

Introduction

I know of two standard references for the basic theory of Witt vectors: some exercises in Lang’s *Algebra* and a section in Serre’s *Local Fields*. I recently decided to try to understand Witt vectors and started working through the exercises in Lang. I soon decided that I would not be able to remember all the crazy formulas, so I put away Lang and started trying to work it out on my own. These notes summarize my thoughts. It may be that the only way really to understand Witt vectors is to work it out for yourself—surely, a certain amount of staring at the formulas is necessary—and so these notes may be useless. Perhaps they are best used as a guide to help you do the same work I did, and they may allow you to do it in less time than it took me.

If you decide to read no further than this introduction, here are some things to remember: the basic example of Witt vectors is

$$W(\mathbb{F}_p) = \mathbb{Z}_p;$$

the identification is

$$a \stackrel{\text{def}}{=} (a_0, a_1, a_2, \dots) \leftrightarrow \chi(a_0) + \chi(a_1)p + \chi(a_2)p^2 + \dots,$$

where $\chi: \mathbb{F}_p \rightarrow \mathbb{Z}_p$ is the Teichmüller character: $\overline{\chi(a)} = a$ (the bar denoting reduction modulo p) and $\chi(a)^p = \chi(a)$ (so that $\chi(a) \in \{0\} \cup \mu_{p-1}(\mathbb{Z}_p)$). Unfortunately, the basic example is not quite interesting enough to illustrate everything you want to do with Witt vectors, so you need the following generalization:

$$W(\mathbb{F}_q) = \mathbb{Z}_p[\mu_{q-1}],$$

where q is a power of p . The identification is given by

$$a \stackrel{\text{def}}{=} (a_0, a_1, a_2, \dots) \leftrightarrow \chi(a_0) + \chi(a_1)^{p^{-1}}p + \chi(a_2)^{p^{-2}}p^2 + \dots,$$

where χ again denotes the Teichmüller character and $a \mapsto a^{p^{-1}}$ is the inverse of the Frobenius automorphism of \mathbb{F}_q over \mathbb{F}_p .

If you decide to read beyond this introduction, you will see why these formulas are the only ones which can possibly work.

Notation

p denotes a prime number.

$q = p^d$ denotes a power of p .

\mathbb{F}_q is the field with q elements; it is an extension of degree d over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

$\chi: \mathbb{F}_q \rightarrow \overline{\mathbb{Q}_p}$ denotes the Teichmüller character, as above.

Main Idea

The basic idea of Witt vectors is to build \mathbb{Z}_p from \mathbb{F}_p . In principle, it is possible to do this without knowing about \mathbb{Z}_p , but this approach seems unmotivated to me. I will assume some knowledge of \mathbb{Z}_p (such as existence of the Teichmüller character).

The basic idea is that a p -adic number (*i.e.*, an element of \mathbb{Z}_p) is a power series in p , with coefficients $0, 1, \dots, p - 1$:

$$a_0 + a_1p + a_2p^2 + \dots$$

Therefore it should be possible to identify a p -adic number with an infinite sequence

$$a = (a_0, a_1, a_2, \dots) \quad \text{with} \quad a_n \in \mathbb{F}_p.$$

The only trouble is how to define addition and multiplication: when you add $p - 1$ to itself, you should get $(p - 2) + 1 \cdot p$ and so forth. Unfortunately, I can think of no good way to do this. (Presumably, neither could Witt.)

Modified Main Idea

Of course, when you think of a p -adic number as a power series in p with coefficients in \mathbb{F}_p , you really lift the coefficients to \mathbb{Z}_p . The obvious way to do this is to lift them to $0, 1, \dots, p-1$. I was once told that another good choice is to use the Teichmüller representatives. Recall: in \mathbb{F}_p , every non-zero number is a $(p-1)$ th root of 1; by Hensel's lemma, for each $a \in \mathbb{F}_p^\times$ there is a $\chi(a) \in \mathbb{Z}_p$ such that $\chi(a)$ is also a $(p-1)$ th root of 1 and $\overline{\chi(a)} = a$; also set $\chi(0) = 0$; then $\chi(a)$ is called the *Teichmüller representative* of a and χ is called the *Teichmüller character*. (One can include 0 with the others by noting that $\chi(a)^p = \chi(a)$ for all a .)

