18.786 PROBLEM SET 4

Fix a prime p throughout. All rings are assumed commutative (and certainly unital).

The week's homework is meant to give an introduction to *Witt vectors*.[1] This is an important topic in its own right, but for us, the motivating problem is to get our hands on unramified extensions of local fields, which we know in our heart of hearts must be something very concrete.

First, the purely characteristic p version:

(1) Let $K = \mathbb{F}_p((t))$. Show that the unique degree n unramified extension of K is $\mathbb{F}_{p^n}((t))$. Deduce that $\overline{\mathbb{F}}_p[[t]]$ is the t-adic completion of the ring of integers in the maximal unramified extension of $\mathbb{F}_p((t))$.

In particular, we obtain a "formula" for unramified extensions of $\mathbb{F}_q((t))$ which is defined for any $\mathbb{F}_q$-algebra, such that when we input $\mathbb{F}_{q^n}$, we obtain the degree n unramified extension (namely, this formula sends A to $A((t))$).

Witt vectors give a version of this for p-adic fields instead: roughly, instead of Laurent series in the abstract variable t, we will get (something like) Laurent series in p. However, to get a nicely behaved theory in this mixed characteristic setting, smart[2] people teach us that we should restrict to *perfect* algebras: these are the $\mathbb{F}_p$-algebras A for which the *Frobenius map* $A \overset{x \mapsto x^p}{\to} A$ is an isomorphism.

Then the ring $W(A)$ of *Witt vectors* is a p-adically complete[3] ring characterized by the universal property that for R a p-adically complete ring, giving a continuous (with respect to the p-adic topology) map $W(A) \to R$ is the same as giving a map $A \to R/p$.[4]

There are formal arguments that the Witt vectors actually exist, i.e., there is some $W(A)$ with the above universal property. So we will assume it for this assignment, and by the end we will more or less see how to construct them very explicitly by hand. Moreover, you can assume that $W(A)$ is *flat* over $\mathbb{Z}_p$, i.e., p is a non-zero divisor in $W(A)$ (formal arguments can provide this too).

(2) Show that $W(A)/p$ is canonically isomorphic to A.

Updated: March 10, 2016.

[1] Under somewhat restrictive hypotheses.

[2] It's not so much that they're smart as that they're experienced. By the end of this assignment, we too will understand why having an inverse to Frobenius is helpful.

[3] R being *p-adically complete* means that $R \xrightarrow{\simeq} \varprojlim R/p^n$. E.g., $\mathbb{F}_p$-algebras count, or more generally, $\mathbb{Z}/p^n$-algebras. Note p-adically complete algebras carry a *p-adic topology*: this is the Tychonoff topology on the projective limit, i.e., a sequence converges to zero if and only if for every n the sequence eventually only takes values in $p^n R$.

[4] Of course, all of this should be functorial in R.

(3) (a) Show that $W(\mathbb{F}_p) = \mathbb{Z}_p$.
(b) More generally, for $q = p^n$, show that $W(\mathbb{F}_q)$ is the ring of integers in the[5] degree n unramified extension of $\mathbb{Q}_p$.
(c) More generally, for any $K/\mathbb{Q}_p$ a local field with residue field $\mathbb{F}_q$, show that $W(\mathbb{F}_{q^n}) \otimes_{W(\mathbb{F}_q)} \mathcal{O}_K$ is the ring of integers in the degree n unramified extension of K.
(d) (There is no actual exercise here.) The Frobenius automorphism of $\mathbb{F}_q$ induces a (continuous) automorphism of $W(\mathbb{F}_q)$, and therefore of $W(\mathbb{F}_{q^n}) \otimes_{W(\mathbb{F}_q)} \mathcal{O}_K$, and therefore of its field of fractions. Observe that this automorphism generates the Galois group $\mathbb{Z}/n\mathbb{Z}$ of this extension.
(e) Show that $W(\overline{\mathbb{F}}_p)$ is the p-adic completion of the ring of integers in the maximal unramified extension of $\mathbb{Q}_p$. Make sure to explain why we need to take a p-adic completion here.

Witt vectors are closely related to *tilting*, a certain operation that takes a p-adically complete algebra R and produces a perfect $\mathbb{F}_p$-algebra. We digress to play with this operation for a bit.

Namely, define $R^\flat$ (the *tilt* of R) as the projective limit of the diagram:

$$\ldots \xrightarrow{x \mapsto x^p} R \xrightarrow{x \mapsto x^p} R \xrightarrow{x \mapsto x^p} R.$$

Note that these maps are multiplicative but not additive if $p \neq 0$ in R, so $R^\flat$ only has a multiplicative structure (for now). You should think of elements of $R^\flat$ as the data of an element $x \in R$, plus compatible choices of $x^{\frac{1}{p^n}}$ for all $n \geqslant 0$.

