THE RING OF WITT VECTORS

Leslie G. Roberts

I discuss the ring of (big or universal) Witt vectors $\Lambda(A)$, of a commutative ring A. The ring $\Lambda(A)$, or variants of it, arises in several ways in Commutative Algebra, Algebraic Number Theory, Algebraic Geometry, Algebraic Topology, and Algebraic K-Theory, and undoubtedly elsewhere. I have been fascinated by Witt Vectors for many years, but they are still very mysterious objects to me. I will not to attempt a more detailed motivation here, but some of the applications hinted at above appear below, and in the references.

These notes are based on talks I gave in the Curves Seminar in January, February, and March of 1996. For some time I have wanted to give at least an informal exposition of the material in Section 5. I was motivated to give the talks at this time by the appearance of divided powers in the lectures of Tony Geramita [5,Lecture 9]. Nothing here is claimed to be original except for the speculation in Section 5 on the relation between the P's and the Q's. However there is some novelty in the presentation. In particular I have not seen the universal polynomials Q defined as they are here in (4.2), (4.3.3). I learned about this approach from Barry Dayton, but have not seen it in print. Several accounts of Witt vectors are listed in the bibliography. Much of these notes are my attempt to understand Bergman's sections on Witt vectors in [1]. The denominator $f^n g^n$ in (4.3.1), (4.4) seems to be a satisfactory answer to Bergman's lament in the footnote at the bottom of page 190 in [1]. Grothendieck also has this correction term in [2, page 29 (in the numbering at the bottom of the page), (1.17 bis)].

I would like to thank the audience for attending my lectures and (especially Ernst Kani) for offering helpful suggestions. My talks got to the end of Section 8. Section 9 was added later in order to reach a more natural stopping point.

Throughout, $\mathbb{N} = \{1, 2, 3, \ldots\}$, the natural numbers.

1. The additive structure of Λ(A).

Let A be a commutative ring with unit. A formal power series over A is an expression of the form $f = a_0 + a_1 t + a_2 t^2 + a_3 t^3 + \ldots = \Sigma_{i=0}^{\infty} a_i t^i$ ($a_i \in A$). If also $g = b_0 + b_1 t + b_2 t^2 + b_3 t^3 + \ldots$ we define $f + g$ by just adding the coefficients, i.e.

(1.1) $$f + g := \Sigma_{i=0}^{\infty} (a_i + b_i) t^i.$$

We also define the product by

$$fg := \Sigma_{i=0}^{\infty} c_k t^k \text{ where } c_k = \Sigma_{i+j=k} a_i b_j. \tag{1.2}$$

Note that the expression for c_k is a finite sum so our definition of the product makes sense. We do not assume that A has a topology (and if it does, we ignore the topology). These operations make the set of formal power series over A into a commutative ring with unit which is denoted $A[[t]]$. A polynomial $f = a_0 + a_1 t + a_2 t^2 + a_3 t^3 + \ldots + a_n t^n$ is regarded as an element of $A[[t]]$ by taking $a_i = 0$ for $i >$n.

Let $\Lambda(A) = 1 + tA[[t]]$ be the set of all formal power series with constant term 1. An element f of $\Lambda(A)$ is a (possibly) infinite sum $f = 1 + a_1 t + a_2 t^2 + a_3 t^3 + \ldots$. First observe that $\Lambda(A)$ is an abelian group under multiplication of formal power series. The "zero" element for the abelian group $\Lambda(A)$ is the power series 1. We obtain the "negative" of $f \in \Lambda(A)$ by formally inverting power series: if $f = 1 + a_1 t + a_2 t^2 + a_3 t^3 + \ldots + a_n t^n + \ldots$ we wish to find $g = 1 + b_1 t + b_2 t^2 + b_3 t^3 + \ldots$ such that $fg = 1$. Setting the coefficients of t^i (in fg) equal to zero we obtain equations

$$\begin{gathered} a_1 + b_1 = 0 \\ a_2 + a_1 b_1 + b_2 = 0 \\ a_3 + a_2 b_1 + a_1 b_2 + b_3 = 0 \\ \ldots. \end{gathered} \tag{1.3}$$

These equations can be solved recursively for the b_i yielding

$$\begin{gathered} b_1 = -a_1 \\ b_2 = a_1^2 - a_2 \\ b_3 = -a_1^3 + 2a_1 a_2 - a_3 \\ \ldots. \end{gathered} \tag{1.4}$$

I do not know a useful explicit formula for the b_j as functions of the a_i. Note that b_j depends only on $\{a_1, \ldots, a_j\}$ and that the coefficients of these polynomials are integers which are independent of A.

2. The ghost map.

We now try to change this multiplicative abelian group into an additive abelian group. One way to do this is to take logarithms. If $\mathbb{Q} \subseteq A$ we can define $\log(f)$ by substituting $f-1$ in place of x in the formal power series $\log(1+x) := x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \dots$. This substitution yields a series $\log(f) \in tA[[t]]$ because only the finite sum $x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \dots + (-1)^i \frac{x^i}{i}$ contributes to the coefficient of t^i. Similarly, again assuming that $\mathbb{Q} \subseteq A$, for $g \in tA[[t]]$ we can define $e^g \in \Lambda(A)$ by substituting g in place of x in the series $e^x := 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$. For convenience of typing I will sometimes write $\exp(g)$ instead of e^g. The usual properties of exp and log are satisfied. In particular we have (for $f_i \in \Lambda(A), g_i \in tA[[t]]$)

(2.1.1) $$\log(f_1 f_2) = \log(f_1) + \log(f_2)$$

(2.1.2) $$\exp(g_1 + g_2) = \exp(g_1)\exp(g_2)$$

(2.1.3) $$\exp(\log(f_1)) = f_1$$

(2.1.4) $$\log(\exp(g_1)) = g_1$$

Furthermore, given $f = a_0 + a_1 t + a_2 t^2 + a_3 t^3 + \dots \in A[[t]]$ we can define f' $(= \frac{df}{dt})$ by $f' := a_1 + 2a_2 t + 3a_3 t^2 + \dots$. There is no limit involved here. This is purely an algebraic definition. Then all the usual properties of differentiation are satisfied, including

(2.1.5) $$\frac{d}{dt}\log(f) = \frac{f'}{f}$$

If we use log we require that $\mathbb{Q} \subseteq A$. However because $\frac{d}{dt}(g_1 + g_2) = \frac{d}{dt}(g_1) + \frac{d}{dt}(g_2)$, we have that $f \to \frac{d}{dt}\log(f)$ is also a homomorphism from the multiplicative group $\Lambda(A)$ to the additive group $A[[t]]$. This homomorphism does not require that $\mathbb{Q} \subseteq A$, since $\frac{f'}{f}$ is defined over any commutative ring. Furthermore, from the rules of differentiation we have $fg \to \frac{(fg)'}{fg} = \frac{f'g + fg'}{fg} = \frac{f'}{f} + \frac{g'}{g}$ which checks that $f \to \frac{f'}{f}$ is a homomorphism without using property (2.1.1) of log. Thus for any commutative ring A and $f \in \Lambda(A)$ we define the homomorphism

(2.2) $$gh : \Lambda(A) \to tA[[t]]$$

by $gh(f) = -\frac{tf'}{f}$. Here $\Lambda(A)$ is an abelian group under multiplication of formal power series, as described above, and $tA[[t]]$ is an abelian group under addition of formal power series. The factor $(-t)$ does not change the fact that we have a homomorphism, and will turn out to be convenient later. Because of the t, we land in $tA[[t]]$ instead of $A[[t]]$. The name "gh" stands for "ghost". Suppose that $f = 1 + \Sigma_{i=1}^{\infty} a_i t^i$, and $gh(f) = \Sigma_{i=1}^{\infty} w_i t^i$. From the formula $f \cdot gh(f) = -tf'$ we obtain

$$(1 + a_1 t + a_2 t^2 + a_3 t^3 + \ldots)(w_1 t + w_2 t^2 + w_3 t^3 + \ldots) = -a_1 t - 2a_2 t^2 - 3a_3 t^3 + \ldots$$

Multiplying out and comparing coefficients of powers of t we obtain equations

(2.3)
$$w_1 + a_1 = 0$$

$$w_2 + a_1 w_1 + 2a_2 = 0$$

$$\ldots\ldots.$$

$$w_n + a_1 w_{n-1} + \ldots a_{n-1} w_1 + n a_n = 0$$

If we are given $\{a_i\}_{i \geq 1}$ we can solve these equations recursively for $\{w_j\}_{j \geq 1}$, obtaining

(2.3.1)
$$w_i = W_i(a_1, \ldots, a_i)$$

where W_i is a polynomial in i variables, with coefficients in $\mathbb{Z}$. For example $w_1 = -a_1, w_2 = a_1^2 - 2a_2, \ldots$. Furthermore W_i is independent of A. Similarly if $\mathbb{Q} \subseteq A$ we can recursively solve (2.3) for the a_i, obtaining

(2.3.2)
$$a_i = A_i(w_1, \ldots, w_i)$$

where the A_i are polynomials independent of A with coefficients in $\mathbb{Q}$.

Presumably gh is called the ghost map because the co-ordinates w_i ("ghost co-ordinates") of $f \in \Lambda(A)$ do not really exist unless $\mathbb{Q} \subseteq$A. Nonetheless we will see that one can sometimes prove something about $\Lambda(A)$ by working with the w_i as if they did exist.

If $\mathbb{Q} \subseteq A$ then gh is an isomorphism. We can find the inverse by solving the equation $g = -\frac{tf'}{f}$ for f. Namely $\frac{-g}{t} = \frac{f'}{f} = \frac{d}{dt}\log(f), -\int \frac{g}{t} = \log(f)$ and $f = \exp(-\int \frac{g}{t})$. Note that $\frac{g}{t} \in A[[t]]$ and by $\int$ applied to an element of $A[[t]]$ we mean the antiderivative with constant of integration 0, i.e. $\int(b_0 + b_1t + b_2t^2 + b_3t^3 + \ldots) = b_0t + b_1\frac{t^2}{2} + b_2\frac{t^3}{3} + b_3\frac{t^4}{4} + \ldots$. If $g \in tA[[t]]$ we will write $gh^{-1}(g)$ for $\exp(-\int \frac{g}{t})$. It is straightforward to check that gh^{-1} is a two sided inverse to gh so gh is an isomorphism of abelian groups:

$$(\mathbf{2.4}) \qquad gh : \Lambda(A) \xrightarrow{\cong} tA[[t]] \text{ (if } \mathbb{Q} \subseteq A)$$

3. The ring structure on $\Lambda(\mathbf{A})$.

The abelian group $tA[[t]]$ can be made into a ring in several different ways. First of all we can identify $tA[[t]]$ with $\Pi_{i=1}^{\infty}A$ by

$$a_1t + a_2t^2 + a_3t^3 + \ldots \Leftrightarrow (a_1, a_2, a_3, \ldots)..$$

The set $\Pi_{i=1}^{\infty}A$ is a ring under co-ordinatewise addition and multiplication. In this ring structure on $\Pi_{i=1}^{\infty}A$ the variable t is just a place holder. (Of course t is still needed in the definitions of gh and gh^{-1}.) If g_1 and g_2 are elements of $tA[[t]]$ I will denote this co-ordinatewise product by $g_1 \cdot g_2$. Then (still assuming that $\mathbb{Q} \subseteq A$) we can define a multiplication $*$ on $\Lambda(A)$ by

$$(\mathbf{3.1}) \qquad f_1 * f_2 = gh^{-1}(gh(f_1) \cdot gh(f_2)).$$

It is then automatic that $\Lambda(A)$ is a (commutative) ring (with unit), addition being the usual multiplication of power series, and multiplication $*$. We will now try to describe $f * g$ more explicitly. Suppose $f = 1 + a_1t + a_2t^2 + a_3t^3 + \ldots + a_nt^n + \ldots$ and $g = 1 + b_1t + b_2t^2 + b_3t^3 + \ldots$ Then $f * g = 1 + c_1t + c_2t^2 + c_3t^3 + \ldots + c_nt^n + \ldots$. From (2.3.*) it is clear that there exist polynomials $P_n \in \mathbb{Q}[X_1, \ldots, X_n; Y_1, \ldots, Y_n]$, independent of A, such that

$$(\mathbf{3.2}) \qquad c_n = P_n(a_1, \ldots, a_n; b_1, \ldots, b_n).$$

Thus $*$ is determined by its behaviour on polynomials. In order to find c_n it suffices to compute $f * g$ where $f = 1 + a_1t + a_2t^2 + a_3t^3 + \ldots + a_nt^n$ and $g = 1 + b_1t + b_2t^2 + b_3t^3 + \ldots + b_nt^n$. To get started we will consider $(1 + a_1t) * (1 + b_1t)$. We have

$$gh(1 + a_1t) = \frac{(-t)(1 + a_1t)'}{(1 + a_1t)} = (-a_1t)(1 - a_1t + a_1^2t^2 - a_1^3t^3 + \ldots) =$$

$$-a_1t + a_1^2t^2 - a_1^3t^3 + \ldots.$$

The negative signs are a bit of a nuisance so instead we consider

$$gh(1 - a_1t) = a_1t + a_1^2t^2 + a_1^3t^3 + \ldots\ . \text{ Similarly}$$

$$gh(1 - b_1t) = b_1t + b_1^2t^2 + b_1^3t^3 + \ldots\ . \text{ Hence}$$

$(1 - a_1t) * (1 - b_1t) = gh^{-1}(a_1b_1t + a_1^2b_1^2t^2 + a_1^3b_1^3t^3 + \ldots) = 1 - a_1b_1t$. That is

(3.3) $$(1 - a_1t) * (1 - b_1t) = 1 - a_1b_1t.$$

The unit element of $tA[[t]]$ is clearly $t + t^2 + t^3 + \ldots$ and $gh(1 - t) = t + t^2 + t^3 + \ldots$ so $1 - t$ is the unit element of the ring $\Lambda(A)$.