The idea now is to identify the infinite sequence

$$a = (a_0, a_1, a_2, \dots) \quad \text{with} \quad a_n \in \mathbb{F}_p$$

(the *Witt vector* a) with the p -adic number

$$\chi(a_0) + \chi(a_1)p + \chi(a_2)p^2 + \dots$$

The question is this: how should Witt vectors be added and multiplied so that this identification will respect addition and multiplication? Let a and b be Witt vectors and let c be the Witt vector such that

$$\sum_{n=0}^{\infty} \chi(c_n)p^n = \sum_{n=0}^{\infty} \chi(a_n)p^n + \sum_{n=0}^{\infty} \chi(b_n)p^n.$$

This is equivalent to the sequence of congruences

$$\begin{aligned} \chi(c_0) &\equiv \chi(a_0) + \chi(b_0) \pmod{p} \\ \chi(c_0) + \chi(c_1)p &\equiv \chi(a_0) + \chi(a_1)p + \chi(b_0) + \chi(b_1)p \pmod{p^2} \\ \chi(c_0) + \chi(c_1)p + \chi(c_2)p^2 &\equiv \chi(a_0) + \chi(a_1)p + \chi(a_2)p^2 + \chi(b_0) + \chi(b_1)p + \chi(b_2)p^2 \pmod{p^3} \\ &\vdots \end{aligned}$$

Obviously, the first congruence implies that $c_0 = a_0 + b_0$. The second congruence becomes

$$\chi(c_1) \equiv \frac{\chi(a_0) + \chi(b_0) - \chi(c_0)}{p} + \chi(a_1) + \chi(b_1) \pmod{p}.$$

The question now is this: we know that the above quotient is a (p -adic) integer; how can its reduction \pmod{p} be expressed in terms of a_0 and b_0 ? After some thought, one realizes that the first congruence implies

$$\begin{aligned} \chi(c_0) &= \chi(c_0)^p \stackrel{!}{\equiv} (\chi(a_0) + \chi(b_0))^p \pmod{p^2} \\ &= \chi(a_0)^p + \chi(b_0)^p + p[\chi(a_0)^{p-1}\chi(b_0) + \frac{p-1}{2}\chi(a_0)^{p-2}\chi(b_0)^2 + \dots + \chi(a_0)\chi(b_0)^{p-1}] \\ &= \chi(a_0) + \chi(b_0) + p[\chi(a_0)^{p-1}\chi(b_0) + \dots + \chi(a_0)\chi(b_0)^{p-1}], \end{aligned}$$

according to the following

Lemma:

If $x \equiv y \pmod{p}$ then $x^p \equiv y^p \pmod{p^2}$; more generally, if $x \equiv y \pmod{p^k}$ then $x^{p^r} \equiv y^{p^r} \pmod{p^{k+r}}$ (assuming $k \neq 0$). (Proof left to the reader.)

Therefore

$$c_1 = \overline{\chi(c_1)} = \overline{\chi(a_1)} + \overline{\chi(b_1)} - \left[\overline{\chi(a_0)^{p-1}\chi(b_0)} + \dots + \overline{\chi(a_0)\chi(b_0)^{p-1}} \right] = a_1 + b_1 - \left[a_0^{p-1}b_0 + \dots + a_0b_0^{p-1} \right].$$

