TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 341, Number 1, January 1994

# SUBGROUP RIGIDITY IN FINITE DIMENSIONAL GROUP ALGEBRAS OVER $p$-GROUPS

GARY THOMPSON

ABSTRACT. In 1986, Roggenkamp and Scott proved in [RS1]

**Theorem 1.1.** *Let $G$ be a finite $p$-group for some prime $p$, and $S$ a local or semilocal Dedekind domain of characteristic* 0 *with a unique maximal ideal containing $p$ (for example, $S = \mathbb{Z}_p$ where $\mathbb{Z}_p$ is the $p$-adic integers). If $H$ is a subgroup of the normalized units of $SG$ with $|H| = |G|$, then $H$ is conjugate to $G$ by an inner automorphism of $SG$.*

In the Appendix of a later paper [S], Scott outlined a possible proof of a related result:

**Theorem 1.3.** *Let $S$ be a complete, discrete valuation domain of characteristic* 0 *having maximal ideal $\wp$ and residue field $F \cong S/\wp$ of characteristic $p$. Let $G$ be a finite $p$-group, and let $U$ be a finite group of normalized units in $SG$. Then there is a unit $w$ in $SG$ such that $wUw^{-1} \leq G$.*

The author later filled in that outline to give a complete proof of Theorem 1.3 and, at the urging of Scott, has been able to extend that result to

**Theorem 1.2.** *Let $S$ be a complete, discrete valuation ring of characteristic* 0 *having maximal ideal $\wp$ containing $p$. Let $A$ be a local $S$-algebra that is finitely generated as an $S$-module, and let $G$ be a finite $p$-group. Then any finite, normalized subgroup of the $S$-algebra $\mathscr{A} = A \otimes_S SG$ is conjugate to a subgroup of $G$.*

## 1. INTRODUCTION

The isomorphism problem for group rings was first posed in 1940 by Graham Higman who asked, "For finite groups $G$ and $H$, does $\mathbb{Z}G \simeq \mathbb{Z}H \Rightarrow G \simeq H$?" Dade [D] found counterexamples to the analogous question for $\mathscr{F}G \simeq \mathscr{F}H$ where $\mathscr{F}$ represented the family of all fields (i.e., $FG \simeq FH$ for any field $F$). Significant positive results have been achieved by Higman [H] in 1940 for abelian groups over $\mathbb{Z}$, Whitcomb [Wh] in 1968 for metabelian groups over $\mathbb{Z}$, and Roggenkamp and Scott [RS2] in 1986 for abelian by nilpotent groups over $\mathbb{Z}$. Roggenkamp and Scott also proved the following result in [RS2]:

**Theorem 1.1.** *Let $G$ be a finite $p$-group for some prime $p$, and $S$ a local or semilocal Dedekind domain of characteristic* 0 *with a unique maximal ideal*

Received by the editors November 29, 1990 and, in revised form, November 4, 1991.
1991 *Mathematics Subject Classification.* Primary 16A26; Secondary 16A10, 20C05, 20C10, 20C11.

*containing $p$ (for example, $S = \mathbb{Z}_p$ where $\mathbb{Z}_p$ is the $p$-adic integers). If $H$ is a subgroup of the normalized units of $SG$ with $|H| = |G|$, then $H$ is conjugate to $G$ by an inner automorphism of $SG$.*

This result provides a partial answer to a conjecture of Zassenhaus that runs as follows: Let $G$ be a finite group and $H$ a finite subgroup of the units of $\mathbb{Z}G$ of augmentation 1. If $|H| = |G|$ then there exists a unit $u$ in $\mathbb{Q}G$ such that $uHu^{-1} = G$. Obviously any positive result for the Zassenhaus conjecture for a class of finite groups provides a positive result for the isomorphism problem. It is important to note, however, that Roggenkamp and Scott have recently come up with a metabelian group $G$ for which the isomorphism problem holds true and that provides a counterexample to the Zassenhaus conjecture [RS3].

The main result in this paper is, in a sense, a version of the Zassenhaus conjecture.

**Theorem 1.2.** *Let $S$ be a complete, discrete valuation ring of characteristic $0$ having maximal ideal $\wp$ containing $p$. Let $A$ be a local $S$-algebra that is finitely generated as an $S$-module, and let $G$ be a finite $p$-group. Then any finite, normalized subgroup of the $S$-algebra $\mathscr{A} = A \otimes_S SG$ is conjugate to a subgroup of $G$. (Note that $\mathscr{A} \simeq AG$.)*

By letting $A = S$, one easily obtains

**Theorem 1.3.** *Let $S$ be a complete, discrete valuation domain of characteristic $0$ having maximal ideal $\wp$ and residue field $F \cong S/\wp$ of characteristic $p$. Let $G$ be a finite $p$-group, and let $U$ be a finite group of normalized units in $SG$. Then there is a unit $w$ in $SG$ such that $wUw^{-1} \leq G$.*

Combining Theorem 1.3 with Theorem 1.1, we immediately get the following corollary, the first part of which is even equivalent to Theorem 1.3.

**Corollary 1.4.** (1) *Any finite group of normalized units in $SG$ can be embedded in a finite normalized group basis of $SG$.*

(2) *Any normalized torsion unit in $SG$ can be embedded in a finite group basis of $SG$.*

Roggenkamp and Scott proved the $S = \mathbb{Z}_p$ version of Theorem 1.3 for $p = 2$ in 1986 [RS1, R1]. Scott, working in the spirit of [RS2], also proved in the Appendix of [S] the same version for groups of order $p^3$ in the case where $s^p = 1$, where $s \in G$ is a particular group element that will be introduced in §4. In that same Appendix he also suggested an inductive argument for the general $p^n$ case. Finally, Weiss [W] established the $S = \mathbb{Z}_p$ version for any finite $p$-group $G$. The results obtained by Weiss, as well as by Roggenkamp and Scott, generalized without comment to unramified extensions of $\mathbb{Z}_p$. Weiss was able to prove his version of Theorem 1.3 by first establishing the following result about permutation modules and generalized permutation lattices:

**Theorem 1.5.** *Let $\zeta$ be a primitive $p$th root of unity, set $\pi = 1 - \zeta$, and set $R = \mathbb{Z}_p[\zeta]$. Let $M$ be an $R$-representation of the finite $p$-group $G$ so that $\overline{M} = M/\pi M$ is a permutation $\mathbb{F}_p$-module of $G$. Then $M$ is a generalized permutation lattice for $G$.*

In the spring of 1989, Roggenkamp generalized the above result to obtain a proof of Theorem 1.3. His generalized version of Theorem 1.5 runs as follows:

**Theorem 1.6.** *Let $R$ be a complete Dedekind domain of finite rank of characteristic zero with residue field $\mathbb{F}$ of characteristic $p > 0$, and let $\pi$ be a parameter of $R$; i.e.* $\operatorname{rad} R = \pi R$. *For an $R$-module $M$, and for some fixed natural number $t$, define $R^{\sim}$ to be $R/\pi^t R$, and define $M^{\sim}$ to be $M/\pi^t M$.*

(1) *Assume that $R$ either does not contain a primitive $p$th root of unity, or if it contains a primitive $p$th root of unity $\zeta$ then $\pi^t R \subset (1-\zeta)R$. Then an $RG$-lattice $M$ is a generalized permutation module if and only if $M^{\sim}$—note that we are always assuming that the various $U$-actions on $R^{\sim}$ are induced from the $U$-actions on $R$ where $U \leq G$—is one.*

(2) *If $\pi^t R \not\subseteq (1-\zeta)R$, then there is an $RG$-lattice $M$ that is no: a generalized permutation module, but $M^{\sim}$ is a generalized permutation module.*

Roggenkamp's independent work was done at about the same time the author independently established Theorem 1.3 for his Doctoral dissertation. Our approach, however, gives a more constructive, or at least algorithmic, approach to the problem, and it has been possible to apply the ideas and arguments found in the dissertation to a more general setting. Subsequent investigations and discussions with Leonard Scott finally led to the formulation and proof of Theorem 1.2. The ideas and results found in §3 are closely related to the results and ideas found in [RS2]. The reduction in §4 is an adaptation of the argument found in the Appendix of [S]. The difficult arguments in §5 provide the key results needed to modify the sketch contained in the Appendix of [S] into a complete argument, while removing any restrictions on $s^p$. Finally, §6 discusses three possible generalizations/applications of the first five chapters. First, an improvement to the conclusion of Proposition 5.2 is hinted at. Then some possible applications of the techniques of §§2 through 6 to nontorsion units in group rings over groups of order $p^3$ are mentioned. Last of all, there is a comment on the possibility of proving Theorem 1.2 using a more general domain $S$.

Before we begin, several definitions and notational conventions need to be made. First of all, we shall frequently refer to the set of elements $\{1 \otimes g\}$ in $\mathscr{A}$ as $G$. It should be clear from the context when we are referring to the group $G$ and when we are referring to $G \subseteq \mathscr{A}^*$. We shall also do this when discussing subgroups of $G$ (such as $H$) or elements of $G$ (such as $t$). Let $\{y_i\}$ be a basis for $A$ over $S$, where $y_1 = 1$. If $\{g_j\}$ comprise the elements of $G$, then the set $\{y_i \otimes g_j\}$ is a basis for $\mathscr{A}$ over $S$. Define the augmentation map $\varepsilon\colon \mathscr{A} \to A$ by $\sum_{i,j} s_{i,j}(y_i \otimes g_j) \mapsto \sum_{i,j} s_{i,j} y_i$. Define an element $x \in \mathscr{A}$ to be *normalized* if $x$ has augmentation 1. Finally, given the unit $u \in \mathscr{A}$ and the element $x \in \mathscr{A}$, ${}^u x$ is understood to represent $uxu^{-1}$.

## 2. Preliminaries

Given a discrete valuation domain $S$, a finite $p$-group $G$, and a local, $S$-algebra $A$ that is finitely generated as an $S$-module as described in the introduction, we wish to show that any finite group of normalized units $U$ in the tensor algebra $\mathscr{A} = A \otimes_S SG$ is conjugate by a unit in $\mathscr{A}$ to some subgroup $H$ of $G$. We already know by [RS2] that this is true in the case $A = S$ and $|U| = |G|$. A key idea in that proof was to take some subgroup $\Omega$ of $U \cap G$ and to expand $\Omega$ via conjugation arguments. The same idea will work in the present setting, too. Accordingly, define $\Omega$ to be some subgroup of $U \cap G$ such that $\Omega \trianglelefteq U$ and $\Omega \trianglelefteq G$.

For any commutative ring $R$, and any group $G$ with normal subgroup $N \trianglelefteq G$, define $I(RN)$, or $I(N)$, to be the ideal in $RG$ generated by $\{n-1 \colon n \in N\}$. It is well known that the kernel of $RG \to R(G/N)$ is $I(N)$. Moreover, if $R$ is a local ring with $p \in \operatorname{rad} R$ and $G$ is a $p$-group, then $RG$ itself is a local ring with maximal ideal $\wp RG + I(G) = \operatorname{rad} RG$, and $\operatorname{rad} RG$ is nilpotent modulo $\wp RG$. Note that since $RG$ is a local ring, only units map to units in the map $RG \to R(G/N)$. Finally, we have the following lemma about radicals of subalgebras:

**Lemma 2.1.** (1) *Let $R$ be a commutative ring, $A$ an $R$-algebra that is finitely generated as an $R$-module, and $B$ an $R$-subalgebra of $A$. Then $B \cap \operatorname{rad} A \subseteq \operatorname{rad} B$.*

(2) *Conversely, suppose $R$ is a commutative local ring with maximal ideal $\wp$. Let $A$ be an $R$-algebra such that $\wp A \subseteq \operatorname{rad} A$, and let $B$ be an $R$-subalgebra of $A$ which is finitely generated as an $R$-module. Then $\operatorname{rad} B \subseteq \operatorname{rad} A$.*

*Proof.* (1) Let $x \in B \cap \operatorname{rad} A$. It suffices to show that $1+x$ is invertible in $B$. Since $x \in \operatorname{rad} A$, $1+x$ is certainly invertible in $A$. Consider now the following diagram where $f$ and $g$ are multiplication by $1+x$ and $h$ is multiplication by $\overline{1+x}$.

$$\begin{tikzcd}
0 \arrow[r] & B \arrow[r] \arrow[d, "f"] & A \arrow[r] \arrow[d, "g"] & A/B \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & B \arrow[r] & A \arrow[r] & A/B \arrow[r] & 0
\end{tikzcd}$$

By the Snake Lemma, $\ker h \simeq \operatorname{coker} f$. However, $A/B$ is a finitely generated $R$-module, and in such modules an epic endomorphism is an isomorphism (see Theorem 2.4 of [M]). Thus $\ker h = 0 = \operatorname{coker} f$, and so $f$ is onto. Hence $1+x$ is invertible in $B$.

