ_F satisfies an equation over the maximal unramified extension of $\mathbf{Q}_p$ contained in $\mathbf{Q}_p(\xi_F)$ and this gives a polynomial over $W_{p^\infty}(k)$

$$\Psi_F(\xi_F) = 0, \quad \Psi_F(X) = X^e + b_1 X^{e-1} + \ldots + b_e \tag{18.3}$$

with the properties

(18.4) $\Psi_F(X)$ is a polynomial over $W_{p^\infty}(\mathbf{F}_q)$ which is irreducible over the quotient field $W_{p^\infty}(\mathbf{F}_q) \otimes \mathbf{Q}_p = K_q$

(18.5) If ξ is a root of $\Psi_F(X)$, then $\mathbf{Q}_p(\xi)/K_q$ is totally ramified

(18.6) $[\mathbf{Q}_p(b_1,\ldots,b_e):\mathbf{Q}_p]v_p(b_e)$ divides r where $q = p^r$ and v_p is the normalized exponential valuation on K_q.

$\Psi_F(X)$ is called the characteristic polynomial of the one dimensional formal group F. It now turns out (Honda) that these polynomials classify finite height one dimensional formal groups over finite fields.

The classification results of this section can be deduced from the general theory described in §17 above but can in fact be easier handled by various other more direct means (often involving the functional equation lemma).

19. CARTIER'S FIRST THEOREM

The infinite dimensional formal group law $\hat{W}(X,Y)$ plays a very special role in formal group theory. Part of the reason is

19.1. Cartier's first theorem.
Let $\gamma_0(t) \in C(\hat{W})$ *over a ring* A *be the curve* $(t,0,0,\ldots,0)$. *Then for each curve* $\gamma(t)$ *of a commutative formal group* F *over* A *there exists a unique homomorphism of formal groups* $\alpha_\gamma : \hat{W} \to F$ *such that* $C(\alpha_\gamma)(\gamma_0(t)) = \gamma(t)$.

Thus the functor $F \mapsto C(F)$ of formal groups over A to *Cart*(A) modules is represented by the formal group $\hat{W}$.

20. $U(\hat{W})$

As befits such an important and special object as the formal group of Witt vectors its covariant bialgebra is very nice

THEOREM 21.1. $U(\hat{W}) = \mathbf{Z}[Z_1,Z_2,\ldots]$ *as a* $\mathbf{Z}$*-algebra and the comultiplication is given by* $Z_n \mapsto \Sigma_{i+j=n} Z_i \otimes Z_j$ *with* $Z_0 = 1$.

On the other hand $\hat{W}$, as the notation suggests, is the formal completion of the group valued functor $A \mapsto W(A)$ of the big Witt vectors and via the isomorphism $W(A) \tilde{\to} \Lambda(A) = \{1 + a_1 t + a_2 t^2 + \ldots : a_i \in A\}$ is represented by the algebra $R(W) = \mathbf{Z}[X_1,X_2,\ldots]$. The addition is given by the polynomials $\Sigma_n'(X,Y) = \Sigma_{i+j=n} X_i Y_j$, $X_0 = Y_0 = 1$. That is by the comultiplication $X_n \mapsto \Sigma_{i+j=n} X_i \otimes X_j$ on $R(W)$. This is the "same" object as $U(\hat{W})$.

This "accident" is in fact an autoduality which can be understood in terms of the representation property 19.1 of $\hat{W}$ and Cartier-duality.

All this makes $U \approx U(\hat{W}) \approx R(W) \approx \cdots$ a remarkable object which certainly deserves deeper study, especially because it also occurs in still other guises in various parts of algebra such as the universal λ-ring in one generator, the ring of representations $\bigoplus_n R(S_n)$, where is S_n the symmetric group on n-letters, and the cohomology ring $H^*(BU;\mathbf{Z})$, where BU is the classifying space for complex vector bundles. The study and understanding of U in its various guises is (and has been for a number of years) a (slowly evolving) research project of mine.

21. REMARKS ON NONCOMMUTATIVE FORMAL GROUP THEORY

So far I have talked almost exclusively about commutative formal groups and moreover have concentrated on the phenomena which occur away from these objects over (algebraically closed) fields of characteristic zero. Naturally, because over a field of characteristic zero commutative formal groups are not interesting. That changes of course if one admits noncommutative formal groups and one subject one could pursue is to develop for say, noncommutative formal groups over algebraically closed fields (of any characteristic), all the possible analogues of (ordinary) (algebraic) Lie group and group theory. Much can be done and substantial amounts have been done, cf. [7].