It takes considerably more work to derive the expression for c_2 . I encourage you to spend a few minutes trying. If you do so, you will probably notice that you rarely use the fact that a_n, b_n , and c_n are Teichmüller representatives (*i.e.*, that $a_n^p = a_n$ *etc.*). If you try not to use this fact, you find that you are analyzing the congruences

$$\begin{aligned}\chi(c_0) &\equiv \chi(a_0) + \chi(b_0) \pmod{p} \\ \chi(c_0)^p + \chi(c_1)p &\equiv \chi(a_0)^p + \chi(a_1)p + \chi(b_0)^p + \chi(b_1)p \pmod{p^2} \\ \chi(c_0)^{p^2} + \chi(c_1)^p p + \chi(c_2)p^2 &\equiv \chi(a_0)^{p^2} + \chi(a_1)^p p + \chi(a_2)p^2 + \chi(b_0)^{p^2} + \chi(b_1)^p p + \chi(b_2)p^2 \pmod{p^3} \\ &\vdots\end{aligned}$$

Furthermore, you rarely use the fact that you are working modulo a power of p . You begin to suspect the existence of some universal formula...

Next Idea

Suppose that there are “universal formulas”

$$z_n = \alpha_n(x_0, \dots, x_n, y_0, \dots, y_n)$$

(*i.e.*, a sequence of polynomials $\alpha_0, \alpha_1, \alpha_2, \dots$ with $\alpha_n \in \mathbb{Z}[x_0, \dots, x_n, y_0, \dots, y_n]$) such that

$$\begin{aligned}z_0 &= x_0 + y_0; \\ z_0^p + z_1p &= x_0^p + x_1p + y_0^p + y_1p; \\ z_0^{p^2} + z_1p + z_2p^2 &= x_0^{p^2} + x_1p + x_2p^2 + y_0^{p^2} + y_1p + y_2p^2; \\ &\vdots \\ \sum_{k=0}^n z_k p^{n-k} p^k &= \sum_{k=0}^n x_k p^{n-k} p^k + \sum_{k=0}^n y_k p^{n-k} p^k \\ &\vdots\end{aligned}$$

Letting $c_n = \alpha_n(a_0, \dots, a_n, b_0, \dots, b_n)$ in \mathbb{F}_p , it would then follow that

$$\begin{aligned}\sum_{k=0}^{\infty} \chi(c_k) p^k &\equiv \sum_{k=0}^n \chi(c_k) p^k = \sum_{k=0}^n \chi(c_k)^{p^{n-k}} p^k \\ &\stackrel{!}{\equiv} \sum_{k=0}^n \chi(a_k)^{p^{n-k}} p^k + \sum_{k=0}^n \chi(b_k)^{p^{n-k}} p^k \\ &= \sum_{k=0}^n \chi(a_k) p^k + \sum_{k=0}^n \chi(b_k) p^k \\ &\equiv \sum_{k=0}^{\infty} \chi(a_k) p^k + \sum_{k=0}^{\infty} \chi(b_k) p^k \pmod{p^{n+1}}\end{aligned}$$

because

$$\begin{aligned}c_k &= \alpha_k(a_0, \dots, a_k, b_0, \dots, b_k) \\ \chi(c_k) &\equiv c'_k \stackrel{\text{def}}{=} \alpha_k(\chi(a_0), \dots, \chi(a_k), \chi(b_0), \dots, \chi(b_k)) \pmod{p} \\ \chi(c_k)^{p^{n-k}} &\equiv (c'_k)^{p^{n-k}} \pmod{p^{n+1-k}} \\ \chi(c_k)^{p^{n-k}} p^k &\equiv (c'_k)^{p^{n-k}} p^k \pmod{p^{n+1}} \\ \sum_{k=0}^n \chi(c_k)^{p^{n-k}} p^k &\equiv \sum_{k=0}^n (c'_k)^{p^{n-k}} p^k = \sum_{k=0}^n \chi(a_k)^{p^{n-k}} p^k + \sum_{k=0}^n \chi(b_k)^{p^{n-k}} p^k \pmod{p^{n+1}}.\end{aligned}$$