(2) The proof of part (2) follows instantly from Proposition 5.22 of [CR2]: Let $R$ be a commutative local ring with maximum ideal $\wp$. Let $B$ be an $R$-algebra that is finitely generated as an $R$-module. Then $\wp B \subseteq \operatorname{rad} B$, and there is some positive integer $k$ such that $(\operatorname{rad} B)^k \subseteq \wp B$. □

Returning to our tensor algebra $\mathscr{A}$, let us first note by 5.22 of [CR2] that $\wp\mathscr{A} \subseteq \operatorname{rad}\mathscr{A}$ and that $\operatorname{rad}\mathscr{A}$ is nilpotent module $\wp\mathscr{A}$. Using the fact that any ideal that is nilpotent modulo the radical must be contained in the radical, it is easy to show that $J = \operatorname{rad} A \otimes_S SG + A \otimes_S \operatorname{rad} SG \subseteq \operatorname{rad}\mathscr{A}$. Since $\mathscr{A}/J \simeq A/\operatorname{rad} A$, which is some division ring $\mathscr{D}$, $\mathscr{A}$ itself must be a local ring with radical $J$. Since $A$ is a local ring, the basis $\{y_i\}$ for $A$ over $S$ may be chosen so that each $y_i \equiv 1$ modulo $\operatorname{rad} A$. Hence each $y_i \otimes g_j \equiv 1$ modulo $\operatorname{rad}\mathscr{A}$ since the augmentation map $\varepsilon$ maps units to units and radicals to radicals. Let $|G| = p^\nu$. If $\nu = 0$ then $U = 1 \otimes e$ where $e$ is the identity of the group $G$ and the theorem is true. Proceed now by induction on $\nu$. Since $U \cdot Z(G)$ is still a finite group of normalized units, we may assume without loss of generality that $Z(G) \subseteq U \cap \Omega$. The strategy is to enlarge $\Omega$. First of all, choose an element $c \in Z(G)$ such that $c^p = 1$, and let $C = \langle c \rangle$. By the comments above, $\mathscr{A}/(c-1)\mathscr{A} \simeq A \otimes_S S(G/C)$. According to the induction hypothesis, for some unit $z \in \mathscr{A}$ there is a subgroup $H$ of $G$ such that $H \equiv {}^zU$ modulo $(c-1)\mathscr{A}$. We require that $\Omega$ be centralized by $z$. Now select some $t \in H \backslash \Omega$ such that $t^p \in \Omega$ and $\bar{t} \in Z(H/\Omega)$. The idea is to replace $\Omega$ with $\langle \Omega, t \rangle$. Note that

$(c-1)^p \equiv 0 \pmod{p}$. Hence some sort of argument based on completeness seems feasible. One potential difficulty is the fact that $c-1$ is a zero divisor. Much of the following argument does not require that $c-1$ not be a zero divisor. Ultimately, however, it does become a problem. The solution is to introduce $\Lambda = \mathscr{A}/\underline{c}\mathscr{A}$ where $\underline{c} = 1 + c + \cdots + c^{p-1}$. Now $\pi$, the image of $c-1$, is no longer a zero divisor, $\Lambda$ is still a local ring, and $\operatorname{rad}\mathscr{A} \twoheadrightarrow \operatorname{rad}\Lambda$. If we let $\zeta$ be the image of $c$ and $R = S[\zeta]$, then $\pi^{p-1} = wp$ for some unit $w \equiv -1 \pmod{\pi R}$. An important question now is, "Does conjugation carry over from $\Lambda$ to $\mathscr{A}$ in a reasonable manner?" The answer is fortunately yes and can be found in the following three results, which are generalizations of Lemma 2.4, Corollary 2.4.1, and Proposition 2.5 in [RS2].

**Lemma 2.2.** *There is a pullback diagram*

$$\begin{tikzcd}
\mathscr{A} \arrow[r] \arrow[d] & \Lambda \arrow[d] \\
\mathscr{A}/(c-1)\mathscr{A} \arrow[r] & \Lambda/\pi\Lambda
\end{tikzcd}$$

*Moreover,* $\Lambda/\pi\Lambda \simeq A \otimes_S k(G/C)$ *where* $k = S/pS$.

**Corollary 2.3.** *The group* $G$ *maps bijectively onto its image in the units of* $\Lambda$.

**Proposition 2.4.** *Let* $\Lambda_H$ *be the image of* $SH$ *in* $\Lambda$. *Then every* $R$*-linear monomorphism* $\alpha$ *of* $\Lambda_H$ *into the order* $\Lambda$ *which is the identity modulo* $\pi\Lambda$ *comes from a unique* $S$*-monomorphism of* $SH$ *into* $\mathscr{A}$ (*denoted also by* $\alpha$) *which fixes* $C$ *pointwise and induces the identity on* $S(H/C)$ (*hence automatically preserves augmentation*). *Conversely, any such monomorphism* $\alpha$ *of* $SH$ *into* $\mathscr{A}$ *induces an* $R$*-monomorphism of* $\Lambda_H$ *into* $\Lambda$ *which is the identity modulo* $\pi\Lambda$. *Moreover,*

(a) $\alpha$ *is induced by an inner automorphism of* $\mathscr{A}$ *if and only if* $\alpha$ *is induced by an inner automorphism of* $\Lambda$.

(b) $\alpha$ *stabilizes* $H \subseteq SH$ (*that is,* $\alpha$ *is induced by a group automorphism of* $H$) *if and only if* $\alpha$ *stabilizes* $H \subseteq \Lambda_H$.

(c) *In fact,* $\alpha$ *stabilizes setwise* (*or pointwise*) *any given subset of* $H \subseteq SH$ *if and only if* $\alpha$ *stabilizes setwise* (*or pointwise*) *the corresponding subset of* $H \subseteq \Lambda_H$.

Let $U$ now also represent the image of ${}^zU$ in $\Lambda$. Then the congruence $H \equiv {}^zU \pmod{(c-1)\mathscr{A}}$ translates to $H \equiv U \pmod{\pi\Lambda}$. Use this congruence to choose $u \in U$ such that $t \equiv u \pmod{\pi\Lambda}$ and define a function $\gamma\colon H \to \Lambda$ by $(1+\pi\gamma(g))g \leftrightarrow g$. It is easy to see that $\gamma(gh) = \gamma(g) + {}^g\gamma(h) + \pi\gamma(g){}^g\gamma(h)$ and that $\gamma|_\Omega = 0$. Thus $\gamma$ is an additive cocycle modulo $\pi\Lambda$ that is trivial on the subgroup $\Omega$. Moreover, the image of $\gamma$ lies in $\Lambda^\Omega$, the fixed points of $\Lambda$ under conjugation by elements of $\Omega$, and these fixed points are precisely the image of $\mathscr{A}^\Omega$ in $\Lambda$ [RS2, Lemma 3.1]. Furthermore, by Lemma 2.1 $\operatorname{rad}\Lambda^\Omega = \Lambda^\Omega \cap \operatorname{rad}\Lambda$, and by Proposition 5.22 of [CR2] (stated in the proof of part (2) of Lemma 2.1) $\operatorname{rad}\Lambda$ is nilpotent modulo $\wp\Lambda$. Since $\wp | p$, and since $\pi | p$, $\operatorname{rad}\Lambda$ is nilpotent modulo $\pi\Lambda$.

The set of conjugacy class sums $\underline{x}$ for $x \in G$ under conjugation by $\Omega$ forms a basis for $(SG)^\Omega$ over $S$, and the set of images of the tensors of these class sums with the $\{y_i\}$ (the $S$-basis for $A$ over $S$) in $\Lambda$ contains a basis for $\Lambda^{\Omega}$ over $R$ (see §3.1.1 of [RS2]). Let $B$ be such a basis and denote an element of $B$ by $y \otimes \underline{\Omega(g)}$ for some $y \in A$ and $g \in G$. Then there are three possibilities for the action of $t$ on $y \otimes \underline{\Omega(g)}$:

(0) ${}^t(y \otimes \underline{\Omega(g)}) = y \otimes \underline{\Omega(g)}$.

($f$) $y \otimes \underline{\Omega(g)}$, ${}^t(y \otimes \underline{\Omega(g)})$, ..., ${}^{t^{p-1}}(y \otimes \underline{\Omega(g)})$ are $R$-independent.

($\zeta$, $i$) ${}^t(y \otimes \underline{\Omega(g)}) = y \otimes \zeta^i \underline{\Omega(g)}$ for some integer $i$. We allow this notation for all integers $i$, but the possibilities with $0 < i < p$ are disjoint from each other and the above cases.

Now define $\Lambda_0$ to be the $R$-submodule of all $R$-linear combinations of $y \otimes \underline{\Omega(g)}$'s satisfying condition (0), and define $\Lambda_f$ and $\Lambda_i$ similarly. Also, set

$$\Lambda_{\zeta} = \sum_{0<i<p} \Lambda_i.$$

The sum $\Lambda_0 + \Lambda_{\zeta} + \Lambda_f$ is then direct, as is the above sum for $\Lambda_{\zeta}$. Define $\gamma_0$, $\gamma_f$, $\gamma_i$, and $\gamma_{\zeta}$ to be the projections of $\gamma$ onto the appropriate subspaces of $\Lambda^{\Omega}$.

The following proposition appears as Proposition 1.6.1 in [RS2] and falls into the category of those identities that are obvious once someone else has been considerate enough to work them out for you.

**Proposition 2.5.** *Let $\Lambda$ be a ring, $z$ an element of $\Lambda$ with $1+z$ invertible, and $x$ an element of $\Lambda$. Let $[\ ,\ ]$ denote the ring-theoretic commutator ($[a, b] = ab - ba$ for $a, b \in \Lambda$). Then*

$$(1+z)x(1+z)^{-1} = x + [z, x](1+z)^{-1}. \tag{2.1}$$

For $x \in \Lambda$ define $T(x) = x + {}^t x + \cdots + {}^{t^{p-1}} x$. We now conclude §2 with the following lemma:

**Lemma 2.6.** *The free part of $\gamma(t)$, namely $\gamma_f(t)$, is in* $\operatorname{rad} \Lambda^{\Omega}$. *In fact, $U$ may be modified by conjugation so that the new $\gamma_f(t) \in \pi\Lambda_f$ while changing neither $\gamma_0(t)$ nor $\gamma_{\zeta}(t)$ modulo $\pi\Lambda^{\Omega}$.*

*Proof.* Since $t^p \in \Omega$, $\gamma(t^p) = 0$. However, recall that given $g, h \in H$, $\gamma(gh) = \gamma(g) + {}^g\gamma(h) + \pi\gamma(g){}^g\gamma(h)$. Thus $0 = \gamma(t^p) = T(\gamma(t)) + \pi\lambda$ for some $\lambda \in \Lambda^{\Omega}$. It is easy to see that $T(\gamma(t)) = p\gamma_0(t) + T(\gamma_f(t))$, and so

$$T(\gamma_f(t)) \equiv 0 \pmod{\pi\Lambda^{\Omega}}.$$

Since $\Lambda_f$ is a free module for the cyclic group $\langle \Omega, t\rangle/\Omega$, there is some $y \in \Lambda_f$ such that ${}^t y - y \equiv \gamma_f(t) \pmod{\pi\Lambda^{\Omega}}$. In particular $\gamma_f(t) \in \operatorname{rad}\Lambda^{\Omega}$. Moreover, note that for any integer $n > 0$, $(1+\pi y)^{-1} \equiv 1 - \pi y + (\pi y)^2 - \cdots + (-1)^{n-1}(\pi y)^{n-1} \pmod{\pi^n \Lambda}$. Thus applying Proposition 2.5,

$$\begin{aligned}
{}^{(1+\pi y)}u &= u + [\pi y, u](1+\pi y)^{-1} \\
&= t + \pi\gamma(t)t + \pi[y, t + \pi\gamma(t)t](1+\pi y)^{-1} \\
&\equiv t + \pi\gamma(t)t + \pi[y, t] \pmod{\pi^2\Lambda^{\Omega}} \\
&\equiv (1 + \pi\gamma(t) + \pi(y - {}^t y))t \pmod{\pi^2\Lambda^{\Omega}} \\
&\equiv (1 + \pi\gamma_0(t) + \pi\gamma_{\zeta}(t))t \pmod{\pi^2\Lambda^{\Omega}}. \quad \square
\end{aligned}$$