(4) (a) Let R be any ring. For $x, y \in R$, show that $x = y \mod pR$ implies that $x^{p^n} = y^{p^n} \mod p^{n+1}R$ for every n.
(b) Suppose that $p^{n+1} = 0$ in R. For $x \in R/p$ and $x^{\frac{1}{p^n}}$ a chosen p^n-th root of x, show that x admits a *unique* lift to an element $[x] \in R$ such that there exists (possibly non-unique) $y \in R$ with $y^{p^n} = [x]$ and $y = x^{\frac{1}{p^n}} \mod pR$.
(c) Show that for R p-adically complete, the map $R^\flat \to (R/p)^\flat$ is a bijection.
(d) Deduce that (with R p-adically complete) the multiplicative monoid structure on $R^\flat$ upgrades to an algebra structure, and that the resulting algebra is a perfect $\mathbb{F}_p$-algebra.
(e) Show that for $x, y \in R^\flat$ (with R p-adically complete), their sum in $R^\flat$ is computed by the formula:

$$\lim_{n \to \infty} (x^{\frac{1}{p^n}} + y^{\frac{1}{p^n}})^{p^n}.$$

[5] "The" is a bad word here: there is a unique up to non-unique unramified degree n extension of a nonarchimedean local field K, where the nonuniqueness is because Frobenius acts on it. However, if we also fix an isomorphism of the residue field of our unramified extension with a fixed degree n extension $\mathbb{F}_q$ of $\mathbb{F}_p$, it is unique up to unique isomorphism.

Here the limit is taken with respect to the p-adic topology on R. Note that this formula only defines an element of R, so part of the exercise is also to find the compatible p^n-th roots to obtain an actual element of $R^\flat$.

(5) For A a perfect $\mathbb{F}_p$-algebra, show that $W(A)^\flat$ is canonically isomorphic to A.

Note that there is a canonical multiplicative projection $R^\flat \to R$ for any R. In particular, we obtain a canonical multiplicative map $A = W(A)^\flat \to W(A)$. This map is denoted $x \mapsto [x]$, and is called the *Teichmuller lift*.

(The analogous thing in the pure characteristic p setting is the canonical map $A \to A((t))$, which is both multiplicative and additive.)

(6) Describe the Teichmuller map explicitly for $A = \mathbb{F}_q$ $(q = p^n)$.

(7) Show that for $x \in A$ as above, $[x]$ projects to $x \in A = W(A)/p$.

(8) Use Exercise (4b) to construct the Teichmuller lift without mentioning tilting. Check the multiplicativity of your construction.

(9) For R p-adically complete, define a canonical map:

$$\theta : W(R^\flat) \to R$$

using the universal property of Witt vectors. For $x \in R^\flat$, show that:

$$\theta([x]) = x \in R.$$

(Here we abuse notation in letting x also denote the induced element of R).

(10) Choose a set-theoretic splitting of the projection map $W(A) \to A$, and denote it by $x \mapsto \tilde{x}$.

For any $x \in A$, show that $[x]$ is equal to:

$$\lim_{n\to\infty} (\widetilde{x^{\frac{1}{p^n}}})^{p^n} \in W(A)$$

where again, the limit is take with respect to the p-adic topology. (This formula should be read as follows: lift $x^{\frac{1}{p^n}} \in A$ to $W(A)$ in some random way, raise this to the p^n-th power, and pass to the limit over n.)

(11) (a) Show that every element of $W(A)$ can be written uniquely as:

$$\sum_{n\geqslant 0} [x_n] p^n.$$

(b) For every $x, y \in A$, show that:

$$[x] + [y] = [x + y] - \sum_{i=1}^{p-1} \binom{p}{i} [x^{\frac{i}{p}} y^{\frac{p-i}{p}}] \qquad \text{mod } p^2 W(A).$$

(c) Explicitly construct $W(A)/p^2$. As a start, every element can be uniquely written as $[x] + [y]p$ for some $x, y \in A$ (i.e., $W(A)/p^2 = A \times A$ as a set). What is the addition law? What is the multiplication law? Check that the formulae you write are well-defined, actually give a commutative ring structure, and that $W(A)/p^2$

satisfies the appropriate universal property. Also check that $W(A)/p^2$ is flat[6] over $\mathbb{Z}/p^2\mathbb{Z}$.

(d) Provide a similar formula for addition of Teichmuller representatives modulo p^n for any n.

[6]A hint, if you're not comfortable with flatness yet: first show that a module M over $\mathbb{Z}/p^2\mathbb{Z}$ is flat if and only if the multiplication by p map $M \to M$ induces an isomorphism between M/pM and pM.

18.786 Number Theory II: Class Field Theory

Spring 2016