Notation

For a Witt vector $x = (x_0, x_1, x_2, \dots)$, let

$$x^{(n)} \stackrel{\text{def}}{=} x_0^{p^n} + x_1^{p^{n-1}} p + \dots + x_k^{p^{n-k}} p^k + \dots + x_n p^n.$$

Also, let

$$\begin{aligned} \phi: \mathbb{Z}[x_0, x_1, x_2, \dots, y_0, y_1, y_2, \dots] &\longrightarrow \mathbb{Z}[x_0, x_1, x_2, \dots, y_0, y_1, y_2, \dots] \\ \alpha(x_0, x_1, x_2, \dots, y_0, y_1, y_2, \dots) &\mapsto \alpha(x_0^p, x_1^p, x_2^p, \dots, y_0^p, y_1^p, y_2^p, \dots). \end{aligned}$$

Inductive Step:

$$\begin{aligned} x^{(n)} &\stackrel{\text{def}}{=} x_0^{p^n} + x_1^{p^{n-1}} p + \dots + x_{n-1}^{p^{n-1}} p^{n-1} + x_n p^n \\ &= (x_0^p)^{p^{n-1}} + (x_1^p)^{p^{n-2}} p + \dots + (x_{n-1}^p)^{p^{n-1}} + x_n p^n \\ &= \phi(x^{(n-1)}) + x_n p^n, \end{aligned}$$

so if $z^{(n)} = x^{(n)} + y^{(n)}$ for all n then

$$z_n = x_n + y_n + \frac{\phi(x^{(n-1)} + y^{(n-1)}) - [z_0^{p^n} + z_1^{p^{n-1}} p + \dots + z_{n-1} p^{n-1}]}{p^n};$$

$$\phi(x^{(n-1)} + y^{(n-1)}) = \phi(z^{(n-1)}) = \sum_{k=0}^{n-1} \phi(z_k^{p^{n-1-k}} p^k) = \sum_{k=0}^{n-1} \phi(z_k)^{p^{n-1-k}} p^k;$$

$$\phi(z_k) \equiv z_k^p \pmod{p}; \quad \phi(z_k)^{p^{n-1-k}} \equiv z_k^{p^{n-k}} \pmod{p^{n-k}}; \quad \phi(z_k)^{p^{n-1-k}} p^k \equiv z_k^{p^{n-k}} p^k \pmod{p^n};$$

$$\phi(x^{(n-1)} + y^{(n-1)}) \equiv \sum_{k=0}^{n-1} \phi(z_k)^{p^{n-k}} p^k \pmod{p^n}$$

$$z_n \in \mathbb{Z}[x_0, x_1, \dots, x_n, y_0, y_1, \dots, y_n].$$

Conclusion

There are polynomials $\alpha_n \in \mathbb{Z}[x_0, x_1, \dots, x_n, y_0, y_1, \dots, y_n]$ ($n = 0, 1, 2, \dots$) such that $(\forall n) \alpha^{(n)} = x^{(n)} + y^{(n)}$; *i.e.*,

$$\alpha_0^{p^n} + \alpha_1^{p^{n-1}} p + \dots + \alpha_n p^n = x_0^{p^n} + x_1^{p^{n-1}} p + \dots + x_n p^n + y_0^{p^n} + y_1^{p^{n-1}} p + \dots + y_n p^n.$$

It follows that if $a_0, a_1, \dots, b_0, b_1, \dots \in \mathbb{F}_p$ and $c_n = \alpha_n(a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_n)$ then

$$\begin{aligned} (\forall n) \quad &\chi(c_0) + \chi(c_1) p + \dots + \chi(c_n) p^n \equiv \\ &\equiv \chi(a_0) + \chi(a_1) p + \dots + \chi(a_n) p^n + \chi(b_0) + \chi(b_1) p + \dots + \chi(b_n) p^n \pmod{p^{n+1}}; \\ &\sum_{k=0}^{\infty} \chi(c_k) p^k = \sum_{k=0}^{\infty} \chi(a_k) p^k + \sum_{k=0}^{\infty} \chi(b_k) p^k. \end{aligned}$$