## 3. The case where $t$ centralizes $C_G(H/C) \cap C_G(\Omega)$

By Lemma 2.6 we may assume that $\gamma_f(t) \in \pi\Lambda^\Omega$. Pushing $\gamma_\zeta(t)$ and $\gamma_0(t)$ down into $\pi\Lambda^\Omega$ is considerably more difficult. Section 3 is devoted to handling the case where $t$ centralizes $C_{G/C}(H/C) \cap C_G(\Omega)$. We observed in §2 that $\operatorname{rad}\Lambda$ is nilpotent modulo $\pi\Lambda$. Hence by Lemma 2.1 $\operatorname{rad}\Lambda^\Omega$ is nilpotent modulo $\pi\Lambda^\Omega$. Furthermore, some elementary calculations show that each $\gamma_i(t)$ is centralized by $H$ modulo $\pi\Lambda^\Omega$. These observations lead to the following lemma:

**Lemma 3.1.** *If $t$ centralizes $C_G(H/C) \cap C_G(\Omega)$, then $\gamma_i(t) \in \operatorname{rad}\Lambda^\Omega$ for $1 \leq i \leq p-1$.*

*Proof.* The proof is almost identical to that of Claim 2 in §3.3 of [RS2]. First of all, let $\tilde{\wp} = \wp + \pi R$. Note that $(\wp + (c-1)SC + \underline{c}SG)SG = \wp G + (c-1)SG + \underline{c}SG = \wp G + (c-1)SG + pSG = \wp G + (c-1)SG$. Thus

$$\begin{aligned}\Lambda/\tilde{\wp}\Lambda &\cong A \otimes_S (SG/I(SC)G)/((\wp G + I(SC)G)/I(SC)G) \\ &\cong A \otimes_S S(G/C)/(\wp G/(\wp G \cap I(SC)G)).\end{aligned}$$

Moreover, $\wp G \cap I(SC)G = \wp G \cap (c-1)SG = (c-1)\wp G = I(\wp C)G$. Thus $\Lambda/\tilde{\wp}\Lambda \cong A \otimes_S S(G/C)/\wp(G/C) \cong A \otimes_S (S/\wp)(G/C) = A \otimes_S F(G/C)$.

Since each $\gamma_i(t)$ is centralized by $H$ modulo $\pi\Lambda^\Omega$ the image of $\gamma_i(t)$ in $\Lambda/\tilde{\wp} \cong A \otimes_S F(G/C)$ must be a linear combination of $H/C$-class sums. If a coset $xC$ lies in $C_G(H/C) \cap C_G(\Omega)$ then $t$ centralizes $x$. Thus $\underline{\Omega(x)}$ is in $\Lambda_0$ and so does not contribute to $\gamma_i(t)$. Therefore all $H/C$ classes whose sums appear with a nonzero coefficient in the expression for the image of $\gamma_i(t)$ in $A \otimes_S F(G/C)$ have cardinality greater than one. The corresponding sums thus lie in the radical of $A \otimes_S F(G/C)$. By Proposition 5.22 of [CR2], $\operatorname{rad}\Lambda = \phi^{-1}(\operatorname{rad}(A \otimes_S F(G/C)))$ where $\phi\colon \Lambda \to \Lambda/\wp\Lambda$. Thus $\gamma_i(t) \in \operatorname{rad}\Lambda^\Omega$. □

As was mentioned before, $\operatorname{rad}\Lambda^\Omega$ is nilpotent modulo $\pi\Lambda^\Omega$. Lemma 3.1 thus provides a small first step toward pushing $\gamma_i(t)$ down into $\pi\Lambda^\Omega$. One shortcoming of the decomposition $\Lambda^\Omega = \Lambda_0 + \Lambda_\zeta + \Lambda_f$ is that it gives a direct sum for modules but not for rings since none of $\Lambda_0$, $\Lambda_\zeta$, and $\Lambda_f$ are closed under multiplication. The multiplicative behavior of these submodules is very nice, however, with respect to certain parts of $\operatorname{rad}\Lambda^\Omega$. We shall exploit this nice behavior throughout the rest of the paper.

In the next two paragraphs, we are going to introduce some notation and results taken from §3.3.1 of [RS2]. The proofs for these results can either be found in [RS2] or done by the reader.

For starters, let us define $L$ to be the ring of points in $\Lambda^\Omega$ fixed by $t$ modulo $\pi\Lambda^\Omega$, let $I = \pi\Lambda^\Omega + T(\Lambda_f)$, and set $L_j = I + \Lambda_j$. Note that $I \subseteq \operatorname{rad}\Lambda^\Omega$. Also, $I \trianglelefteq L$ and $E = L/I$ is a $\mathbb{Z}/p\mathbb{Z}$-graded ring with $j$th grade $L_j$. Call an $R$-submodule $M$ of $L$ graded if its image in $E$ is graded, that is, if $I + M = \sum_j (I + M) \cap L_j$. If $M$ is graded set $M_j = (I + M) \cap L_j = I + (M \cap L_j)$. Thus $I \subseteq M_j$, and $M_j$ is contained in $I + M$, but perhaps not in $M$. The powers of $M$ are also graded, and we write $M_j^k$ for $(M^k)_j$. Moreover, if we define $\operatorname{pr}_j\colon \Lambda^\Omega \to \Lambda_j$ to be the projection map, reducing $j$ modulo $p$, then the equation $M_j = I + \operatorname{pr}_j(M)$ holds for all graded $R$-submodules $M$ of $L$, and $\operatorname{pr}_j(I) \subseteq \pi\Lambda^\Omega$.

Now define $D_i = L_i \cap \operatorname{rad} \Lambda^\Omega = I + (\Lambda_i \cap \operatorname{rad} \Lambda^\Omega)$, and set $D = \sum D_j$. Note that $\operatorname{pr}_0(D) \equiv \operatorname{pr}_\zeta(D) \equiv \operatorname{pr}_f(D) \equiv 0 \pmod{\operatorname{rad} \Lambda^\Omega}$. Moreover, $D \trianglelefteq L$ and $D$ is a graded $R$-submodule of $L$. By the above paragraph $D^k + I = \sum D_i^k$ where $D_i^k = (D^k + I) \cap L_i = I + (D^k \cap L_i)$. Also, by Lemma 3.1, $\gamma_i(t) \in D_i$ for $1 \le i \le p-1$. Suppose now for some $m \ge n \ge 0$ that $\gamma_0(t) \in \pi^n \Lambda^\Omega$ and that $\gamma_f(t)$, $\gamma_\zeta(t) \in \pi^m \Lambda^\Omega$ (but if $m = 0$, assume $\gamma_f(t) \in \pi \Lambda^\Omega$ by Lemma 2.6).

**Lemma 3.2.** *Suppose integers $r \ge k \ge 1$ have been chosen such that for $1 \le i \le p-1$ each $\gamma_i(t) \equiv \pi^m \theta_i \pmod{\pi^m(D^{k+1} + I) + \pi^{m+1}\Lambda^\Omega}$, with $\theta_i \in D_{k,r}$ where $D_{k,r} = D^k \cap \Lambda_i \cap \operatorname{rad}^r \Lambda^\Omega$. Then $u$ may be conjugated by a unit in $\Lambda$ so that the new $\gamma_i(t) \equiv \pi^m \theta_i \pmod{\pi^m(D^{k+1} + I) + \pi^{m+1}\Lambda^\Omega}$ where $\theta_i$ is now in $D_{k,r+1}$, while $\gamma_0(t)$ remains in $\pi^n \Lambda^\Omega$ and $\gamma_f(t)$ remains in $\pi^m \Lambda^\Omega$.*

*Proof.* Let $d = \sum_{i=1}^{p-1} \frac{1}{i} \gamma_i(t)$. Since each $\gamma_i(t) \in \operatorname{rad} \Lambda^\Omega$, $d$ is also in the radical of $\Lambda^\Omega$. Thus $1 + d$ is invertible and so, using a modified version of formula 2.1, one gets

$$^{1+d}u = u + (\pi[d, \gamma(t)] + (1 + \pi\gamma(t))[d, t]t^{-1})t(1+d)^{-1}t^{-1}t.$$

Observe that $[d, t]t^{-1} = d - {}^t d = \sum_{i=1}^{p-1} \frac{1}{i}(1 - \zeta^i)\gamma_i(t)$. By hypothesis $\gamma_i(t) \in \pi^m \Lambda^\Omega$, and $\zeta^i - 1 \equiv i\pi \pmod{\pi^2}$ since $1$ is a double root of the polynomial $f(x) = (x^i - 1) - i(x - 1)$. Hence $[d, t]t^{-1} \equiv -\pi\gamma_\zeta(t) \pmod{\pi^{m+2}\Lambda^\Omega}$. In particular,

$$\pi\gamma(t)[d, t]t^{-1} \equiv 0 \pmod{\pi^{m+2}\Lambda^\Omega}.$$

Also,

$$\begin{aligned} t(1+d)^{-1}t^{-1} &= (1 + {}^t d)^{-1} = 1 - {}^t d + ({}^t d)^2 - \cdots \\ &\equiv 1 \qquad \pmod{\pi^{m+1}\Lambda^\Omega + \pi^m(D^k + I)}. \end{aligned}$$

Hence

$$[d, t](1+d)^{-1}t^{-1} \equiv -\pi\gamma_\zeta(t) \qquad \pmod{\pi^{m+2}\Lambda^\Omega + \pi^{m+1}(D^{2k} + I)}.$$

(If $m > 0$ then the $\pi^{m+1}(D^{2k} + I)$ term is actually contained in $\pi^{m+2}\Lambda^\Omega$.)

