
Problem 1 (v): Let B denote a commutative ring with unit, let $(W(B), \oplus, \odot)$ denote the ring of Witt vectors with coefficients in B, and let F denote Frobenius. If $b \in W(B)$ then $F(b) \equiv b^p := \underbrace{b \odot \ldots \odot b}_{p \text{ times}} \mod pW(B)$.

Proof: Let $B_1 := \mathbb{Z}[(X_b)_{b\in B}]$. Note that multiplication with p is injective on B_1 and that the ring endomorphism $\varphi : B_1 \to B_1$ with $\varphi(f((X_b)_{b\in B})) := f((X_b^p)_{b\in B})$ satisfies $\varphi(f) \equiv f^p \mod pB_1$ for all $f \in B_1$.

By 2.6 (i), 2.8 (ii) and 2.10 (ii) of the lecture $\Phi_{B_1} : W(B_1) \to B_1^{\mathbb{N}}$ is an injective ring homomorphism with image

$$\text{(1)} \qquad \operatorname{im}(\Phi_{B_1}) = \{(c_n)_{n\geq 0} \in B_1^{\mathbb{N}} \mid \varphi(c_n) \equiv c_{n+1} \mod p^{n+1}B_1 \text{ for all } n \geq 0\}.$$

Let $\tilde{b} \in B_1$ and set $a = (a_n)_{n\geq 0} := \Phi_{B_1}(\tilde{b})$. By 2.12 of the lecture we have

$$\Phi_{B_1}(F(\tilde{b}) \ominus \tilde{b}^p) = f_{B_1}(\Phi_{B_1}(\tilde{b})) - \Phi_{B_1}(\tilde{b})^p = f_{B_1}(a) - a^p.$$

If $n \geq 0$ then the n-th component of this family is $a_{n+1} - a_n^p$. By (1) and the properties of φ this is contained in pB_1, i.e. we can write $a_{n+1} - a_n^p = pc_n$ with $c_n \in B_1$. Note that

$$pc_{n+1} - p\varphi(c_n) = a_{n+2} - \varphi(a_{n+1}) - (a_{n+1}^p - \varphi(a_n)^p).$$

Here $a_{n+2} - \varphi(a_{n+1}) \in p^{n+2}B_1$ and $a_{n+1} - \varphi(a_n) \in p^{n+1}B_1$ by (1). By 1.17 of the lecture the latter implies $a_{n+1}^p - \varphi(a_n)^p \in p^{n+2}B_1$. Taking everything together we obtain $pc_{n+1} - p\varphi(c_n) \in p^{n+2}B_1$. However, multiplication with p is injective on B_1. Therefore, $c_{n+1} - \varphi(c_n) \in p^{n+1}B_1$ for all $n \geq 0$. By (1) this implies $c = (c_n)_{n\geq 0} \in \operatorname{im}(\Phi_{B_1})$, say $c = \Phi_{B_1}(d)$ with $d \in W(B_1)$. Thus,

$$\Phi_{B_1}(F(\tilde{b}) \ominus \tilde{b}^p) = p\Phi_{B_1}(d) = \Phi_{B_1}(pd).$$

Since Φ_{B_1} is injective this gives $F(\tilde{b}) \ominus \tilde{b}^p = pd \in pW(B_1)$.

Now consider the surjective ring homomorphism $\rho : B_1 \to B$ sending X_b to b for all $b \in B$. The induced ring homomorphism $W(\rho) : W(B_1) \to W(B)$ is surjective, too. Given $b \in W(B)$ choose $\tilde{b} \in W(B_1)$ with $W(\rho)(\tilde{b}) = b$. The map $W(\rho)$ commutes with the Frobenius endomorphisms of $W(B)$ and $W(B_1)$, respectively, because the Frobenii are given by evaluation of polynomials with integer coefficients. Writing $F(\tilde{b}) \ominus \tilde{b}^p = pd$ as above, we get

$$\begin{aligned} F(b) \ominus b^p &= F(W(\rho)(\tilde{b})) \ominus W(\rho)(\tilde{b})^p = W(\rho)(F(\tilde{b})) \ominus W(\rho)(\tilde{b})^p \\ &= W(\rho)(F(\tilde{b}) \ominus \tilde{b}^p) \\ &= W(\rho)(pd) = pW(\rho)(d) \in pW(B). \qquad \square \end{aligned}$$