Products

Now let

$$\sum_{k=0}^{\infty} \chi(c_k) p^k = \sum_{k=0}^{\infty} \chi(a_k) p^k \cdot \sum_{k=0}^{\infty} \chi(b_k) p^k$$

in \mathbb{Z}_p . Can we express c_n in terms of $a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_n$? Guided by what we have already done, we look for polynomials π_0, π_1, \dots with $\pi_n \in \mathbb{Z}[x_0, x_1, \dots, x_n, y_0, y_1, \dots, y_n]$ such that $\pi^{(n)} = x^{(n)}y^{(n)}$. If such a sequence exists and we let $c_n = \pi_n(a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_n)$ then

$$\begin{aligned}
(\forall k) \quad \chi(c_k) &\equiv \pi_k(\chi(a_0), \chi(a_1), \dots, \chi(a_k), \chi(b_0), \chi(b_1), \dots, \chi(b_k)) \pmod{p}; \\
(\forall k, n) \quad \chi(c_k)^{p^{n-k}} &\equiv \pi_k(\chi(a_0), \chi(a_1), \dots, \chi(a_k), \chi(b_0), \chi(b_1), \dots, \chi(b_k))^{p^{n-k}} \pmod{p^{n+1-k}}; \\
(\forall k, n) \quad \chi(c_k)^{p^{n-k}} p^k &\equiv \pi_k(\chi(a_0), \chi(a_1), \dots, \chi(a_k), \chi(b_0), \chi(b_1), \dots, \chi(b_k))^{p^{n-k}} p^k \pmod{p^{n+1}}; \\
(\forall n) \quad \sum_{k=0}^{\infty} \chi(c_k) p^k &\equiv \sum_{k=0}^n \chi(c_k) p^k = \sum_{k=0}^n \chi(c_k)^{p^{n-k}} p^k \equiv \\
&\equiv \sum_{k=0}^n \pi_k(\chi(a_0), \chi(a_1), \dots, \chi(a_k), \chi(b_0), \chi(b_1), \dots, \chi(b_k))^{p^{n-k}} p^k = \\
&= \sum_{k=0}^n \chi(a_k)^{p^{n-k}} p^k \cdot \sum_{k=0}^n \chi(b_k)^{p^{n-k}} p^k = \sum_{k=0}^n \chi(a_k) p^k \cdot \sum_{k=0}^n \chi(b_k) p^k \equiv \\
&\equiv \sum_{k=0}^{\infty} \chi(a_k) p^k \cdot \sum_{k=0}^{\infty} \chi(b_k) p^k \equiv \pmod{p^{n+1}}.
\end{aligned}$$

To show that such polynomials exist, work by induction: $\pi_0 = x_0 y_0$, of course, and if $\pi^{(n-1)} = x^{(n-1)} y^{(n-1)}$ then we can solve $\pi^{(n)} = x^{(n)} y^{(n)}$ for π_n :

$$\begin{aligned}
\pi_0^n + \pi_1^{p^{n-1}} p + \dots + \pi_{n-1}^{p^n} p^{n-1} + \pi_n p^n &= \pi^{(n)} = x^{(n)} y^{(n)} = \\
&= (\phi(x^{(n-1)}) + x_n p^n) (\phi(y^{(n-1)}) + y_n p^n) \\
&= \phi(x^{(n-1)}) \phi(y^{(n-1)}) + (\phi(x^{(n-1)}) y_n + x_n \phi(y^{(n-1)}) + x_n y_n p^n) p^n; \\
\pi_n &= \frac{\phi(x^{(n-1)} y^{(n-1)}) - [\pi_0^{p^n} + \pi_1^{p^{n-1}} p + \dots + \pi_{n-1}^{p^n} p^{n-1}]}{p^n} + \phi(x^{(n-1)}) y_n + x_n \phi(y^{(n-1)}) + x_n y_n p^n;
\end{aligned}$$