Now take $f = 1 + a_1t + a_2t^2 + a_3t^3 + \ldots + a_nt^n$ and $g = 1 + b_1t + b_2t^2 + b_3t^3 + \ldots + b_nt^n$. Since (3.2) is independent of the ring we can take the a_i, b_j to be indeterminates over A. More precisely, let $\{\lambda_i, \mu_i\}$ $(1 \leq i \leq n,)$ be independent indeterminates over A, and let $a_i = (-1)^i(i^{th}$ elementary symmetric function in the λ's), $b_i = (-1)^i(i^{th}$ elementary symmetric function in the μ's). For example, if $n = 3$ then $a_1 = -\lambda_1 - \lambda_2 - \lambda_3, a_2 = \lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3$ and $a_3 = -\lambda_1\lambda_2\lambda_3$. Then the a_i, b_i are independent indeterminates over A and $f = \Pi_{i=1}^n(1 - \lambda_it)$ and $g = \Pi_{i=1}^n(1 - \mu_it)$. (The λ_i can be thought of as (reciprocal) formal roots of f.) Now using the distributive law for the ring $\Lambda(A[\{\lambda_i\}, \{\mu_j\}])$ we obtain that $f * g = \Pi_{1 \leq i,j \leq n}(1 - \lambda_it) * (1 - \mu_jt) = \Pi_{1 \leq i,j \leq n}(1 - \lambda_i\mu_jt) = 1 + c_1t + c_2t^2 + c_3t^3 + \ldots + c_nt^n + c'_{n+1}t^n + \ldots + c'_{n^2}t^{n^2}$. (The c_i are correct as required in (3.1) only up to t^n, hence the change in notation to c'_i if $i > n$. If we require c_k for $k > n$ just take $n \geq$k.) We now have that the c_i $(1 \leq i \leq n)$ are symmetric functions in $\{\lambda_i\}$ and in $\{\mu_i\}$ $(1 \leq i \leq n)$, and hence are polynomials in $\{a_i, b_i\}(1 \leq i \leq n)$. That is, the polynomials P_i in (3.2) have integer coefficients. The first few examples are

(3.4) $$P_1(a_1; b_1) = -a_1b_1$$

$$P_2(a_1, a_2; b_1, b_2) = a_1^2b_2 - 2a_2b_2 + a_2b_1^2$$

$$P_3(a_1, a_2, a_3; b_1, b_2, b_3) = -(a_1^3b_3 + a_3b_1^3 - 3a_1a_2b_3 - 3a_3b_1b_2 + 3a_3b_3 + a_1a_2b_1b_2)$$

$$\ldots.$$

The P_n rapidly become very complicated (see (3.5) below for a more extensive list), and as far as I know there is no closed form expression for them. However it is clear from the construction that P_n is homogeneous of degree n in the a's if we assign degree i to a_i and also homogeneous of degree n in the b's if we assign degree i to b_i. Also P_n is invariant under interchanging a_i and b_i $(1 \leq i \leq n)$.

Note that $gh(\Pi_{i=1}^{n}(1-\lambda_i t)) = \Sigma_{i=1}^{n} gh(1-\lambda_i t) = \Sigma_{i=1}^{n}\Sigma_{j=1}^{\infty}\lambda_i^j t^j = \Sigma_{j=1}^{\infty}(\Sigma_{i=1}^{n}\lambda_i^j)t^j$ from which we see that $w_j = \Sigma_{i=1}^{n}\lambda_i^j$. Thus the w_j is the j^{th} power sum of the λ_i and a_j is (up to sign) the j^{th} elementary symmetric function of the λ_i. Indeed the formulas (2.3) are just Newton's formulas relating these symmetric functions (taking into account the signs).

The polynomials P_n determine the ring structure of $\Lambda(A)$. If $f = 1 + a_1 t + a_2 t^2 + a_3 t^3 + \ldots + a_n t^n + \ldots$ and $g = 1 + b_1 t + b_2 t^2 + b_3 t^3 + \ldots + b_n t^n + \ldots$ then

$$f * g = 1 + \Sigma_{i \geq 1} P_i(a_1, \ldots, a_i; b_1, \ldots, b_i)t^i$$

(here the a's are no longer indeterminates over A, but specific elements of A which we plug into the polynomials). Since the P_i have coefficients in $\mathbb{Z}$ we can use this as the definition of $f * g$ even if $\mathbb{Q}$ is not contained in A. I claim that $*$ makes $\Lambda(A)$ into a ring. The ring axioms can all be expressed as identities in the P_n. For example consider the associative law for multiplication:

$$[(1 + a_1 t) * (1 + b_1 t)] * (1 + c_1 t) = (1 + P_1(a_1; b_1)t) * (1 + c_1 t) = 1 + P_1(P_1(a_1; b_1); c_1)t.$$

Similarly $(1+a_1 t)*[(1+b_1 t)*(1+c_1 t)] = (1+a_1 t)*(1+P_1(b_1; c_1)t) = 1+P_1(a_1; P_1(b_1; c_1))t$. The associative law for multiplication in $\Lambda(A)$ is thus equivalent to $P_1(P_1(a_1; b_1); c_1) = P_1(a_1; P_1(b_1; c_1))$ for all rings A and all $a_1, b_1, c_1 \in A$. These identities are known to hold over $\mathbb{Q}$ for all $a_1, b_1, c_1 \in \mathbb{Q}$, and hence we have an equality $P_1(P_1(X; Y); Z) = P_1(X; P_1(Y; Z))$ in $\mathbb{Q}[X, Y, Z]$ for indeterminates X, Y, Z. The coefficients of P_1 actually lie in $\mathbb{Z}$ so we have $P_1(P_1(X; Y); Z) = P_1(X; P_1(Y; Z))$ in $\mathbb{Z}[X, Y, Z]$. Hence we have $P_1(P_1(a_1; b_1); c_1) = P_1(a_1; P_1(b_1; c_1))$ for all elements a_1, b_1, c_1 in any commutative ring, as we wished to show. (Of course $P_1(X; Y) = XY$ so the above identities are all trivial. My intention is only to illustrate the idea.) There are similar identities involving P_n for $n \geq 1$, from which we conclude that for any commutative ring A, $\Lambda(A)$ is a commutative ring with unit, the addition of $\Lambda(A)$ being multiplication of formal power series, and the multiplication being $*$. We still have a map

$$gh : \Lambda(A) \to tA[[t]]$$

of commutative rings, which we claim is a ring homomorphism. We already know that $gh(f_1 + f_2) = gh(f_1) + gh(f_2)$ so it suffices to show that $gh(f_1 * f_2) = gh(f_1) \cdot gh(f_2)$ for polynomials f_1 and f_2 of degree n in $\Lambda(A)$. Suppose $f_1 = 1 + \Sigma_{i=1}^n a_i t^i$ and $f_2 = 1 + \Sigma_{i=1}^n b_i t^i$. If $\mathbb{Q} \subseteq A$ we have $gh(f_1 * f_2) = gh(f_1) \cdot gh(f_2)$ by definition of $*$. This equality can be expressed as identities in the P's which hold for all $a_i, b_i \in \mathbb{Q}$, hence which hold universally, proving that gh preserves multiplication as well as addition, hence is a ring homomorphism.

The homomorphism gh need not be either injective or surjective. For example, if the characteristic of A is p then $gh(1 + t^p) = 0$, and t^2 is not in the image of gh unless 2 is a unit, as we see by setting $w_2 = 1, w_1 = 0$ in the second equation of (2.3).

The formula (3.3) determines the multiplication of $\Lambda(A)$. Formula (3.3) could have been taken as true by definition, and the multiplication developed from there. However I find (3.1) easier to remember, and I can better understand proofs based on (3.1). Instead of (3.3) some expositions start with $(1 + a_1 t) * (1 + a_2 t) = (1 + a_1 a_2 t)$ [2], [3 (exercises)], [4]. This gives an isomorphic ring $\Lambda(A)$ (via $t \to -t$), but will necessitate assorted sign changes throughout the discussion.

(3.5) Examples. Here is a more extensive list of the P_i, calculated with Mathematica using (3.1) and (3.2). Here $a[i]$ means a_i, $b[i]$ means b_i and $p[i]$ is P_i. The list is given far enough for the calculation in (5.3).

```
p[1] = -(a[1]*b[1])

p[2] = a[2]*b[1]^2 + a[1]^2*b[2] - 2*a[2]*b[2]

p[3] = -(a[3]*b[1]^3) - a[1]*a[2]*b[1]*b[2] + 3*a[3]*b[1]*b[2] -
    a[1]^3*b[3] + 3*a[1]*a[2]*b[3] - 3*a[3]*b[3]

p[4] = a[4]*b[1]^4 + a[1]*a[3]*b[1]^2*b[2] - 4*a[4]*b[1]^2*b[2] +
    a[2]^2*b[2]^2 - 2*a[1]*a[3]*b[2]^2 + 2*a[4]*b[2]^2 +
    a[1]^2*a[2]*b[1]*b[3] - 2*a[2]^2*b[1]*b[3] - a[1]*a[3]*b[1]*b[3] +
```

```
    4*a[4]*b[1]*b[3] + a[1]^4*b[4] - 4*a[1]^2*a[2]*b[4] +
    2*a[2]^2*b[4] + 4*a[1]*a[3]*b[4] - 4*a[4]*b[4]

p[5] = -(a[5]*b[1]^5) - a[1]*a[4]*b[1]^3*b[2] + 5*a[5]*b[1]^3*b[2] -
    a[2]*a[3]*b[1]*b[2]^2 + 3*a[1]*a[4]*b[1]*b[2]^2 -
    5*a[5]*b[1]*b[2]^2 - a[1]^2*a[3]*b[1]^2*b[3] +
    2*a[2]*a[3]*b[1]^2*b[3] + a[1]*a[4]*b[1]^2*b[3] -
    5*a[5]*b[1]^2*b[3] - a[1]*a[2]^2*b[2]*b[3] +
    2*a[1]^2*a[3]*b[2]*b[3] + a[2]*a[3]*b[2]*b[3] -
    5*a[1]*a[4]*b[2]*b[3] + 5*a[5]*b[2]*b[3] - a[1]^3*a[2]*b[1]*b[4] +
    3*a[1]*a[2]^2*b[1]*b[4] + a[1]^2*a[3]*b[1]*b[4] -
    5*a[2]*a[3]*b[1]*b[4] - a[1]*a[4]*b[1]*b[4] + 5*a[5]*b[1]*b[4] -
    a[1]^5*b[5] + 5*a[1]^3*a[2]*b[5] - 5*a[1]*a[2]^2*b[5] -
    5*a[1]^2*a[3]*b[5] + 5*a[2]*a[3]*b[5] + 5*a[1]*a[4]*b[5] -
    5*a[5]*b[5]

p[6] = a[6]*b[1]^6 + a[1]*a[5]*b[1]^4*b[2] - 6*a[6]*b[1]^4*b[2] +
    a[2]*a[4]*b[1]^2*b[2]^2 - 4*a[1]*a[5]*b[1]^2*b[2]^2 +
    9*a[6]*b[1]^2*b[2]^2 + a[3]^2*b[2]^3 -
    2*a[2]*a[4]*b[2]^3 + 2*a[1]*a[5]*b[2]^3 - 2*a[6]*b[2]^3 +
    a[1]^2*a[4]*b[1]^3*b[3] - 2*a[2]*a[4]*b[1]^3*b[3] -
    a[1]*a[5]*b[1]^3*b[3] + 6*a[6]*b[1]^3*b[3] +
    a[1]*a[2]*a[3]*b[1]*b[2]*b[3] - 3*a[3]^2*b[1]*b[2]*b[3] -
    3*a[1]^2*a[4]*b[1]*b[2]*b[3] + 4*a[2]*a[4]*b[1]*b[2]*b[3] +
    7*a[1]*a[5]*b[1]*b[2]*b[3] - 12*a[6]*b[1]*b[2]*b[3] +
    a[2]^3*b[3]^2 - 3*a[1]*a[2]*a[3]*b[3]^2 +
    3*a[3]^2*b[3]^2 + 3*a[1]^2*a[4]*b[3]^2 -
    3*a[2]*a[4]*b[3]^2 - 3*a[1]*a[5]*b[3]^2 +
    3*a[6]*b[3]^2 + a[1]^3*a[3]*b[1]^2*b[4] -
    3*a[1]*a[2]*a[3]*b[1]^2*b[4] + 3*a[3]^2*b[1]^2*b[4] -
    a[1]^2*a[4]*b[1]^2*b[4] + 2*a[2]*a[4]*b[1]^2*b[4] +
    a[1]*a[5]*b[1]^2*b[4] - 6*a[6]*b[1]^2*b[4] +
    a[1]^2*a[2]^2*b[2]*b[4] - 2*a[2]^3*b[2]*b[4] -
```

```
2*a[1]^3*a[3]*b[2]*b[4] + 4*a[1]*a[2]*a[3]*b[2]*b[4] -
3*a[3]^2*b[2]*b[4] + 2*a[1]^2*a[4]*b[2]*b[4] +
2*a[2]*a[4]*b[2]*b[4] - 6*a[1]*a[5]*b[2]*b[4] + 6*a[6]*b[2]*b[4] +
a[1]^4*a[2]*b[1]*b[5] - 4*a[1]^2*a[2]^2*b[1]*b[5] +
2*a[2]^3*b[1]*b[5] - a[1]^3*a[3]*b[1]*b[5] +
7*a[1]*a[2]*a[3]*b[1]*b[5] - 3*a[3]^2*b[1]*b[5] +
a[1]^2*a[4]*b[1]*b[5] - 6*a[2]*a[4]*b[1]*b[5] -
a[1]*a[5]*b[1]*b[5] + 6*a[6]*b[1]*b[5] + a[1]^6*b[6] -
6*a[1]^4*a[2]*b[6] + 9*a[1]^2*a[2]^2*b[6] - 2*a[2]^3*b[6] +
6*a[1]^3*a[3]*b[6] - 12*a[1]*a[2]*a[3]*b[6] + 3*a[3]^2*b[6] -
6*a[1]^2*a[4]*b[6] + 6*a[2]*a[4]*b[6] + 6*a[1]*a[5]*b[6] - 6*a[6]*b[6]
```