Finally we must dissect the term involving $[d, \gamma(t)]$. First off,

$$\begin{aligned} [d, \gamma(t)] &= \sum_{i=1}^{p-1} \frac{1}{i} \left[ \gamma_i(t), \gamma_0(t) + \sum_{i=0}^{p-1} \gamma_i(t) + \gamma_f(t) \right] \\ &\equiv \sum_{i=1}^{p-1} \frac{1}{i} [\gamma_i(t), \gamma_0(t)] \qquad \pmod{\pi^{m+1}\Lambda^\Omega + \pi^m(D^{2k} + I)} \end{aligned}$$

since $\gamma_f(t)$ is assumed to be in $\pi\Lambda^\Omega$ and each $\gamma_i(t)$ is in $\pi^m D^k$. Now define $\Lambda_l$ to be the $R$-submodule of $\Lambda^\Omega$ generated by $\{\underline{\Omega(y)} : y \notin C_G(\Omega)\}$, define $\Lambda_s$ to be the $R$-submodule of $\Lambda^\Omega$ generated by $\{\underline{\Omega(y)} : y \in C_G(\Omega)\}$, and define $\operatorname{pr}_l$ and $\operatorname{pr}_s$ to be the corresponding projections. Here the $l$ and the $s$ stand for "long class sum" and "short class sum" respectively. Clearly each of $\Lambda^\Omega$, $\Lambda_0, \ldots$ has a direct sum decomposition into a short part and a long part. Also clear is the fact that $g \notin C_G(\Omega) \Leftrightarrow \underline{\Omega(g)} \in \operatorname{rad} \Lambda^\Omega$. Thus $\Lambda_l^\Omega \subseteq \operatorname{rad} \Lambda^\Omega$ so that $\operatorname{pr}_l \gamma_0(t) \in \operatorname{rad} \Lambda^\Omega$ which implies that $\operatorname{pr}_l \gamma_0(t) \in D_0 \subseteq D$. Thus

$$[\gamma_i(t), \operatorname{pr}_l \gamma_0(t)] \equiv 0 \qquad \pmod{\pi^m(D^{k+1} + I)}.$$

On the other hand, if $g \in C_G(\langle \Omega, t\rangle)$ then

$$\begin{aligned}[\gamma_i(t), g] &\equiv \pi^m(\theta_i g - g\theta_i) \pmod{\pi^{m+1}\Lambda^\Omega + \pi^m(D^{k+1} + I)}\\ &\equiv 0 \pmod{\pi^{m+1}\Lambda^\Omega + \pi^m(D^{k+1} + I) + \pi^m(D_{k,r+1} + I)}.\end{aligned}$$

Thus

$$^{1+d}u \equiv u - \pi\gamma_\zeta(t)t \qquad \pmod{\pi^{m+2}\Lambda^\Omega + \pi^{m+1}(D^{k+1} + I) + \pi^{m+1}(D_{k,r+1} + I)}$$

which completes the proof of Lemma 3.2. □

Since $\operatorname{rad}\Lambda^\Omega$ is nilpotent modulo $\pi\Lambda^\Omega$ one may repeatedly apply Lemma 3.2 to produce $\gamma_i(t) \equiv 0 \pmod{\pi^{m+1}\Lambda^\Omega + \pi^m(D^{k+1} + I)}$. Thus Lemma 3.2 allows one to increase the value of $k$. However $D$ is also nilpotent modulo $\pi\Lambda^\Omega$ and $\operatorname{pr}_i(I) \subseteq \pi\Lambda^\Omega$, and so additional applications of Lemma 3.2 prove

**Proposition 3.3.** *Suppose $m \geq n \geq 0$ with $\gamma_\zeta(t), \gamma_f(t) \in \pi^m\Lambda^\Omega$, and $\gamma_0(t) \in \pi^n\Lambda^\Omega$. Then $u$ may be conjugated by a unit of $\Lambda^\Omega$ so that the new $\gamma_\zeta(t) \in \pi^{m+1}\Lambda^\Omega$ while $\gamma_0(t)$ and $\gamma_f(t)$ stay in $\pi^n\Lambda^\Omega$ and $\pi^m\Lambda^\Omega$ respectively.*

So long as $p - 1 + n \geq m$, Lemmas 3.4 and 3.5 of [RS2] may be applied to obtain $\gamma_\zeta(t), \gamma_f(t) \in \pi^{m+1}\Lambda^\Omega$. Once $\gamma_\zeta(t), \gamma_f(t) \in \pi^{p-1+n}\Lambda^\Omega$, §3.4.1 of [RS2] yields $p(\gamma_0(t) + w(\gamma_0(t))^p) \equiv -T(\gamma_f(t)) \pmod{\pi^{p+n}\Lambda^\Omega}$. Note that $T(\gamma_f(t)) \in \pi^{p-1+n}\operatorname{rad}\Lambda^\Omega \supseteq \pi^{p+n}\Lambda^\Omega$. Because $\pi$ is not a zero divisor in $\Lambda$ one now obtains

$$\gamma_0(t) + w(\gamma_0(t))^p \equiv 0 \pmod{\pi^n \operatorname{rad}\Lambda^\Omega}$$

so that $\gamma_0(t) + w(\gamma_0(t))^p \in \operatorname{rad}\Lambda^\Omega$. Since $w \equiv -1 \pmod{\operatorname{rad}\Lambda}$, $\gamma_0(t)$ is a root modulo $\operatorname{rad}\Lambda$ of the polynomial $f(x) = x^p - x$. But $\Lambda/\operatorname{rad}\Lambda \cong \mathscr{D}$ so that the image of $\gamma_0(t)$ in $\Lambda/\operatorname{rad}\Lambda$ is in the field $\mathbb{F}_p$. Suppose $\gamma_0(t) \notin \operatorname{rad}\Lambda$. Then $\gamma_0(t) \equiv b \pmod{\operatorname{rad}\Lambda}$ for some $1 \leq b \leq p-1$. Choose a group homomorphism $\psi \colon H \to C$ such that $\Omega \leq \ker\psi$ and $\psi(t) = c^b$. If we define a group automorphism $\beta \colon H \to H$ by $\beta(g) = g\psi(g)$ and extend $\beta$ to $\Lambda_H$, then

$$\begin{aligned}\beta(t) &= t + \pi(1 + \zeta + \cdots + \zeta^{b-1})t\\ &\equiv t + \pi bt \qquad \pmod{\pi \operatorname{rad}\Lambda}\\ &\equiv t + \pi\gamma(t)t \qquad \pmod{\pi\operatorname{rad}\Lambda}.\end{aligned}$$

Thus $\beta(t) \equiv u \pmod{\pi\operatorname{rad}\Lambda}$. Hence we may replace $t$ with $\beta(t)$ and argue as before, this time having the additional assumption that $\gamma(t) \in \operatorname{rad}\Lambda$. After applying Lemmas 2.6 and 3.1 we may even conclude that $\gamma_0(t) \in \operatorname{rad}\Lambda$, and this inclusion is not altered by any of the arguments following Lemma 3.1. The argument contained in the last full paragraph of 3.6 of [RS2]—starting with "Since $p - 1 > 0, \ldots$ "—may now be applied to prove

**Proposition 3.4.** *Suppose $\gamma(t) \in \pi^n\Lambda^\Omega$. Then $u$ may be conjugated by a unit in $\Lambda$ so that the new $\gamma(t) \in \pi^{n+1}\Lambda$.*

Taking a limit as $n \to \infty$ now drives $\gamma(t)$ to $0$, and so $\Omega$ may be enlarged to include $t$. This concludes the proof of Theorem 2.1 in the case where $t$ centralizes $C_G(H/C) \cap C_G(\Omega)$.

## 4. The case where $\gamma_i(t) \notin \operatorname{rad}\Lambda^\Omega$: Taking out the trash

In §3 we assumed that $t$ centralized $C_G(H/C) \cap C_G(\Omega)$. The value of that assumption is that it implies that $\gamma_i(t) \in \operatorname{rad}\Lambda^\Omega$. Suppose now that $t$ does not centralize $C_G(H/C) \cap C_G(\Omega)$ and that $\gamma_i(t)$ is not in $\operatorname{rad} \Lambda^\Omega$. The idea then is simple enough—just conjugate $u$ by a unit in $\Lambda$ so that the new $\gamma_i(t) \in \operatorname{rad} \Lambda^\Omega$. In the process of finding such a unit in $\Lambda$ and showing that that unit does the job, we will make use of an explicit description of $\Lambda_i$ and of the multiplicative relationships between $\Lambda_0$, $\Lambda_f$, and the $\Lambda_i$.

Since $t$ does not centralize $C_G(H/C) \cap C_G(\Omega)$ it is possible to choose some $s \in C_G(H/C) \cap C_G(\Omega)$ such that ${}^t s = \zeta s$. Then $\Lambda_i = s^i \Lambda_0$ for $0 \leq i \leq p-1$. Thus express $\Lambda^\Omega$ as the direct sum $\sum_{i=0}^{p-1} (s-1)^i \Lambda_0 + \Lambda_f$, and for some $x_i \in \Lambda_0$ and $\lambda_f \in \Lambda_f$ let $\gamma(t) = \sum_{i=0}^{p-1} (s-1)^i x_i + \lambda_f$. The idea is to specialize $\gamma(t)$'s form enough to conclude that the $\gamma_i(t)$ are in $\operatorname{rad} \Lambda^\Omega$.

**Lemma 4.1.** *Let* $x \in \operatorname{rad}^b \Lambda^\Omega$. *If* $x \in \Lambda_0$, *then* $xs \in \Lambda_\zeta$. *If* $x \in \Lambda_f$, *then* $xs \in \Lambda_f$. *In either case,*

$$x(s-1)^i = \sum_{j=0}^{i} \binom{i}{j} (s-1)^{i-j} f_{i,j}(x)$$

*where* $f_{i,j}(x) = \sum_{k=0}^{j} (-1)^k \binom{j}{k}{}^{s^{k-i}} x$. *The coefficient* $f_{i,0}(x) \in \operatorname{rad}^b \Lambda^\Omega$, *and the remaining* $f_{i,j}(x) \in \operatorname{rad}^{b+1} \Lambda^\Omega$.

*Proof.* Recall that $s \in C_G(H/C) \cap C_G(\Omega)$. Thus $\underline{\Omega(g)}s = \underline{\Omega(gs)}$ for any $g \in G$. The assertions about the product $xs$ follow immediately.

The equations for $x(s-1)^i$ and the $f_{i,j}(x)$ can be proven using a straightforward, albeit messy, induction argument.

Since $s \equiv 1 \pmod{\operatorname{rad} \Lambda^\Omega}$, $f_{i,0}(x) = {}^{s^{-i}}x \equiv x \pmod{\operatorname{rad}^b \Lambda^\Omega}$. Similarly, $f_{i,j}(x) \equiv (\sum_{k=0}^{j} (-1)^k \binom{j}{k}) x \pmod{\operatorname{rad}^{b+1} \Lambda^\Omega} \equiv 0 \pmod{\operatorname{rad}^{b+1} \Lambda^\Omega}$ since $\sum_{k=0}^{j} (-1)^k \binom{j}{k} = 0$. □

The virtue of this lemma is that $\operatorname{rad} \Lambda^\Omega$ is nilpotent modulo $\pi \Lambda^\Omega$, and we now know that "commuting" expressions with powers of $s-1$ preserves in some sense powers of $\operatorname{rad} \Lambda^\Omega$.

The strategy now is to modify $\gamma(t)$ so that it resembles $(s-1)^{p-1} x$ for some $x \in \Lambda_0$. If $\gamma(t)$ actually was $(s-1)^{p-1} x$ then it is clear that $\gamma_i(t) \in \operatorname{rad} \Lambda^\Omega$ for $1 \leq i \leq p-1 \Leftrightarrow x \in \operatorname{rad} \Lambda^\Omega$. However $x \in \operatorname{rad} \Lambda^\Omega$ is equivalent to $x_s \in \operatorname{rad} \Lambda^\Omega$ where $x_s$ is the projection of $x$ onto $\Lambda_s$.

**Lemma 4.2.** *Let* $x, y \in \Lambda^\Omega$. *Then* (i) $x, y \in \Lambda_s^\Omega \Rightarrow xy \in \Lambda_s^\Omega$;

(ii) $x \in \Lambda_s^\Omega$ *and* $y \in \Lambda_l^\Omega$, *or* $x \in \Lambda_l^\Omega$ *and* $y \in \Lambda_s^\Omega \Rightarrow xy \in \Lambda_l^\Omega$;

(iii) $x, y \in \Lambda_l^\Omega \Rightarrow \operatorname{pr}_s(xy) \equiv 0 \pmod{\pi^{p-1} \Lambda^\Omega}$.

*Proof.* Parts (i) and (ii) are trivial since $\Lambda_s$ is generated by the tensors of the basis elements $y_i$ with the group $C_G(\Omega)$. For the third claim, assume without loss of generality that $x = 1 \otimes \underline{\Omega(g)}$ and $y = 1 \otimes \underline{\Omega(h)}$ for some $g, h \in G$. If $\operatorname{pr}_s(xy) \neq 0$, then we may also assume without loss of generality that $gh \in C_G(\Omega)$. Part (iii) now follows from the fact that $p$ divides the orders of the $\Omega$-orbits of $g$ and $h$ and the observation that ${}^\omega(gh) = {}^\omega g {}^\omega h$ for any $\omega \in \Omega$. □

**Lemma 4.3a.** *Suppose* $\gamma(t) = (s-1)^{p-1} x + \pi^n \sum_{i=0}^{p-2} (s-1)^i x_i + \lambda_f$ *where* $n \geq 0$, $x, x_i \in \Lambda_0$, *and, by Lemma* 2.2, $\lambda_f \in \pi \Lambda_f$. *Suppose also that* $\operatorname{pr}_s(\lambda_f) \equiv 0$

$(\operatorname{mod} \pi^{\mu}\Lambda_f)$ *for some* $\mu \leq p-1$. *Then* $u$ *may be conjugated by some unit in* $\Lambda^{\Omega}$ *so that the new* $\gamma(t)$ *will look like* $(s-1)^{p-1}x + \pi^{n+1}y + \lambda_f$ *where* $x \in \Lambda_0$, $y \in \Lambda_0 + \Lambda_{\zeta}$, $\lambda_f \in \Lambda_f$, *and* $\operatorname{pr}_s(\lambda_f) \equiv 0 \pmod{\pi^{\mu}\Lambda^{\Omega}}$ *for the same* $\mu$.

