Journal of Pure and Applied Algebra 32 (1984) 191-217
North-Holland

NOETHERIAN COHOMOLOGY RINGS AND FINITE LOOP SPACES WITH TORSION

D.L. RECTOR
University of California, Irvine, CA 92717, USA

Communicated by J.D. Stasheff
Received 7 October 1982

This paper discusses the structure of mod-p cohomology rings that are finitely generated as algebras. The motivation for this work was a desire to understand the cohomology of classifying spaces of finite loop spaces - that is, of spaces whose loop spaces have the homotopy types of finite complexes.

If G is a compact connected Lie group that has no torsion at a prime p, then the mod-p cohomology of its classifying space BG can be determined knowing only the action of the Weyl group W of G on a maximal torus T; for

$$H^*(BG; \mathbb{F}_p) = H^*(BT; \mathbb{Z})^W \otimes \mathbb{F}_p$$

[4; Proposition 29.2]. If, in addition, p does not divide the order of W, then $H^*(BG; \mathbb{F}_p) = H^*(BT; \mathbb{F}_p)^W$, and severe restrictions are placed on W and $H^*(BG; \mathbb{F}_p)$ for purely algebraic reasons; indeed, W must be a generalized reflection group, and $H^*(BG; \mathbb{F}_p)$ must be one of a short list of examples [7], [6; Ch. 2, §5]. J.F. Adams and Clarence Wilkerson [17], [2] showed that these algebraic restrictions hold equally for an appropriate p-torsion free finite loop space G by recovering notions of its maximal torus and Weyl group from the cohomology of its classifying space as an algebra over the Steenrod algebra. They showed that $H^*(BG; \mathbb{F}_p)$ can be embedded as an unstable algebra over the Steenrod algebra in an algebraic closure isomorphic to an $H^*(BT; \mathbb{F}_p)$; the Weyl group of G is then defined as the Galois group of this extension of algebras. The object of this paper is to extend the notion of a Weyl group to finite loop spaces with torsion, or at least to those - perhaps all - whose classifying spaces have Noetherian cohomology. The results given here apply to all Noetherian mod-p cohomology rings.

The right extension of the notion of Weyl group is suggested by the following theorem of Quillen [12]. Let G be any compact Lie group. An *elementary abelian p-group in G* is a finite subgroup E of G such that $E \approx \mathbb{Z}/p \times \cdots \times \mathbb{Z}/p$; the number of factors of $\mathbb{Z}/p$ in E is called the *rank* of E. Let $\mathscr{A}(G)$ be the category that has

(1) as objects the elementary abelian p-groups E in G, and

(2) as maps the monomorphisms induced by conjugations in G - that is,

monomorphisms $i: E \to E'$ such that $i(x) = gxg^{-1}$ for some $g \in G$ and all $x \in E$.

The mod-p cohomology functor sending E to $H^*(E; \mathbb{F}_p)$ is a contravariant functor from $\mathscr{A}(G)$ to the category of rings; the inclusions $E \hookrightarrow G$ induce a ring homomorphism

$$H^*(BG; \mathbb{F}_p) \to \varprojlim H^*(E; \mathbb{F}_p)$$

where the limit is taken over the category $\mathscr{A}(G)$. Quillen's main theorem [12; 6.2] asserts that this map is an F-isomorphism; an *F-isomorphism* is a homomorphism $f: A \to B$ of rings of characteristic p such that

(1) $x \in \operatorname{Ker}(f) \Rightarrow x^r = 0$ for some $r > 0$, and

(2) $y \in B \Rightarrow \exists r \geq 0$: $y^{p^r} \in \operatorname{Im}(f)$.

(These two conditions mean that the varieties of geometric points associated to A and B are isomorphic.)

The category $\mathscr{A}(G)$ generalizes the Weyl group of G in the following sense. If T is a maximal torus of G, then T contributes to $\mathscr{A}(G)$ an elementary abelian p-group

$$E_T = \{x \in T \mid x^p = 1\};$$

W acts on E_T as a group of automorphisms. If G is connected and p-torsion free, then all elementary abelian p-groups in G are contained in E_T [3; Theorem B]. Furthermore, all automorphisms of objects in $\mathscr{A}(G)$ are induced by elements of W (see Proposition 4.11 below). To reconstruct $\mathscr{A}(G)$ from $H^*(BG; \mathbb{F}_p)$, we will use the following observations:

(1) If G is a compact Lie group, there is a one-to-one correspondence between conjugacy classes of elementary abelian p-groups in G and prime ideals of $H^*(BG; \mathbb{F}_p)$ that are homogeneous and stable under the action of the mod-p Steenrod algebra [12; 2.2, 12.1]. The elementary abelian p-group E corresponds to the ideal

$$P = \operatorname{Ker}(H^*(BG; \mathbb{F}_p) \to \Gamma E), \quad \text{where } \Gamma E = H^*(E; \mathbb{F}_p)/\sqrt{0}$$

($\sqrt{0} = \{x \mid x^r = 0 \text{ some } r > 0\}$ is the ideal of nilpotent elements).

(2) If Λ is a Noetherian cohomoloy ring, then Λ has finitely many homogeneous ideals P that are stable under the action of the Steenrod algebra; each Λ/P is an integral domain over the Steenrod algebra. By the construction of Adams and Wilkerson, each Λ/P can be embedded in an algebraic closure Γ such that Γ is integral over Λ/P and $\Gamma \approx \Gamma E$ where E is an elementary abelian p-group. In case $\Lambda = H^*(BG; \mathbb{F}_p)$, E may be taken to be an object of $\mathscr{A}(G)$ corresponding to P.

Thus, consider the category $\mathscr{E}$ whose objects are integral embeddings $\Lambda/P \hookrightarrow \Gamma$, $\Gamma = \Gamma E$, and whose maps are commutative diagrams

$$\begin{array}{ccc} \Gamma & \longrightarrow & \Gamma' \\ \uparrow & & \uparrow \\ \Lambda/P & \longrightarrow & \Lambda/P' \end{array}$$

where $P \subseteq P'$; $\mathscr{E}$ is a generalization of a Galois group. There is a covariant functor Γ from $\mathscr{E}$ into the category of rings that sends $\Lambda/P \hookrightarrow \Gamma$ to Γ. The two main results of this paper are

(1) $\Lambda \to \varprojlim \Gamma$ *is an F-isomorphism* (Theorem 1.4).

(2) *If G is a compact Lie group and* $\Lambda = H^*(BG; \mathbb{F}_p)$, *then there is an equivalence of categories* $\mathscr{A}(G)^{\mathrm{op}} \to \mathscr{E}$ (Theorem 1.6).

In the proofs of these theorems, standard results about ideals in Noetherian rings and in integral extensions of rings (see, for example, [5], [10], or [13]) will be used without specific references being given. With one exception, proofs can be found in [9] and [15] that the needed results hold for ideals that are homogeneous and stable under the action of the Steenrod algebra; the exception is treated in section four of this paper.

Siu P. Lam has given independent proofs of most of the results in this paper (Thesis, Cambridge University and [1]). He and J.F. Adams have recently generalized these results to a somewhat larger class of unstable algebras over the Steenrod algebra – those having an upper bound on the number of algebraically independent elements in them (private communication).

I would like to thank J.F. Adams and Clarence Wilkerson for much inspiration and encouragement. I would also like to thank R. James Milgram for introducing me to the Dickson invariants.

1. The fundamental category of a Noetherian cohomology ring

Fix a prime p. Let $\mathbb{F}_p$ be the field of p-elements, and let $\mathscr{B} = \mathscr{B}(p)$ be the $\mathbb{F}_p$-Hopf algebra of mod-p reduced powers. For p-odd, $\mathscr{B}(p)$ is the sub-Hopf algebra of the mod-p Steenrod algebra $\mathscr{A}(p)$ generated by $P^0, P^1, P^2, \ldots$. If $p=2$, $\mathscr{B} = \mathscr{A}(2)$; I shall then write P^i for Sq^i. Let $d=2$ for p-odd and $d=1$ for $p=2$. By the term $\mathscr{B}$*-algebra*, I shall mean a graded $\mathscr{B}$-algebra that satisfies the Cartan formula. Such an algebra Λ is *unstable* if $x \in \Lambda^n$ implies

$$P^i x = \begin{cases} 0, & di > n, \\ x^p, & di = n. \end{cases}$$

In particular, $\Lambda^n = 0$ for $n < 0$.

An *elementary abelian p-group E* of *rank n* is a direct sum of n-copies of $\mathbb{Z}/p$. Let

$$\Gamma E = H^*(E; \mathbb{F}_p)/\sqrt{0},$$

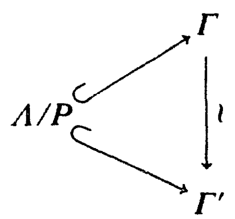
where in any algebra, $\sqrt{0}$ denotes the nil radical. Then ΓE is an unstable $\mathscr{B}$-algebra, and $\Gamma E = \mathbb{F}_p[t_1, \ldots, t_n]$, $\deg t_i = d$. The action of $\mathscr{B}$ on ΓE is determined by $P^1 t_i = t_i^p$.

Let Λ be an unstable $\mathscr{B}$-algebra – for instance $H^*(BG; \mathbb{F}_p)$ where G is a finite loop space. *Assume throughout this discussion that Λ is Noetherian as an $\mathbb{F}_p$-algebra.* An ideal $I \subseteq \Lambda$ that is homogeneous and $\mathscr{B}$-stable will be called a *$\mathscr{B}$-ideal.* Let P be a prime $\mathscr{B}$-ideal, and consider the connected Noetherian integral domain Λ/P. By theorems of Adams and Wilkerson [2; §1, §4], there exists an unstable $\mathscr{B}$-algebra Γ and a $\mathscr{B}$-algebra embedding $\Lambda/P \hookrightarrow \Gamma$ such that Γ is an algebraic closure of Λ/P in the category of unstable $\mathscr{B}$-algebras, and Γ satisfies the following:

1.1. (1) There exists an elementary abelian p-group E such that $\Gamma \approx \Gamma E$; in fact, $E = (\Gamma^d)^*$.

(2) Γ is finitely generated as a Λ/P-module [2; Theorem 1.8].

(3) If $\Lambda/P \hookrightarrow \Gamma'$ is another such embedding, then there is a commuting diagram of $\mathscr{B}$-algebras

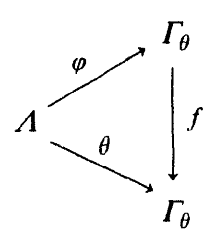


(4) The extension of graded quotient fields $Q(\Lambda/P) \hookrightarrow Q(\Gamma)$ is a normal extension of graded fields, and Γ is the integral closure of Λ/P in $Q(\Gamma)$. The Galois group of this extension consists of homogeneous $\mathscr{B}$-isomorphisms induced by automorphisms of E.

1.2. Definition. The *fundamental category* $\mathscr{E}(\Lambda)$ of a Noetherian, unstable $\mathscr{B}$-algebra Λ is defined as follows:

(1) An object of $\mathscr{E}(\Lambda)$ is a $\mathscr{B}$-map $\varphi : \Lambda \to \Gamma_\varphi$ such that φ is a finite morphism and $\Gamma_\varphi \approx \Gamma E$ for some elementary abelian p-group E. (Recall that a morphism $f : A \to B$ of rings is *finite* if B is finitely generated as an A module with the module structure induced by f.) Thus, φ induces a finite embedding of Λ/P_φ in an algebraic closure Γ_φ, where $P_\varphi = \mathrm{Ker}(\varphi)$ is a prime $\mathscr{B}$-ideal.

(2) A map of $\mathscr{E}(\Lambda)$ is a commutative diagram



of $\mathscr{B}$-algebras. Denote this diagram by $f : \varphi \to \theta$.