4. Another ring structure on $\Lambda(\mathbf{A})$.

If $\mathbb{Q} \subseteq A$ we have the isomorphism

$$gh : \Lambda(A) \xrightarrow{\cong} tA[[t]]$$

The right hand side $tA[[t]]$ has other multiplications besides the co-ordinatewise multiplication $\cdot$ considered above. For example we might consider the usual power series multiplication of $tA[[t]]$ (indicated simply by juxtaposition), which together with the addition yields a ring without unit. We can use this to make $\Lambda(A)$ into a ring without unit, with addition being multiplication of power series, and multiplication $\blacksquare$ defined by

$$f_1 \blacksquare f_2 = gh^{-1}(gh(f_1)gh(f_2)) \tag{4.1}$$

For example we have $gh(1-t) = \frac{t}{1-t}$. Squaring we get $\frac{t^2}{(1-t)^2}$. Dividing by t and integrating we get $\int \frac{t}{(1-t)^2} = \frac{t}{1-t} + \log(1-t)$ (making sure that we take the antiderivative with 0 constant term). Taking $\exp(-$this expression$)$ we obtain $(1-t)\blacksquare(1-t) = \exp(\frac{-t}{1-t})\frac{1}{1-t} = 1 - \frac{t^2}{2} + \ldots$. Thus we see that $\blacksquare$ requires denominators, and if f_1 and f_2 are polynomials $f_1 \blacksquare f_2$ need not even be rational.

We have better luck if we use the multiplication $\otimes$ defined on $tA[[t]]$ by $t^m \otimes t^n = \binom{m+n}{n} t^{m+n}$. (The n^{th} power of t under $\otimes$ is then $(n!)t^n$ and t^n is a divided power.) Use this to define a multiplication

$$f_1 \square f_2 = gh^{-1}(gh(f_1) \otimes gh(f_2)) \tag{4.2}$$

on $\Lambda(A)$. Then we have

$$gh(1-(\lambda+\mu)t) = \Sigma_{n=1}^{\infty}(\lambda+\mu)^n t^n$$
$$gh(1-\lambda t) = \Sigma_{n=1}^{\infty}\lambda^n t^n$$
$$gh(1-\mu t) = \Sigma_{n=1}^{\infty}\mu^n t^n$$

so that

$$gh\frac{(1-(\lambda+\mu)t)}{(1-\lambda t)(1-\mu t)} = \Sigma_{n=1}^{\infty}[(\lambda+\mu)^n - \lambda^n - \mu^n]t^n = \Sigma_{d\geq 2}(\Sigma_{i+j=d, i\geq 1, j\geq 1}\binom{d}{i}\lambda^i\mu^j)t^d$$
$$= (\Sigma_{n=1}^{\infty}\lambda^n t^n)\otimes(\Sigma_{n=1}^{\infty}\mu^n t^n).$$

Thus we see that

$$\textbf{(4.3.1)} \qquad (1-\lambda t)\Box(1-\mu t) = \frac{(1-(\lambda+\mu)t)}{(1-\lambda t)(1-\mu t)}.$$

Replacing λ and μ by $-\lambda, -\mu$ we obtain

$$\textbf{(4.3.2)} \qquad (1+\lambda t)\Box(1+\mu t) = \frac{(1+(\lambda+\mu)t)}{(1+\lambda t)(1+\mu t)}.$$

Replacing t by $-t$ has the same effect, so we do not have the same sign convention problem we had in Section 3 with $*$. Again using (2.3) and the definition of $\otimes$ we find that if

$f_1 = 1 + a_1 t + a_2 t^2 + a_3 t^3 + \ldots + a_n t^n + \ldots$ and $f_2 = 1 + b_1 t + b_2 t^2 + b_3 t^3 + \ldots$ then

$$\textbf{(4.3.3)} \qquad f_1\Box f_2 = 1 + \Sigma_{n=1}^{\infty}Q_n(a_1,\ldots,a_{n-1};b_1,\ldots,b_{n-1})t^n$$

where the Q_i are polynomials independent of A with coefficients in $\mathbb{Q}$. The polynomial Q_n cannot contain a_n or b_n since the coefficient of the t^n term of $(\Sigma_{i=1}^{\infty}u_i t^i)\otimes(\Sigma_{i=1}^{\infty}v_i t^i)$ does not contain u_n or v_n. We can thus compute Q_{n+1} (as well as Q_i for $i < n+1$) by taking f_1 and f_2 to be polynomials of degree n. By temporarily taking indeterminates λ_i, μ_i over A and setting $a_i = (-1)^i(i^{th}$ elementary symmetric function in the $\lambda_i)$, $b_i = (-1)^i(i^{th}$ elementary symmetric function in the $\mu_i)$ and using the distributive law in $\Lambda(A)$ we conclude from (4.3.1) that

(4.4) $f_1 \Box f_2 = (1 + a_1t + a_2t^2 + a_3t^3 + \ldots + a_nt^n)\Box(1 + b_1t + b_2t^2 + b_3t^3 + \ldots + b_nt^n) =$
$((1 - \lambda_1 t)(1 - \lambda_2 t)\ldots(1 - \lambda_n t))\Box((1 - \mu_1 t)(1 - \mu_2 t)\ldots(1 - \mu_n t)) =$

$$\Pi_{1\leq i,j\leq n}(1 - \lambda_i t)\Box(1 - \mu_j t) = \frac{\Pi_{1\leq i,j\leq n}(1 - (\lambda_i + \mu_j)t}{f^n g^n}$$

The last expression is symmetric in the λ 's and the μ's from which we conclude that the coefficients of the Q's in fact lie in $\mathbb{Z}$. A heuristic reason for the denominator is that without it $f\Box g$ would change when extra roots λ_i equal to zero are added.

Now let A be an arbitrary commutative ring. Since the Q's have coefficients in $\mathbb{Z}$, given two elements $f_1 = 1 + a_1t + a_2t^2 + a_3t^3 + \ldots + a_nt^n + \ldots$ and $f_2 = 1 + b_1t + b_2t^2 + b_3t^3 + \ldots$ in $\Lambda(A)$ we can define

(4.5) $$f_1\Box f_2 = 1 + \Sigma_{n=1}^{\infty} Q_n(a_1, \ldots, a_{n-1}; b_1, \ldots, b_{n-1})t^n$$

The commutative and associative laws for $\Box$, as well as the distributive law, and the fact that gh is a homomorphism of rings without unit are all expressed in terms of identities over $\mathbb{Z}$ amongst the Q's. These identities are independent of A and are equalities of polynomials since they hold if A contains $\mathbb{Q}$, which is infinite. Thus the same properties hold for any commutative ring. That is, for all commutative rings A, the operations of multiplication of formal power series (as addition) and $\Box$ (as multiplication) make $\Lambda(A)$ into a commutative ring without unit, and gh is a ring homomorphism.

From the definition of $\Box$ it follows that P_n is homogeneous of degree n in the a's and b's combined if we assign degree i to a_i and to b_i. Also Q_n is invariant under interchanging a_i and b_i $(1 \leq i \leq n)$. (This is the commutative law for $\Box$). Furthermore every non-zero term in Q_n has both a's and b's in it.

It is worth noting that the behaviour of the numerator in (4.4) is related to the way that Chern classes of vector bundles behave under tensor product. If V and W are two vector bundles of ranks m and n respectively with Chern polynomials $f = 1 + c_1t + c_2t^2 + c_3t^3 + \ldots + c_mt^m$ and $g = 1 + d_1t + d_2t^2 + d_3t^3 + \ldots + d_nt^n$ then the Chern polynomial of $V \otimes W$ is $\Pi_{1\leq i\leq n, 1\leq j\leq n}(1 + (\lambda_i + \mu_j)t)$ where f formally factors as $f = \Pi_{i=1}^n(1 + \lambda_i t)$ and g as $g = \Pi_{i=1}^n(1 + \mu_i t)$. Similarly the Chern polynomial of $V \oplus W$ is fg (the usual multiplication of polynomials). Formal manipulations with Chern polynomials can then be used in the Schubert calculus to answer enumerative problems in Algebraic Geometry, for which the Schubert Maple package of Sheldon Katz may be useful.

I will not attempt to say what vector bundles are, or where $V, W, c_i, d_i, \lambda_i$ or μ_i live. These remarks are intended only to give an idea of one of the motivations for formal considerations like those with $\Lambda(A)$.

(4.6) Examples Here is a list of examples of the Q's. These were calculated with Mathematica using (4.2) and (4.5). (I also did the calculation using the Schubert package, as described above, obtaining the same result). As in (3.5) $q[i]$ means Q_i, $a[i]$ is a_i and $b[i]$ is b_i. This is the file newq.m1 loaded in the calculation of (5.3).

```
q[1] = 0

q[2] = -(a[1]*b[1])

q[3] = a[1]^2*b[1] - 2*a[2]*b[1] + a[1]*b[1]^2 - 2*a[1]*b[2]

q[4] = -(a[1]^3*b[1]) + 3*a[1]*a[2]*b[1] - 3*a[3]*b[1] -
    a[1]^2*b[1]^2 + 3*a[2]*b[1]^2 - a[1]*b[1]^3 +
    3*a[1]^2*b[2] - 6*a[2]*b[2] + 3*a[1]*b[1]*b[2] - 3*a[1]*b[3]

q[5] = a[1]^4*b[1] - 4*a[1]^2*a[2]*b[1] + 2*a[2]^2*b[1] +
    4*a[1]*a[3]*b[1] - 4*a[4]*b[1] + a[1]^3*b[1]^2 -
    4*a[1]*a[2]*b[1]^2 + 6*a[3]*b[1]^2 + a[1]^2*b[1]^3 -
    4*a[2]*b[1]^3 + a[1]*b[1]^4 - 4*a[1]^3*b[2] +
    12*a[1]*a[2]*b[2] - 12*a[3]*b[2] - 4*a[1]^2*b[1]*b[2] +
    12*a[2]*b[1]*b[2] - 4*a[1]*b[1]^2*b[2] + 2*a[1]*b[2]^2 +
    6*a[1]^2*b[3] - 12*a[2]*b[3] + 4*a[1]*b[1]*b[3] - 4*a[1]*b[4]

q[6] = -(a[1]^5*b[1]) + 5*a[1]^3*a[2]*b[1] - 5*a[1]*a[2]^2*b[1] -
    5*a[1]^2*a[3]*b[1] + 5*a[2]*a[3]*b[1] + 5*a[1]*a[4]*b[1] -
    5*a[5]*b[1] - a[1]^4*b[1]^2 + 5*a[1]^2*a[2]*b[1]^2 -
    3*a[2]^2*b[1]^2 - 7*a[1]*a[3]*b[1]^2 + 10*a[4]*b[1]^2 -
    a[1]^3*b[1]^3 + 5*a[1]*a[2]*b[1]^3 - 10*a[3]*b[1]^3 -
    a[1]^2*b[1]^4 + 5*a[2]*b[1]^4 - a[1]*b[1]^5 +
    5*a[1]^4*b[2] - 20*a[1]^2*a[2]*b[2] + 10*a[2]^2*b[2] +
```

```
20*a[1]*a[3]*b[2] - 20*a[4]*b[2] + 5*a[1]^3*b[1]*b[2] -
20*a[1]*a[2]*b[1]*b[2] + 30*a[3]*b[1]*b[2] + 5*a[1]^2*b[1]^2*b[2] -
20*a[2]*b[1]^2*b[2] + 5*a[1]*b[1]^3*b[2] - 3*a[1]^2*b[2]^2 +
10*a[2]*b[2]^2 - 5*a[1]*b[1]*b[2]^2 - 10*a[1]^3*b[3] +
30*a[1]*a[2]*b[3] - 30*a[3]*b[3] - 7*a[1]^2*b[1]*b[3] +
20*a[2]*b[1]*b[3] - 5*a[1]*b[1]^2*b[3] + 5*a[1]*b[2]*b[3] +
10*a[1]^2*b[4] - 20*a[2]*b[4] + 5*a[1]*b[1]*b[4] - 5*a[1]*b[5]
```

5. The relation between the P's and the Q's.

Now I would like to consider the question of whether or not there is any relation between the P's and the Q's. A few years ago Mark Krusemeyer, while visiting Queen's, noticed the following:

(5.1.1) $$P_1 = Q_2 = -a_1 b_1$$

(5.1.2) $$P_2 = a_2 b_1^2 + a_1^2 b_2 - 2a_2 b_2 \text{ and } Q_3 = a_1^2 b_1 + a_1 b_1^2 - 2a_2 b_1 - 2a_1 b_2.$$

We can change P_2 to Q_3 by the following rule: in a given monomial in the a's and b's lower the indices by one in all possible ways, with $a_1 \to 0$ and $b_1 \to 0$. Thus $a_2 b_1^2 \to a_1 b_1^2, a_1^2 b_2 \to a_1^2 b_1$, and $-2a_2 b_2 \to -2a_2 b_1 - 2a_1 b_2$ so altogether $P_2 \to Q_3$.