*Proof.* Let $m$ be maximal such that $x_i \in \operatorname{rad}^m \Lambda^{\Omega}$ for $0 \leq i \leq p-2$. Define $k = \min\{i\colon x_i \notin \operatorname{rad}^{m+1}\Lambda^{\Omega}\}$. Now set $v = \frac{1}{k+1}(s-1)^{k+1}x_k$ and consider

$$^{(1+\pi^n v)}u = u + (\pi^{n+1}[v, \gamma(t)] + (1+\pi\gamma(t))\pi^n[v, t]t^{-1})t(1+\pi^n v)^{-1}t^{-1}t.$$

By Lemmas 4.1 and 4.2 $\operatorname{pr}_s \operatorname{pr}_f(^{(1+\pi^n v)}u) \equiv 0 \pmod{\pi^{\mu}\Lambda^{\Omega}}$ and the claim about $\lambda_f$ is established. Henceforth all statements in the proof will be modulo $\Lambda_f$. First,

$$\begin{aligned}[v, \gamma(t)] \equiv \frac{1}{k+1}\Bigg(&(s-1)^{k+1}x_k(s-1)^{p-1}x - (s-1)^{p-1}x(s-1)^{k+1}x_k \\ &+ \pi^n\sum_{i=0}^{p-2}\{(s-1)^{k+1}(x_k(s-1)^i x_i) - (s-1)^i(x_i(s-1)^{k+1}x_k)\}\Bigg) \\ \equiv &\sum_{i=0}^{p-1}(s-1)^i y_i \qquad \pmod{\pi\Lambda^{\Omega}}\end{aligned}$$

where $y_i \in \operatorname{rad}^{m+1}\Lambda^{\Omega}$ for $0 \leq i \leq k$ and $y_i \in \operatorname{rad}^m \Lambda^{\Omega}$ for $k+1 \leq i \leq p-1$ by Lemma 4.2 and the fact that $(s-1)^{p+e} \equiv (s-1)^e(s^p-1) \pmod{\pi^{p-1}\Lambda^{\Omega}}$. Note that $s^p$ is in $\operatorname{pr}_s(\Lambda^{\Omega})$.

Also

$$\begin{aligned}[v, t]t^{-1} = v - {}^t v &= \frac{1}{k+1}((s-1)^{k+1} - (\zeta(s-1)+\pi)^{k+1})x_k \\ &\equiv \frac{1}{k+1}((1-\zeta^{k+1})(s-1)^{k+1} - (k+1)\pi\zeta^k(s-1)^k)x_k \pmod{\pi^2\Lambda^{\Omega}} \\ &\equiv -\pi(s-1)^k x_k + (s-1)^{k+1}z \pmod{\pi^2\Lambda^{\Omega}}\end{aligned}$$

for $z = (1-\zeta^{k+1})/(k+1)x_k$ which is obviously in $\pi \operatorname{rad}^m \Lambda^{\Omega} \cap \Lambda_0$. In particular, $\pi\gamma(t)[v, t] \equiv 0 \pmod{\pi^2\Lambda^{\Omega}}$.

Finally, $t(1+\pi^n v)^{-1}t^{-1} = (1+\pi^{n\,t}v)^{-1}$, and by the preceding paragraph $\pi^{n\,t}v \equiv \pi^n(s-1)^{k+1}x_k \pmod{\pi^{n+1}\Lambda^{\Omega}}$. Let $\theta = (s-1)^{k+1}x_k$ and consider the infinite sum $1 - \pi^n\theta + \pi^{2n}\theta^2 - \cdots$. Since $\theta \in \operatorname{rad}\Lambda^{\Omega}$ this sum will converge to $(1+\pi^{n\,t}v)^{-1}$, and so we see by Lemma 4.2 that

$$(1+\pi^{n\,t}v)^{-1} \equiv 1 + \pi^n\sum_{i=0}^{p-1}(s-1)^i z_i \qquad \pmod{\pi^{n+1}\Lambda^{\Omega}}$$

with $z_i \in \operatorname{rad}^{m+1}\Lambda^{\Omega}$ for $0 \leq i \leq k$ and $z_i \in \operatorname{rad}^m\Lambda^{\Omega}$ for $k+1 \leq i \leq p-1$. Appealing for one last time to Lemma 4.2 we now have

$$[v, t]t^{-1}t(1+\pi^n v)^{-1}t^{-1} \equiv -\pi(s-1)^k x_k + \pi\sum_{i=0}^{p-1}(s-1)^i w_i \qquad \pmod{\pi^2\Lambda^{\Omega}}$$

where $w_i \in \operatorname{rad}^{m+1}\Lambda^{\Omega}$ for $0 \leq i \leq k$ and $w_i \in \operatorname{rad}^m\Lambda^{\Omega}$ for $k+1 \leq i \leq p-1$.

Thus

$$^{(1+\pi^n v)}u \equiv u - \pi^{n+1}(s-1)^k x_k + \pi^{n+1}\sum_{i=0}^{p-1}(s-1)^i x_i' \qquad (\operatorname{mod} \pi^{n+2}\Lambda^\Omega)$$

where $x_i' \in \operatorname{rad}^{m+1}\Lambda^\Omega$ for $0 \le i \le k$ and $x_i' \in \operatorname{rad}^m \Lambda^\Omega$ for $k+1 \le i \le p-1$. The net effect is to increase $k$ by at least one or to increase $m$ by at least one. Furthermore if $k = p-2$, then $m$ automatically increases by at least one. The lemma now follows from the nilpotence of $\operatorname{rad}\Lambda^\Omega$ modulo $\pi\Lambda^\Omega$. □

*Comments.* (1) Note that the proof of Lemma 4.3a does not require that $(1+\pi\gamma(t))t$ represents a unit of finite order.

(2) The cases where $n \ge 1$ are somewhat simpler than the case $n = 0$. In the former cases the $z_i$ may be taken to be $0$.

(3) Once $n = 1$ one may apply Lemma 2.2—which does require a unit of finite order—to make $\gamma(t)$ look like $(s-1)^{p-1}x + \pi\sum_{i=0}^{p-2}(s-1)^i x_i + \pi\lambda_f$ with $x$, $x_i \in \Lambda_0$ and $\lambda_f \in \Lambda_f$. The proof of Lemma 4.3a will not alter the free part of $\gamma(t)$ modulo $\pi\Lambda^\Omega$ so long as $n \ge 1$. Thus we have:

**Lemma 4.3.** *Given $\gamma(t)$ as in Lemma 4.3a, but with $n \ge 1$, $u$ may be conjugated by some unit in $\Lambda^\Omega$ so that the new $\gamma(t)$ will look like $(s-1)^{p-1}x+\pi^{n+1}y+\pi\lambda_f$ where $x \in \Lambda_0$, $y \in \Lambda_0 + \Lambda_\zeta$, $\lambda_f \in \Lambda_f$, and $\operatorname{pr}_s(\lambda_f) \equiv 0 \pmod{\pi^\mu\Lambda^\Omega}$ for the same $\mu$.*

By Lemma 4.3 we may assume that $\gamma(t) = (s-1)^{p-1}x + \pi^{n+1}y + \pi\lambda_f$ with $n$ as large as we please. It was shown in the discussion preceding Lemma 4.2 that it would be nice if $\gamma(t) = (s-1)^{p-1}x$. The remainder of §4 is devoted to showing that $\gamma(t) = (s-1)^{p-1}x + \pi^n y + \pi\lambda_f$ with $n \ge p-1$ is, modulo some adjustments, just as nice.

Recall from §2 the identity $\gamma(gh) = \gamma(g) + {}^g\gamma(h) + \pi\gamma(g){}^g\gamma(h)$. The equation $0 = \gamma(t^p) = p\gamma(t) + T(\gamma_f(t)) + \pi\lambda$ appearing in the proof of Lemma 2.2 was derived from this identity. Obviously there are some higher powers of $\pi$ running around in that equation, and so a more explicit formula could be useful. For $1 \le r \le i$ and $g \in H$ define

$$T_r^i(\gamma(g)) = \pi^{r-1}\sum_{r,i}\prod_{k=1}^{r} {}^{g_k^j}\gamma(g)$$

where $\sum_{r,i}$ is the summation over the ordered $r$-tuples $(j_1, \dots, j_r)$ such that $0 \le j_1 < j_2 < \cdots < j_r \le i-1$, and the product is ordered with lowest index on the left. It is easy to see that $\gamma(g) = T_1^1(\gamma(g))$ and $\gamma(g^2) = T_1^2(\gamma(g)) + T_2^2(\gamma(g))$. In fact,

**Lemma 4.4.** *Given $g \in H$ and $i \ge 1$, $\gamma(g^i) = \sum_{r=1}^{i} T_r^i(\gamma(g))$.*

*Proof.* The identity follows from a straightforward induction argument.

**Proposition 4.5.** *Suppose $\gamma(t) = (s-1)^{p-1}x + \pi^n y + \pi\lambda_f$ with $x \in \Lambda_0$, $y \in \Lambda_0 + \Lambda_\zeta$, $\lambda_f \in \Lambda_f$, and $n \ge p-1$. Then $u$ can be conjugated by a unit in $\Lambda^\Omega$ so that the new $\gamma(t) = (s-1)^{p-1}x + \pi^n y + \pi\lambda_f$ with $y$, $\lambda_f$, and $n$ as above, and with $x \in \operatorname{rad}\Lambda^\Omega$.*

The proof of Proposition 4.5 has three components. First, the case $p = 2$ is disposed of. Then Lemma 4.6 will perform some fine tuning on $\lambda_f$. This fine tuning will allow us to discard the contributions of $y$ and $\lambda_f$ to the problem, bringing into focus the expression $(s-1)^{p-1}x$. This expression is then carefully analyzed in §5.

*Proof of Proposition* 4.5 *when* $p = 2$. For $p = 2$, it suffices to assume $\gamma(t) = (s-1)x + \pi y$ with $x \in \Lambda_0$ and $y \in \Lambda^\Omega$. We now have

$$\begin{aligned} 0 = \gamma(t^2) &\equiv (s-1)x + {}^t(s-1)x + \pi T(y) \pmod{\pi \operatorname{rad} \Lambda^\Omega} \\ &\equiv (1+\zeta)(s-1)x + \pi x + \pi T(y) \pmod{\pi \operatorname{rad} \Lambda^\Omega}. \end{aligned}$$

Since $1 + \zeta = 0$ and $T(\Lambda^\Omega) \subseteq \operatorname{rad} \Lambda$, we get $0 \equiv \pi x \pmod{\pi \operatorname{rad} \Lambda^\Omega}$, which implies $x \in \operatorname{rad} \Lambda^\Omega$. □

Suppose now that $p > 2$. Recall that $\gamma(t) = (s-1)^{p-1}x + \pi^n y + \pi\lambda_f$. By Lemma 4.4,

$$0 = \gamma(t^p) = \sum_{i=1}^{p} \left( \pi^{i-1} \sum_{i,p} \prod_{k=1}^{i} {}^{t^{j_k}}\gamma(t) \right). \tag{4.1}$$

The $i = 1$ term is just $T(\gamma(t))$, which is congruent to $px + T(\pi\lambda_f)$ modulo $\pi^{p-1} \operatorname{rad} \Lambda^\Omega$. Working modulo $\pi^{p-1} \operatorname{rad} \Lambda^\Omega$, any contribution from $\pi^n y$ to the rest of equation (4.1) will be 0 since $n \geq p-1$. Lemma 4.6 will next allow us to discard any contributions of $\lambda_f$ to equation (4.1.)