If $\Gamma_\varphi \approx \Gamma E$, then the rank of E is the same as the Krull dimension of Γ_φ; denote that number by *rank*(Γ_φ) or *rank*(φ). By choosing a single elementary abelian p-group E of appropriate rank for each prime $\mathscr{B}$-ideal P and considering only embeddings $\Gamma/P \hookrightarrow \Gamma E$, one sees that $\mathscr{E}(\Gamma)$ is equivalent to a small – indeed, finite – category.

Let Γ be the covariant functor from $\mathscr{E}=\mathscr{E}(\Lambda)$ to the category of unstable $\mathscr{B}$-algebras which assigns to each object $\varphi:\Lambda\to\Gamma_\varphi$ the target algebra Γ_φ. Call the pair $(\mathscr{E},\Gamma)$ the *universal cover* of Λ. There is a natural map of $\mathscr{B}$-algebras

$$(1.3)\qquad \Lambda\to\varprojlim\Gamma_\varphi,\quad \varphi\in\mathscr{E}.$$

Following Quillen [12], I shall call a morphism $f:A\to B$ of $\mathbb{F}_p$-algebras a *uniform F-isomorphism* if there exist integers $r>0$, $s\geq 0$ such that

(1) $a\in\operatorname{Ker}(f)\Rightarrow a^r=0$, and

(2) $b\in B\Rightarrow\exists a\in A$ such that $f(a)=(b)^{p^s}$.

The Main Theorem of this paper is the following:

1.4. Theorem. *If Λ is a Noetherian, unstable $\mathscr{B}$-algebra, then the natural map*

$$\Lambda\to\varprojlim\Gamma_\varphi,\quad \varphi\in\mathscr{E}(\Lambda),$$

is a uniform F-isomorphism.

The proof of this theorem, as well as the proofs of the other theorems in this section, will be deferred.

Let $f:\Lambda'\to\Lambda$ be a map of Noetherian, unstable $\mathscr{B}$-algebras; this map induces a functor

$$\tilde f:\mathscr{E}(\Lambda)\to\mathscr{E}(\Lambda')$$

that assigns to each object $\varphi:\Lambda\to\Gamma_\varphi$ the object $\theta:\Lambda'\to\Gamma_\theta$ such that $\theta=f\cdot\varphi$ and Γ_θ is the subalgebra of all elements of Γ_φ that are algebraic over Λ'. There is a commuting diagram

$$\begin{array}{ccc}
\Lambda' & \xrightarrow{\;f\;} & \Lambda \\
\downarrow & & \downarrow \\
\varprojlim_{\theta\in\mathscr{E}(\Lambda')}\Gamma_\theta & \longrightarrow & \varprojlim_{\varphi\in\mathscr{E}(\Lambda)}\Gamma_\varphi
\end{array}$$

induced by $\tilde f$.

1.5. Proposition. *If $f:\Lambda'\to\Lambda$ is a morphism of Noetherian, unstable $\mathscr{B}$-algebras, then f is a uniform F-isomorphism iff $\tilde f$ is an equivalence of categories* (compare [12; Proposition 10.9]).

Let G be a compact Lie group and X a G-space such that X is either compact or is paracompact and has finite cohomological dimension. In the notation of Quillen [12], let $\mathscr{A}(G,X)$ be the category defined by the following:

(1) An object of $\mathscr{A}(G,X)$ is a pair (E,c) where $E\subseteq G$ is an elementary abelian p-

group and c is a connected component of X^E (the fixed point set of E).

(2) A map $(E,c)\to(E',c')$ of $\mathscr{A}(G,X)$ is a homomorphism $\theta: E\to E'$ such that, for some element $g\in G$, $gEg^{-1}\subseteq E'$, $c'\subseteq gc$, and $\theta(x)=gxg^{-1}$ for all $x\in E$.

Let $\Lambda=H_G^*(X;\mathbb{F}_p)$ (equivariant cohomology) and let H be the contravariant functor from $\mathscr{A}(G,X)$ to the cateory of $\mathscr{B}$-algebras given by $H(E,c)=H^*(E;\mathbb{F}_p)/\sqrt{0}$. For each $(E,c)\in\mathscr{A}(G,X)$ there is an equivariant inclusion $(E,c)\hookrightarrow(G,X)$, which induces

$$(E,c)^*: H_G^*(X;\mathbb{F}_p)\to H(E,c).$$

Now $(E,c)^*$ is a finite morphism [11; 2.3], and $H(E,c)=\Gamma E$; thus $\Lambda\to H(E,c)$ is an object in $\mathscr{E}(\Lambda)$; denote this object by $\mathscr{H}(E,c)$. The assignment $(E,c)\Rightarrow\mathscr{H}(E,c)$ is a contravariant functor from $\mathscr{A}(G,X)$ to $\mathscr{E}(\Lambda)$.

1.6. Theorem. *If G is a compact Lie group, and X is a G-space that is either compact or is paracompact and has finite cohomological dimension, then*

$$\mathscr{H}:\mathscr{A}(G,X)^{\mathrm{op}}\to\mathscr{E}(\Lambda),$$

where $\Lambda=H_G^*(X;\mathbb{F}_p)$, *is an equivalence of categories.*

In [12], Quillen described the variety of geometric points associated to the equivariant cohomology ring $H_G^*(X;\mathbb{F}_p)$. His description applies to any Noetherian, unstable $\mathscr{B}$-algebra Λ as follows.

Let Ω be an algebraically closed field of characteristic p. For A an $\mathbb{F}_p$-algebra, let $A(\Omega)$ be the variety of Ω-valued points of A (that is, $\mathbb{F}_p$-homomorphisms $A\to\Omega$), and for $f: A\to B$ a morphism of $\mathbb{F}_p$-algebras, let $f^\Omega: B(\Omega)\to A(\Omega)$ denote the induced map of varieties. If E is an elementary abelian p-group of rank n, then $\Gamma E(\Omega)$ is an affine space of dimension n; denote that space by $E\otimes\Omega$. Let

$$(E\otimes\Omega)^+=E\otimes\Omega-\bigcup_{E'<E}(E'\otimes\Omega).$$

If $\varphi:\Lambda\to\Gamma_\varphi$ is an object of $\mathscr{E}(\Lambda)$, then $E_\varphi\otimes\Omega=\Gamma_\varphi(\Omega)$ is an affine space, and there is an affine map $\varphi^\Omega: E_\varphi\otimes\Omega\to\Lambda(\Omega)$. Let

$$V_\varphi=\varphi^\Omega(E_\varphi\otimes\Omega),\qquad V_\varphi^+=\varphi^\Omega(E_\varphi\otimes\Omega)^+.$$

Finally, let $W(\varphi)$ be the group of automorphisms of φ in the category $\mathscr{E}(\Lambda)$; $W(\varphi)=\mathrm{Gal}(\Gamma_\varphi/\mathrm{Im}\,\varphi)$. Then $W(\varphi)$ acts as a group of automorphisms on the varieties $E_\varphi\otimes\Omega$, and $\varphi^\Omega g^\Omega=\varphi^\Omega$ for all $g\in W(\varphi)$.

1.7. Theorem (Stratification Theorem). *If* Λ *is a Noetherian, unstable* $\mathscr{B}$*-algebra, then*

(1) *There is a homeomorphism of varieties*

$$\varinjlim_{\varphi\in\mathscr{E}(\Lambda)} E_\varphi\otimes\Omega\to\Lambda(\Omega).$$

(2) *If I is a set of representatives of the isomorphism classes of $\mathscr{E}(\Lambda)$, then*

$$\Lambda(\Omega)=\coprod_{\varphi\in I} V_\varphi^+$$

is a disjoint union of locally closed, irreducible affine subvarieties.

(3) *W_φ acts freely on $(E_\varphi\otimes\Omega)^+$, for each $\varphi\in\mathscr{E}(\Lambda)$, and $V_\varphi^+=(E_\varphi\otimes\Omega)^+/W_\varphi$; V_φ is the closure of V_φ^+, and $V_\varphi\subseteq V_{\varphi'}$ iff there is a morphism from φ' to φ in $\mathscr{E}(\Lambda)$.*

(4) *The irreducible components of $\Lambda(\Omega)$ are the V_φ such that φ is minimal in the sense that $\varphi'\to\varphi\in\mathscr{E}(V)\Rightarrow\varphi'\to\varphi$ is an equivalence.*

2. Elementary properties of $\mathscr{E}(\Lambda)$; proofs of 1.6, 1.7

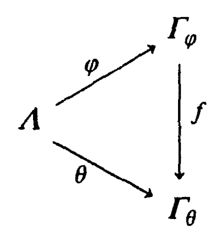
Fix a Noetherian, unstable $\mathscr{B}$-algebra Λ, and let $(\mathscr{E},\Gamma)$ be its universal cover. In the discussion below, all ideals mentioned will be assumed to be $\mathscr{B}$-ideals. The most important fact for understanding prime $\mathscr{B}$-ideals is the following:

2.1. Lemma (Serre [14; Proposition (1)]). *If E is an elementary abelian p-group, and $P\subseteq\Gamma E$ is a prime $\mathscr{B}$-ideal, then $\exists E'\subseteq E$ such that*

$$P=\operatorname{Ker}(\Gamma E\to\Gamma E').$$

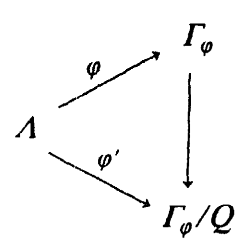
As an illustrative application, consider

2.2. Lemma. *Let $\varphi:\Lambda\to\Gamma_\varphi$ and $\theta:\Lambda\to\Gamma_\theta$ be objects in $\mathscr{E}$; let $P_\varphi=\operatorname{Ker}\varphi$ and $P_\theta=\operatorname{Ker}\theta$. Then there is a map*

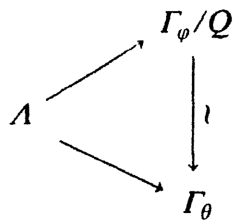


in $\mathscr{E}$ if and only if $P_\varphi\subseteq P_\theta$. Furthermore, each such f is epic; $P_\varphi=P_\theta$ iff f is an isomorphism.

Proof (Adams and Wilkerson [2; 1.10]). Suppose $P_\varphi\subseteq P_\theta$. Since φ is a finite morphism (in particular, Γ_φ is an integral extension of $\operatorname{Im}\varphi$), there is, by the Cohen-Seidenberg going up theorem, a prime $\mathscr{B}$-ideal $Q\subseteq\Gamma_\varphi$ such that $\varphi^{-1}(Q)=P_\theta$. Thus, there is a commutative diagram



where $\operatorname{Ker}\varphi' = P_\theta$. By Lemma 2.1, $\Gamma_\varphi/Q \simeq \Gamma E$ for some elementary abelian p-group E. By 1.1(3), there is a diagram



Composition of these diagrams gives the morphism f.

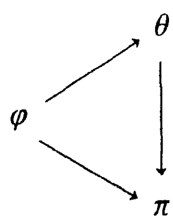
Now, consider a map $f:\varphi\to\theta$ in $\mathcal{E}$; we wish to show that f is epic. Arguing as above, we may assume that $P_\varphi = P_\theta = 0$. Then the monomorphisms φ and θ are finite; therefore, Γ_φ and Γ_θ must have the same Krull dimension as Λ [13; Ch. III, Proposition 3]. Again arguing as above, $\operatorname{Im}(f)$ is of the form ΓE and is finite over Λ; thus, $\operatorname{Im}(f)$ has the same Krull dimension as Λ. But the Krull dimension of ΓE is the same as the dimension of $E \approx (\Gamma E)^d$ as a $\mathbb{F}_p$-vector space. Thus, $\dim \Gamma_\varphi^d = \dim \Gamma_\theta^d = \dim(\operatorname{Im} f)^d$, and f is an isomorphism.