(5.1.3) $$P_3 = -a_1^3 b_3 - a_3 b_1^3 + 3a_1 a_2 b_3 + 3a_3 b_1 b_2 - 3a_3 b_3 - a_1 b_1 a_2 b_2 \text{ and}$$

$$Q_4 = -6a_2 b_2 - a_1^3 b_1 - a_1 b_1^3 + 3a_1 a_2 b_1 + 3a_1 b_1 b_2 - a_1^2 b_1^2 - 3a_3 b_1 - 3a_1 b_3 + 3a_1^2 b_2 + 3a_2 b_1^2.$$

This time we lower indices in a monomial by two in all possible ways, either one subscript by two or two subscripts by one each, again with $a_1 \to 0$ and $b_1 \to 0$. This time we get $P_3 \to (-a_1^3 b_1) + (-a_1 b_1^3) + (3a_1^2 b_2 + 3a_1 a_2 b_1) + (3a_1 b_1 b_2 + 3a_2 b_1^2) + (-3a_2 b_2 - 3a_1 b_3 - 3a_3 b_1) + (-a_1^2 b_1^2)$ which we see is equal to Q_4 except for a term $-3a_2 b_2$ instead of $-6a_2 b_2$. This is clearly too close to be a coincidence. One might continue, lowering subscripts by i-1 in an attempt to convert P_i to Q_{i+1}. We first remark that the degrees come out correctly: P_i is of degree $2i$ and $2i - (i-1) = i + 1 =$ degree of Q_{i+1}. I tested more examples with the following

Mathematica program, which gives a precise definition of the rule. (This is the file drop3.m loaded in the session log given below.)

(5.2) Mathematica program.

```
drop[n_, (x_)[i_]] := x[i - n]

drop[0, M_] := M

drop[n_, M_Plus] := drop[n, First[M]] + drop[n, Rest[M]]

drop[n_, (A_Integer)*(M_)] := A*drop[n, M]

drop[n_, M_] := Module[{first, rest}, {first, rest} = decomp[M];

    Sum[drop[i, first]*drop[n - i, rest], {i, 0, n}]]

decomp[M_] := Module[{vars = Variables[M], first, rest},

    first = First[vars]; rest = M/first; {first, rest}]

a[i_] := 0 /; i < 1
b[i_] := 0 /; i < 1
```

Some examples are given below. Lines 4-9 verify the calculation changing P_2 to Q_3 (twice). Line 10 verifies the computation attempting to change P_3 to Q_4. Line 11 applies the rule to $P_4 \to Q_5$. Note that the difference between Q_5 and the rule applied to P_4 is six terms out of 22. Line 13 applies the rule to $P_5 \to Q_6$. This time the error is 20 terms out of 43.

(5.3) Mathematica session log

Mathematica 2.2 for DOS 387

```
Copyright 1988-93 Wolfram Research, Inc.

In[1]:= << "math9\\drop3.m"

In[2]:= << "math11\\newp.m";

In[3]:= << "math11\\newq.m1";

In[4]:= drop[1,p[2]]
```

```
Out[4]= a[1]^2 b[1] + a[1] b[1]^2 - 2 (a[2] b[1] + a[1] b[2])

In[5]:= q[3]

Out[5]= a[1]^2 b[1] - 2 a[2] b[1] + a[1] b[1]^2 - 2 a[1] b[2]

In[6]:= %-%%

Out[6]= -2 a[2] b[1] - 2 a[1] b[2] + 2 (a[2] b[1] + a[1] b[2])

In[7]:= Expand[%]

Out[7]= 0

In[8]:= drop[1,p[2]]-q[3]

Out[8]= 2 a[2] b[1] + 2 a[1] b[2] - 2 (a[2] b[1] + a[1] b[2])

In[9]:= drop[1,p[2]]-q[3]//Expand

Out[9]= 0

In[10]:= drop[2,p[3]]-q[4]//Expand

Out[10]= 3 a[2] b[2]

In[11]:= drop[3,p[4]]-q[5]//Expand

Out[11]= -(a[1] a[2] b[1]^2 ) - 4 a[1] a[2] b[2] + 8 a[3] b[2] -
    a[1]^2 b[1] b[2] - 4 a[2] b[1] b[2] + 8 a[2] b[3]

In[12]:= q[5]

Out[12]= a[1]^4 b[1] - 4 a[1]^2 a[2] b[1] + 2 a[2]^2 b[1] +
    4 a[1] a[3] b[1] - 4 a[4] b[1] + a[1]^3 b[1]^2 - 4 a[1] a[2] b[1]^2 +
    6 a[3] b[1]^2 + a[1]^2 b[1]^3 - 4 a[2] b[1]^3 + a[1] b[1]^4 -
    4 a[1]^3 b[2] + 12 a[1] a[2] b[2] - 12 a[3] b[2] -
    4 a[1]^2 b[1] b[2] + 12 a[2] b[1] b[2] - 4 a[1] b[1]^2 b[2] +
    2 a[1] b[2]^2 + 6 a[1]^2 b[3] - 12 a[2] b[3] + 4 a[1] b[1] b[3] -
    4 a[1] b[4]

In[13]:= drop[4,p[5]]-q[6]//Expand
```

```
Out[13]= 2 a[1]^2 a[2] b[1]^2 - a[2]^2 b[1]^2 -
    3 a[1] a[3] b[1]^2 + a[1] a[2] b[1]^3 + 5 a[1]^2 a[2] b[2] -
    5 a[2]^2 b[2] - 10 a[1] a[3] b[2] + 15 a[4] b[2] +
    a[1]^3 b[1] b[2] + 3 a[1] a[2] b[1] b[2] - 15 a[3] b[1] b[2] +
    2 a[1]^2 b[1]^2 b[2] + 5 a[2] b[1]^2 b[2] -
    a[1]^2 b[2]^2 - 5 a[2] b[2]^2 - 15 a[1] a[2] b[3] +
    25 a[3] b[3] - 3 a[1]^2 b[1] b[3] - 10 a[2] b[1] b[3] +
    15 a[2] b[4]

In[14]:= Length[%]

Out[14]= 20

In[15]:= {Length[p[5]],Length[q[6]]}

Out[15]= {28, 43}
```

It seems clear that the rule defined above gives a first approximation to Q_{i+1}. However I have not been able to derive an exact rule, nor have I been able to explain the partial success of the present rule. I have tried some variants, but always with worse results. It seems unlikely that a rule (such as the one above) which has difference operators on subscripts (without taking into account the values of the subscripts) can be exact, since it seems (from the $P_3 \to Q_4$ case) that $a_1 b_1 a_2 b_2$ is converted to $a_1^2 b_1^2$ whereas $a_3 b_3$ is converted to $2a_2 b_2$ (plus other terms) yet both have a drop of one in each of two different subscripts.

6. Another set of co-ordinates for Λ(A).

Now consider the equation

(6.1) $$1 + a_1 t + a_2 t^2 + a_3 t^3 + \ldots = (1 - x_1 t)(1 - x_2 t^2)(1 - x_3 t^3)\ldots$$

If we compare coefficients of t^n $(n \geq 1)$ we obtain equations

(6.2) $$a_i = \Sigma(-1)^j x_{i_1} x_{i_2} \ldots x_{i_j} = R_i(x_1, \ldots, x_i) \ (i \geq 1)$$

where the summation is over all partitions $i = i_1 + i_2 + \ldots + i_j$ where $i_1 < i_2 < \ldots < i_j$. For example

(6.3) $$a_1 = -x_1$$

$$a_2 = -x_2$$

$$a_3 = x_1 x_2 - x_3$$

$$\dots\dots$$

Since the equations have the form $a_i = -x_i +$ (terms involving $\{x_j\}_{j<i}$), we can solve the equations recursively for x_i ($i \geq 1$) in any commutative ring A, obtaining $x_i = S_i(a_1, \dots, a_i)$ where the S_i are polynomials with integer coefficients, independent of A. I do not know an explicit formula for the S_i. Thus the vector $(x_1, x_2, x_3, \dots.)$ can be thought of as an alternate representation for $f = 1 + a_1 t + a_2 t^2 + a_3 t^3 + \dots \in \Lambda(A)$. Using the polynomials R_i and S_i the operations of $\Lambda(A)$ can be converted into operations on the vectors $(x_1, x_2, x_3, \dots.)$ making the set $\Lambda_{\mathbb{N}}(A)$ of such sequences into a commutative ring isomorphic to $\Lambda(A)$. (See (6.11) for the notation $\Lambda_{\mathbb{N}}$.) Unless indicated otherwise I will continue to use juxtaposition to indicate the addition of this ring, and * to indicate the multiplication. The zero element (unit for addition) is $(0, 0, 0, 0, \dots)$ and the 1 (unit for multiplication) is $(1, 0, 0, 0, \dots)$. We will obtain that if $\underline{x} = (x_1, x_2, x_3, \dots.)$ and $\underline{y} = (y_1, y_2, y_3, \dots.)$ then $\underline{xy} = (z_1, z_2, z_3 \dots)$ and $\underline{x} * \underline{y} = (z'_1, z'_2, z'_3 \dots)$ where $z_i = z_i(x_1, \dots, x_i; y_1, \dots, y_i)$ and $z'_i = z'_i(x_1, \dots, x_i; y_1, \dots, y_i)$ for universal polynomials with integer coefficients. I will spare the reader a new set of names! These polynomials can also be found by using the ghost map. We have

(6.4) $$gh(1 - x_i t^i) = \frac{-ti(-x_i t^{i-1})}{1 - x_i t^i} = \frac{i x_i t^i}{1 - x_i t^i} = i(x_i t^i + x_i^2 t^{2i} + x_i^3 t^{3i} + \dots)$$

Then if $gh(\Pi_{i\geq 1}(1 - x_i t^i)) = w_1 t + w_2 t^2 + w_3 t^3 + \dots$ we obtain by comparing coefficients of t^i with (6.4)

(6.5) $$w_n = \Sigma_{i|n} i x_i^{n/i}$$

For example

(6.6) $$w_1 = x_1$$

$$w_2 = x_1^2 + 2x_2$$

$$w_3 = x_1^3 + 3x_3$$

$$w_4 = x_1^4 + 2x_2^2 + 4x_4$$

$$\cdots .$$

These equations can be solved over $\mathbb{Q}$ for x_n in terms of w_j $(j \mid n)$. If we then use gh and gh^{-1} to compute the above mentioned polynomials $z_i = z_i(x_1, \ldots, x_i; y_1, \ldots, y_i)$ and $z'_i = z'_i(x_1, \ldots, x_i; y_1, \ldots, y_i)$ we conclude that z_i and z'_i depend only on x_j and y_j for $j \mid i$. This makes these new polynomials simpler than the P's that we considered earlier, especially when i is a prime power. A few examples are

(6.7)
$$z_1 = x_1 + y_1$$

$$z_2 = x_2 - x_1 y_1 + y_2$$

$$z_3 = x_3 - x_1^2 y_1 - x_1 y_1^2 + y_3$$

(6.8)
$$z'_1 = x_1 y_1$$

$$z'_2 = x_2 y_1^2 + x_1^2 y_2 + 2x_2 y_2$$

$$z'_3 = x_3 y_1^3 + x_1^3 y_3 + 3x_3 y_3$$

Finally we should not forget that there are also universal polynomials for $\underline{x}^{-1}$ (the inverse of $\underline{x}$ in the abelian group $\Lambda_{\mathbb{N}}(A)$). Namely if as above $\underline{x} = (x_1, x_2, x_3, \ldots .)$ and $\underline{x}^{-1} = (x'_1, x'_2, x'_3, \ldots .)$ then x'_i is a polynomial with integer coefficients in x_j $(j \mid i)$. A few examples are

(6.9)
$$x'_1 = -x_1$$

$$x'_2 = -x_2 - x_1^2$$

$$x'_3 = -x_3$$

The formulas (6.7), (6.8), (6.9) are copied from the attached computer printouts (6.12)-(6.14). From $(1 - x_1 t)(1 - x_p t^p)(1 + x_1 t)(1 + x_p t^p) = (1 - x_1^2 t^2)(1 - x_p^2 t^{2p})$ we conclude that $x'_p = -x_p$ for all odd primes p, as suggested by the calculations in (6.9).