**Lemma 4.6.** *Let* $\operatorname{pr}_s(\pi\lambda_f) \in \pi^m \Lambda^\Omega \backslash \pi^{m+1} \Lambda^\Omega$ *where* $m \leq p-2$. *Then it is possible to conjugate* $u$ *by a unit in* $\Lambda$ *so that the new* $\gamma(t)$ *satisfies* $\operatorname{pr}_s \operatorname{pr}_f(\gamma(t)) \in \pi^{m+1}\Lambda^\Omega$.

*Proof.* By Lemmas 4.1 and 4.2, and by equation (4.1),

$$0 = \operatorname{pr}_s \operatorname{pr}_f(\gamma(t^p)) \equiv \operatorname{pr}_s(T(\pi\lambda_f)) \pmod{\pi^{m+1}\Lambda^\Omega}.$$

Since $\lambda_f$ is a free module for the cyclic group $\langle \Omega, t \rangle / \Omega$, there is some $y \in \pi^m \Lambda_f$ such that $\operatorname{pr}_s(\pi\lambda_f) \equiv {}^t y - y \pmod{\pi^{m+1}\Lambda^\Omega}$. Thus

$$\begin{aligned} {}^{(1+\pi y)}u &= u + (\pi[y, t]t^{-1} + \pi^2[y, \gamma(t)t]t^{-1})t(1+\pi y)^{-1} \\ &\equiv u + \pi(y - {}^t y)t \pmod{\pi^{m+2}\Lambda^\Omega}. \end{aligned}$$

Thus the short part of the new $\gamma_f(t)$ is in $\pi^{m+1}\Lambda^\Omega$. Applying Lemma 4.3 now finishes the proof of Lemma 4.6. □

Using Lemma 4.6, we may now assume that $\operatorname{pr}_s(\pi\lambda_f) \equiv 0 \pmod{\pi^{p-1}\Lambda^\Omega}$. By Lemmas 4.1 and 4.2 and the fact that $T(\Lambda^\Omega) \subseteq \operatorname{rad} \Lambda^\Omega$, the contribution of $\pi\lambda_f$ to the short part of equation (4.1) is 0 modulo $\pi^{p-1} \operatorname{rad} \Lambda^\Omega$. Thus we may assume $\gamma(t) = (s-1)^{p-1}x$. In fact, Lemma 4.2 even allows us to assume $x = x_s$.

## 5. The case where $\gamma_i(t) \notin \operatorname{rad} \Lambda^\Omega$: divide and conquer

In §4 we derived the equation

$$0 = \sum_{i=1}^{p} \left( \pi^{i-1} \sum_{i,p} \prod_{k=1}^{i} {}^{t^{j_k}}\gamma(t) \right).$$

Working modulo $\pi^{p-1}\operatorname{rad}\Lambda^{\Omega}$, the comments at the end of §4 now allow us to assume without loss of generality that $\gamma(t) = (s-1)^{p-1}x$ for some $x \in \operatorname{pr}_s \Lambda_0$. Then $T(\gamma(t)) = px$, and so we are led to examine the congruence

$$(5.1) \qquad 0 \equiv px + \sum_{i=2}^{p} \pi^{i-1} \sum_{i,p} \prod_{k=1}^{i} {}^{t^{j_k}}(s-1)^{p-1}x \qquad (\operatorname{mod} \pi^{p-1}\operatorname{rad}\Lambda^{\Omega}).$$

Clearly the $i = p$ term in the above sum is $0$ modulo $\pi^{p-1}\operatorname{rad}\Lambda^{\Omega}$. Also, it is easy to see using Pascal's triangle that $(s-1)^{p-1} \equiv s^{p-1} + s^{p-2} + \cdots + 1$ modulo $\pi^{p-1}$. Hence our attention now turns to the expression

$$(5.2) \qquad \sum_{i=2}^{p-1} \pi^{i-1} \sum_{i,p} \prod_{k=1}^{i} {}^{t^{j_k}}(s^{p-1} + \cdots + 1)x \qquad (\operatorname{mod} \pi^{p-1}\operatorname{rad}\Lambda^{\Omega}).$$

Let $M = \sum_{i=2}^{p-1} \pi^{i-1} \sum_{i,p} \prod_{k=1}^{i} {}^{t^{j_k}}(s^{p-1} + \cdots + 1)x$. Recall that we are now assuming that $x$ is in $\operatorname{pr}_s \Lambda_0$. Thus $\operatorname{pr}_l(M) = \operatorname{pr}_f(M) = 0$. For $1 \le k \le p-1$ choose $y_k \in \Lambda_0$ such that $M = \sum_{k=1}^{p-1}(s-1)^k y_k$. Clearly $\operatorname{pr}_{p-1}(M) = y_{p-1}$. Thus $y_{p-1} \equiv 0 \pmod{\pi^{p-1}\Lambda^{\Omega}}$. From this we obtain $\operatorname{pr}_{p-2}(M) \equiv y_{p-2} \equiv 0$ $(\operatorname{mod} \pi^{p-1}\Lambda^{\Omega})$. Continuing thus, we see that $y_k \equiv 0 \pmod{\pi^{p-1}\Lambda^{\Omega}}$ for $1 \le k \le p-1$. Therefore, in order to complete the proof of Proposition 5.5 it suffices to show that $\operatorname{pr}_0(M) \equiv 0 \pmod{\pi^{p-1}\operatorname{rad}\Lambda^{\Omega}}$. In fact, a little bit of elbow grease indicates that much more is actually true.

Define $x_r = s^{-r}xs^r$. Note that $s^p \in \Lambda_0$, $s^r \equiv 1 \pmod{\operatorname{rad}\Lambda^{\Omega}}$ for any $r$, and $x_r \equiv x \pmod{\operatorname{rad}\Lambda^{\Omega}}$ for any $r$. With a little care, one can now show with some direct calculations that if $p = 3$ and $i = 2$ then $\pi^2$ divides the coefficient of each $x_i$. Similarly, $\pi^4$ divides the coefficient of each $x_i$ when $p = 5$ and $i = 2$. In both cases, the $i = 2$ summand of $\operatorname{pr}_0(M)$ is then easily shown to be $0$ modulo $\pi^{p-1}\operatorname{rad}\Lambda^{\Omega}$. These two examples now suggest the following preliminary result:

**Lemma 5.1.** *Suppose $i = 2$ and $p \ge 3$. Let $\zeta f_{\sigma_1}(\zeta)$ be the coefficient of $s^p x_{\sigma_1} x$ where $1 \le \sigma_1 \le p-1$. Then*

(i) $f_{p-1}(\zeta) = 1 + 2\zeta + \cdots + (p-1)\zeta^{p-2}$;

(ii) $1$ *is a root of multiplicity* $p-2$, *modulo* $p$, *of* $f_{p-1}(x)$;

(iii) $\zeta f_{p-1}(\zeta) \equiv -\pi^{p-2} \pmod{\pi^{p-2}\operatorname{rad}\Lambda^{\Omega}}$;

(iv) $f_{\sigma_1}(\zeta) \equiv -\sigma_1^{-1} f_{p-1}(\zeta) \pmod{p}$ *where* $1 \le \sigma_1^{-1} \le p-1$ *is the multiplicative inverse of* $\sigma_1$ *in* $\mathbb{F}_p$. *Also, the coefficient* $f_0(x)$ *of* $x^2$ *is* $\binom{p}{2}$.

*Proof.* (i) The coefficient of $s^p x_{p-1} x$ in the two-fold product

$${}^{t^k}(s^{p-1} + \cdots + 1)x^{t^j}(s^{p-1} + \cdots + 1)x$$

is $\zeta^k \zeta^{pj-j} = \zeta^{k-j}$. Since ${}^t\lambda = \lambda$ for all $\lambda \in \Lambda_0$, it is possible to calculate $f_{p-1}(\zeta)$ simply by letting $k = 0$ and multiplying $\zeta^{-j} = \zeta^{p-j}$ by $p-j$. Thus the coefficient of $s^p x_{p-1} x$ is equal to $\zeta + 2\zeta^2 + \cdots + (p-1)\zeta^{p-1}$.

(ii) Let $g_{p-1}(x) = (x^p - 1)/(x-1)$. Note that

$$g_{p-1}(x) \equiv (x-1)^p/(x-1) \equiv (x-1)^{p-1} \qquad (\operatorname{mod} p).$$

Clearly $g_{p-1}(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ and $g_{p-1}(x) = f_{p-1}(x)$. Thus $f_{p-1}(x) \equiv (p-1)(x-1)^{p-2} \equiv -(x-1)^{p-2} \pmod{p}$.

(iii) Part (iii) follows from part (ii) since $\zeta \equiv 1 \pmod{\operatorname{rad} \Lambda^{\Omega}}$.

(iv) As in part (i), the coefficient of $s^p x_{\sigma_1} x$ in the two-fold product

$$(s^{p-1} + \cdots + 1)x^{t^j}(s^{p-1} + \cdots + 1)x$$

is $\zeta^{\sigma_1 j}$. Thus working $\bmod p$,

$$\zeta f_{\sigma_1}(\zeta) = \sum_{j=1}^{p-1}(p-j)\zeta^{\sigma_1 j} \equiv \sum_{k \in \mathbb{F}_p^*} -\sigma_1^{-1} k \zeta^k = -\sigma_1^{-1}\zeta f_{p-1}(\zeta).$$

Finally, the coefficient of $x^2$ is simply the number of two-fold products. It is easy to see that this number is the number of ordered two-tuples $(k, j)$ such that $0 \le k < j \le p-1$ which is $\binom{p}{2}$. □

By parts (iii) and (iv) of Lemma 5.1,

$$\begin{aligned}
\sum_{\sigma_1=1}^{p-1} f_{\sigma_1}(\zeta)/\pi^{p-2} &\equiv \sum_{\sigma_1=1}^{p-1} -\sigma_1^{-1} f_{p-1}(\zeta)/\pi^{p-2} \\
&\equiv \sum_{\sigma_1=1}^{p-1} \sigma_1^{-1} \qquad (\operatorname{mod} \pi^{p-2} \operatorname{rad} \Lambda^{\Omega}) \\
&\equiv \binom{p}{2} \equiv 0 \qquad (\operatorname{mod} \pi^{p-2} \operatorname{rad} \Lambda^{\Omega}).
\end{aligned} \tag{5.3}$$

This now suggests a strategy for dealing with $\operatorname{pr}_0(M)$. Arrange and collect summands in $\operatorname{pr}_0(M)$ arising from the various $i$-fold products according to products of the $x_{\sigma_k}$, and show that the coefficients of these products are divisible by an appropriate power of $\pi$. Then accumulate the remainders after factoring out all the $\pi$'s and hope for the best.

Consider a particular $i$-fold product

$$(s^{p-1} + \cdots + 1)x^{t^{j}1}(s^{p-1} + \cdots + 1)x^{t^{j}2}(s^{p-1} + \cdots + 1)x \cdots {}^{t^{j}i-1}(s^{p-1} + \cdots + 1)x$$

where $j_0 = 0$ and $1 \le j_1 < \cdots < j_{i-1} \le p-1$. For $2 \le i \le p-2$, $0 \le m_1, m_2, \ldots, m_{i-1} \le p-1$, $0 \le k \le p-1$, and $1 \le l \le i-1$ define $\sigma_l = m_1 + m_2 + \cdots + m_l$ and $\sigma = \sigma_{i-1} + k$. For a fixed value of $i$, let $\vec{m}$ represent the $i-1$-tuple $(m_1, \ldots, m_{i-1})$. The coefficient then of the term $f(k, \vec{m}) = s^k s^{\sigma_{i-1}} x_{\sigma_{i-1}} \cdots x_{\sigma_1} x$ in the above $i$-fold product is immediately seen to be $\zeta^{m_1 j_1 + m_2 j_2 + \cdots + m_{i-1} j_{i-1}}$. The total coefficient of $f(k, \vec{m})$ in expression (5.2) can be found by letting $t^e$ act on the above $i$-fold product for permissible values of $e$, namely for $0 \le e \le p - 1 - j_{i-1}$, and accumulating the individual coefficients of $f(k, \vec{m})$ at each value of $e$. The total coefficient of $f(k, \vec{m})$ in expression (5.2) is thus

$$\sum_{j_{i-1}=i-1}^{p-1} (1 + \cdots + \zeta^{\sigma(p-1-j_{i-1})})\zeta^{m_{i-1}j_{i-1}} \sum_{j_{i-2}=i-2}^{j_{i-1}-1} \zeta^{m_{i-2}j_{i-2}} \cdots \sum_{j_1=1}^{j_2-1} \zeta^{m_1 j_1}. \tag{5.4}$$

If we denote this sum by $S(k, \vec{m})$, then

$$\operatorname{pr}_0(M) \equiv \sum_{i=2}^{p-1} \pi^{i-1} \sum_{\mathscr{E}} S(\rho_0(\vec{m}), \vec{m}) f(\rho_0(\vec{m}), \vec{m}) \qquad (\operatorname{mod} \pi^{p-1} \operatorname{rad} \Lambda^{\Omega})$$

where $\mathscr{E} = \{(m_1, \dots, m_{i-1})\colon 0 \leq m_1, \dots, m_{i-1} \leq p-1\}$ and $\rho_0(\vec{m})$ is defined to be the unique value of $k \in [0, p-1]$ such that $\sigma = \sigma_{i-1} + k \equiv 0 \pmod{p}$.