2.3. Proposition. *The universal cover* $(\mathcal{E},\Gamma)$ *of a Noetherian, unstable* $\mathcal{A}$*-algebra* Λ *satisfies the following:*

(1) $\mathcal{E}$ *is equivalent to a category with finitely many objects.*

(2) Γ *is a functor from* $\mathcal{E}$ *to the category of* $\mathcal{A}$*-algebras; for* $\varphi\in\mathcal{E}$, *there exists an elementary abelian p-group E such that* $\Gamma_\varphi \simeq \Gamma E$, *and if* $\varphi\to\theta\in\mathcal{E}$, *then* $\Gamma_\varphi\to\Gamma_\theta$ *is epic.*

(3) *If* $\varphi\to\theta$ *and* $\varphi\to\pi$ *are two maps in* $\mathcal{E}$ *such that* $\operatorname{Ker}(\Gamma_\varphi\to\Gamma_\theta)\subseteq\operatorname{Ker}(\Gamma_\varphi\to\Gamma_\pi)$, *then there is a commutative diagram*



in $\mathcal{E}$; *if* $\operatorname{Ker}(\Gamma_\varphi\to\Gamma_\theta)=\operatorname{Ker}(\Gamma_\varphi\to\Gamma_\pi)$, *then* $\theta\to\pi$ *is an equivalence. All endomorphisms in* $\mathcal{E}$ *are isomorphisms.*

(4) *If* $\varphi\in\mathcal{E}$, *and P is a prime* $\mathcal{A}$*-ideal of* Γ_φ, *then there exists* $\varphi\to\theta\in\mathcal{E}$ *such that* $P=\operatorname{Ker}(\Gamma_\varphi\to\Gamma_\theta)$; *if P is the maximal ideal of* Γ_φ, *then* θ *is a final object of* $\mathcal{E}$.

(5) Γ *is faithful and* $\mathcal{E}$ *has a final object.*

(6) $\mathcal{E}$ *is closed under cofibred coproducts.*

Proof. Statements (2) to (5) follow from the definitions of $\mathcal{E}$ and Γ and from Lemmas 2.1 and 2.2. These statements imply (6) in the following way. Let $f:\varphi\to\theta$ and $g:\varphi\to\pi$ be maps in $\mathcal{E}$, and let $P_f\subseteq\Gamma_\varphi$ and $P_g\subseteq\Gamma_\varphi$ be the kernels of f and g. I assert that P_f+P_g is prime. For identify Γ_φ with ΓE, where E is an elementary abelian p-group. Then there are subspaces E_f, $E_g \subseteq E$ such that $P_f = \operatorname{Ker}(\Gamma E \to \Gamma E_f)$ and $P_g = \operatorname{Ker}(\Gamma E \to \Gamma E_g)$. Let $P = \operatorname{Ker}(\Gamma E \to \Gamma(E_f \cap E_g))$; then $P = P_f + P_g$. There is an object $\eta \in \mathcal{E}$ such that $\Gamma_\eta \xrightarrow{\sim} \Gamma_\varphi / P$, and by (3), there is a commuting diagram

$$\begin{array}{ccc} \varphi & \xrightarrow{f} & \theta \\ {\scriptstyle g}\big\downarrow & & \big\downarrow \\ \pi & \longrightarrow & \eta \end{array}$$

It is now straightforward to verify that this is a cofibre square.

Finally, to prove (1), it suffices to note two things. First, there are finitely many morphisms between objects in $\mathcal{E}$ since those morphisms are determined by maps between two finite vector spaces. Second, the isomorphism classes of objects in $\mathcal{E}$ are in one-to-one correspondence with the prime $\mathcal{A}$-ideals in Λ. And

2.4. Lemma. *If Λ is a Noetherian, unstable $\mathcal{A}$-algebra, then Λ has finitely many prime $\mathcal{A}$-ideals.*

Proof. Since Λ is Noetherian, it has finitely many minimal prime ideals. Let $P \subseteq \Lambda$ be a minimal prime ideal, and let $\varphi : \Lambda \to \Gamma E$ be a finite morphism with kernel P. By the going up theorem, if $P' \subseteq \Lambda$ is a prime containing P, then there is a prime $Q \subseteq \Gamma E$ such that $P' = \varphi^{-1}(Q)$. But there are finitely many prime $\mathcal{A}$-ideals $Q \subseteq \Gamma E$ since they correspond to sub vector spaces of E.

Proof of Theorem 1.7. Together with the main theorem, the above proposition provides the properties of $\mathcal{E}$ and Γ used by Quillen to prove the Stratification Theorem [12; §9, §10].

2.5. Proposition. *Let $\mathcal{E}$ be a category and Γ a functor from $\mathcal{E}$ to the category of $\mathcal{A}$-algebras satisfying* 2.3(1) *and* 2.3(2). *Then*

$$\Lambda = \varprojlim \Gamma_\varphi, \quad \varphi \in \mathcal{E},$$

is a reduced, Noetherian, unstable $\mathcal{A}$-algebra. Furthermore, each projection $\Lambda \to \Gamma_\varphi$ is a finite morphism.

This proposition will be proved in Section 5.

Proof of Theorem 1.6. In view of Proposition 1.5, Theorem 1.6 is subsumed under the following:

2.6. Theorem. *Let $\mathcal{E}$ be a category, and let Γ be a functor from $\mathcal{E}$ to the category* *of $\mathscr{B}$-algebras. Then the pair $(\mathscr{E},\Gamma)$ is equivalent to the universal cover of a Noetherian, unstable $\mathscr{B}$-algebra if and only if $\mathscr{E}$ and Γ satisfy* 2.3(1) *to* 2.3(5). *In that case, there is a natural equivalence*

$$\mathscr{H}: \mathscr{E} \to \mathscr{E}(\Lambda) \quad \textit{where } \Lambda = \varprojlim \Gamma_\varphi,\ \varphi \in \mathbb{E}.$$

Proof. Let $\Lambda = \varprojlim \Gamma_\varphi$, $\varphi \in \mathscr{E}$. For each $\varphi \in \mathscr{E}$, the projection $\Lambda \to \Gamma_\varphi$ is a finite morphism; thus, this projection is an object of $\mathscr{E}(\Lambda)$; call it $\mathscr{H}_\varphi$. Clearly $\mathscr{H}$ is a functor. To complete the proof, we must show that $\mathscr{H}$ is an equivalence of categories. The argument given here relies on the reader checking the details in Quillen's proof of the Stratification Theorem. A more transparent proof, not appealing to the Stratification Theorem, will be given in Section 6.

Using the Stratification Theorem, simply note that $\mathscr{H}$ induces a diagram of varieties

$$\begin{array}{ccc} \varinjlim_{\mathscr{E}(\Lambda)} \Gamma & \xrightarrow{\ \lim \mathscr{H}\ } & \varinjlim_{\mathscr{E}} \Gamma \\ & \searrow \wr \quad \wr \swarrow & \\ & \Lambda(\Omega) & \end{array}$$

By Quillen's proof [12; §9, §10], conditions 2.3(1) to 2.3(6) imply a stratification

$$\Lambda(\Omega) = \coprod V_\varphi^+$$

(notation as in 1.7) where the disjoint union is taken over a set of representatives φ of the isomorphism classes of $\mathscr{E}$. $\varinjlim \mathscr{H}$ maps this stratification to the one given in Theorem 1.7. By Quillen's proof of [12; Proposition 1.10], $\mathscr{H}$ is an equivalence.

Remark. As a set of axioms, 2.3(1) to 2.3(5) are somewhat redundant. In particular, the second and third assertions in 2.3(3) can be derived from the first assertion and the other axioms.

3. Proof of the Main Theorem

Throughout this section, let Λ be a Noetherian, unstable $\mathscr{B}$-algebra. The following proposition is a partial generalization of the Chinese Remainder Theorem.

3.1. Proposition. *The map induced by quotients*

$$\Lambda \to \varprojlim \Lambda/P,$$

where P runs over the prime $\mathscr{B}$-ideals of Λ, is a uniform F-isomorphism.

Proof. Since the minimal prime ideals of Λ are $\mathscr{B}$-ideals, the kernel of the above morphism is $\sqrt{0}$. Let $M_1, \dots, M_n$ be the minimal prime ideals of Λ. An element x of $\varprojlim \Lambda/P$ can be represented uniquely as an n-tuple $(x_1, \dots, x_n)$, $x_i \in \Lambda/M_i$, such that, for all i and j, x_i and x_j reduce to the same element of Λ/P whenever $M_i + M_j \subseteq P$. Suppose, inductively, that there exists $y \in \Lambda$ such that $x_i \equiv y \pmod{M_i}$ for each $1 \le i < k$. Let

$$I = \bigcap_{i=1}^{k-1} M_i.$$

If P is a prime $\mathscr{A}$-ideal of Λ such that $I + M_k \subseteq P$, then $y - x_k \in P$. Since the intersection of all such ideals is $\sqrt{I + M_k}$, $y - x_k \in \sqrt{I \in M_k}$. Thus, for some m, $(y - x_k)^m \in I + M_k$. We may assume that m is a power of p. Thus, $(y - x_k)^m = y^m - x_k^m = a - b$, where $a \in I$, $b \in M_k$. Put

$$z = (y^m - a) = (x_k^m - b).$$

Then $z \equiv x_i^m \pmod{M_i}$ for $1 \le i \le k$. Thus the map $\Lambda \to \varprojlim \Lambda_P$ is an F-isomorphism. Since $\varprojlim \Lambda_P$ is Noetherian, the map is a uniform F-isomorphism.

Let $(\mathscr{E}, \Gamma)$ be the universal cover of Λ. For each object $\varphi : \Lambda \to \Gamma_\varphi$ of $\mathscr{E}$, let

$$\bar{\Lambda}_\varphi = \{x \in \Gamma_\varphi \mid x^{p^r} \in \operatorname{Im} \varphi \text{ for some } r\}.$$

If $f : \varphi \to \theta \in \mathscr{E}$, then $f : \bar{\Lambda}_\varphi \to \bar{\Lambda}_\theta$ since the property of having a p-th root in Γ_φ is determined by Steenrod operations [2; Theorem 1.2]. Thus $\varphi \Rightarrow \bar{\Lambda}_\varphi$ is a subfunctor of Γ. Let

$$\text{(3.2)} \qquad \bar{\Lambda} = \varprojlim \bar{\Lambda}_\varphi, \quad \varphi \in \mathscr{E}.$$

There is a natural map $\Lambda \to \bar{\Lambda}$ which is universal for maps of Λ into reduced, unstable $\mathscr{A}$-algebras that are closed under purely inseparable extension (that is, satisfy [2; (1.2.2)]).

3.3. Proposition. *The natural map $\Lambda \to \bar{\Lambda}$ is a uniform F-isomorphism, and $\mathscr{E}(\Lambda) \simeq \mathscr{E}(\bar{\Lambda})$. if $f : \Lambda' \to \Lambda$ is a map of Noetherian, unstable $\mathscr{A}$-algebras, then the induced map $\bar{f} : \bar{\Lambda}' \to \bar{\Lambda}$ is an isomorphism iff f is an F-isomorphism.*

Proof. Let $\varphi, \theta \in \mathscr{E}$, and let $P_\varphi = \operatorname{Ker} \varphi$, $P_\varphi = \operatorname{Ker} \theta$. Then there is a commutative diagram

$$\begin{array}{ccc} & \nearrow & \Gamma_\varphi \\ \Lambda & & f \downarrow \wr \\ & \searrow & \Gamma_\theta \end{array}$$

iff $P_\theta = P_\varphi$; the induced isomorphism $\bar{\Lambda}_\varphi \xrightarrow{\sim} \bar{\Lambda}_\theta$ does not depend on the choice of f since p-th roots are unique in an $\mathbb{F}_p$-integral domain. Therefore, the inverse limit

(3.2) may be taken to be a limit over the category of prime $\mathscr{B}$-ideals of Λ. Now, for each φ, $\Lambda/P_\varphi \to \bar{\Lambda}_\varphi$ is an F-isomorphism, and a finite limit of F-isomorphisms is again an F-isomorphism. By Proposition 3.1, $\Lambda \to \bar{\Lambda}$ is an F-isomorphism.

