Mathematics 223a Homework due October 14

October 8, 2008

1 Witt Vectors: part I

1.1 The Witt straighteners

Fix p a prime number. Consider the polynomials

$$w_n(X_0, X_1, \ldots, X_n) \;=\; \sum_{i=0}^{n} p^i X_i^{p^{n-i}} \;\in\; \mathrm{Z}[X_0, X_1, \ldots, X_n]$$

so we have:

$$\begin{aligned} w_0(X_0) &= X_0 \\ w_1(X_0, X_1) &= X_o^p + pX_1 \\ w_2(X_0, X_1, X_2) &= X_o^{p^2} + pX_1^p + p^2 X_2 \end{aligned}$$

$$\cdots$$

Note that we can invert these equations, expressing the X's in terms of the w's (*not* over Z, but) over the ring $\mathrm{Z}[1/p]$. In particular

$$X_n = \frac{1}{p^n} w_n(X_0, X_1, \ldots, X_n) \, +$$

a polynomial in the $w_j(X_0, X_1, \ldots, X_j)$*'s for* $j < n$ *with coefficients in* $\mathrm{Z}[1/p]$.

1.2 The "sum" polynomials

Exercise 1 *Show that there is a unique collection of polynomials*

$$
\begin{array}{rcl}
S_0(X_0;Y_0) & \in & \mathrm{Z}[1/p][X_0;Y_0] \\
S_1(X_0,X_1;Y_0,Y_1) & \in & \mathrm{Z}[1/p][X_0,X_1;Y_0,Y_1] \\
S_2(X_0,X_1,X_2;Y_0,Y_1,Y_2) & \in & \mathrm{Z}[1/p][X_0,X_1,X_2;Y_0,Y_1,Y_2] \\
& \cdots & \\
S_n(X_0,X_1,\ldots X_n;Y_0,Y_1,\ldots Y_n) & \in & \mathrm{Z}[1/p][X_0,X_1,\ldots X_n;Y_0,Y_1,\ldots Y_n] \\
& \cdots &
\end{array}
$$

such that

$$w_n(S_0,S_1,\ldots S_n) \;=\; w_n(X_0,X_1,\ldots,X_n) \;+\; w_n(Y_0,Y_1,\ldots,Y_n) \;\in\; \mathrm{Z}[1/p].$$

Hint: Use the fact mentioned at the end of the previous subsection.

Exercise 2 *Show that*

$$
\begin{array}{rcl}
S_0(X_0;Y_0) & = & X_0+Y_0 \\
S_1(X_0,X_1;Y_0,Y_1) & = & X_1+Y_1+\dfrac{X_0^p+Y_0^p-(X_0+Y_0)^p}{p}
\end{array}
$$

Exercise 3 *Show that your argument for Exercise 1 generalizes as follows: Given any polynomial* $\mathcal{T}(A;B)\in \mathrm{Z}[A;B]$ *there is a unique collection of polynomials*

$$
\begin{array}{rcl}
T_0(X_0;Y_0) & \in & \mathrm{Z}[1/p][X_0;Y_0] \\
T_1(X_0,X_1;Y_0,Y_1) & \in & \mathrm{Z}[1/p][X_0,X_1;Y_0,Y_1] \\
T_2(X_0,X_1,X_2;Y_0,Y_1,Y_2) & \in & \mathrm{Z}[1/p][X_0,X_1,X_2;Y_0,Y_1,Y_2] \\
& \cdots & \\
T_n(X_0,X_1,\ldots X_n;Y_0,Y_1,\ldots Y_n) & \in & \mathrm{Z}[1/p][X_0,X_1,\ldots X_n;Y_0,Y_1,\ldots Y_n] \\
& \cdots &
\end{array}
$$

such that

$$w_n(T_0,T_1,\ldots T_n) \;=\; \mathcal{T}(w_n(X_0,X_1,\ldots,X_n);w_n(Y_0,Y_1,\ldots,Y_n)) \;\in\; \mathrm{Z}[1/p].$$

Note: If $\mathcal{T}(A;B) = A \cdot B$, the T_i's are the P_i's of the lecture.

Exercise 4 *Let R be a commutative ring in which p is invertible, and $W(R)$ the "candidate-ring" of Witt vectors in R (as in the lecture) meaning that as a set it is equal to $R^{\mathbf{N}} = R \times R \times \cdots$ with elements given as "vectors' $(r_o, r_1, r_2, \dots)$ where the entries r_j are in R, and the candidate "sum" $(+)$ is given by*

$$(r_0, r_1, \dots) + (r'_0, r'_1, \dots) \;=\; (S_0(r_0, r'_0), S_1(r_0, r_1; r'_0, r'_1) \dots),$$

and the candidate "product" $(\times)$ by

$$(r_0, r_1, \dots) \times (r'_0, r'_1, \dots) \;=\; (P_0(r_0, r'_0), P_1(r_0, r_1; r'_0, r'_1) \dots),$$

show that $W(R)$ is a commutative ring with unit.