It is clear, from lifting to $\Lambda(A)$ and multiplying, that if for all i either $x_i = 0$ or $y_i = 0$ then $(x_1, x_2, \ldots) + (y_1, y_2, \ldots) = (x_1 + y_1, x_2 + y_2, \ldots)$. In particular $(x_1, x_2, x_3, \ldots) = (x_1, 0, 0, \ldots) + (0, x_2, 0, \ldots) + (0, 0, x_3, 0, \ldots)$. (Here it is more convenient to use $+$ for the addition of $\Lambda(A)$.) From this it follows that in the expressions for z_n in (6.7), (6.12) every term except x_n and y_n contains both x_i and y_i for some $i, 0 < i < n$.

Let $m, n \in \mathbb{N}$ $(= \{1, 2, 3, \ldots\})$. From (6.4) we have $gh(1 - x_m t^m) = m(x_m t^m + x_m^2 t^{2m} + x_m^3 t^{3m} + \ldots)$ and $gh(1 - x_n t^n) = n(x_n t^n + x_n^2 t^{2n} + x_n^3 t^{3n} + \ldots)$. When we multiply $gh(1 - x_m t^m)$ and $gh(1 - x_n t^n)$ coefficientwise the only non-zero terms will be in co-ordinates that are multiples of N=LCM(m, n). Thus $gh(1 - x_m t^m) \cdot gh(1 - x_n t^n) = mn\Sigma_{k\geq 1} x_m^{Nk/m} x_n^{Nk/n} t^{Nk} = gh((1 - x_m^{N/m} x_n^{N/n} t^N)^{mn/N})$. From this we conclude by the usual universal argument that

(6.10) $(1 - x_m t^m) * (1 - x_n t^n) = (1 - x_m^{N/m} x_n^{N/n} t^N)^{mn/N} = (1 - x_m^{n/M} x_n^{m/M} t^N)^M$ (where M=GCD(m, n)).

An example of (6.10) is $(1 - at^4) * (1 - bt^6) = (1 - a^3 b^2 t^{12})^2$. Using (6.10), it is easy to show that $z'_p = x_1^p y_p + x_p y_1^p + p x_p y_p$ for all primes p, as suggested by the calculations in (6.8).

(6.11) Truncation. Let S be a non-empty subset of $\mathbb{N} = \{1, 2, 3, \ldots\}$ such that if $n \in S$ then any divisor of n (in $\mathbb{N}$) is also in S. Some examples of such sets S are $\mathbb{N}$ itself, $\underline{P} = \{1, p, p^2, \ldots.\} = \{p^i\}_{i\geq 0}$, $\underline{P}_n = \{1, p, p^2, \ldots, p^n\}$. Necessarily $1 \in S$. Since the universal polynomials (6.7), (6.8), (6.9) depend only on the divisors of the integer in question we can use these polynomials to put a ring structure on $\Lambda_S(A) := \{(x_1, x_{s_2}, x_{s_3}, \ldots)\}$ where $S = \{1, s_2, s_3, \ldots\}$. There is a surjective ring homomorphism $\pi_S : \Lambda(A) \to \Lambda_S(A)$ given by $\pi_S(\Pi_{i\geq 1}(1 - x_i t^i)) = (x_1, x_{s_2}, x_{s_3}, \ldots)$. When computing in $\Lambda_S(A)$ it is sometimes helpful to lift to $\Lambda(A)$, using (6.10) to calculate $*$.

(6.12) The formulas (6.7) by computer.

```
X[1] = x[1] + y[1]

X[2] = x[2] - x[1]*y[1] + y[2]

X[3] = x[3] - x[1]^2*y[1] - x[1]*y[1]^2 + y[3]

X[4] = x[4] - x[1]^3*y[1] + x[1]*x[2]*y[1] - 2*x[1]^2*y[1]^2 -
```

```
    x[1]*y[1]^3 - x[2]*y[2] + x[1]*y[1]*y[2] + y[4]

X[5] = x[5] - x[1]^4*y[1] - 2*x[1]^3*y[1]^2 -
    2*x[1]^2*y[1]^3 - x[1]*y[1]^4 + y[5]

X[6] = x[6] - x[1]^5*y[1] + x[1]*x[2]^2*y[1] +
    x[1]^2*x[3]*y[1] - 3*x[1]^4*y[1]^2 - x[1]^2*x[2]*y[1]^2 +
    x[1]*x[3]*y[1]^2 - 4*x[1]^3*y[1]^3 - 3*x[1]^2*y[1]^4 -
    x[1]*y[1]^5 - x[2]^2*y[2] + 2*x[1]*x[2]*y[1]*y[2] -
    x[1]^2*y[1]^2*y[2] - x[2]*y[2]^2 + x[1]*y[1]*y[2]^2 -
    x[3]*y[3] + x[1]^2*y[1]*y[3] + x[1]*y[1]^2*y[3] + y[6]
```

(6.13) The formulas (6.8) by computer.

```
X[1] = x[1]*y[1]

X[2] = x[2]*y[1]^2 + x[1]^2*y[2] + 2*x[2]*y[2]

X[3] = x[3]*y[1]^3 + x[1]^3*y[3] + 3*x[3]*y[3]

X[4] = x[4]*y[1]^4 - x[1]^2*x[2]*y[1]^2*y[2] -
    2*x[2]^2*y[1]^2*y[2] - 2*x[1]^2*x[2]*y[2]^2 -
    x[2]^2*y[2]^2 + 2*x[4]*y[2]^2 + x[1]^4*y[4] +
    2*x[2]^2*y[4] + 4*x[4]*y[4]

X[5] = x[5]*y[1]^5 + x[1]^5*y[5] + 5*x[5]*y[5]

X[6] = x[6]*y[1]^6 - x[1]^2*x[2]^2*y[1]^4*y[2] -
    2*x[2]^3*y[1]^4*y[2] - x[1]^4*x[2]*y[1]^2*y[2]^2 -
    4*x[1]^2*x[2]^2*y[1]^2*y[2]^2 - 4*x[2]^3*y[1]^2*y[2]^2 -
    2*x[1]^4*x[2]*y[2]^3 - 4*x[1]^2*x[2]^2*y[2]^3 -
    2*x[2]^3*y[2]^3 + x[3]^2*y[2]^3 + 2*x[6]*y[2]^3 -
    x[1]^3*x[3]*y[1]^3*y[3] - 3*x[3]^2*y[1]^3*y[3] +
    x[2]^3*y[3]^2 - 3*x[1]^3*x[3]*y[3]^2 - 3*x[3]^2*y[3]^2 +
    3*x[6]*y[3]^2 + x[1]^6*y[6] + 2*x[2]^3*y[6] + 3*x[3]^2*y[6] +
    6*x[6]*y[6]
```

(6.14) The formulas (6.9) by computer.

```
X[1] = -x[1]

X[2] = -x[1]^2 - x[2]

X[3] = -x[3]

X[4] = -x[1]^4 - x[1]^2*x[2] - x[2]^2 - x[4]

X[5] = -x[5]

X[6] = x[1]^4*x[2] + x[1]^2*x[2]^2 - x[3]^2 - x[6]
```

7. Idempotents and products of rings.

My goal in the rest of these notes is to determine the structure of $\Lambda(\mathbb{Z}/p\mathbb{Z})$, p a prime, and to relate this to the "Witt vectors" that first arise over p [1, page 175], [3]. This requires the study of idempotents in $\Lambda(A)$.

I have assumed familiarity with products of rings. The relationship between product decompositions and idempotents may be less familiar so I will discuss that briefly now. Let R_1 and R_2 be rings (commutative with unit, as always). Then the product ring $R = R_1 \Pi R_2$ is the set of ordered pairs (r_1, r_2), $r_1 \in R_1$, $r_2 \in R_2$ with co-ordinatewise addition and multiplication. Let $e_1 = (1,0)$ and $e_2 = (0,1)$. It is easily checked that $e_1^2 = e_1, e_2^2 = e_2, e_1 + e_2 = (1,1)$ (which is the unit of R), and $e_1 e_2 = 0$. Furthermore the ideal Re_1 of R is a ring which is isomorphic to R_1 (also $Re_2 \cong R_2$). Similarly the product ring $R_1 \Pi R_2 \Pi \ldots \Pi R_n$ (also written $\Pi_{i=1}^n R_i$) is the set of n-tuples $(r_1, \ldots, r_n)$, $r_i \in R_i$ with co-ordinatewise operations. More generally one can define the product $\Pi_{i \in X} R_i$ over an arbitrary index set X. Previously we had the product $\Pi_{i=1}^\infty A$ over the infinite set $\mathbb{N}$.

Now let R be any commutative ring. An element $e \in R$ such that $e^2 = e$ is called an idempotent. Every R contains the idempotents 0 and 1. Any other idempotent is referred to as non-trivial. Suppose that R contains a non-trivial idempotent e. Then $f = 1 - e$ is also a non-trivial idempotent, and $ef = 0$. The ideals Re and Rf are rings (with unit), and the map $r \to (re, rf)$ induces an isomorphism of commutative rings $R \cong Re \Pi Rf$. More generally a finite set of idempotents $\{e_1, \ldots, e_n\}$ is called orthogonal if $e_i e_j = 0$ for $i \neq j$ and $\Sigma_{i=1}^n e_i = 1$. The homomorphism $R \to \Pi_{i=1}^n Re_i$ defined by $r \to (re_1, \ldots, re_n)$ is an isomorphism.

Aside from finite products we will work also with the infinite product $\Pi_{i=1}^{\infty} A$. Here we have idempotents δ_i ($i \in \mathbb{N}$), namely δ_i has i^{th} co-ordinate equal to 1 and all other co-ordinates equal to 0. We can add an infinite number of elements $f_j \in \Pi_{i=1}^{\infty} A$ as long as in each co-ordinate we add only a finite number of elements of A. For example we will write $\Sigma_{i=1}^{\infty} \delta_i = 1$, although we should remember that this is not the addition of the ring structure of $\Pi_{i=1}^{\infty} A$. (Indeed when we write $\Pi_{i=1}^{\infty} A \cong tA[[t]]$ we are implicitly permitting such infinite addition.) Similarly we can form infinite products as long as in each co-ordinate all but a finite number of the elements being multiplied are 1 (or one element is 0). The ring $\Pi_{i=1}^{\infty} A$ has lots of idempotents. Namely let S be any subset of $\mathbb{N}$. Let ϵ_S be the element of $\Pi_{i=1}^{\infty} A$ which has 1 in the i^{th} co-ordinate if $i \in S$, and 0 if $i \notin S$. Clearly ϵ_S is an idempotent of $\Pi_{i=1}^{\infty} A$. We have $\epsilon_{\mathbb{N}} = 1$ and $\epsilon_{\emptyset} = 0$. For other subsets $S \subseteq \mathbb{N}$, ϵ_S is non-trivial. Any partition of $\mathbb{N}$ as a finite disjoint union gives a finite set of orthogonal idempotents and hence a product decomposition of $\Pi_{i=1}^{\infty} A$. For example $\mathbb{N} = E \coprod O$, where E is the set of even integers and O is the odd integers. This yields a product decomposition $\Pi_{i=1}^{\infty} A \cong (\Pi_{i even} A)\Pi(\Pi_{i odd} A)$.

If $\mathbb{Q} \subseteq A$ we have our isomorphism $gh : \Lambda(A) \to \Pi_{i=1}^{\infty} A$. If e is an idempotent of $\Pi_{i=1}^{\infty} A$ then $gh^{-1}(e)$ is an idempotent of $\Lambda(A)$. In particular $\Lambda(\mathbb{Q})$ has lots of idempotents. But do any of these idempotents live in $\Lambda(\mathbb{Z})$ (or in geometric language, is Spec($\Lambda(\mathbb{Z})$) disconnected)? It follows from [1, Appendix to Lecture 26, C] that in fact $\Lambda(\mathbb{Z})$ has no non-trivial idempotents, but I will not pursue this further. However we shall soon see that if appropriate integers are invertible in A, then $\Lambda(A)$ does have non-trivial idempotents.