$$\phi(x^{(n-1)} y^{(n-1)}) = \phi(\pi^{(n-1)}) = \phi(\pi_0)^{p^{n-1}} + \dots + \phi(\pi_{n-1})^p p^{n-1};$$

$$\phi(\pi_k) \equiv \pi_k^p \pmod{p}; \quad \phi(\pi_k)^{p^{n-1-k}} \equiv \pi_k^{p^{n-k}} \pmod{p^{n-k}}; \quad \phi(\pi_k)^{p^{n-1-k}} p^k \equiv \pi_k^{p^{n-k}} p^k \pmod{p^n};$$

$$\pi_n \in \mathbb{Z}[x_0, x_1, \dots, x_n, y_0, y_1, \dots, y_n].$$

Other Finite Fields

We can now describe \mathbb{Z}_p algebraically, starting from \mathbb{F}_p : an element of \mathbb{Z}_p can be identified with a Witt vector (infinite sequence) $a = (a_0, a_1, a_2, \dots)$ of elements of \mathbb{F}_p ; addition and multiplication are given by the universal polynomials α_n, π_n ($n = 0, 1, 2, \dots$):

$$\begin{aligned}
a + b &= (\alpha_0(a_0, b_0), \alpha_1(a_0, a_1, b_0, b_1), \dots) \\
ab &= (\pi_0(a_0, b_0), \pi_1(a_0, a_1, b_0, b_1), \dots).
\end{aligned}$$

(Of course, we realize that $a \leftrightarrow \sum_{k=0}^{\infty} \chi(a_k) p^k \in \mathbb{Z}_p$, etc.)

If we start with \mathbb{F}_q ($q = p^f$), can we construct finite extensions of \mathbb{Z}_p by taking Witt vectors $a = (a_0, a_1, a_2, \dots)$ with $a \in \mathbb{F}_q$? Let $\chi: \mathbb{F}_q \rightarrow \mathbb{Z}_p[\mu_{q-1}]$ denote the Teichmüller character. We can identify a with $\chi(a_0) + \chi(a_1)p + \chi(a_2)p^2 + \dots$. This gives a bijection between Witt vectors and $\mathbb{Z}_p[\mu_{q-1}]$, but it does *not* respect addition. Indeed, let $c = a + b$ as Witt vectors. Then $\chi(c_0)^p \neq \chi(c_0)$ (for some choices of a_0, b_0 , assuming $q > p$) so there is no reason to expect $c_0^p + c_1 p = a_0^p + a_1 p + b_0^p + b_1 p$ to imply $\chi(c_0) + \chi(c_1) p \stackrel{?}{\equiv} \chi(a_0) + \chi(a_1) p + \chi(b_0) + \chi(b_1) p \pmod{p^2}$. I do not actually have an example in which this fails; consider this an exercise.

The solution is to associate the Witt vector $a = (a_0, a_1, a_2, \dots)$ with

$$\chi(a_0) + \chi(a_1)^{p^{-1}} p + \chi(a_2)^{p^{-2}} p^2 + \dots \in \mathbb{Z}_p[\mu_{q-1}].$$

This makes sense: the Frobenius map $\alpha \mapsto \alpha^p$ is an isomorphism on \mathbb{F}_q and on μ_{q-1} (and extends to an isomorphism of $\mathbb{Z}_p[\mu_{q-1}]$ or $\mathbb{Q}_p[\mu_{q-1}]$) and $\alpha \mapsto \alpha^{p^{-1}}$ is its inverse. (Of course, we could write $\chi(a_k^{p^{-k}})$ instead of $\chi(a_k)^{p^{-k}}$.) It is easy to check that this bijection is also a homomorphism between the set of Witt vectors over \mathbb{F}_q and $\mathbb{Z}_p[\mu_{q-1}]$.