To see that $\mathscr{E}(\Lambda) = \mathscr{E}(\Lambda')$, note first that, by the construction and the uniqueness of p-th roots, $\mathscr{E}(\Lambda)$ is a full subcategory of $\mathscr{E}(\Lambda)$. Now $\Lambda \to \bar{\Lambda}$ is finite since $\bar{\Lambda}$ is a subalgebra of the finitely generated Λ-module $\prod \Gamma_\varphi$, where φ runs over a set of representatives of the isomorphism classes of $\mathscr{E}(\Lambda)$. Thus, finally, if $\varphi \in \mathscr{E}(\bar{\Lambda})$, then $\Lambda \to \bar{\Lambda} \to \Gamma_\varphi$ is an object of $\mathscr{E}(\Lambda)$.

To complete the proof, let $f: \Lambda' \to \Lambda$ be an F-isomorphism. If $\varphi \in \mathscr{E}(\Lambda)$, then $f^{-1}(P_\varphi)$ is a prime $\mathscr{B}$-ideal of Λ' and $\Lambda'/f^{-1}(P_\varphi) \hookrightarrow \Lambda/P_\varphi$ is a purely inseparable extension. Now, an F-isomorphism of Noetherian $\mathbb{F}_p$-algebras is finite; thus, $\Lambda' \to \Lambda \to \Gamma_\varphi$ is an object of $\mathscr{E}(\Lambda')$, and $\bar{\Lambda}'_{\varphi \circ f} \xrightarrow{\sim} \bar{\Lambda}_\varphi$. Consequently, $\bar{\Lambda}' \to \bar{\Lambda}$ is epic. Finally, if P' is a prime $\mathscr{B}$-ideal of Λ', then there exists an object $\varphi \in \mathscr{E}(\Lambda)$ such that $f^{-1}(P_\sigma) = P'$. Thus, $\bar{\Lambda}' \to \bar{\Lambda}$ is monic.

Proof of Proposition 1.5. The previous proposition shows that an F-isomorphism induces an equivalence of categories. The other half of 1.5 is an easy consequence of the Main Theorem.

Proof of Theorem 1.4. The first step in proving the Main Theorem is to show that we may suppose Λ to be an integral domain. Let P be a prime $\mathscr{B}$-ideal of Λ, and let $\mathscr{E}_P$ be the full subcategory of $\mathscr{E}$ that consists of objects φ such that $P \subseteq P_\varphi$. Then the quotient map $\Lambda \to \Lambda/P$ induces an isomorphism of $\mathscr{E}(\Lambda/P)$ with $\mathscr{E}_p$. The assignment

$$P \Rightarrow \varprojlim \Gamma_\varphi, \quad \varphi \in \mathscr{E}_P,$$

is a contravariant functor on the category of prime $\mathscr{B}$-ideals in Λ. A straightforward categorical argument proves

3.4. Lemma.

$$\varprojlim_{\varphi \in \mathscr{E}} \Gamma_\varphi \xrightarrow{\sim} \varprojlim_{P} \varprojlim_{\varphi \in \mathscr{E}_P} \Gamma_\varphi.$$

In view of this and Proposition 3.1, we may suppose for the remainder of this section that Λ is a Noetherian, unstable $\mathscr{B}$-integral domain.

Fix an integral extension $\Lambda \hookrightarrow \Gamma$ such that $\Gamma = \Gamma E$, E an elementary abelian p-group. Every object of $\mathscr{E}$ is isomorphic to one of the form $\Lambda \to \Gamma/Q$, where Q is a prime $\mathscr{B}$-ideal of Γ. Similarly, for each prime $\mathscr{B}$-ideal P of Λ, every object of $\mathscr{E}_P$ is isomorphic to one of the form $\Lambda/P \to \Gamma/Q$ where Q lies over P (that is, where $Q \cap \Lambda = P$). We may replace $\mathscr{E}$ and the $\mathscr{E}_P$ by their full subcategories of objects of the above forms.

Let $L \subseteq \Gamma$ be the inverse limit of all Γ/Q where Q runs over the prime $\mathscr{B}$-ideals of Γ. We will prove that $\Lambda \hookrightarrow L$ is an F-isomorphism (that is, a purely inseparable extension) by induction on the Krull dimension of Λ. Therefore, we may assume that

(3.5) $\Lambda/(\Lambda \cap Q) \hookrightarrow L/(L \cap Q)$

is an F-isomorphism for all non-zero prime $\mathscr{B}$-ideals Q of Λ. By the proof of Proposition 3.3, we may assume that Λ and L are closed in Γ under purely inseparable extensions. We are reduced to showing that $\Lambda = L$. Let

$$J = \{x \in \Lambda \mid xL \subseteq \Lambda\}.$$

Then J is a $\mathscr{B}$-ideal. Fix a minimal prime $\mathscr{B}$-ideal P of Λ such that $J \subseteq P$. Then P is not the zero ideal since J is not zero. Indeed, L is a finite Λ-module and is contained in the field of quotients of Λ. Therefore, a common denominator of a set of generators of L over Λ is an element of J.

3.6. Lemma. *If P contains the maximal ideal of Λ, then $\Lambda = L$.*

Proof. Since P contains the unique maximal ideal of Λ, P is the only prime ideal of Λ containing J, for P contains every such prime ideal and is minimal. Consequently, $P = \sqrt{J}$, and there exists $r \geq 0$ such that $x^{p^r} \in J$ for all $x \in P$. Let $x \in L$ satisfy an equation

$$x^m + a_{m-1}x^{m-1} + \cdots + a_0 = 0$$

with each $a_i \in \Lambda$. Then

$$x^{mp^r} + a_{m-1}^{p^r} x^{(m-1)p^r} + \cdots + a_0^{p^r} = 0.$$

Since P contains all the elements of Λ of nonzero degree, each $a_i^{p^r} \in J$. Thus $x^{mp^r} \in \Lambda$ and $x^{mp^{2r}} \in J$. Choose s so that $p^s \geq mp^{2r}$. Then $x^{p^s} = x^{mp^{2r}} x^{p^s - mp^{2r}} \in \Lambda$. Since Λ is closed in L under purely inseparable extension, $\Lambda = L$.

To complete the proof of 1.4, we reason by contradiction. Assume $\Lambda \neq L$. Then P does not contain the maximal ideal of Λ. Let $\tilde{\Lambda}$ and $\tilde{L}$ denote the graded localizations of Λ and L with respect to the homogeneous multiplicative system $\Lambda - P$. Then $\tilde{\Lambda}$ is a local $\mathscr{B}$-algebra, and $\tilde{\Lambda}/P\tilde{\Lambda}$ is the field of quotients of Λ/P.

3.7. Lemma. *$\tilde{\Lambda}$ is closed in $\tilde{L}$ under purely inseparable extension. If $\Lambda \neq L$, then $\tilde{\Lambda} \neq \tilde{L}$.*

Proof. Let $(a/z)^p \in \tilde{\Lambda}$ where $a \in L$ and $z \in \Lambda - P$. For some $y \in \Lambda - P$, $y(a/z)^p \in \Lambda$. Thus, $(ya)^p \in \Lambda$. Since Λ is assumed to be closed under purely inseparable extension, $ya \in \Lambda$. This proves the first assertion. Now suppose $\tilde{\Lambda} = \tilde{L}$. Let $a_1, \ldots, a_r$ generate L as a Λ-module, and let $a_1 = b_1/z_1, \ldots, a_r = b_r/z_r$, where $b_i \in \Lambda$ and $z_i \in \Lambda - P$. If $z = z_1 \cdots z_r$, then $za_i \in \Lambda$ for each i; thus, $zL \subseteq \Lambda$ and $z \in P$. But this is a contradiction since P is prime. Thus $\tilde{\Lambda} \neq \tilde{L}$.

Let $\tilde{P} = P\tilde{\Lambda}$ and $\tilde{J} = J\tilde{\Lambda}$. Then $\tilde{J}\tilde{L} \subseteq \tilde{\Lambda}$, and $\tilde{P}$ is the only prime ideal of $\tilde{\Lambda}$ containing $\tilde{J}$. It follows that $\tilde{P}$ is the radical of $\tilde{J}$, and

(3.8) $x \in \tilde{P}\tilde{L} \Rightarrow x^{p^r} \in \tilde{\Lambda}$

for some r. Let $Q_1, \dots, Q_s \subseteq \tilde{L}$ be the prime $\mathscr{B}$-ideals lying above $\tilde{P}$. Since $\tilde{P}$ is maximal, each Q_i is maximal. By the inductive assumption (3.5), each inclusion

$$(3.9) \qquad \tilde{\Lambda}/\tilde{P} \hookrightarrow \tilde{L}/\tilde{Q}_i$$

is a purely inseparable extension of fields. The following lemma contradicts the hypothesis that $\Lambda \neq L$:

3.10. Lemma. *There exists $t \geq 0$ such that*

$$x \in \tilde{L} \Rightarrow x^{p^t} \in \tilde{\Lambda}.$$

Proof. By (3.8), it suffices to show that, for some $u \geq 0$, $x \in \tilde{L} \Rightarrow x^{p^u} \in \tilde{P}\tilde{L}$. Since the extensions (3.9) are purely inseparable, there are integers $r_1, \dots, r_s \geq 0$ such that

$$x \in \tilde{L} \Rightarrow x^{p^{r_i}} \in \tilde{\Lambda} + Q_i$$

for each $i = 1, \dots, s$. It follows that

$$x \in \tilde{L} \Rightarrow x^{p^{r_1 + \cdots + r_s}} \in \tilde{\Lambda} + (Q_1 \cap \cdots \cap Q_s).$$

But $Q_1, \dots, Q_s$ are all the associated prime ideals to $\tilde{P}\tilde{L}$; therefore, $Q_1 \cap \cdots \cap Q_s$ is the radical of $\tilde{P}\tilde{L}$ and the result follows.

4. Integral closure and its consequences

The object of this section is to recover for graded algebras standard results about integral Galois extensions (see Lang [10; IX, §2], for example). These results will be used in section six to prove Theorems 1.6 and 2.6.

Fix, throughout this discussion, the following notation and hypotheses:

4.1. *Let Λ be a graded integral domain over $\mathbb{F}_p$ that is integrally closed in its graded field of quotients K. Let L be a finite graded Galois extension of K with Galois group G, and let Γ be the integral closure of Λ in L. Let $P \subseteq \Lambda$ be a homogeneous prime ideal.* An ideal $Q \subseteq \Gamma$ is said to *lie over P* if $Q \cap \Lambda = P$; such an ideal is homogeneous.

4.2. Proposition. *If Q and Q' are prime ideals of Γ lying over P, then $\exists \sigma \in G$ such that $\sigma Q = Q'$.*

Proof. The standard proof (see, for example, [13; III, Proposition 4]) works in the graded case.

To prove the next few results, we need the following simple technical lemmas. Let H be a subgroup of G, Q an ideal of Γ and $x \in \Gamma$, let

$$N_t(x) = \prod (t + \sigma(x)), \quad \sigma \in H$$

where t is an indeterminant. Then

$$N_t(x) = t^r + c_1(x)t^{r-1} + \cdots + c_r(x) \quad \text{where } r = |H|.$$

4.3. Lemma. *Let $r = p^e m$, $(m,p) = 1$. Then the binomial coefficient $\binom{r}{p^e}$ is a unit in $\mathbb{F}_p$.*

Proof. $(1+t)^{p^e m} \equiv (1+t^{p^e})^m \pmod p$; therefore,

$$\binom{r}{p^e} \equiv \binom{m}{1} \pmod p.$$

The *normalized reduced trace* of x relative to H is

$$\operatorname{rtr}(H,x) = c_{p^e}(x) \Big/ \binom{r}{p^e}.$$

4.4. Lemma. $\operatorname{rtr}(H,x)$ *is H-invariant, and if $\sigma(x) \equiv x \pmod Q$ for all $\sigma \in H$, then*

$$rtr(H,x) \equiv x^{p^e} \pmod Q,$$

where $|H| = p^e m$, $(m,p) = 1$.