We have seen in (6.4) that $gh(1-x_n t^n) = n(x_n t^n + x_n^2 t^{2n} + x_n^3 t^{3n} + \ldots)$ and in particular that $gh(1-t^n) = n(t^n + t^{2n} + t^{3n} + \ldots)$. If S is the subset of $\mathbb{N}$ consisting of multiples of n, then we will write ϵ_n instead of ϵ_S. Thus we have $gh(1-t^n) = n(t^n + t^{2n} + t^{3n} + \ldots) = n\epsilon_n$. Except for the n, we have that $gh(1-t^n)$ is an idempotent. If $(1-t^n)^{1/n}$ can be defined in $\Lambda(A)$ then we will have $gh(1-t^n)^{1/n} = \epsilon_n$, at least if n is a non-zero-divisor in A, which leads us to expect that $(1-t^n)^{1/n}$ will be an idempotent of $\Lambda(A)$. If $f \in \Lambda(A)$, by $f^{1/n}$ (n^{th} root of f) we mean an element $g \in \Lambda(A)$ such that $g^n =$ f. Suppose that n is a unit in A (of course, by $n \in A$ we mean the sum $1 + 1 + \ldots + 1$ of n 1's). I claim then that $f \in \Lambda(A)$ has a unique n^{th} root (equivalently n is a unit in $\Lambda(A)$). For suppose that $f = 1 + a_1 t + a_2 t^2 + a_3 t^3 + \ldots + a_n t^n + \ldots$ and that $g = 1 + b_1 t + b_2 t^2 + b_3 t^3 + \ldots + b_n t^n + \ldots$ is the proposed n^{th} root of f. Then by comparing coefficients of t^i in the equation $f = g^n$

we obtain a system of equations of the form $a_1 = nb_1, \ldots, a_n = nb_n +$ (lower b's) which we can solve recursively (and uniquely) for the b_i in terms of the a_i. We can also find g by the binomial series. Write $f = 1 + x$, where $x \in tA[[t]]$. Then $f^{1/n} = (1+x)^{1/n} = 1 + \Sigma_{i=1}^{\infty} \binom{1/n}{i} x^i$. The binomial coefficient $\binom{1/n}{i}$ is defined to be $\frac{\frac{1}{n}(\frac{1}{n}-1)\ldots(\frac{1}{n}-i+1)}{i!}$. This rational number can be written in the form $\frac{a}{n^d}$ for $a \in \mathbb{Z}$ and d an integer ≥ 0, which then can be interpreted as an element of A by replacing $1/n$ by the (necessarily unique) inverse of n in A. That $\binom{1/n}{i}$ has the indicated form is not obvious. You might try to prove this as an exercise. For example $\binom{1/3}{4} = \frac{(1/3)(-2/3)(-5/3)(-8/3)}{1.2.3.4} = -10/3^5$. The sum $\Sigma_{i=1}^{\infty} \binom{1/n}{i} x^i$ makes sense because $x \in tA[[t]]$, so the coefficient of any power of t is a finite sum. We note that the integer "n" in $\Lambda(A)$ is the series $(1-t)^n$ ($1-t$ being the unit of $\Lambda(A)$). The uniquely defined series $(1-t)^{1/n}$ will be denoted "$1/n$" and is the multiplicative inverse of "n" in $\Lambda(A)$ (i.e. $(1-t)^n * (1-t)^{1/n} = 1-t$, which can be proved by the distributive law). Furthermore $(1-t)^{1/n} * f = f^{1/n}$. We now have (assuming n is a unit in A) that $(1-t^n)^{1/n}$ does live in $\Lambda(A)$ and that $gh(1-t^n)^{1/n} = \epsilon_n$. From (6.10) we have $(1-t^n) * (1-t^n) = (1-t^n)^n$ from which it follows, using the distributive law, that $(1-t^n)^{1/n} * (1-t^n)^{1/n} = (1-t^n)^{1/n}$ so $\epsilon_n := (1-t^n)^{1/n}$ is indeed idempotent in $\Lambda(A)$. (I know that this is confusing. Try translating into the usual ring notation of $+$ and multiplication.)

Finally we see that $\Lambda(\mathbb{Z})$ is not an integral domain. For we have $(1-t^n) * (1-t^n) = (1-t^n)^n = (1-t^n) * (1-t)^n$ (the first equality is (6.10), the second is multiplication by "n"). Equivalently we have $(1-t^n) * [\frac{1-t^n}{(1-t)^n}] = 1$ (1 being the "zero" element of $\Lambda(A)$). Clearly in $\Lambda(\mathbb{Z})$ we have $1 - t^n \neq (1-t)^n$ if $n > 1$, so $\Lambda(\mathbb{Z})$ is not an integral domain.

Now let $S = \{1, p, p^2, p^3, \ldots\}$, p a prime number, and let T be the set of all primes but p. I will write $\epsilon_{<p>}$ for ϵ_S in this case. Then in $\Pi_{n=1}^{\infty} A$, we have

(7.1) $$\epsilon_{<p>} = \Pi_{q \in T}(1 - \epsilon_q) \ (= t + t^p + t^{p^2} + t^{p^3} + \ldots)$$

Both sides of the equal sign are idempotent and have $w_i = 0$ if i is divisible by some prime in T, 1 if not. To give an explicit example take $p = 3$. Then in the first 11 co-ordinates we have

$$1 - \epsilon_2 = 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ \ldots$$

$$1 - \epsilon_5 = 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ \ldots$$

$$1-\epsilon_7 = 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ \ldots$$

$$1-\epsilon_{11} = 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ \ldots$$

$$\Pi_{q\in T}(1-\epsilon_q) = 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ldots$$

Subsequent $q \in T$ will not change the first 11 co-ordinates of $\Pi_{q\in T}(1-\epsilon_q)$. We see that $\Pi_{q\in T}(1-\epsilon_q)$ has 1 in co-ordinates $1, 3, 3^2, \ldots$ and 0 elsewhere.

Now assume that $\mathbb{Q} \subseteq A$ and continue to let $S = \{1, p, p^2, p^3, \ldots\}$. Write $\epsilon_{<p>} = (w_1, w_2, \ldots)$. Then $gh^{-1}(\epsilon_{<p>})$ is an idempotent of $\Lambda(A)$. Write $gh^{-1}(\epsilon_{<p>}) = 1 + a_1 t + a_2 t^2 + \ldots$ where $a_i \in \mathbb{Q}$. I claim that $a_i \in \mathbb{Z}[T^{-1}]$ where by $\mathbb{Z}[T^{-1}]$ I mean that we invert the primes in T, or equivalently $a_i = b_i/c_i$ where $b_i, c_i \in \mathbb{Z}, p \nmid c_i, i \geq 1$. ($\mathbb{Z}[T^{-1}]$ is the local ring $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$ at the prime (p).) To see the claim note that a_n depends only on w_i $(i \leq n)$, hence a_n is the coefficient of t^n in $gh^{-1}(\Pi_{1\leq q\leq n,\ q\in T}(1-\epsilon_q)) = *_{q\in T, q\leq n}[\frac{1-t}{(1-t^q)^{1/q}}]$ and we have seen that the latter is of the form $1 + a'_1 t + a'_2 t^2 + \ldots$ where $a'_i \in \mathbb{Z}[T^{-1}]$. We conclude that

$$\textbf{(7.1.2)} \qquad E_{<p>} := gh^{-1}(\epsilon_{<p>})$$

lives in $\Lambda(A)$ whenever all primes but p are invertible in A and is the canonical image of an element of $\Lambda(\mathbb{Z}[T^{-1}])$ which we might denote by $*_{q\in T}[\frac{1-t}{(1-t^q)^{1/q}}]$. This infinite product in fact converges in an appropriate topology on $\Lambda(A)$ or on $\Lambda(\mathbb{Z}[T^{-1}])$. Furthermore $gh(E_{<p>}) = \epsilon_{<p>}$ whenever all primes in T are invertible in A.

Continue to assume that all primes in T are invertible in A and that $S = \{1, p, p^2, p^3, \ldots\}$. Then $E_{<p>} * \Lambda(A)$ is a ring which is contained in $\Lambda(A)$ (although with identity element $E_{<p>}$ rather than the unit element $1-t$ of $\Lambda(A)$). I will write $\Lambda_{<p>}(A)$ for $\Lambda_S(A)$ if $S = \{1, p, p^2, p^3, \ldots\}$. (This ring is usually called $W(A)$ in the literature, for example (3, section 4), but I prefer a notation including the prime p.) I claim that under these hypotheses the map

$$\textbf{(7.2)} \qquad E_{<p>} * \Lambda(A) \to \Lambda_{<p>}(A).$$

induced by the truncation homomorphism $\pi_{<p>} : \Lambda(A) \to \Lambda_{<p>}(A)$ is an isomorphism of rings.

Proof of (7.2): (1) If $\mathbb{Q} \subseteq A$ we have an isomorphism $gh : \Lambda(A) \to \Pi_{i=1}^{\infty} A$ and $gh(E_{<p>}) = \epsilon_{<p>}$ so $E_{<p>} * \Lambda(A) \to \epsilon_{<p>}\Pi_{i=1}^{\infty} A$ is an isomorphism of rings.
(2) Let $\wp : \Pi_{i=1}^{\infty} A \to \epsilon_{<p>}\Pi_{i=1}^{\infty} A$ be the canonical projection. For all A we have a commutative diagram of ring homomorphisms
(7.3)

$$\begin{array}{ccc} \Lambda(A) & \stackrel{\wp\circ gh}{\longrightarrow} & \epsilon_{<p>}\Pi_{i=1}^{\infty}(A) \\ \pi_{<p>} \downarrow & \nearrow \tau & \\ \Lambda_{<p>}(A) & & \end{array}$$

where $\wp \circ gh$ factors through $\Lambda_{<p>}(A)$ because the w_i $(i \in S)$ depend only on the x_i $(i \in S)$. Furthermore $\pi_{<p>}$ is always onto.
(3) If all primes in T are invertible in A then (7.3) restricts to
(7.4)

$$\begin{array}{ccc} E_{<p>} \circ \Lambda(A) & \stackrel{\wp\circ gh}{\longrightarrow} & \epsilon_{<p>}\Pi_{i=1}^{\infty}(A) \\ \pi_{<p>} \downarrow & \nearrow \tau & \\ \Lambda_{<p>}(A) & & \end{array}$$

where $\pi_{<p>}(E_{<p>}) = (1, 0, 0, 0, \ldots)$ (the unit element of $\Lambda_{<p>}(A)$). The this follows from $gh(E_{<p>}) = \epsilon_{<p>}$ by solving the equations (6.6) over $\mathbb{Q}$ for $x_1, x_p, x_{p^2}, \ldots$, obtaining $x_1 = 1$, $x_p = 0$, $x_{p^2} = 0, \ldots$. The latter hold in any A since $E_{<p>}$ lives in $\Lambda(\mathbb{Z}[T^{-1}])$. Thus $\pi_{<p>}$ remains a surjective ring homomorphism.
(4) If in addition $\mathbb{Q} \subseteq A$ the top arrow of (7.4) becomes the isomorphism of part (1). By diagram chasing in (7.4) we then have that $\pi_{<p>}$ is an isomorphism. The inverse η to $\pi_{<p>}$ is defined by lifting $f \in \Lambda_{<p>}(A)$ to $\Lambda(A)$ in any way, and then multiplying by $E_{<p>}$. To define η in a definite way, lift $(x_1, x_p, \ldots) \in \Lambda_{<p>}(A)$ to $(1 - x_1 t)(1 - x_p t^p)\ldots$ and then $*$ with $E_{<p>}$. This calculation shows that η is defined by universal polynomials over $\mathbb{Z}[T^{-1}]$.
(5) Because η and $E_{<p>}*$ are both defined by universal polynomials over $\mathbb{Z}[T^{-1}]$ the checking that η is a ring homomorphism and an inverse to $\pi_{<p>}$ works assuming only that the primes of T are invertible in A. Thus (7.3) is an isomorphism whenever the primes of T are invertible in A, as we wished to show. (But note that $\wp \circ gh$ may not be an isomorphism unless p is invertible in A).

8. Λ(A) in characteristic p.

Now we assume that $A \neq 0$ is of characteristic $p > 0$. That is, p is a positive prime, and in A the sum $1+1+\ldots+1$ (p times) is zero. We will continue to denote the truncation set $\{1, p, p^2, \ldots\}$ by S, and $\Lambda_S(A)$ by $\Lambda_{<p>}$. In $\Lambda(A)$ we have $(1-t)^p = 1 - t^p$ so the element "p" (sum of p 1's in $\Lambda(A)$ or $\Lambda_{<p>}(A)$) has $x_p = 1$ and $x_i = 0$ for $i \neq p$. In other words

"p" $= (0, 1, 0, 0, 0, \ldots) \in \Lambda_{<p>}(A)$.

Similarly "p^i", the sum of p^i 1's in $\Lambda(A)$ or $\Lambda_{<p>}(A)$ (equal also to the i^{th} power of "p" in the ring structure of $\Lambda(A)$ or $\Lambda_{<p>}(A)$) is equal to $(0, 0, \ldots, 1, 0, \ldots)$ where the 1 is in the p^i position.