Generalizations and Applications

If A is any ring, let $W(A) = W_p(A)$ be the ring of Witt vectors $a = (a_0, a_1, a_2, \dots)$ with $a_n \in A$ and addition and multiplication given by the universal polynomials α_n, π_n ($n = 0, 1, 2, \dots$).

Lang gives a more general definition: for $1 \leq N \in \mathbb{Z}$, he lets

$$X^{(N)} \stackrel{\text{def}}{=} \sum_{d|N} dX_d^{N/d}.$$

(Actually, I am changing notation slightly.) In particular, if we replace N with p^n and let $d = p^k$, $X^{(p^n)} = \sum_{k=0}^n p^k X_{p^k}^{p^{n-k}}$, so that if $x_n \stackrel{\text{def}}{=} X_{p^n}$ then $x^{(n)} = X^{(p^n)}$. Using the fact that X_1, X_2, \dots can be recovered (as polynomials with integral coefficients) from the coefficients of

$$f_X(t) \stackrel{\text{def}}{=} \prod_{N=1}^{\infty} (1 - X_N t^N) \stackrel{!}{=} \exp\left(-\sum_{N=1}^{\infty} \frac{1}{N} X^{(N)} t^N\right) \in \mathbb{Z}[X_1, X_2, \dots][[t]],$$

Lang shows that there are universal polynomials $Z_1, Z_2, \dots \in \mathbb{Z}[X_1, X_2, \dots, Y_1, Y_2, \dots]$ such that $Z^{(N)} = X^{(N)} + Y^{(N)}$; similarly for multiplication. The formulas for Witt vectors that I have derived follow by taking $x_n = X_{p^n}$, etc.. Thus $W_p(A)$ is a quotient of a ring of universal (*i.e.*, independent of p) Witt vectors; I will temporarily denote this ring $W(A)$. (Lang mistakenly says that $W_p(A)$ is a *subring* of $W(A)$, not a quotient. More precisely, he claims that the set of Witt vectors $(a_1, a_2, a_3, \dots) \in W(A)$ for which $a_N = 0$ unless $N = p^n$ forms a subring, which is clearly false.)

There may be some applications of these “universal” Witt vectors, and of the power series $f_X(t)$; I do not know. Lang also uses Witt vectors to develop the “Kummer theory” (Artin-Schreier theory?) of a perfect field k of characteristic p , *i.e.*, to describe the Abelian extensions of k of exponent a power of p .

Serre shows that for any $\Phi \in \mathbb{Z}[X, Y]$ there is a sequence of polynomials $\beta_0, \beta_1, \beta_2, \dots$ with $\beta_n \in \mathbb{Z}[X_0, X_1, \dots, X_n, Y_0, Y_1, \dots, Y_n]$ such that $\beta^{(n)} = \Phi(X^{(n)}, Y^{(n)})$. I proved the cases $\Phi(X, Y) = X + Y$ and $\Phi(X, Y) = XY$; the general case follows from these two cases, or it can be deduced similarly. Serre gives a more sophisticated proof, for which he has other applications in mind. Serre uses Witt vectors to study the structure of complete discrete valuation rings.

Both Lang and Serre have good reasons to be concise. Perhaps the whole point of this rather leisurely treatment is that if you want to understand Witt vectors, you should start with the idea of building \mathbb{Z}_p out of \mathbb{F}_p and see that you are forced to consider

$$x^{(n)} \stackrel{\text{def}}{=} x_0^{p^n} + x_1^{p^{n-1}} p + \dots + x_k^{p^{n-k}} p^k + \dots + x_n p^n.$$

The more concise approach starts off “Let $x^{(n)} = \dots$ ”

The Maps F and V

Now that the basic examples have been hammered in, definitions like

$$F(a_0, a_1, a_2, \dots) = (a_0^p, a_1^p, a_2^p, \dots)$$

and

$$V(a_0, a_1, a_2, \dots) = (0, a_0, a_1, a_2, \dots)$$

should present no difficulty. Since F is trivial on $W(\mathbb{F}_p) = \mathbb{Z}_p$, look at the more interesting example of $W(\mathbb{F}_q) = \mathbb{Z}_p[\mu_{q-1}]$. It is clear that F gives the Frobenius automorphism of $\mathbb{Z}_p[\mu_{q-1}]$. At first glance it looks as though V is multiplication by p , but a closer look shows that $F \circ V = V \circ F$ corresponds to multiplication by p . In general, F is a ring automorphism and V is an additive homomorphism.