**Proposition 5.2.** *Let $p \geq 3$ and $2 \leq i \leq p-1$. Then for any $\vec{m} \in \mathscr{E}$, $S(\rho_0(\vec{m}), \vec{m}) \equiv 0 \pmod{\pi^{p-i}\Lambda^{\Omega}}$.*

*Comments.* Since $\sigma \equiv 0 \pmod{p}$, expression (5.4) assumes the form

$$\sum_{j_{i-1}=i-1}^{p-1} (p - j_{i-1})\zeta^{m_{i-1}j_{i-1}} \sum_{j_{i-2}=i-2}^{j_{i-1}-1} \zeta^{m_{i-2}j_{i-2}} \dots \sum_{j_1=1}^{j_2-1} \zeta^{m_1 j_1}.$$

Since we are going to be working modulo $\pi^{p-i}$ for $2 \leq i \leq p-1$, we will demonstrate the same congruence for a slightly different version of the above expression, namely

$$\sum_{j_{i-1}=i-1}^{p-1} j_{i-1}\zeta^{m_{i-1}j_{i-1}} \sum_{j_{i-2}=i-2}^{j_{i-1}-1} \zeta^{m_{i-2}j_{i-2}} \dots \sum_{j_1=1}^{j_2-1} \zeta^{m_1 j_1}. \tag{5.5}$$

The proof is by induction on $i$. If $i = 2$ then the proposition is true by parts (iii) and (iv) of Lemma 5.1. In turn, part (iii) of Lemma 5.1 was a trivial consequence of part (ii). Recall that the proof of part (ii) relied on differentiating the polynomial $g_{p-1}(x) = (x^p - 1)/(x-1) \bmod p$. A careful scrutiny of expression (5.5) indicates that it represents a sum of derivatives of polynomials similar to $g_{p-1}(x)$. In accordance with the previous notation, let $g_n(x) = 1 + x + \cdots + x^{n-1} = (x^n - 1)/(x-1)$. A key element in the proof of Proposition 5.2 is determining just how one should go about differentiating these polynomials.

**Lemma 5.3** (A calculus teacher's nightmare). *For $1 \leq q \leq n-1$, the $q$th derivative $g_n^{(q)}(x)$ of $g_n(x)$ is*

$$\sum_{r=0}^{q-1} (-1)^r n(n-1)\cdots(n-q+r+1) r! \binom{q}{r} x^{n-q+r}(x-1)^{-r-1}$$
$$+ (-1)^q q!(x^n - 1)(x-1)^{-q-1}.$$

*Proof.* This lemma is easily proved using an elementary but grotesquely messy inductive argument.

*Proof of Proposition* 5.2. By the comments following the statement of Proposition 5.2, it suffices to show that

$$\sum_{j_{i-1}=i-1}^{p-1} j_{i-1}\zeta^{m_{i-1}j_{i-1}} \sum_{j_{i-2}=i-2}^{j_{i-1}-1} \zeta^{m_{i-2}j_{i-2}} \dots \sum_{j_1=1}^{j_2-1} \zeta^{m_1 j_1}$$

is congruent to $0$ modulo $\pi^{p-i}$. The fourth part of Proposition 5.1 shows that this congruence holds for $i = 2$. Proceeding by induction, we must now show that

$$\sum_{j_i=i}^{p-1} j_i \zeta^{m_i j_i} \sum_{j_{i-1}=i-1}^{j_i-1} \zeta^{m_{i-1}j_{i-1}} \dots \sum_{j_1=1}^{j_2-1} \zeta^{m_1 j_1} \equiv 0 \pmod{\pi^{p-i-1}\Lambda^{\Omega}}.$$

Denote this sum by $S(\vec{m})$. If $\vec{m} \equiv \vec{0} \pmod{p}$ then we are just looking at the coefficient of $x^{i+1}$, and that is simply the number of ordered $i$-tuples $0 \leq j_1 < \cdots < j_i \leq p-1$. This number is $\binom{p}{i}$, which is $0$ modulo $\pi^{p-1}$. Assume then that some $m_k \not\equiv 0 \pmod{p}$.

*Claim* 1. Let $\tilde{\vec{m}} = (m_2, \ldots, m_i)$, and set

$$S'(\vec{m}) = \sum_{j_i=i-1}^{p-1} j_i \zeta^{m_i j_i} \sum_{j_{i-1}=i-2}^{j_i-1} \zeta^{m_{i-1} j_{i-1}} \ldots \sum_{j_1=0}^{j_2-1} \zeta^{m_1 j_1}.$$

Then $S(\vec{m}) = S'(\vec{m}) - S(\tilde{\vec{m}})$.

*Proof*. The sums $S(\vec{m})$ and $S'(\vec{m})$ are the same except for some extra summands in $S'$. These extra summands occur whenever one of the indices $j_k$ assumes the value $k-1$. However, $j_k = k-1 \Rightarrow j_l = l-1$ for any $l < j$. In particular, $j_1 = 0$. Thus the extra summands in $S'$ occur precisely when $j_1 = 0$. Since $j_1 = 0 \Rightarrow \zeta^{m_1 j_1} = 1$, the extra summands are just $S(\tilde{\vec{m}})$. □

By the induction hypothesis, $S(\tilde{\vec{m}}) \equiv 0 \pmod{\pi^{p-i}}$. It is now necessary to show that $S'(\vec{m}) \equiv 0 \pmod{\pi^{p-i-1}}$. By the discussion preceding claim 1, we may assume that $\vec{m} \not\equiv \vec{0} \pmod{p}$. If $m_1 \equiv 0 \pmod{p}$ then choose maximal $k$ such that $m_1 \equiv m_2 \equiv \cdots \equiv m_k \equiv 0 \pmod{p}$, and set $k = 0$ if $m_1 \not\equiv 0 \pmod{p}$. Observe that $\sum_{j_k=k-1}^{j_{k+1}-1} \sum_{j_{k-1}=k-2}^{j_k-1} \cdots \sum_{j_1=0}^{j_2-1} 1$ is the number of $k$-tuples $0 \leq j_1 < \cdots < j_k \leq j_{k+1} - 1$, which is just

$$\binom{j_{k+1}}{k} = 1/k! j_{k+1}(j_{k+1}-1)\cdots(j_{k+1}-(k-1)).$$

Such an expression is suggestive of a coefficient occurring in the $k$th derivative of a polynomial of degree $j_{k+1}$. There are now three possible cases, depending on the value of $k$, involved in completing the proof of Proposition 5.2.

*Case* 1. $k = 0$. In this case

$$\begin{aligned} S'(\vec{m}) &= \sum_{j_i=i-1}^{p-1} j_i \zeta^{m_i j_i} \sum_{j_{i-1}=i-2}^{j_i-1} \zeta^{m_{i-1} j_{i-1}} \ldots \sum_{j_1=0}^{j_2-1} \zeta^{m_1 j_1} \\ &= (\zeta^{m_1} - 1)^{-1} \sum_{j_i=i-1}^{p-1} j_i \zeta^{m_i j_i} \sum_{j_{i-1}=i-2}^{j_i-1} \zeta^{m_{i-1} j_{i-1}} \ldots \sum_{j_2=1}^{j_3-1} \zeta^{m_2 j_2} (\zeta^{m_1 j_2} - 1) \\ &= (\zeta^{m_1} - 1)^{-1} (S(m_1 + m_2, m_3, \ldots, m_i) - S(m_2, \ldots, m_i)) \end{aligned}$$

which is 0 modulo $\pi^{(p-i)-1}$ by the induction hypothesis.

*Case* 2. $1 \leq k \leq i-2$. Now assume that $m_1 \equiv \cdots \equiv m_k \equiv 0 \pmod{p}$. By the observation above,

$$\begin{aligned} S'(\vec{m}) = \frac{1}{k!} \sum_{j_i=i-1}^{p-1} j_i \zeta^{m_i j_i} \sum_{j_{i-1}=i-2}^{j_i-1} \zeta^{m_{i-1} j_{i-1}} \\ \cdots \sum_{j_{k+1}=k}^{j_{k+2}-1} \zeta^{m_{k+1} j_{k+1}} j_{k+1}(j_{k+1}-1)\cdots(j_{k+1}-(k-1)). \end{aligned}$$

The same argument that gave us the equation $S(\vec{m}) = S'(\vec{m}) - S(\tilde{\vec{m}})$ can now be applied to the above equation for $S'(\vec{m})$. However, when we let the index $j_{k+1}$ take on the value $k-1$ we get $0$. Thus

$$S'(\vec{m}) = \frac{1}{k!} \sum_{j_i=i-2}^{p-1} j_i \zeta^{m_i j_i} \sum_{j_{i-1}=i-3}^{j_i-1} \zeta^{m_{i-1} j_{i-1}} \cdots \sum_{j_{k+1}=k-1}^{j_{k+2}-1} \zeta^{m_{k+1} j_{k+1}} j_{k+1}(j_{k+1}-1)\cdots(j_{k+1}-(k-1)).$$

The above reasoning may be applied $k-1$ more times to obtain

$$S'(\vec{m}) = \frac{1}{k!} \sum_{j_i=i-k-1}^{p-1} j_i \zeta^{m_i j_i} \sum_{j_{i-1}=i-k-2}^{j_i-1} \zeta^{m_{i-1} j_{i-1}} \cdots \sum_{j_{k+1}=0}^{j_{k+2}-1} \zeta^{m_{k+1} j_{k+1}} j_{k+1}(j_{k+1}-1)\cdots(j_{k+1}-(k-1)). \tag{5.6}$$

The summation corresponding to the index $j_{k+1}$ is strongly suggestive of a $k$th derivative. A few minor modifications will now allow us to use Lemma 5.3. In particular,

$$\begin{aligned}
&\sum_{j_{k+1}=0}^{j_{k+2}-1} \zeta^{m_{k+1} j_{k+1}} j_{k+1}(j_{k+1}-1)\cdots(j_{k+1}-(k-1)) \\
&\quad = \zeta^{m_{k+1} k} \sum_{j_{k+1}=0}^{j_{k+2}-1} \zeta^{m_{k+1}(j_{k+1}-k)} j_{k+1}(j_{k+1}-1)\cdots(j_{k+1}-(k-1)) \\
&\quad = \zeta^{m_{k+1} k} g_{j_{k+2}}^{(k)}(\zeta^{m_{k+1}}).
\end{aligned}$$

Now substitute the above equation into equation (5.6) and apply Lemma 5.3 to obtain

$$\begin{aligned}
S'(\vec{m}) = \zeta^{m_{k+1} k}/k! &\sum_{j_i=i-k-1}^{p-1} j_i \zeta^{m_i j_i} \sum_{j_{i-1}=i-k-2}^{j_i-1} \zeta^{m_{i-1} j_{i-1}} \cdots \sum_{j_{k+2}=1}^{j_{k+3}-1} \zeta^{m_{k+2} j_{k+2}} \\
&\cdot \left\{ \sum_{r=0}^{k-1} (-1)^r j_{k+2} \cdots (j_{k+2}-k+r+1) r! \right. \\
&\qquad \cdot \binom{k}{r} (\zeta^{m_{k+1}})^{j_{k+2}-k+r} (\zeta^{m_{k+1}}-1)^{-r-1} \\
&\qquad \left. + (-1)^k k! ((\zeta^{m_{k+1}})^{j_{k+2}} - 1)(\zeta^{m_{k+1}}-1)^{-k-1} \right\}.
\end{aligned} \tag{5.7}$$