Now consider the formulae (6.10). Suppose $i \leq j$. Then $\mathrm{LCM}(p^i, p^j) = p^j$ and $\mathrm{GCD}(p^i, p^j) = p^i$. Thus (6.10) becomes

$$(8.1) \qquad (1 - x_{p^i} t^{p^i}) * (1 - x_{p^j} t^{p^j}) = (1 - x_{p^i}^{p^{j-i}} x_{p^j} t^{p^j})^{p^i} = (1 - x_{p^i}^{p^j} x_{p^j}^{p^i} t^{p^{i+j}})$$

In particular, taking $i = 1, x_p = 1$ we obtain (in $\Lambda(A)$)

"p" $* (1 - x t^{p^j}) = (1 - t^p) * (1 - x t^{p^j}) = (1 - x^p t^{p^{j+1}})$. Thus in $\Lambda_{<p>}(A)$ we have

$$(8.2) \qquad \text{“}p\text{”} * (x_1, x_p, x_{p^2} \ldots) = (0, x_1^p, x_p^p, x_{p^2}^p \ldots)$$

i.e. multiplication by "p" shifts right and raises to the p^{th} power. Now I claim

(8.3) Lemma. Suppose that A is an integral domain of characteristic p. Then $\Lambda_{<p>}(A)$ is an integral domain of characteristic 0.

Proof. Let $f, g \in \Lambda_{<p>}(A)$ be non-zero. Write $f = (0, 0, 0, \ldots, x_{p^i}, *)$ and $g = (0, 0, 0, \ldots, y_{p^j}, *)$ where x_{p^i} and y_{p^j} are non-zero elements of A. Then by (8.1) we have that the product of f and g in $\Lambda_{<p>}(A)$ is equal to $(0, 0, \ldots, 0, x_{p^i}^{p^j} y_{p^j}^{p^i}, * \ldots)$ where $x_{p^i}^{p^j} y_{p^j}^{p^i}$ is in the p^{i+j} co-ordinate. Since A is an integral domain $x_{p^i}^{p^j} y_{p^j}^{p^i} \neq 0$, and we conclude that $\Lambda_{<p>}(A)$ is an integral domain. We already know that "n" is invertible in $\Lambda_{<p>}(A)$ if $\mathrm{GCD}(n, p) = 1$. Thus $\Lambda_{<p>}(A)$ must either be of characteristic p or characteristic 0. By (8.2) we cannot have characteristic p, so $\Lambda_{<p>}(A)$ is of characteristic 0.

(8.4) Lemma. Let A be a field of characteristic p. For $f \in \Lambda_{<p>}(A), f \neq 0$, define $v(f) := i$ where i is the smallest natural number such that the p^i-th co-ordinate of f is non-zero. Then we have (writing the ring operations of $\Lambda_{<p>}(A)$ in the usual way)

$$v(fg) = v(f) + v(g) \tag{8.4.1}$$

$$v(f+g) \geq \min(v(f), v(g)) \tag{8.4.2}$$

Proof. Property (8.4.1) follows from the proof of (8.3). Property (8.4.2) follows from the universal polynomials (6.7). The p^i co-ordinate of $f+g$ depends only on the co-ordinates $p^j (j \leq i)$ of f and g, and if all the latter co-ordinates are 0, so is the p^i co-ordinate of $f+g$, from which (8.4.2) follows.

(8.5) Lemma. Let A be any field of characteristic p. Then $\Lambda_{<p>}(A)$ is a local ring with maximal ideal $M = \{(0, *, * \ldots)\} = \{f \in \Lambda_{<p>}(A) : v(f) > 0\}$ (all elements of $\Lambda_{<p>}(A)$ with first co-ordinate 0).

Proof. The surjection $\Lambda_{<p>}(A) \to A$ given by projection $(x_1, x_p, \ldots) \to x_1$ is a ring homomorphism because the first universal polynomial in (6.7) and in (6.8) are $z_1 = x_1 + y_1$ and $z'_1 = x_1 y_1$ respectively. This shows that M is a maximal ideal. We will complete the proof of (8.5) by showing that if $g \in \Lambda_{<p>}(A)$ and $v(g) = 0$, then g is a unit in $\Lambda_{<p>}(A)$. Let $g = (x_1, x_p, \ldots)$ with $x_1 \neq 0$. In the universal polynomials (6.8) I claim that $z'_{p^n} = x_1^{p^n} y_{p^n}$ + terms in y_{p^i} with $i < n$. Given this claim, we can recursively solve for the co-ordinates y_{p^i} in the equation $g * (y_1, y_p, \ldots) = (1, 0, 0, 0, \ldots)$ from which we conclude that g is a unit in $\Lambda_{<p>}(A)$ and (8.5) follows. To see the claim, lift to $\Lambda(A)$: we have

$$[(1 - x_1 t)(1 - x_p t^p)(1 - x_{p^2} t^{p^2}) \ldots] * [(1 - y_1 t)(1 - y_p t^p)(1 - y_{p^2} t^{p^2}) \ldots]$$

Multiply this out using (8.1) and the distributive law of $\Lambda(A)$. The lowest power of t that contains y_{p^n} in its coefficient is t^{p^n}, from $(1 - x_1 t) * (1 - y_{p^n} t^{p^n}) = 1 - x_1^{p^n} y_{p^n} t^{p^n}$. Other contributions to the coefficient of t^{p^n} involve only y_{p^i} for $i < n$, so z'_{p^n} is as claimed, completing the proof.

(8.6) Lemma. Let A be a perfect field of characteristic p. Then the only non-zero ideals of $\Lambda_{<p>}(A)$ are the powers $M^i = \{(0, 0, \ldots, 0, * \ldots.)\}$ (with non-zero elements only in co-ordinates p^i or greater), and M^i is generated by "p^i".

Proof. Let I be a non-zero ideal of $\Lambda_{<p>}(A)$. Let $i = \min(v(f) \mid f \in I, f \neq 0\}$. Let $h \in I$ with $v(h) = i$. By (8.2), (using the assumption that A is perfect which implies that p^i-th roots exist in A for all $i \geq 0$) we have that h="p^i"$*g$ where $v(g) = 0$. By (8.5) g is a unit so "p^i" $\in I$. From this it follows that "p^i" generates I, that $I = M^i$, and M^i is as described in the statement of the Lemma.

(8.7) Theorem. If A is a perfect field of characteristic p, and $S = \{p^i\}_{i \geq 0}$ then $\Lambda_{<p>}(A) := \Lambda_S(A)$ is a complete discrete valuation ring of characteristic 0, with maximal ideal M generated by "p".

Proof. In view of (8.3), (8.5), (8.6) and a suitable characterization of discrete valuation ring (e.g. Proposition 9.2 of Atiyah-Macdonald, Introduction to Commutative Algebra, Addison-Wesley, 1969) we have that $\Lambda_{<p>}(A)$ is a discrete valuation ring of characteristic 0 with maximal ideal M generated by "p", and associated valuation v as in (8.4). We need only show that $\Lambda_{<p>}(A)$ is complete in the valuation v. Let $f = (a_1, a_p, a_{p^2}, \ldots)$, $g = (b_1, b_p, b_{p^2}, \ldots..)$. I claim that $v(f - g) = i$ where the first co-ordinate in which f and g differ is the p^i-th. To see this lift to $\Lambda(A)$. The difference $f - g$ in $\Lambda_{<p>}(A)$ lifts to $F = [(1-a_1t)(1-a_pt^p)(1-a_{p^2}t^{p^2})\ldots]/[(1-b_1t)(1-b_pt^p)(1-b_{p^2}t^{p^2})\ldots]$. If f and g differ first in co-ordinate p^i, terms in t^{p^j} cancel for $j < i$, and $F = (1 - (a^{p^i} - b^{p^i})t^{p^i})$ (terms involving only higher powers of t). This proves the claim. From this we see that a sequence $\{\underline{x}_1, \underline{x}_2, \ldots \underline{x}_n \ldots\}$ in $\Lambda_{<p>}(A)$ where $\underline{x}_i = (x_{i1}, x_{ip}, \ldots)$ $i \geq 1$) is a Cauchy sequence if and only if each sequence $\{x_{ip^j}\}$ (j fixed, i varying) stabilizes at some value y_{p^j} as $i \to \infty$. Clearly $\{\underline{x}_1, \underline{x}_2, \ldots \underline{x}_n \ldots\}$ converges to the element $(y_1, y_p, y_{p^2} \ldots) \in \Lambda_{<p>}(A)$ completing the proof of (8.7).

We remark that if A is a field of characteristic p, but not perfect, then M^i is strictly smaller than $\{f \in \Lambda_{<p>}(A) : v(f) \geq i\}$ and $\Lambda_{<p>}(A)$ is not a valuation ring. The first observation follows from (8.1), which implies, for example, that every element of M^2 is of the form $(0, 0, a, \ldots)$ with $a \in A^p$. If x is an element of the quotient field of $\Lambda_{<p>}(A)$, then either x or $1/x$ (the multiplicative inverse of x under $*$) is in $\Lambda_{<p>}(A)$. Consider $x = c/$"p", where c is of the form $(0, 0, a, \ldots)$ with $a \notin A^p$. Then $v(x) = 1$ so $1/x$ cannot be in $\Lambda_{<p>}(A)$ since all elements y of the latter have $v(y) \geq 0$. But also $x \notin \Lambda_{<p>}(A)$, by the above discussion.

For convenience of notation, in the rest of this section I will denote an arbitrary element of $\Lambda_{<p>}(A)$ by $(x_0, x_1, \ldots,)$ so that what we formerly called x_{p^i} will now be denoted by x_i, $i \geq 1$. The map $f : A \to \Lambda_{<p>}(A)$ defined by $f(a) = (a, 0, 0, \ldots)$ preserves multiplication but not addition (6.7), (6.8). If we write the operations of $\Lambda_{<p>}(A)$ as "+" and juxtaposition instead of respectively juxtaposition and * we can (by the discussion after (6.9)) write $x = (x_0, 0, 0, 0, \ldots..) + (0, x_1, 0, 0, \ldots..) + (0, 0, x_2, \ldots..) + \ldots$. Applying (8.2) to the latter we get $x = f(x_0) + f(x_1)^{p^{-1}}$"$p$"$+f(x_2)^{p^{-2}}$"$p^2$" $+ \ldots$. Now let $A = \mathbb{Z}/p\mathbb{Z}$ and let $\hat{\mathbb{Z}}_p$ denote the p-adic integers. The expression for x simplifies to $x = f(x_0) + f(x_1)$"p"$+f(x_2)$"p^2" $+ \ldots$. Every element a of $\hat{\mathbb{Z}}_p$ has a unique expansion in the form $a = a_0 + a_1 p + a_2 p^2 + \ldots$ where each a_i is either 0 or a primitive $(p-1)^{st}$ root of unity in $\hat{\mathbb{Z}}_p$. The p possible values for the coefficients a_i map under reduction mod p bijectively onto the elements of $\mathbb{Z}/p\mathbb{Z}$, say $a_i \to \bar{a}_i$. The unique ring homomorphism $\mathbb{Z} \to \Lambda(\mathbb{Z}/p\mathbb{Z})$ is an inclusion by (8.3). This extends to a unique homomorphism $\mathbb{Z}_{(p)} \to \Lambda(\mathbb{Z}/p\mathbb{Z})$ since all primes but p are invertible in $\Lambda(\mathbb{Z}/p\mathbb{Z})$, and then by continuity to an inclusion $\rho : \hat{\mathbb{Z}}_p \to \Lambda(\mathbb{Z}/p\mathbb{Z})$. Since a_i is a $(p-1)^{st}$ root of unity so is $\rho(a_i)$ and since ρ commutes with the "mod p" maps to $\mathbb{Z}/p\mathbb{Z}$ we have that $\rho(a_i) = f(\bar{a}_i)$. Thus we have $\rho(a) = \rho(a_0 + a_1 p + a_2 p^2 + \ldots) = \rho(a_0) + \rho(a_1)$"$p$" $+\rho(a_2)$"p^2" $+ \ldots = f(\bar{a}_0) + f(\bar{a}_1)$"$p$" $+f(\bar{a}_2)$"p^2" $+\ldots$. Since the a_i are arbitrary $(p-1)^{st}$ roots of unity, ρ is onto, hence an isomorphism.

More generally if A is any perfect field of characteristic p then $\Lambda(A)$ is the unique (up to canonical isomorphism) discrete valuation ring of characteristic 0 such that $v(p) = 1$ and $\Lambda(A)/p\Lambda(A) \cong A$ (the proof of uniqueness can be found in [6, II §5]). If R is such a discrete valuation ring then there is a map $f : R/pR \to R$ that preserves multiplication (so that $f(0) = 0$ and if $a \neq 0$ $f(a)$ has p^i-th roots for all i). Every element $a \in R$ has a unique expansion $a = a_0 + a_1^{p^{-1}} p + a_2^{p^{-2}} p^2 + \ldots$ where $a_i = f(\bar{a}_i)$. The map $\rho : R \to \Lambda_{<p>}(A)$ defined by $\rho(a) = f(\bar{a}_0) + f(\bar{a}_1)^{p^{-1}}$ "p"$+f(\bar{a}_2)^{p^{-2}}$"p^2"$+\ldots$, (which corresponds to $(\bar{a}_0, \bar{a}_1, \bar{a}_2, \ldots)$ in the vector notation used above for $\Lambda_{<p>}(A)$) is an isomorphism (page 49 of [6] and page 175 of [1]).

9. The Verschiebung and the Frobenius.

In this final section I will describe the complete structure of $\Lambda(\mathbb{Z}/p\mathbb{Z})$. In order to do this it is helpful to introduce two homomorphisms $V_n, F_n : \Lambda(A) \to \Lambda(A)$ (A any commutative ring, $n \in \mathbb{N}$).