Continuing the notation 4.1, let Q be a prime ideal of Γ lying over P, and let

$$G_Q = \{\sigma \in G \mid \sigma(Q) \subseteq Q\}.$$

G_Q is called the *decomposition group* of Q. Let $L^d \subseteq L$ be the fixed field of G_Q; let $\Gamma^d = \Gamma \cap L^d$ and $Q^d = Q \cap L^d$. Then Q is the only prime ideal of Γ lying above Q^d (by the above proposition).

4.5. Proposition. *Let S be the multiplicative system of homogeneous elements of Λ not in P. Then the extension of fields*

$$S^{-1}\Lambda/P \hookrightarrow S^{-1}\Gamma^d/Q^d$$

is purely inseparable.

Proof. We may assume that P is maximal so that $S^{-1}\Lambda/P = \Lambda/P$; then Q is also maximal, and $S^{-1}\Gamma^d/Q^d = \Gamma^d/Q^d$. Let $\sigma_1, \ldots, \sigma_n$ be a set of coset representatives of G/G_Q. Then the prime ideals of Γ^d lying over P are $\sigma_1(Q^d), \ldots, \sigma_n(Q^d)$. Let $x \in \Gamma^d$ such that

$$y \equiv \sigma_i(x) \pmod{\sigma_i(Q^d)}$$

for each $i = 1, \ldots, n$. Then $\sigma(y) \equiv x \pmod{Q^d}$ for all $\sigma \in G$. By Lemma 4.4,

$$\operatorname{rtr}(G,y) \equiv x^{p^e} \pmod{Q^d} \quad \text{and} \quad \operatorname{rtr}(G,y) \in \Lambda.$$

4.6. Corollary. *Suppose, in addition, that $\Gamma = \Gamma E$, E an elementary abelian p-group, and suppose that $Q = \mathrm{Ker}(\Gamma E \to \Gamma E')$ where E' is a subvector space of E of dimension one. Then $\Lambda/P \hookrightarrow \Gamma^d/Q^d$ is a purely inseparable extension.*

Proof. If E' and E'' are distinct subspaces of E of dimension one, then $E' \cap E'' = 0$. Thus, in the above proof, $Q + \sigma(Q)$ is the augmentation ideal of Γ whenever $\sigma \notin G_Q$. Consequently, the Chinese Remainder Theorem may be applied to the elements $\sigma_i(x)$ and ideals $\sigma_i(Q^d)$ whenever x has non-zero degree. Therefore, the above proof goes through without first localizing.

4.7. Proposition. *Under the hypotheses* 4.1, *if Q is a prime of Γ, and if Γ/Q is integrally closed, then the purely inseparable closure of Γ^d/Q^d in Γ/Q is integrally closed in its graded field of quotients.*

Proof. Let $x, y \in \Gamma^d$, $y \notin Q^d$, represent elements $\bar{x}, \bar{y}$ of Γ^d/Q^d such that $\bar{y} \neq 0$. Suppose that $\bar{z} = \bar{x}/\bar{y}$ is integral over Γ^d/Q^d. Since Γ/Q is integrally closed, $\exists z \in \Gamma$ such that z represents $\bar{z}$. Then $\mathrm{rtr}(G_Q, Z) \in \Gamma^d$, and

$$\mathrm{rtr}(G_Q, Z) \equiv z^{p^e} \pmod{Q},$$

for $\sigma(\bar{z}) = \sigma(\bar{x})/\sigma(\bar{y}) = \bar{z}$ when $\sigma \in G_Q$.

4.8. Theorem. *In addition to the hypotheses* 4.1, *let Q be a prime ideal of Γ lying over P, and let $\bar{K}$ and $\bar{L}$ be the graded fields of quotients of Λ/P and Γ/Q respectively. Let G_Q be the decomposition group of Q. Then $\bar{L}$ is a normal extension of $\bar{K}$, and the natural map*

$$G_Q \to \mathrm{Gal}(\bar{L}/\bar{K})$$

induced by reduction modulo Q is an epimorphism.

Proof. By localizing at P we may assume that P is maximal; then Q is maximal, $\bar{K} = \Lambda/P$, and $\bar{L} = \Gamma/Q$. Let $x \in \Gamma$ represent $\bar{x} \in \Gamma/Q$, and let $f(X)$ be the irreducible polynomial of x. Since Λ is integrally closed, f has coefficients in Λ, and f factors into linear factors in Γ. Therefore, the reduction $\bar{f}$ of f mod Q factors into linear factors in Γ/Q and the irreducible polynomial of $\bar{x}$ over Λ/P is a factor of $\bar{f}$. It follows that Γ/Q is normal over Λ/P.

By Proposition 4.5, we may assume that $\Gamma^d = \Lambda$; then Q is the only prime ideal of Γ lying above P, and Γ is local. Let $\tau \in \mathrm{Gal}(\bar{L}/\bar{K})$. We must construct $\sigma \in G$ such that the reduction $\bar{\sigma}$ of σ modulo Q is equal to τ. It will suffice to check that $\bar{\sigma} = \tau$ on the maximal separable extension of $\bar{K}$ in $\bar{L}$. We will induct on the degree of L over K.

Let $\bar{K}(\bar{x})$ be a non-trivial separable extension of $\bar{K}$ in $\bar{L}$. Let $x \in \Gamma$ represent $\bar{x}$. Since $K(\bar{x})$ is separable, $K(\bar{x}) = K(\bar{x}^{p^s})$ for any $s \leq 0$; thus, we may suppose that x is separable over K. We may further suppose that no conjugate of x represents $\bar{x}$, for let

$$H=\{\sigma\in G\mid \sigma(x)\equiv x \pmod{Q}\};$$

then $\mathrm{rtr}(H,x)$ represents x^{p^e}, for some e, and is fixed by H. Since Λ is integrally closed, x has a monic irreducible polynomial $f(X)$ with coefficients in Λ; the reduction $\bar{f}$ of f mod P is the irreducible polynomial of $\bar{x}$ over $\bar{K}$ since distinct conjugates of x reduce to distinct conjugates of $\bar{x}$. Thus $\tau(\bar{x})$ is a zero of $\bar{f}(X)$; let σ be chosen so that $\sigma(x)$ is the corresponding zero of $f(X)$.

Let $\Sigma=\Lambda[x]$. The quotient field of Σ is $K(x)$, and $\Sigma/(\Sigma\cap Q)=\bar{K}(\bar{x})$; the reduction of σ mod Q agrees with τ on $\bar{K}(\bar{x})$. It now suffices to show that Σ is integrally closed, for then the theorem can be applied inductively with Λ replaced by Σ and τ replaced by $(\bar{\sigma})^{-1}\tau$.

4.9. Lemma. *Let Λ be an integrally closed graded domain, K its field of fractions, L a finite-dimensional separable graded K-algebra, and Γ the integral closure of Λ in L. Suppose $w_1,\dots,w_n$ is a homogeneous basis of l over K contained in Γ; then there is a unique basis $w_1^*,\dots,w_n^*$ of L over K for which $\mathrm{Tr}_{L/K}(w_iw_j^*)=\delta_{ij}$ (Kronecker index); if $d=D_{L/K}(w_1,\dots,w_n)$ is the discriminant of the basis $w_1,\dots,w_n$, then $d\neq 0$, and*

$$\sum_{i=1}^{n}\Lambda w_i\subseteq\Gamma\subseteq\left(\sum_{i=1}^{n}\Lambda w_i^*\right)\subseteq d^{-1}\left(\sum_{i=1}^{n}\Lambda w_i\right).$$

Proof. The proof of Bourbaki [5; V, §1.6, Lemma 3] works in the graded case.

To apply this lemma to Σ, notice that $1,x,\dots,x^{n-1}$ is a basis of Σ over Λ, where $n=\deg(f)$. Let $d=D_{K(x)/K}(1,x,\dots,x^{n-1})$. Since the conjugates of x are in one-to-one correspondence with the conjugates of $\bar{x}, d$ reduces mod Q to $\bar{d}=D_{\bar{K}(\bar{x})/\bar{K}}(1,\bar{x},\dots,\bar{x}^{n-1})$. But $\bar{K}(\bar{x})$ is separable; thus $\bar{d}\neq 0$, and $d\notin P$. And Λ is local; thus $d^{-1}\in\Lambda$. By the lemma, the integral closure of Σ is contained in $d^{-1}\Sigma=\Sigma$. Thus Σ is integrally closed.

4.10. Corollary. *Under the hypotheses of Theorem 4.8, the separable degree of $\bar{L}$ over $\bar{K}$ is finite.*

A theorem of Borel [3; Theorem B] states that if G is a compact, connected Lie group with no p-torsion, then any elementary abelian p-group is contained in a torus. As an illustration of Theorem 4.8, I give the following amusing generalization.

4.11. Proposition. *Let G be a compact connected lie group without p-torsion, let E be an elementary abelian p-group in G, and let $\theta: E\to E$ be an automorphism induced by conjugation (that is, $\theta\in\mathcal{A}(G)$). Then θ is induced by an element of the Weyl group $W(G)$.*

Proof. Let T be a maximal torus containing E. Since G has no p-torsion, $H^*(BG;\mathbb{F}_p)$ is a polynomial algebra on generators of even degree [4; Proposition 7.2, Theorem 19.1]. Thus $H^*(BG;\mathbb{F}_p)$ is integrally closed. Apply Quillen's main theorem [12; 6.2] and Theorem 4.8 with $\Gamma=H^*(BT;\mathbb{F}_p)$, $\Lambda=H^*(BG;\mathbb{F}_p)$, and $\Gamma/Q=H^*(BE;\mathbb{F}_p)$. Then $\mathrm{Gal}(\bar{L}/\bar{K})$ is the automorphism group of E in $\mathscr{A}(G)$. It now suffices to show that Γ^W is a purely inseparable extension of Λ, for then $\mathrm{Gal}(\Gamma/\Lambda)$ is a quotient of W. Now $H^*(BG;\mathbb{F}_p)=H^*(BT;\mathbb{Z})^W\otimes\mathbb{F}_p$ [4; Proposition 29.2]; thus we only need

4.12. Lemma. *Let $\Sigma=\mathbb{Z}[t_1,\dots,t_n]$, $\deg t_i=2$, and let G be a finite group of homogeneous automorphisms of Σ. Then $(\Sigma\otimes\mathbb{F}_p)^G$ is a purely inseparable extension of $\Sigma^\Gamma\otimes\mathbb{F}_p$. If $p\nmid |G|$, then the two are equal.*

Proof. Let $x\in\Sigma$ be fixed under G modulo $p\Sigma$. Then $\mathrm{rtr}(G,x)$ is fixed under G, and

$$\mathrm{rtr}(G,x)\equiv x^{p^e} \pmod{p\Sigma}$$

where $|G|=p^e m$, $(m,p)=1$. If $p\nmid |G|$, $\mathrm{rtr}(G,x)\equiv x \pmod{p\Sigma}$.

5. Polynomial invariants

This section contains a review of facts about polynomial invariants of $\mathrm{Gl}(n,\mathbb{F}_p)$ that are needed for the rest of this paper or are useful in understanding Noetherian cohomology rings. Most of the results given here are to be found in other sources and are stated without proof. Proposition 5.8 may be new. At the end of this section, Proposition 2.5 is proved.