2 p-adically complete rings

Let R be a topological ring (commutative with unit) such that p is not a zero-divisor in R, and R the projective limit of the system of (discrete) quotient rings

$$\cdots R/p^{\nu+1}R \to R/p^{\nu}R \to \cdots \to R/p^2R \to R/pR.$$

E.g., R is separated and complete with respect the topology defined by the system of ideals $\{p^{\nu}R\}_{\nu}$ (its *p-adic topology*). Suppose further that R/pR is a perfect ring in the sense that the p-th power mapping, $\phi : R \to R$ $(x \mapsto x^p)$ induces an automorphism of R/pR.

2.1 Multiplicative lifting of the residual ring

Exercise 5 1. *For each $\alpha \in R/pR$, denote by $r(\alpha) \in R$ a lifting of α; i.e., an element such that $r(\alpha) \equiv \alpha$ mod pR. Now let us "improve" our liftings as follows. Form the sequence*

$$\nu \mapsto r_{\nu}(\alpha) := (r(\phi^{-\nu}(\alpha))^{p^{\nu}}.$$

Show that the above sequence converges in the p-adic topology. Let $\tilde{\alpha} = \lim_{\nu} r_{\nu}(\alpha) \in R$ denote the limit.

2. *Show that this mapping $\tau : R/pR \to R$ (i.e., $\alpha \mapsto \tilde{\alpha}$) is the unique multiplicative mapping of R/pR to R that lifts the natural projection $R \to R/pR$. I.e., $\tilde{\alpha} \equiv \alpha$ mod pR. Note, then, that it makes sense to take p^i-th roots of any element of R in the image of $\tau : R/pR \to R$; for $\tilde{\alpha}^{p^{-i}} = \tau(\phi^{-i}\alpha)$.*

3. *Show that any element r of R can be uniquely represented as a power series in p, as follows:*

$$r = \sum_{i=0}^{\infty} \tilde{\beta}_i p^i$$

with $\beta_i = \phi^{-i}(\alpha_i) \in R/pR$ *(*$i = 0, 1, \ldots$*). It turns out to be particularly useful to "code" the element* r *in terms of the data* $(\alpha_0, \alpha_1, \ldots, \alpha_i, \ldots)$*. Provisionally, then, refer to*

$$(\alpha_0, \alpha_1, \ldots, \alpha_i, \ldots) \in R/pR^{\mathbf{N}}$$

as the **vector that stands for** r*.*

4. *If* R/pR *is a finite field of* q *elements, the ring* R *contains primitive* $(q-1)$*-st roots of unity.*

3 Witt Vectors: part II

Let $S_0, S_1, S_2, \ldots$ be the series of polynomials in $\mathbf{Z}[1/p]$ such that

$$w_n(S_0, S_1, \ldots S_n) \;=\; w_n(X_0, X_1, \ldots, X_n) \;+\; w_n(Y_0, Y_1, \ldots, Y_n) \;\in\; \mathrm{Z}[1/p].$$

This sequence of exercises is meant to show that they have integral coefficients.

3.1 An interesting p-adically complete ring

Let

$$\mathcal{R} := \mathrm{Z}[\ldots, X_i^{p^{-j}}, \ldots; \ldots, Y_k^{p^{-\ell}}, \ldots; \text{ with } i, j, k, l = 0, 1, 2, \ldots]$$

where the X_i, Y_k are all independent variables and we have adjoined, as well, all p-power roots of these variables. Then

$$\mathcal{R}/p\mathcal{R} := \mathbf{F}_p[\ldots, X_i^{p^{-j}}, \ldots; \ldots, Y_k^{p^{-\ell}}, \ldots; \text{ with } i, j, k, l = 0, 1, 2, \ldots]$$

is a perfect ring of characteristic p, and let

$$R = \lim_{\nu} \mathcal{R}/p^{\nu}\mathcal{R}.$$

Exercise 6 *Show that* p *is not a zero divisor in* R*. So* R *imbeds in* $R[1/p]$*. Give a complete description of the canonical lifting*

$$\mathcal{R}/p\mathcal{R} = R/pR \longrightarrow R.$$

Exercise 7 *In particular, the vector in* $R/pR^{\mathbf{N}}$ *that stands for* $\sum_{i=0}^{\infty} X_i^{p^{-i}} p^i \in R$ *is* $(X_0, X_1, X_2, \ldots) \in R/pR^{\mathbf{N}}$*. We can think if this as "a general element," and* $\sum_{i=0}^{\infty} Y_i^{p^{-i}} p^i \in R$ *as another. Let us try to add these two "general elements" together:*

