On surjectivity of the Witt vector Frobenius

Kiran S. Kedlaya

Department of Mathematics, Massachusetts Institute of Technology
Department of Mathematics, University of California, San Diego; kedlaya@ucsd.edu

AMS Western Sectional Meeting
Special Session on Arithmetic Geometry
Honolulu, March 4, 2012

Joint work with Chris Davis; manuscript in preparation. Slides available at http://math.mit.edu/~kedlaya/papers/talks.shtml.

Supported by NSF, DARPA, MIT, UCSD.

Witt vectors and the ghost map

Fix a prime number p. There is a unique way to equip the set $W(R)$ of infinite sequences $(x_1, x_p, x_{p^2}, \dots)$ over an arbitrary (commutative unital) ring R with a ring structure, functorially in R, so that the *ghost map*

$$w : (x_1, x_p, x_{p^2}, \dots) \mapsto (x_1, x_1^p + p x_p, x_1^{p^2} + p x_p^p + p^2 x_{p^2}, \dots)$$

defines a ring homomorphism to the ordinary product $R \times R \times \cdots$. The ring $W(R)$ is the *ring of p-typical Witt vectors* over R.

This construction is most commonly used when R of characteristic p and *perfect*, i.e., the Frobenius map $\varphi : x \mapsto x^p$ is bijective. In this case, $W(R)$ is the unique p-adically separated and complete ring with $W(R)/pW(R) \cong R$. However, the general construction is of interest in crystalline cohomology, p-adic Hodge theory, algebraic K-theory, ...

The Frobenius map

There is a unique way to equip each ring $W(R)$ with an endomorphism F, functorially in R, so that the diagram

$$\begin{array}{ccc} W(R) & \xrightarrow{w} & R \times R \times \cdots \\ \downarrow F & & \downarrow E \\ W(R) & \xrightarrow{w} & R \times R \times \cdots \end{array}$$

commutes with E equal to the left shift operator.

If R is of characteristic p, then F coincides with the functoriality map $W(\varphi)$.

Injectivity of the Frobenius map

If R is of characteristic p, then F is injective iff φ is injective iff R is reduced.

If R is not of characteristic p, then F is *never* injective. A standard lemma (Cartier-Dieudonné-Dwork) shows that there is an element of $W(\mathbb{Z})$ with ghost image $(p, 0, 0, \dots)$; this maps to a nonzero element of $W(R)$ in the kernel of F.

Surjectivity of the Frobenius map

If R is of characteristic p, then F is surjective iff φ is surjective. For instance, this happens if R is perfect.

If R is not of characteristic p, it is somewhat rare for F to be surjective. A typical example where F is surjective is the valuation subring of a spherical completion of an algebraic closure of $\mathbb{Q}_p$. (The metric completion does not suffice!)

Surjectivity at finite levels

Surjectivity of F becomes somewhat more common if instead of looking at infinite Witt vectors, we look at truncations. For each nonnegative integer n, let $W_{p^n}(R)$ be the set of finite sequences $(x_1, x_p, \dots, x_{p^n})$ with ring structure inherited from $W(R)$; then the Witt vector Frobenius induces a map $F : W_{p^{n+1}}(R) \to W_{p^n}(R)$. We will say R is *Witt-perfect* if these maps are surjective for all n.

Note that $F : W_p(R) \to W_1(R)$ is the map $(x_1, x_p) \mapsto (x_1^p + px_p)$, which is surjective iff $\varphi : R/(p) \to R/(p)$ is surjective. This is not sufficient to imply that R is Witt-perfect; for instance, $R = \mathbb{Z}$ is not Witt-perfect. However, if $F : W_{p^2}(R) \to W_p(R)$ is surjective, then R is Witt-perfect.

Equivalent conditions for Witt-perfectness

The following conditions are (nontrivially) equivalent.

- R is Witt-perfect.
- The image of $F : W_{p^2}(R) \to W_p(R)$ contains $(x, 0)$ for all $x \in R$.
- Every element of R is congruent to a p-th power modulo pI_1, where $I_1 = \{x \in R : x^p \in pR\}$. The same is then true modulo pI_n for all n, where $I_n = \{x \in R : x^p \in pI_{n-1}\}$. (It is not true modulo $\cup pI_n$, though: that implies surjectivity of $F : W(R) \to W(R)$!)
- $\varphi : R/(p) \to R/(p)$ is surjective and there exists $r, s \in R$ with $r^p + p \in psR$ and $s^N \in pR$ for some $N > 0$. This then implies that for every $r \in R$, there exists $s \in R$ with $s^p - pr \in p^2R$.

Almost purity

Tate showed that if K is a "sufficiently ramified" algebraic extension of $\mathbb{Q}_p$ and L is a finite extension of K, then

$$\mathrm{Trace} : \mathfrak{m}_L \to \mathfrak{m}_K$$

is surjective. For instance, this holds if $\mathbb{Q}_p(\mu_{p^\infty}) \subseteq K$. (More generally, it holds if K is *arithmetically profinite*, e.g., if K contains a p-adic Lie extension of $\mathbb{Q}_p$.)

This was later generalized by Faltings in his *almost purity theorem*, and further generalized by Gabber-Ramero, K-Liu, and Scholze.

Using the language of Witt-perfect rings, one can give a clean formulation of a general form of almost purity.

Witt-perfectness and almost purity

For R-modules $M_1, M_2 \subseteq M$, we say M_1, M_2 are *almost equal* if $I(M_1/(M_1 \cap M_2)) = I(M_2/(M_1 \cap M_2)) = 0$ for every ideal I of definition for the p-adic topology on R.

Theorem (Davis-K, following K-Liu and Scholze)

Let R be a p-torsion-free, Witt-perfect ring which is integrally closed in $R_p = R[p^{-1}]$. Let S_p be a finite étale R_p-algebra. Let S be an R-subalgebra of S_p which is almost equal to the integral closure of R.

(a) *The ring S is also Witt-perfect.*

(b) *For every ideal I of definition for the p-adic topology on R, there exist a finite free R-module F and R-module homomorphisms $S \to F \to S$ whose composition is multiplication by some $t \in R$ with $I \subseteq (t, p)$.*

(c) *Within $\mathrm{Hom}_{R_p}(S_p, R_p)$, the images of S (via the trace map) and $\mathrm{Hom}_R(S, R)$ are almost equal.*

Examples

For example, we may take $R = \mathfrak{o}_K$ for $K = \mathbb{Q}_p(\mu_{p^\infty})$. This recovers Tate's theorem.

We may also take $R = K[T_1^{\pm 1/p^\infty}, \dots, T_n^{\pm 1/p^\infty}]$. This example plus some variations recover Faltings's theorem.

We may even take R to be the integral closure of $\mathbb{Z}$ in $\mathbb{Q}^{\mathrm{ab}}$. This is Witt-perfect for every p at once! This hints at the possibility of doing p-adic Hodge theory "uniformly in p"...