Let $\mathbb{F}_q$ be the finite field with q-elements, $q=p^e$. Let $\Gamma_n=\mathbb{F}_q[x_1,\dots,x_n]$ be the graded polynomial algebra on n-indeterminants of degree d. Then $\mathrm{Gl}(n,\mathbb{F}_q)$ acts on Γ_n by extension of its natural action on the $\mathbb{F}_q$-vector space Γ_n^d. Let Δ_n be the ring of polynomial invariants

$$\Delta_n=\Gamma_n^{\mathrm{Gl}(n,\mathbb{F}_q)}.$$

Recall the description of Δ_n due to Dickson. For distinct non-negative integers $e_1,\dots,e_n$, let

$$[e_1,\dots,e_n]=\begin{vmatrix} x_1^{q^{e_1}} & x_2^{q^{e_1}} & \cdots & x_n^{q^{e_1}} \\ x_1^{q^{e_2}} & x_2^{q^{e_2}} & \cdots & x_n^{q^{e_2}} \\ \vdots & \vdots & & \vdots \\ x_1^{q^{e_n}} & x_2^{q^{e_n}} & \cdots & x_n^{q^{e_n}} \end{vmatrix}.$$

If $g\in\mathrm{Gl}(n,\mathbb{F}_q)$, then $g([e_1,\dots,e_n])=\det(g)\cdot[e_1,\dots,e_n]$. Put

$$D_{n,i}=[0,1,\dots,i-1,i+1,\dots,n],\qquad L_n=D_{n,n}.$$

5.1. Theorem (L.E. Dickson [8]). (1) *$q_{n,i} = D_{n,i}/L_n$ is a polynomial for $0 \le i \le n$. In particular, $q_{n,0} = L_n^{q-1}$, and $q_{n,n} = 1$.*

(2) *The algebra Δ_n of invariants of* $\mathrm{Gl}(n, \mathbb{F}_q)$ *is* $\mathbb{F}_q[q_{n,0}, \dots, q_{n,n-1}]$.

(3) *The algebra of invariants of* $\mathrm{Sl}(n, \mathbb{F}_q)$ *is* $\mathbb{F}_q[L, q_{n,1}, \dots, q_{n,n-1}]$.

(4) $$\deg(L_n) = d \cdot \frac{q^n - 1}{q - 1}, \qquad \deg(q_{n,i}) = d(q^n - q^i).$$

(5) *Let $\Phi_n(\xi) = \prod(\xi - \alpha)$, $\alpha \in \Gamma_n^d$, ξ an indeterminant; then*

$$\Phi_n(\xi) = \xi^{q^n} + \sum_{s=0}^{n-1} (-1)^{n-s} q_{n,s} \xi^{q^s}.$$

(6) $$q_{n,0} = \prod \alpha, \qquad \alpha \in \Gamma_n^d, \quad \alpha \ne 0.$$

5.2. Proposition. *Let $f: \Gamma_n \to \Gamma_{n-j}$ be an epimorphism. Then for $n \ge j > 0$,*

$$f(L_n) = 0, \qquad f(q_{n,i}) = \begin{cases} (q_{n-j,i-j})^{q^j}, & j \le i < n, \\ 0, & \textit{otherwise}. \end{cases}$$

Proof. We may assume $j = 1$, and

$$f(x_i) = \begin{cases} x_i, & 0 \le i < n, \\ 0, & i = n. \end{cases}$$

L'Hopital's rule works for polynomials over $\mathbb{F}_q$. It is easy to check that

$$\frac{\partial}{\partial x_n} D_{n,i}\big|_{x_n=0} = \begin{cases} D_{n-1,i-1}^q, & i > 0, \\ 0, & i = 0. \end{cases}$$

The result follows.

Now specialize to $q = p$; put $d = 2$ for p odd and $d = 1$ for $p = 2$. Equip Γ_n with its unique structure as an unstable $\mathscr{A}$-algebra. Let $Q^0, Q^1, Q^2, \dots$ be the derivations on Γ_n given inductively by [2; §2]

$$\begin{cases} Q^0 x = kx \quad \text{for } x \in {\Gamma_n}^{dk}, \\ Q^1 = P^1, \\ Q^{i+1} = P^{p^i} Q^i - Q^i P^{p^i}. \end{cases}$$

5.3. Proposition ([11], [18]). *For $0 \le i < n$ and $0 \le k < n$,*

(1) $$P^{p^i}(L_n) = \begin{cases} L_n \cdot q_{n,n-1}, & i = n-1, \\ 0, & 0 \le i < n-1. \end{cases}$$

(2) $$P^{p^i}(q_{n,k}) = \begin{cases} -q_{n,k} q_{n,n-1}, & i = n-1, \\ q_{n,k-1}, & i = k-1, \\ 0, & \textit{otherwise}. \end{cases}$$

5.4. Proposition ([18]). *The formulas* 5.3(2) *imply that for* $0<i<n$ *and* $0\le k<n$,

(1) $$Q^i q_{n,k}=\begin{cases}(-1)^{k-1}q_{n,0}, & i=k,\\ 0, & i\neq k.\end{cases}$$

(2) $$Q^n q_{n,k}=(-1)^n q_{n,k}q_{n,0}.$$

(3) $$Q^0 q_{n,k}=\begin{cases}-q_{n,0}, & k=0,\\ 0, & k\neq 0.\end{cases}$$

(4) $$Q^n+\sum_{i=0}^{n-1}(-1)^{n-i}q_{n,i}Q^i\equiv 0 \quad on\ \Gamma_n.$$

The following characterization of the elements $q_{n,i}$ by the action of the Steenrod algebra on them is due to Adams and Wilkerson.

5.5. Theorem ([2; Theorem 5.1]). *There is a unique relation on* Γ_n *of the form*

$$Q^n+c_{n-1}Q^{n-1}+\cdots+c_0Q^0\equiv 0$$

where $c_0,\dots,c_{n-1}\in\Gamma_n$. *Thus* $c_i=(-1)^{n-i}q_{n,i}$.

5.6. Corollary. *The elements* $q_{n,i}$ *of* Γ_n *are characterized by the formulas* 5.3(2). *The element* $L_n\in\Gamma_n$ *is characterized by* 5.3(1) *up to multiplication by a unit.*

Proof. The last assertion follows from the equation $L_n^{p-1}=q_{n,0}$.

We will require certain generalizations of the $q_{n,i}$'s. Let P be a prime $\mathscr{B}$-ideal of Γ_n, and let $\Gamma_n/P\simeq\Gamma_s$. Put

$$q_{n,P}=\prod\alpha,\quad \alpha\in(\Gamma_n-P)^d.$$

5.7. Proposition. *Let* P *and* Q *be prime* $\mathscr{B}$*-ideals of* Γ_n, *and let* $\Gamma_n/P\simeq\Gamma_s$, $\Gamma_n/Q\simeq\Gamma_t$. *Then*

(1) $q_{n,P}$ *reduces to zero in* Γ_n/Q *unless* $Q\subseteq P$.
(2) $q_{n,P}$ *reduces to* $(q_{s,0})^{p^{n-s}}\in\Gamma_n/P$.
(3) *If* $Q\subseteq P$, $q_{n,P}$ *reduces to* $(q_{t,P/Q})^{p^{n-t}}\in\Gamma_n/Q$.
(4) *If* $f:\Gamma_n\to\Gamma_n$ *is an automorphism such that* $f(P)=Q$, *then* $f(q_{n,P})=q_{n,Q}$.

Proof. If $Q\not\subseteq P$, then $\exists\alpha\in(\Gamma_n-P)^d$ such that $\alpha\in Q$; therefore, $q_{n,P}\equiv 0\ (\mathrm{mod}\ Q)$. If $Q\subseteq P$, the order of Q^d is p^{n-t}, and modulo Q

$$q_{n,P}\equiv\prod\alpha^{p^{n-t}},\quad \alpha\in(\Gamma_n/Q-P/Q)^d.$$

5.8. Proposition. *For* $0\le s<n$,

$$q_{n,s}=\sum q_{n,P}$$

where the sum runs over all prime $\mathscr{B}$*-ideals* P *of* Γ_n *such that* $\Gamma_n/P\simeq\Gamma_s$.

Proof. Let $x = \sum q_{n,p}$. Clearly x is an invariant of $\mathrm{Gl}(n, \mathbb{F}_p)$, and $\deg(x) = d(p^n - p^s)$. A straightforward exercise in elementary number theory shows that the only monomial in $q_{n,0}, \ldots, q_{n,n-1}$ having degree $d(p^n - p^s)$ is $q_{n,s}$. Therefore, x is a multiple of $q_{n,s}$. But for any prime $\mathscr{B}$-ideal P such that $\Gamma_n/P \simeq \Gamma_s$, x reduces modulo P to $q_{s,0}^{p^{n-s}}$. By Proposition 5.2, $x = q_{n,s}$.

Proof of Proposition 2.5. Let $\mathscr{E}$ be a category and Γ a functor on $\mathscr{E}$ satisfying 2.3(1) and 2.3(2). For $\varphi \in \mathscr{E}$, let

$$\Delta_\varphi = (\Gamma_\varphi)^{\mathrm{Aut}(\Gamma_\varphi)}.$$

There is an isomorphism $\Gamma_\varphi \xrightarrow{\sim} \Gamma_n$ for $n = \mathrm{rank}(\Gamma_\varphi)$; such an isomorphism induces an isomorphism $\Delta_\varphi \xrightarrow{\sim} \Delta_n$, which does not depend on the choice of $\Gamma_\varphi \xrightarrow{\sim} \Gamma_n$. Let $q_{\varphi,i} \to q_{n,i}$ under the isomorphism $\Delta_\varphi \xrightarrow{\sim} \Delta_n$. Since each $\Gamma_\theta \to \Gamma_\varphi$ is epic for $\theta \to \varphi \in \mathscr{E}$, $\Delta_\theta \to \Delta_\varphi$ and Δ is a functor on $\mathscr{E}$. Let

$$\Delta = \varprojlim_{\varphi \in \mathscr{E}} \Delta_\varphi;$$

Δ is a sub-$\mathscr{B}$-algebra of $\Lambda = \varprojlim \Gamma_\varphi$.

We may assume that $\mathscr{E}$ has finitely many objects. For $\varphi \in \mathscr{E}$, let $r(\varphi) = \mathrm{rank}(\Gamma_\varphi)$ and let

$$n = \sup\{r(\varphi) \mid \varphi \in \mathscr{E}\}.$$

For each $\varphi \in \mathscr{E}$, let $\Delta_n \to \Gamma_\varphi$ be the unique map induced by any epimorphism $\Gamma_n \to \Gamma_\varphi$. Then all diagrams

$$\begin{array}{ccc} & & \Gamma_\theta \\ & \nearrow & \\ \Delta_n & & \downarrow \\ & \searrow & \\ & & \Gamma_\varphi \end{array}$$

commute for $\varphi \to \theta \in \mathscr{E}$. Thus there are inclusions $\Delta_n \hookrightarrow \Delta \hookrightarrow \Lambda \hookrightarrow \prod \Gamma_\varphi$. By 5.1 and 5.2, each $\Delta_n \to \Gamma_\varphi$ is a finite morphism, for Γ_φ may be obtained from the image of $\Delta_n \to \Gamma_\varphi$ by adjoining finitely many integral algebraic elements. Therefore $\prod \Gamma_\varphi$, $\varphi \in \mathscr{E}$, is a finitely generated Δ_n-module. Since Δ_n is Noetherian, so are Δ and Λ. This proves 2.5.

6. Proof of Theorems 1.6 and 2.6

6.1. Proposition. *Let $\mathscr{E}$ be a category and Γ a functor that satisfy 2.3(1) to 2.3(5). Let $\Lambda = \varprojlim \Gamma_\varphi$, $\varphi \in \mathscr{E}$. Then there is an integer $e \geq 0$ such that, for each $\varphi \in \mathscr{E}$, there exists $\upsilon_\varphi \in \Lambda$ that satisfies:*

(1) *If $\theta \in \mathscr{E}$, then υ_φ reduces to zero in Γ_θ unless there exists $\theta \to \varphi$ in $\mathscr{E}$.*

(2) *υ_φ reduces to $(q_{\varphi,0})^{p^{e-s}} \in \Gamma_\varphi$ where $s = \mathrm{rank}(\Gamma_\varphi)$ and $q_{\varphi,0} = \prod \alpha$, $\alpha \in \Gamma_\varphi^d$, $\alpha \neq 0$.*

(3) *More generally, for* $\theta\to\varphi$, υ_φ *reduces to*

$$\upsilon_{\varphi,\theta}=\sum (q_{\theta,P})^{p^{e-s}}\in\Gamma_\theta$$

where $s=\mathrm{rank}(\Gamma_\theta)$, *P runs over all prime* $\mathscr{B}$*-ideals of* Γ_θ *for which there exists* $\theta\to\varphi\in\mathscr{E}$ *such that* $P=\mathrm{Ker}(\Gamma_\theta\to\Gamma_\varphi)$, *and* $q_{\theta,P}=\prod\alpha$, $\alpha\in(\Gamma_\theta-P)^d$.