1. *Show that one can express the element in R that is the sum of the elements $\sum_{i=0}^{\infty} X_i^{p^{-i}} p^i \in R$ and $\sum_{i=0}^{\infty} Y_i^{p^{-i}} p^i \in R$ as*

$$\sum_{i=0}^{\infty} \tilde{\beta}_i p^i.$$

where $\beta_i = \phi^{-i}(\alpha_i)$ and α_i is a polynomial in the "$X^{p^{-i}}$-variables" with indices $\leq i$ and the "$Y^{p^{-i}}$-variables" with indices $\leq i$ and with coefficients in $\mathbf{F}_p$, in R/pR. Working modulo p^{n+1} we have:

$$\sum_{i=0}^{n} X_i^{p^{-i}} p^i + \sum_{i=0}^{n} Y_i^{p^{-i}} p^i \equiv \sum_{i=0}^{n} \tilde{\beta}_i p^i \mod p^{n+1}$$

where

$$\beta_i = \phi^{-i}(\alpha_i)$$

for $i \leq n$ and the $\alpha_i = \alpha_i(X;Y)$ are polynomials over $\mathbf{F}_p$ in the $X_i^{p^{-j}}$ and the $Y_k^{p^{-\ell}}$ for $i, j, k, \ell \leq n$.

2. *Note that $X_i \mapsto X_i^{p^n}$ and $Y_i \mapsto Y_i^{p^n}$ extends to an automorphism Φ of R that is a "lifting" of the n-th iterate of the Frobenius automorphism, $\phi^n : R/pR \to R/pR$; in particular it sends $\alpha_i(X;Y) \in R/pR$ to $\alpha_i(X;Y)^{p^n}$. The automorphism Φ sends $\sum_{i=0}^{n} X_i^{p^{-i}} p^i$ (our "general element" truncated mod p^{n+1}) to $w_n(X_0, \ldots, X_n)$ and similarly, $\sum_{i=0}^{n} Y_i^{p^{-i}} p^i$ to $w_n(Y_0, \ldots, Y_n)$. It sends $\sum_{i=0}^{n} \tilde{\beta}_i p^i$ to $w_n(\tilde{\alpha}_0, \tilde{\alpha}_1, \ldots, \tilde{\alpha}_n)$.*

3. *Show that*

$$w_n(X_0, \ldots, X_n) + w_n(Y_0, \ldots, Y_n) \equiv w_n(\tilde{\alpha}_0, \tilde{\alpha}_1, \ldots, \tilde{\alpha}_n) \mod p^{n+1}R.$$

4. *Show that if we have any $n+1$ elements $a_i \in R$ such that a_i is a lift of α_i ($i = 0, 1, \ldots, n$) then*

$$w_n(a_0, a_1, \ldots, a_n) \equiv w_n(\tilde{\alpha}_0, \tilde{\alpha}_1, \ldots, \tilde{\alpha}_n) \mod p^{n+1}R.$$

(Hint: remember the form of the polynomial w_n.)

5. *Working in $R[1/p]$, and keeping the notation of the previous exercise, we have*

$$w_n(a_0, a_1, \ldots, a_n) = w_n(S_0, S_1, \ldots, S_n) + p^{n+1}C$$

for some element $C \in R \subset R[1/p]$.

6. *Now set up an inductive format, where we may assume that for $i < n$, the polynomial S_i has integral coefficients, and moreover its image in R is congruent modulo pR to α_i. We can then "improve" the displayed formula above by taking S_i for a_i ($i < n$) and we write:*

$$w_n(S_0, S_1, \ldots, S_{n-1}, a_n) = w_n(S_0, S_1, \ldots, S_{n-1}, S_n) + p^{n+1}C$$

for some element $C \in R \subset R[1/p]$.

7. *Conclude by then showing that $a_n \equiv S_n \mod p^{n+1}$, which establishes the congruence (needed, of course, for the inductive argument) and integrality of S_n.*

Exercise 8 *Show that the argument (described by the previous exercises) that showed* $S_0, S_1, S_2, \ldots$ *to have integral coefficients works in general. Specifically, letting* $\mathcal{T}(A; B) \in \mathrm{Z}[A; B]$ *be any polynomial as in Part I, show that the associated series of polynomials* $T_0, T_1, T_2, \ldots$ *defined in part I all have integral coefficients.*