A More Sophisticated Point of View

I have been talking about “universal polynomials,” such as $\alpha_0, \alpha_1, \dots \in \mathbb{Z}[x_0, x_1, \dots, y_0, y_1, \dots]$. What this means is that $\mathbb{Z}[x_0, x_1, \dots]$ is the *universal example* of a ring with an infinite sequence: given any ring A and a sequence $a = (a_0, a_1, a_2, \dots)$ in A , there is one and only one homomorphism

$$\mathbb{Z}[x_0, x_1, \dots] \longrightarrow A$$

such that $(\forall n) x_n \mapsto a_n$. Similarly, $\mathbb{Z}[x_0, x_1, \dots, y_0, y_1, \dots]$ is the universal example of a ring with *two* infinite sequences. (Yes, two infinite sequences can be “folded” into one sequence, and $\mathbb{Z}[x_0, x_1, \dots, y_0, y_1, \dots] \cong \mathbb{Z}[x_0, x_1, \dots]$, but that is really beside the point.) Thus a “universal formula” $\alpha^{(n)} = x^{(n)} + y^{(n)}$ in $\mathbb{Z}[x_0, x_1, \dots, y_0, y_1, \dots]$ implies $c^{(n)} = a^{(n)} + b^{(n)}$ in any ring A , if we let $c_n \stackrel{\text{def}}{=} \alpha_n(a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_n)$.

Now $W(A)$ is the set of infinite sequences $a = (a_0, a_1, a_2, \dots)$ in A , which is the same thing as the set of ring homomorphisms $\mathbb{Z}[x_0, x_1, \dots] \longrightarrow A$:

$$W(A) = \text{Hom}(\mathbb{Z}[x_0, x_1, \dots], A).$$

Thus the sophisticated way of saying that $\mathbb{Z}[x_0, x_1, \dots]$ is the universal example of a ring with an infinite sequence is to say that $\mathbb{Z}[x_0, x_1, \dots]$ (with the sequence (x_0, x_1, x_2, \dots)) *represents* the functor

$$A \mapsto \{\text{infinite sequences in } A\}.$$

In this point of view, the sequence of “universal polynomials” $\alpha_0, \alpha_1, \dots \in \mathbb{Z}[x_0, x_1, \dots, y_0, y_1, \dots]$ is a homomorphism

$$\mathbb{Z}[x_0, x_1, \dots] \longrightarrow \mathbb{Z}[x_0, x_1, \dots, y_0, y_1, \dots].$$

Since

$$\mathbb{Z}[x_0, x_1, \dots, y_0, y_1, \dots] = \mathbb{Z}[x_0, x_1, \dots] \otimes \mathbb{Z}[x_0, x_1, \dots],$$

this gives, for any ring A , a map

$$W(A) \times W(A) \longrightarrow W(A).$$

Thus $\mathbb{Z}[x_0, x_1, \dots]$ is a Hopf algebra and the functor it represents, $A \mapsto W(A)$, is a group functor. (There are some verifications to be made here. They are exactly the ones you need to make to show that $W(A)$ is a group under addition.) In fact, $A \mapsto W(A)$ is something you do not see every day: it is a *ring* functor. It follows that $\text{Spec } \mathbb{Z}[x_0, x_1, \dots]$ is a group-scheme (in fact, it is even a ring-scheme). It is affine and infinite-dimensional.

You must be thinking: who was complaining about too-concise treatments?