Furthermore, e may be taken to be $\max\{\mathrm{rank}(\Gamma_\varphi)\mid\varphi\in\mathscr{E}\}$.

Proof. Put

$$e=\max\{\mathrm{rank}(\Gamma_\varphi)\mid\varphi\in\mathscr{E}\},$$

and fix $\varphi\in\mathscr{E}$. Let $\upsilon_\varphi\in\prod\Gamma_\theta$, $\theta\in\mathscr{E}$, be the element described above. We must show that $\upsilon_\varphi\in\Lambda$. For each $\theta\in\mathscr{E}$, let

$$S_\theta=\{P\subseteq\Gamma_\theta\mid\exists\theta\to\varphi\in\mathscr{E}\colon P=\mathrm{Ker}(\Gamma_\Theta\to\Gamma_\varphi)\}.$$

Let $f:\theta\to\pi\in\mathscr{E}$. Then $\Gamma f^{-1}:S_\pi\to S_\theta$ is a monomorphism that sends $P\subseteq\Gamma_\pi$ to $\Gamma f^{-1}(P)\subseteq\Gamma_\theta$. Let $Q=\mathrm{Ker}\,\Gamma f$, and let $P\in S_\theta$. If $Q\nsubseteq P$, then $q_{\theta,P}$ reduces to zero in Γ_π (see 5.7). If $Q\subseteq P$, then $P=f^{-1}(P/Q)$, and by 2.3(3), $P/Q\in S_\pi$. Then

$$f(q_{\theta,P})=(q_{\pi,P/Q})^{p^{r(\theta)-r(\pi)}}$$

as required.

Remark. Proposition 6.1 and its proof are a correction of [12; 11.4].

6.2. Proposition. *If* $\mathscr{E}$ *and* Γ *satisfy* 2.3(1) *to* 2.3(5) *and* $\Lambda=\varprojlim\Gamma_\varphi$, $\varphi\in\mathscr{E}$, *then for each* $\varphi\in\mathscr{E}$

$$\mathrm{Aut}_{\mathscr{E}}(\varphi)=\mathrm{Gal}(\Gamma_\varphi/\Lambda_\varphi)\quad\textit{where } \Lambda_\varphi=\mathrm{Im}(\Lambda\to\Gamma_\varphi).$$

Proof. For each $\varphi\in\Gamma_\varphi$, let

$$\Sigma_\varphi=\Gamma_\varphi^{\mathrm{Aut}_{\mathscr{E}}(\varphi)}.$$

I must show that Σ_φ and Λ_φ have the same field of quotients up to purely inseparable extension. Let $\upsilon_\varphi\in\Lambda$ be the element constructed in Proposition 6.1; I will show that

$$(\upsilon_\varphi\Sigma_\varphi)^{p^s}\subseteq\Lambda_\varphi\quad\text{for some } s\geq 0.$$

6.3. Lemma. *Let* $\theta,\varphi\in\mathscr{E}$, *and let* $x\in\upsilon_\varphi\Sigma_\varphi$. *Then for some* $s\geq 0$, *there exists* $y\in\Sigma_\theta$ *such that:*

(1) *For all* $f:\theta\to\varphi\in\mathscr{E}$, $\Gamma f(y)=x^{p^s}$.

(2) *If* $g:\theta\to\pi\in\mathscr{E}$, *then* $\Gamma g(y)=0$ *unless there exists* $\pi\to\varphi\in\mathscr{E}$.

(3) *If* $g:\theta\to\pi\in\mathscr{E}$, *then* $\Gamma g(y)\in\Sigma_\pi$.

Proof. Let $\mathscr{E}_\theta$ be the full subcategory of $\mathscr{E}$ such that π is an object of $\mathscr{E}_\theta$ if and only if there exists a map $\theta \to \pi$ in $\mathscr{E}$. The lemma is non-trivial only when $\varphi \in \mathscr{E}_\theta$. Consider the category $\mathscr{G}_\theta$ constructed as follows. Let the objects of $\mathscr{G}_\theta$ be the prime $\mathscr{B}$-ideals of Γ_θ. If P and Q are objects of $\mathscr{G}_\theta$, let the morphisms from P to Q in $\mathscr{G}_\theta$ be the $\mathscr{B}$-morphisms $\Gamma_\theta/P \to \Gamma_\theta/Q$. If $g:\Gamma_\theta \xrightarrow{\sim} \Gamma_\theta$ is an automorphism such that $g(P)\subseteq Q$, then g induces a morphism $g(P,Q):\Gamma_\theta/P\to\Gamma_\theta/Q$; every morphism of $\mathscr{G}_\theta$ arises in this way. The conditions 2.3(3), 2.3(4), and 2.3(5) mean precisely that we may assume $\mathscr{E}_\theta$ to be a subcategory of $\mathscr{G}_\theta$ that has the same objects as $\mathscr{G}_\theta$ and that has this additional property: if P, Q, and R are prime β-ideals of Γ_θ and if f and g are automorphisms of Γ_θ such that $f(P)\subseteq Q$ and $g(P)\subseteq R$, then $f(P,Q), g(P,R)\in \mathscr{E}_\theta \Rightarrow g\circ f^{-1}(Q,R)\in \mathscr{E}_\theta$. For convenience, we may further assume that each quotient map $\Gamma_\theta/P\to\Gamma_\theta/Q$ is a morphism in $\mathscr{E}_\theta$ whenever $P\subseteq Q$. This is equivalent to picking a preferred map $\theta\to\pi$ for each object π of $\mathscr{E}_\theta$ and identifying π with the kernel of $\Gamma_\theta\to\Gamma_\pi$ and Γ_π with Γ_θ/π; in particular, θ is identified with the zero ideal.

As in the proof of the previous proposition, for $\pi\in\mathscr{E}_\theta$, let

$$S_\pi=\{\eta\subseteq\Gamma_\theta \mid \pi\subseteq\eta \text{ and } \eta\simeq\varphi \text{ in } \mathscr{E}_\theta\}.$$

Let G be the groupoid that has as objects the elements of S_θ and as maps between objects η_0,η_1 all automorphisms g of Γ_θ such that $g(\eta_0)=\eta_1$ and $g(\eta_0,\eta_1)\in\mathscr{E}_\theta$. For each $\eta\in S_\theta$, let $G_\eta=\mathrm{Aut}_G(\eta)$. Then reduction modulo η induces an epimorphism $G_\eta\to\mathrm{Aut}_{\mathscr{E}}(\eta)$, for $\mathrm{Aut}_{\mathscr{E}}(\eta)$ is a subgroup of $\mathrm{Aut}(\Gamma_\eta)$ and $\Gamma_\eta=\Gamma_\theta/\eta$. Let $\Phi_\eta=\Gamma_\theta^{G_\eta}$. If $g:\pi\to\eta$ is a map in G, then g restricts to an isomorphism of Φ_π onto Φ_η, which does not depend on the choice of $g:\pi\to\eta$. Furthermore, all the diagrams

$$\begin{array}{ccc} \Phi_\pi & \xrightarrow[g]{\sim} & \Phi_\eta \\ \downarrow & & \downarrow \\ \Sigma_\pi & \xrightarrow[g(\pi,\eta)]{\sim} & \Sigma_\eta \end{array}$$

commute, where the vertical maps are induced by any maps $\theta\to\pi$ and $\theta\to\eta$ in $\mathscr{E}_\theta$. By 4.7 and 4.8, Σ_η is a purely inseparable extension of $\Phi_\eta/(\Phi_\eta\cap\eta)$.

Let $x\in v_\varphi\Sigma_\varphi$; then $x=v_\varphi x_0$, $x_0\in\Sigma_\varphi$. Choose $s\geq\mathrm{rank}(\Gamma_\theta)-\mathrm{rank}(\Gamma_\varphi)$ and $y_0\in\Phi_\varphi$ such that y_0 reduces to $x_0^{p^s}$ in Γ_φ. There is a power q of $q_{\theta,\varphi}$ such that qy_0 reduces to x^{p^s} in Γ_φ. Put $y_\varphi=qy_0$. For each $\eta\in S_\theta$, let $y_\eta=g(y_\varphi)$ where $g:\varphi\to\eta$ is a map in G; y_η is independent of the choice of g. For any maps $\eta\to\varphi$ and $\theta\to\eta$ in $\mathscr{E}_\theta$, the composition $\Gamma_\theta\to\Gamma_\eta\xrightarrow{\sim}\Gamma_\varphi$ sends y_η to x^{p^s}; furthermore if π is a prime $\mathscr{B}$-ideal of Γ_φ, then $y_\eta\equiv 0 \pmod{\pi}$ unless $\pi\subseteq\eta$. Put

$$y=\sum y_\eta,\quad \eta\in S_\theta.$$

Then, as in the previous proposition, for any $\theta\to\varphi\in\mathscr{E}_\theta$, $\Gamma_\theta\to\Gamma_\varphi$ sends y to x^{p^s}, and for any $\theta\to\pi$ in $\mathscr{E}_\theta, \Gamma_\theta\to\Gamma_\pi$ sends y to zero unless there exists $\pi\to\varphi$ in $\mathscr{E}_\theta$.

Finally, let $f:\theta\to\pi\in\mathscr{E}_\theta$; to prove: $f(y)\in\Sigma_\pi$. Conjugating by an automorphism of π in $\mathscr{E}_\theta$, we may suppose f is the quotient morphism $\Gamma_\theta\to\Gamma_\theta/\pi$. Note that $S_\pi\subseteq S_\theta$

and that the ideals $\eta/\pi \subseteq \Gamma_\pi$ for $\eta \in S_\pi$ are precisely the ideals that arise as kernels of morphisms $\pi \to \varphi$ in $\mathscr{E}_\theta$; therefore, $\mathrm{Aut}_{\mathscr{E}}(\pi)$ acts as a group of automorphisms of S_π. Let $\bar{g} \in \mathrm{Aut}_{\mathscr{E}}(\pi)$. If $\eta \in S_\theta - S_\pi$, then $f(y_\eta) = 0$, and $\bar{g}f(y_\eta) = f(y_\eta)$. Let $\eta \in S_\pi$. There exists $g \in \mathrm{Aut}(\Gamma_\theta)$ such that $g(\pi) = \pi$ and $g(\pi, \pi) = \bar{g}$. Then $g : \eta \to \bar{g}\eta$ in G. Therefore, $g(y_\eta) = y_{\bar{g}\eta}$, and $\bar{g}f(y_\eta) = f(y_{\bar{g}\eta})$. It follows that $\bar{g}f(y) = f(y)$. This proves the lemma.

To complete the proof of the proposition, note that if $\mathscr{E}$ has an initial object the proposition follows immediately from the lemma. Otherwise, induct on the number of isomorphism classes of minimal objects in $\mathscr{E}$. The details are left to the reader. The key ingredients are the above lemma and this fact: if $\pi \in \mathscr{E}$ and $x, y \in \Sigma_\pi$, then $(x - y) \in \upsilon_\pi \Sigma_\pi$ iff $\Gamma f(x) = \Gamma f(y)$ for all $f : \pi \to \eta$ in $\mathscr{E}$ such that f is not an equivalence.