Very little on the other hand is really known about noncommutative formal groups in terms of the kind of questions discussed in these lectures. E.g. about universal noncommutative formal groups of various kinds. We have of course the formal Lie theorem (over a $\mathbf{Q}$-algebra Lie algebras and formal groups are equivalent categories) and there are Lazard's cohomological results on the extension (prolongation) of noncommutative formal group chunks [11]. (A polynomial $F(X,Y)$ of total degree n in $2m$ variables is a formal Lie group chunk of degree n if the conditions $F(X,F(Y,Z)) = F(F(X,Y),Z), F(X,0) = X, F(0,Y) = Y$ hold mod degree $n+1$; a prolongation of

F_n is an F_{n+1} which is an $n+1$-chunk such that $F_{n+1} \equiv F_n$ mod(degree $n+1$)). For commutative chunks F_n extensions always exist and this is the original basis of Lazard's step by step power series approach; for noncommutative chunks this is not necessarily true (except over $\mathbf{Q}$-algebras as LAZARD proves [11]). E.g. the p^2+p chunk $X+Y+X^pY^{p^2}$ does not prolong to a 1-dimensional noncommutative formal group over any field of characteristic p. It seems to me that a judicious mix of the Campbell- Hausdorff-Baker formula with the functional equation formulas could give interesting results (using of course that there are also logarithms in the noncommutative case because of formal Lie theory, cf. §3 above)

A totally different approach is based on the following idea. Because of theorems 21.1 and 19.1 the classifying object $C(F)$ of curves in a commutative formal group can be obtained as the bialgebra homomorphisms $U \to U(F)$, where $U = U(\hat{W})$.

Now there is a very natural noncommutative generalization of the object U namely the noncommutative but cocommutative algebra

$$U_{nc} = \mathbf{Z}\langle Z_1, Z_2, \ldots \rangle, \quad Z_n \mapsto \sum_{i+j=n} Z_i \otimes Z_j, \quad Z_0 = 1$$

of all associative polynomials in $Z_1, Z_2, \ldots$ with the same comultiplication as U.

One can now study the functor $F \mapsto BiAlg(U_{nc}, U(F))$ and the object U_{nc} itself and try to find suitable noncommutative analogous of p-typification, Frobenius and Verschiebung operators, Cartier-Dieudonné modules,... . Substantial progress in this direction has been made by DITTERS [8].

REFERENCES

[1] ARAKI, S., *Typical formal groups in complex cobordism and K-theory,* Lect. Math. Kyoto Univ. **6,** Kinokuniya Book Store, 1973.

[2] BOCHNER, S., *Formal Lie groups,* Ann. of Math. **47** (1946), 192-201.

[3] CARTIER, P., *Groupes algèbriques et groupes formels. Dualité,* Coll. sur la théorie des groupes algèbriques, Bruxelles, 1962, CBRM, 87-112.

[4] CARTIER, P., *Groupes formels associés aux anneaux de Witt generalisés,* CR Acad. Sci. Paris **265** (1967), A50-A52.

[5] CARTIER, P., *Modules associés à une groupe formel commutatif. Courbes typiques,* CR Acad. Sci. Paris **265** (1967), A129-A132.

[6] CHEVALLEY, C., *Théorie des groupes de Lie,* tome II: *groupes algèbriques,* Hermann, 1951.

[7] DIEUDONNE, J., *Introduction to the theory of formal groups,* M. Dekker, 1973.

[8] DITTERS, E., *Groupes formels.* Cours du 3e cycle 73/74, Univ. de Paris XI, Orsay, 1975.

[9] HAZEWINKEL, M., *Formal groups and applications,* Acad. Pr., 1978.

[10] LAZARD, M., *Sur les groupes de Lie formels à un paramètre,* Bull. Soc. Math. de France **83** (1955), 251-274.

[11] LAZARD, M., *Lois de groupes et analyseurs,* Ann. Ec. Norm. Sup. **72** (1955), 299-400.

[12] LAZARD, M., *Commutative formal groups,* LNM **443,** Springer Verlag, 1975.