Define $V_n : \Lambda(A) \to \Lambda(A)$ by $V_n(f(t)) = f(t^n)$. This is a homomorphism of abelian groups, but not of rings if $n > 1$. If $f = (1-x_1t)(1-x_2t^2)(1-x_3t^3)\ldots$, then $V_n(f) = (1-x_1t^n)(1-x_2t^{2n})(1-x_3t^{3n})\ldots$ so in $\Lambda_{\mathbb{N}}(A)$ ($\cong \Lambda(A)$) V_n acts by $V_n(x_1, x_2, x_3, \ldots) = (x_1', x_2', x_3', \ldots)$ where

(9.1) $\quad x_m' = x_{m/n}$ if $n \mid m$ and 0 otherwise.

For example $V_2(x_1, x_2, x_3, \ldots) = (0, x_1, 0, x_2, 0, x_3, \ldots)$.

Suppose that $gh(f(t)) = w_1t + w_2t^2 + \ldots$. Then $gh(f(t^n)) = -nt^nf'(t^n)/f(t^n) = n(w_1t^n + w_2t^{2n} + \ldots)$, so if $gh(V_n(f)) = w_1't + w_2't^2 + \ldots$ then

(9.2) $\quad w_m' = nw_{m/n}$ if $n \mid m$ and 0 otherwise.

Note that $\mathbb{N} - n\mathbb{N}$ (all natural numbers not divisible by n) is a truncation set. (Clearly if n does not divide a, then n does not divide any divisor of a.) The homomorphism V_n is injective, and the image of V_n is the kernel of the truncation map $\Lambda_{\mathbb{N}}(A) \to \Lambda_{\mathbb{N}-n\mathbb{N}}(A)$. Obviously

(9.3)
$$V_m \circ V_n = V_{mn}.$$

The map F_n is somewhat more subtle. In the w co-ordinates F_n turns out to be fairly simple, but since gh is not an isomorphism one has to be careful. In order to define F_n I will initially assume that the complex numbers $\mathbb{C} \subseteq A$. Define $F_n : \Lambda(A) \to \Lambda(A)$ by

(9.4)
$$F_n(f) = \Pi_\zeta(f(\zeta t^{1/n}))$$

where ζ ranges over the n^{th} roots in $\mathbb{C}$ of 1 (so that $t^n - 1$ factors as $\Pi(t-\zeta)$). Replacing t by $t^{-1/n}$ and multiplying by t we have $\Pi_\zeta(1-\zeta t^{1/n}) = 1-t$. To see that the right hand side of (9.4) lies in $\Lambda(A)$ it suffices to check that $F_n(1-x_mt^m)$ lies in $\Lambda(A)$. As in section 6 we will write $M = \text{GCD}(m,n)$ and $N = \text{LCM}(m,n)$. We have that $\zeta_1^m, \ldots, \zeta_n^m$ are the roots (repeated M times) of $x^{n/M} - 1$. Let η range over the n/M^{th} roots of 1. It now follows that $F_n(1-x_mt^m) = \Pi_\zeta(1-x_m\zeta^mt^{m/n}) = (\Pi_\eta(1-x_m\eta t^{m/n}))^M = (1-x_m^{n/M}t^{m/M})^M$. From $mn = MN$ we have

(9.5)
$$F_n(1-x_mt^m) = (1-x_m^{N/m}t^{N/n})^M = (1-x_m^{n/M}t^{m/M})^M$$

Applying (9.5) to $f = 1 + a_1t + a_2t^2 + \ldots = (1-x_1t)(1-x_2t^2)(1-x_3t^3)\ldots$ we see that $F_n(f) \in \Lambda(A)$ indeed $F_n(f) = 1 + \Sigma_{i\geq 1}p_i(x_1, x_2, \ldots)t^i$, where the p_i are polynomials with integer coefficients, independent of A. Furthermore we have

(9.6) $\sum_{i=1}^{n} \zeta_i^a = n$ if a is a multiple of n and 0 otherwise.

We apply (9.6) to determine how F_n behaves on the w co-ordinates, where $gh(f(t)) = w_1 t + w_2 t^2 + \ldots$. For any λ we have $gh(f(\lambda t^{1/n})) = (1/n)(\lambda t^{1/n} w_1 + \lambda^2 t^{2/n} w_2 + \lambda^3 t^{3/n} w_3 + \ldots)$. Letting λ range over the ζ_i, summing, and using (9.6) we obtain $gh(F_n(f(t)) = w_n t + w_{2n} t^{2n} + w_{3n} t^{3n} + \ldots$. that is, if

$$gh(F_n(f(t))) = w'_1 t + w'_2 t^2 + \ldots \text{ then}$$

(9.7)
$$w'_m = w_{mn}$$

The conditions (9.7) define a ring homomorphism $\Pi_{i=1}^{\infty} A \to \Pi_{i=1}^{\infty}$A. Therefore F_n is a ring homomorphism.

Because the p_i mentioned after (9.5) have coefficients in $\mathbb{Z}$ we can use them to define F_n for arbitrary A. By the usual universal polynomial argument using the p_i we obtain that F_n is a ring homomorphism for all A.

We now examine three extreme cases of (9.5). First of all, assume that m and n are relatively prime. Then $M = \mathrm{GCD}(m,n) = 1$, and (9.5) becomes

(9.8)
$$F_n(1 - x_m t^m) = (1 - x_m^n t^m), \ \mathrm{GCD}(m,n) = 1$$

If $n \mid m$ then $N = m$ and $M = n$ and we get

(9.9)
$$F_n(1 - x_m t^m) = (1 - x_m t^{m/n})^n, \ n \mid m$$

If $m \mid n$ then $N = n$ and $M = m$ and we get

(9.10)
$$F_n(1 - x_m t^m) = (1 - x_m^{n/m} t)^m, \ m \mid n$$

As one example we have $F_2(1 - x_m t^m) = (1 - x_m (t^{1/2})^m)(1 - x_m((-1)t^{1/2})^m)$. If m is even this equals $(1 - x_m t^{m/2})^2$ as in (9.9). If m is odd we get $(1 - x_m (t^{1/2})^m)(1 + x_m (t^{1/2})^m) = 1 - x_m^2 t^m$ as in (9.8).

We now have

(9.11)
$$F_n \circ V_n = n$$

This can be checked using (9.9) or by observing that on the w co-ordinates $F_n \circ V_n = n$ (check first assuming that A contains $\mathbb{Q}$ and then use the universal argument). Note that (9.11) is written using additive notation, so that for $f \in \Lambda(A)$, (9.11) means that $F_n(V_n(f)) = f^n$. If n is a unit in A (hence also in $\Lambda(A)$, as was noted in Section 7) we have from (9.11) that $F_n \circ ((1/n)V_n) = 1$ (the identity endomorphism) from which it follows that $((1/n)V_n) \circ F_n$ is an idempotent endomorphism of $\Lambda(A)$. In fact, we have $((1/n)V_n) \circ F_n(1-t) = ((1/n)V_n)(1-t) = (1-t^n)^{1/n}$ which was shown in Section 7 to be an idempotent of $\Lambda(A)$. Furthermore $(1/n)V_n$ is a homomorphism of rings without unit, as can be checked in the w co-ordinates if $\mathbb{Q} \subseteq A$, hence holds whenever n is a unit in A.

As in Section 7 let $S = \{1, p, p^2, \ldots\}$ (p a prime). Suppose that $\mathrm{GCD}(q,p) = 1, q \in \mathbb{N}$. Let $qS = \{q, qp, qp^2, \ldots\}$. The idempotent giving projection of $\Pi_{i=1}^{\infty} A$ onto the co-ordinates qS is $\epsilon_{qS} = t^q + t^{qp} + t^{qp^2} + \ldots$. Clearly in $\Pi_{i=1}^{\infty} A$, $\epsilon_{qS} = \Pi_\alpha(\epsilon_q - \epsilon_{q\alpha})$ as α ranges over all primes except p. (As in Section 7, for $n \in \mathbb{N}, \epsilon_n = t^n + t^{2n} + t^{3n} + \ldots$, the idempotent of $\Pi_{i=1}^{\infty} A$ giving projection onto the co-ordinates that are multiples of n.) If all primes but p are invertible in A, we can define

(9.12) $\quad E_{<q,p>} := *_\alpha \frac{(1-t^q)^{1/q}}{(1-t^{q\alpha})^{1/q\alpha}}$ (α ranging over all primes except p).

Then $E_{<q,p>}$ is an idempotent of $\Lambda(A)$ and $gh(E_{<q,p>}) = \epsilon_{qS}$. We now have

(9.13) Lemma. If all primes but p are invertible in A, then $\Pi_q E_{<q,p>} = 1-t$ (q ranging over all elements of $\mathbb{N}$ that are prime to p). Furthermore if $q_1 \neq q_2$ then $E_{<q_1,p>} * E_{<q_2,p>} = 1$. (Here Π means multiplication of power series, i.e. the addition of $\Lambda(A), 1-t$ is the unit element, and 1 is the 0 element of $\Lambda(A)$), so we obtain an infinite product decomposition of $\Lambda(A)$).

Proof. If $\mathbb{Q} \subseteq A$ we can apply the isomorphism gh. The assertion (9.13) becomes $\Sigma_q \epsilon_{qS} = 1$ and $\epsilon_{q_1 S}\epsilon_{q_2 S} = 0$, both of which are clearly true, so (9.13) holds if $\mathbb{Q} \subseteq A$. But the coefficients of the $E_{<q,p>}$ live in $\mathbb{Z}_{(p)}$ (in the notation of Section 7, $\mathbb{Z}_{(p)} = \mathbb{Z}[T^{-1}]$.) Hence (9.13) holds for all A in which all primes but p are invertible.

Clearly we have $((1/q)V_q)(E_{<p>}) = E_{<q,p>}$ ($E_{<p>}$ is as in Section 7, and is equal to $E_{<1,p>}$ in the notation of (9.12)). Also we have

(9.14) Theorem. If all primes but p are invertible in A, then

$$((1/q)V_q) : E_{<p>} * \Lambda(A) \to E_{<q,p>} * \Lambda(A)$$

is an isomorphism of rings (with inverse F_q) for all q prime to p.

Proof. If $\mathbb{Q} \subseteq A$ we can apply the isomorphism gh and check in the w co-ordinates where the assertion is clear. The result then follows for all A in which all primes but p are invertible, since $E_{<p>}$ and $E_{<q,p>}$ both have coefficients in $\mathbb{Z}_{(p)}$, $(1/q)V_q$ is defined over $\mathbb{Z}[q^{-1}] \subseteq \mathbb{Z}_{(p)}$ and F_q is defined over $\mathbb{Z}$.

Putting (9.13) and (9.14) together we obtain our main result:

(9.15) Theorem. If all primes but p are invertible in A, then $\Lambda(A) \cong \Pi\Lambda_{<p>}(A)$ (one copy for every $q \in \mathbb{N}$, $\mathrm{GCD}(q,p) = 1$) , where $S = \{1, p, p^2, \ldots\}$ and $\Lambda_{<p>}(A)$ is the truncation onto S as defined in (6.11) and Section 7. The product is taken over all natural numbers prime to p. In particular $\Lambda(\mathbb{Z}/p\mathbb{Z}) \cong \Pi\hat{\mathbb{Z}}_p$.

I would like to make one final remark: (in the renumbering introduced in the second last paragraph of section 8) V_p acts on $\Lambda_{<p>}(A)$ by $V_p(x_1, x_2, \ldots) = (0, x_1, x_2, \ldots)$, so the name Verschiebung (which in german means shift) seems appropriate. Furthermore by (9.10) we have that $F_p(1 - x_i t^{p^i}) = (1 - x_i^p t^{p^i})$, i.e. F_p acts by raising the co-ordinates to the p^{th} power. This is consistent with the familiar meaning of Frobenius in algebraic geometry in characteristic p. Also $(F_p \circ V_p)(x_1, x_2, \ldots) = (0, x_1^p, x_2^p, \ldots) =$ "p" $* (x_1, x_2 \ldots)$, so $F_p \circ V_p = p$ agreeing with (9.11). On $\Lambda_{<p>}(A)$ we also have $V_p \circ F_p = p$.

References

1. G.M.Bergman, Appendix on Witt Vectors in "Lectures on Curves on an Algebraic Surface" by D.Mumford, Annals of Mathematics Studies 59, Princeton University Press, 1966.

2. P.Berthelot, A.Grothendieck, and L.Illusie, Théorie des Intersections et Théorème de Riemann-Roch, Lecture Notes in Mathematics 225, Springer-Verlag, 1971.

3. N.Bourbaki, Algèbre Commutative, Chapitre 9, Masson, 1983.

4. W.Fulton and S.Lang, Riemann-Roch Algebra, Springer-Verlag, 1985

5. A.V.Geramita, Inverse Systems of Fat Points: Waring's Problem, Secant Varieties of Veronese Varieties and Parameter Spaces for Gorenstein Ideals, 3-114, Curves Seminar at Queen's X, QPPAM 102, 1996.

6. J.P.Serre, Corps Locaux, Hermann, Paris, 1962.