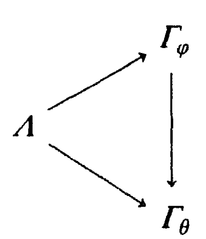
Proof of Theorems 1.6 and 2.6. Let $\mathscr{E}$ be a category and Γ a functor that satisfy 2.3(1) to 2.3(5); let $\Lambda = \varprojlim \Gamma_\varphi$, $\varphi \in \mathscr{E}$. We may suppose that $\mathscr{E}$ is a finite category. To prove: $\mathscr{H} : \mathscr{E} \to \mathscr{E}(\Lambda)$ is an equivalence of categories.

First, I claim that every isomorphism class of $\mathscr{E}(\Lambda)$ contains an object of the form $\Lambda \to \Gamma_\varphi$, $\varphi \in \mathscr{E}$. To see this, let $\theta : \Lambda \to \Gamma_\theta$ be an object of $\mathscr{E}(\Lambda)$, and let $P_\theta = \mathrm{Ker}(\theta)$. As in the proof of 2.5, let $\Pi = \prod \Gamma_\varphi$, $\varphi \in \mathscr{E}$; then $\Lambda \subseteq \Pi$, and Π is a finite Λ-module. By the going-up theorem, there is a prime $\mathscr{B}$-ideal Q of Π such that $P_\theta = Q \cap \Lambda$. Now, every prime $\mathscr{B}$-ideal of Π has the following form: let $\varphi \in \mathscr{E}$ and let P be a prime $\mathscr{B}$-ideal of Γ_φ; then the inverse image of P by the projection $\Pi \to \Gamma_\varphi$ is a prime $\mathscr{B}$-ideal

$$Q(\varphi, P) = \prod_{\pi \neq \varphi} \Gamma_\pi \times P$$

of Π. Thus, there exists $\varphi \in \mathscr{E}$ and $P \subseteq \Gamma_\varphi$ such that $Q = Q(\varphi, P)$. By 2.3(4), there exists $\varphi \to \pi \in \mathscr{E}$ such that $P = \mathrm{Ker}(\Gamma_\varphi \to \Gamma_\pi)$; then $P_\theta = \mathrm{Ker}(\Lambda \to \Gamma_\pi)$. Thus, $\mathscr{H}\pi \simeq \theta$.

Second, let φ and θ be objects of $\mathscr{E}$, and suppose there exists a map $\mathscr{H}\varphi \to \mathscr{H}\theta$ in $\mathscr{E}(V)$; I claim that then there exists a map $\varphi \to \theta$ in $\mathscr{E}$. For a map $\mathscr{H}\varphi \to \mathscr{H}\theta$ is a commutative diagram



Let $\upsilon_\theta \in \Lambda$ be the element constructed in Proposition 6.1. Then υ_θ does not reduce to zero in Γ_φ; therefore, there exists $\varphi \to \theta \in \mathscr{E}$.

Finally, if $\varphi \rightrightarrows \theta$ are two morphisms of $\mathscr{E}$ or $\mathscr{E}(\Lambda)$, then 2.3(3) guarantees the existence of a commutative diagram

$$\begin{array}{ccc} & & \theta \\ & \nearrow & \big\downarrow \wr \\ \varphi & & \\ & \searrow & \\ & & \theta \end{array}$$

in the appropriate category. Thus, to complete the proof we need only show that

$$\mathrm{Aut}_{\mathscr{C}}(\varphi) = \mathrm{Aut}_{\mathscr{C}(\Lambda)}(\mathscr{H}\varphi)$$

for each $\varphi \in \mathscr{C}$; but this is Proposition 6.2.

7. Examples

The example which motivated the foregoing research is the exceptional Lie group F_4. Let $\Lambda = H^*(BF_4;\ \mathbb{F}_3)/\sqrt{0}$.

7.1. Theorem (Toda [15]). *Λ is generated by elements $x_4, x_8, x_{20}, x_{26}, x_{36}, x_{48}$, where $x_i \in \Lambda^{2i}$, and is subject to the relations*

$$x_4x_{26} = 0, \qquad x_8x_{26} = 0, \qquad x_{20}x_{26} = 0,$$

$$\text{(R)} \qquad x_{20}^3 = x_{48}x_4^3 + x_{36}x_8^3 - x_{20}^2x_8^2x_4.$$

Furthermore

$$\mathbb{F}_3[x_4, x_8, x_{20}, x_{36}, x_{48}]/R = H^*(BT;\ \mathbb{F}_3)^W,$$

where T is the maximal torus and W the Weyl group of F_4.

7.2. Corollary.

$$\Lambda = \mathbb{F}_3[x_{26}, x_{36}, x_{48}] \prod_{\mathbb{F}_3[x_{36}, x_{48}]} \mathbb{F}_3[x_4, x_8, x_{20}, x_{36}, x_{48}]/R.$$

7.3. Theorem (Toda [15]). *In $\mathbb{F}_3[x_{26}, x_{36}, x_{48}]$, the reduced power operations are determined by*

$$P^1(x_{26}) = 0, \qquad P^1(x_{36}) = 0, \qquad P^1(x_{48}) = x_{36}^2,$$

$$P^3(x_{26}) = 0, \qquad P^3(x_{36}) = x_{48}, \qquad P^3(x_{48}) = 0,$$

$$P^9(x_{26}) = x_{26}x_{36}, \quad P^9(x_{36}) = -x_{36}^2, \quad P^9(x_{48}) = -x_{36}x_{48}.$$

Let $E_3 \subseteq F_4$ be a maximal elementary abelian 3-group of rank three corresponding to the factor $\mathbb{F}_3[x_{26}, x_{36}, x_{48}]$ in 7.2. Then we may assume that $E_3 \cap T$ is an elementary abelian 3-group of rank two; denote it by E_2. Let $\Gamma_3 = H^*(E_3;\ \mathbb{F}_3)/\sqrt{0}$, $\Gamma_2 = H^*(E_2;\ \mathbb{F}_3)/\sqrt{0}$, and $\Gamma_4 = H^*(BT;\ \mathbb{F}_3)$. By comparing the formulas of 7.3 with 5.3 we prove:

7.4. Proposition. *Under the map $\Lambda \to \Gamma_3$, x_{48} reduces to $q_{3,1}$, x_{36} reduces to $q_{3,2}$ and x_{26} reduces to a non-zero multiple of L_3. Thus, $W(E_3) = \mathrm{Sl}(3, \mathbb{F}_3)$.*

J.F. Adams has confirmed this proposition by direct calculation in F_4 (private communication).

Similarly, observe that in $\mathbb{F}_3[x_{36}, x_{48}]$, the derivations $Q^1, Q^2, \ldots$ are all zero. Thus in Γ_2, the reductions of x_{36} and x_{48} have (unique) cube roots y_{12} and y_{16} [2; Theorem 1.2]. Furthermore,

$$P^1(y_{12}) = y_{16}, \qquad P^1(y_{16}) = 0,$$

$$P^3(y_{12}) = -y_{12}^2, \quad P^3(y_{16}) = -y_{12}y_{16}.$$

Thus $y_{12} = q_{2,1}$, $y_{16} = q_{2,0}$.

7.5. Proposition. *Under the map $\Lambda \to \Gamma_2$, x_{36} reduces to $(q_{2,1})^3$ and x_{48} reduces to $(q_{2,0})^3$. Thus, $W(\Gamma_2) = \mathrm{Gl}(2, \mathbb{F}_3)$.*

I conclude with an example illustrating Theorem 4.8. It is also an example of a Noetherian $\mathscr{B}$-algebra that is not integrally closed.

7.5. Example. Let

$$p = 5, \quad \Gamma = \mathbb{F}_5[x, u, v], \quad \Lambda = \mathbb{F}_5[x, u^2 + v^2, u^2v^2].$$

Then $\Lambda = H^*(BS^1 \times BSp(2); \mathbb{F}_5)$. Map Γ to $\bar{\Gamma} = \mathbb{F}_5[x, y]$ via $x \to x$, $u \to 3(x+y)$, $v \to 4(x-y)$. Then the image of this map is $\bar{\Lambda} = \mathbb{F}_5[x, xy, y^4]$; $\bar{\Lambda}$ is not integrally closed, for $y = (xy)/x$ is integral over $\bar{\Lambda}$. Thus, $\mathrm{Gal}(\bar{\Gamma}/\bar{\Lambda}) = \{1\}$. Map $\bar{\Gamma}$ to $\mathbb{F}_5[y]$ via $x \to 0$.

The image of $\bar{\Lambda}$ in $\mathbb{F}_5[y]$ is $\mathbb{F}_5/[y^4]$; $\mathrm{Gal}(\mathbb{F}_5[y]/\mathbb{F}_5[y^4]) = \mathbb{Z}/4$ generated by $y \to 3y$. $\mathrm{Gal}(\Gamma/\Lambda) = W(S^1 \times \mathrm{Sp}(2))$ is generated by transpositions $u \leftrightarrow -u$, $v \leftrightarrow -v$, and $u \leftrightarrow v$; it is a semi-direct product $(\mathbb{Z}/2 \times \mathbb{Z}/2) \rtimes \mathbb{Z}/2$. $Q = \mathrm{Ker}(\Gamma \to \mathbb{F}_5[y])$ is generated by x and $(3v - u)$; $Q \cap \Lambda$ is generated by x and $u^2 + v^2$. The decomposition group of Q is a $\mathbb{Z}/4$ generated by

$$u \to -v, \qquad v \to u.$$

This transformation maps to $y \to 3y \pmod{Q}$.

References

[1] S.P. Lam, Unstable algebras over the Steenrod algebra, Proc. Aarhus Topology Conference (1982), to appear.

[2] J.F. Adams and C.W. Wilkerson, Finite H-spaces and algebras over the Steenrod algebra, Annals of math. 111 (1980) 95–143.

[3] A. Borel, Sous-groupes commutatifs et torsion des groups de Lie compacts connexes, Tohoku Math. J. (2) 13 (1961) 216–240.

[4] A. Borel, Sur la cohomologie des espaces fibres principaux et des espaces homogenes de groupes de Lie compacts, Annals of math. 57 (1953) 115-206.
[5] N. Bourbaki, Commutative Algebra (Addison-Wesley, Reading, MA, 1972).
[6] N. Bourbaki, Groupes et Algèbres de Lie (Hermann, Paris, 1968).
[7] A. Clark and J. Ewing, The realization of polynomial algebras as cohomology rings, Pacific J. Math. 50 (1974) 425–434.
[8] L.E. Dickson, A fundamental system of invariants of the general modular linear group with a solution of the form problem, Trans. AMS 12 (1911) 75–98.
[9] P.S. Landweber, Associated prime ideals and Hopf algebras, J. Pure Appl. Algebra 3 (1973) 43–58.
[10] S. Lang, Algebra (Addison-Wesley, Reading, MA, 1965).
[11] B.M. Mann and R.J. Milgram, On the Chern classes of the regular representations of some finite groups, Proc. Edinburgh Math. Soc., to appear.
[12] D. Quillen, The spectrum of an equivariant cohomology ring: I, II, Annals of Math. 94 (1971) 549–572, 573–602.
[13] J.P. Serre, Algèbre Locale - Multiplicités, Lecture Notes in Math. 11 (Springer, Berlin, 1965).
[14] J.P. Serre, Sur la dimension cohomologique des groupes profinis, Topology 3 (1965) 413–420.
[15] H. Toda, Cohomology mod 3 of the classifying space BF_4 of the exceptional group F_4, J. Math. Kyoto Univ. 13-1 (1973) 97–115.
[16] W.C. Waterhouse, Notes toward higher differential algebra, J. Pure Appl. Algebra 7 (1976) 121–132.
[17] C.W. Wilkerson, Classifying spaces, Steenrod operations and algebraic closure, Topology 16 (1977) 227–237.
[18] C.W. Wilkerson, A primer on the Dickson invariants, Proc. Northwestern Homotopy Theory Conference, Contemporary Mathematics 18 (Amer. Math. Soc., Providence, RI) 421–434.