Fix a value of $r$ in the interval $[0, k-1]$ and throw away the harmless (invertible) constants $\zeta^{m_{k+1}k}/k!$, $(-1)^r$, $r!$, $\binom{k}{r}$, and $(\zeta^{m_{k+1}})^{-k+r}$ found in the summands corresponding to this value of $r$. The altered summands corresponding to this value of $r$ now look like

$$(\zeta^{m_{k+1}}-1)^{-r-1}\sum_{j_i=i-k-1}^{p-1} j_i\zeta^{m_ij_i}\sum_{j_{i-1}=i-k-2}^{j_i-1}\zeta^{m_{i-1}j_{i-1}}$$
$$\cdots\sum_{j_{k+2}=1}^{j_{k+3}-1} j_{k+2}\cdots(j_{k+2}-k+r+1)\zeta^{m_{k+2}j_{k+2}}\zeta^{m_{k+1}j_{k+2}}$$

which, of course, equals

$$(\zeta^{m_{k+1}}-1)^{-r-1}\sum_{j_i=i-r-2}^{p-1} j_i\zeta^{m_ij_i}\sum_{j_{i-1}=i-r-3}^{j_i-1}\zeta^{m_{i-1}j_{i-1}}$$
$$\cdots\sum_{j_{k+2}=k-r}^{j_{k+3}-1} j_{k+2}\cdots(j_{k+2}-k+r+1)\zeta^{(m_{k+2}+m_{k+1})j_{k+2}}.$$

*Claim* 2. Define $S_{k,r}$ so that the above expression will be equal to $(\zeta^{m_{k+1}}-1)^{-r-1}S_{k,r}$, and set $m'=m_{k+2}+m_{k+1}$. Then

$$S_{k,r}\equiv(k-r)!S(\underbrace{0,\ldots,0}_{k-r\ 0\text{'s}},m',m_{k+3},\ldots,m_i)\qquad(\operatorname{mod}\pi^{p-(i-r-1)}).$$

*Proof*. Note first of all that

$$S(0,\ldots,0,m',m_{k+3},\ldots,m_i)$$
$$=S'(0,\ldots,0,m',m_{k+3},\ldots,m_i)-S(\underbrace{0,\ldots,0}_{k-r-1\ 0\text{'s!}},m',m_{k+3},\ldots,m_i).$$

The second term on the right-hand side of the above equation is congruent to 0 modulo $\pi^{p-(i-r-1)}$ by the induction hypothesis. On the other hand,

$$S'(0,\ldots,0,m',m_{k+3},\ldots,m_i)$$
$$=\sum_{j_{i-r-1}=i-r-2}^{p-1} j_{i-r-1}\zeta^{m_ij_{i-r-1}}\sum_{j_{i-r-2}=i-r-3}^{j_{i-r-1}-1}\zeta^{m_{i-1}j_{i-r-2}}$$
$$\cdots\sum_{j_{k-r+1}=k-r}^{j_{k-r+2}-1}\zeta^{m'j_{k-r+1}}\sum_{j_{k-r}=k-r-1}^{j_{k-r+1}-1}\sum_{j_{k-r-1}=k-r-2}^{j_{k-r}-1}\cdots\sum_{j_1=0}^{j_2-1}1$$
$$=\sum_{j_{i-r-1}=i-r-2}^{p-1} j_{i-r-1}\zeta^{m_ij_{i-r-1}}\cdots\sum_{j_{k-r+1}=k-r}^{j_{k-r+2}-1}\binom{j_{k-r+1}}{k-r}\zeta^{m'j_{k-r+1}}$$
$$=1/(k-r)!\sum_{j_{i-r-1}=i-r-2}^{p-1} j_{i-r-1}\zeta^{m_ij_{i-r-1}}\cdots\sum_{j_{k-r+2}=k-r+1}^{j_{k-r+3}-1}\zeta^{m_{k+3}j_{k}-r+2}$$
$$\cdot\sum_{j_{k-r+1}=k-r}^{j_{k-r+2}-1} j_{k-r+1}\cdots(j_{k-r+1}-(k-r-1))\zeta^{m'j_{k-r+1}}.\square$$

Referring now to Claim 2 and equation (5.7), we see that

$$S_{k,r}\equiv S'(0,\ldots,0,m',m_{k+3},\ldots,m_i)\qquad(\operatorname{mod}\pi^{p-(i-r-1)})$$
$$\equiv0\qquad(\operatorname{mod}\pi^{p-(i-r-1)}+\pi^{p-(i-r)}).$$

Thus

$$(\zeta^{m_{k+1}}-1)^{-r-1}S_{k,r}\equiv 0 \quad (\operatorname{mod}\pi^{p-(i-r)-(r+1)})\equiv 0 \quad (\operatorname{mod}\pi^{p-(i+1)}).$$

Finally, ignoring harmless unit multiplies, the sum

$$\begin{gathered}\zeta^{m_{k+1}k}/k!\sum_{j_i=i-k-1}^{p-1} j_i\zeta^{m_ij_i}\sum_{j_{i-1}=i-k-2}^{j_i-1}\zeta^{m_{i-1}j_{i-1}}\cdots\sum_{j_{k+2}=1}^{j_{k+3}-1}\zeta^{m_{k+2}j_{k+2}}\\ \cdot(-1)^k k!((\zeta^{m_{k+1}})^{j_{k+2}}-1)(\zeta^{m_{k+1}}-1)^{-k-1}\end{gathered}$$

is equal to

$$\pi^{-k-1}(S(m_{k+1}+m_{k+2},m_{k+3},\dots,m_i)-S(m_{k+2},m_{k+3},\dots,m_i)).$$

This expression is congruent to $0$ modulo $\pi^{p-(i-k)}$ by our induction hypothesis. Since $k\geq 1$ we now have $S(\vec{m})\equiv 0 \pmod{\pi^{p-(i+1)}}$ and Proposition 5.2 is proven for the case $1\leq k\leq i-2$.

*Case* 3. $k=i-1$. In this case,

$$\begin{aligned}S(0,0,\dots,0,m_i)&=\sum_{j_i=i}^{p-1}j_i\zeta^{j_im_i}\sum_{j_{i-1}=i-1}^{j_i-1}\sum_{j_{i-2}=i-3}^{j_{i-1}-i}\cdots\sum_{j_1=1}^{j_2-1}1\\ &=\sum_{j_i=i}^{p-1}j_i\zeta^{j_im_i}\binom{j_i-1}{i-1}\\ &=1/(i-1)!\sum_{j_i=i}^{p-1}j_i\cdots(j_i-(i-1))\zeta^{j_im_i} \qquad (5.8)\\ &=\zeta^{im_i}/(i-1)!\sum_{j_i=i}^{p-1}j_i\cdots(j_i-(i-1))(\zeta^{m_i})^{j_i-i}\\ &=\zeta^{im_i}/(i-1)!g_p^{(i)}(\zeta^{m_i}).\end{aligned}$$

Note now that

$$g_p(x)=(x^p-1)/(x-1)\equiv(x-1)^p/(x-1)\equiv(x-1)^{p-1}\quad(\operatorname{mod}\pi^{p-1}).$$

Thus

$$g_p^{(i)}(\zeta^{m_i})\equiv(-1)^i(i)!(\zeta^{m_i}-1)^{p-1-i}\equiv 0\quad(\operatorname{mod}\pi^{p-(i+1)}).$$

This completes the proof of Case 3, which in turn completes the proof of Proposition 5.2. □

A little review is now in order. We are dissecting the zero projection of expression (5.2)

$$\sum_{i=2}^{p-1}\pi^{i-1}\sum_{i,p}\prod_{k=1}^{i}{}^{t^{j_k}}(s^{p-1}+\cdots+1)x\qquad(\operatorname{mod}\pi^{p-1}\operatorname{rad}\Lambda^{\Omega}).$$

For each $i$ such that $2\leq i\leq p-1$, the summands in the zero projection of the $i$-fold products in the above expression can be collected according to the terms

$f(k, \vec{m}) = s^k s^{\sigma_{i-1}} x_{\sigma_{i-1}} \cdots x_{\sigma_1} x$. By Proposition 5.2, it is now known that the coefficients of these $f(k, \vec{m})$ are all $0$ modulo $\pi^{p-i}$. Recall congruence 5.1,

$$0 \equiv px + \sum_{i=2}^{p} \pi^{i-1} \sum_{i,p} \prod_{k=1}^{i} {}^{t^{j_k}}(s-1)^{p-1} x \qquad (\operatorname{mod} \pi^{p-1} \operatorname{rad} \Lambda^{\Omega}).$$

Proposition 5.2 tells us that for any $i$ between $2$ and $p-1$, the coefficient of any $f(k, \vec{m})$ in this congruence is $0$ modulo $\pi^{p-1}$. Not only that, but it is easy to see that all the $f(k, \vec{m})$ are congruent to $1$ modulo $\operatorname{rad} \Lambda^{\Omega}$.

Our ultimate goal is to prove Proposition 4.5 by showing that the expression $\sum_{i=2}^{p} \pi^{i-1} \sum_{i,p} \prod_{k=1}^{i} {}^{t^{j_k}}(s-1)^{p-1} x$ occurring in congruence 5.1 is $0$ modulo $\pi^{p-1} \operatorname{rad} \Lambda^{\Omega}$. This, of course, implies that $x \in \operatorname{rad} \Lambda^{\Omega}$. As we mentioned before, the $i = p$ summand poses no problem. The upshot of the above discussion is that we may assume $x = 1$ while trying to establish the congruence

$$\operatorname{pr}_0 \left( \sum_{i=2}^{p-1} \pi^{i-1} \sum_{i,p} \prod_{k=1}^{i} {}^{t^{j_k}}(s-1)^{p-1} x \right) \equiv 0 \qquad (\operatorname{mod} \pi^{p-1} \operatorname{rad} \Lambda^{\Omega}).$$

The spirit of the remainder of the proof is as follows: The various $t^{j_k}$ "almost" commute with the $(s-1)^{p-1}$'s. Suppose we took $t = 1$. Then

$$\sum_{i,p} \prod_{k=1}^{i} (s-1)^{p-1} = \binom{p}{i} (s-1)^{p-1} \equiv 0 \qquad (\operatorname{mod} \pi^{p-1} \operatorname{rad} \Lambda^{\Omega}).$$

Such thinking is wishful, but in light of congruence 5.3 (referring to the case $i = 2$) it is not totally unrealistic.

It now suffices to show that

$$\pi^{i-1} \sum_{m_{i-1}=0}^{p-1} S(m_1, m_2, \ldots, m_{i-1}) \equiv 0 \qquad (\operatorname{mod} \pi^{p-1} \operatorname{rad} \Lambda^{\Omega}).$$

However, an even better result is possible:

**Proposition 5.4.** *For* $p \geq 3$, $2 \leq i \leq p-1$,

$$\sum_{m_{i-1}=0}^{p-1} S(m_1, m_2, \ldots, m_{i-1}) = 0.$$

*Proof.* Suppose $i = 2$. First note that for any integer $e \not\equiv 0$ modulo $p$, $\sum_{k=0}^{p-1} (\zeta^e)^k = 0$. Thus

$$\sum_{m_1=0}^{p-1} \sum_{j_1=1}^{p-1} j_1 \zeta^{m_1 j_1} = \sum_{j_1=1}^{p-1} j_1 \sum_{m_1=0}^{p-1} \zeta^{m_1 j_1} = 0.$$

Proceed now by induction on $i$. We must show that

$$\sum_{m_i=0}^{p-1} S(m_1, m_2, \ldots, m_i) = 0.$$

*Case* 1. $m_1 \neq 0$. Note that we may assume by the induction hypothesis that $\sum_{m_{i-1}=0}^{p-1} S(\vec{m}) = 0$ for any $i-1$-dimensional vector $\vec{m}$. Thus we have

$$\begin{aligned}
&\sum_{m_i=0}^{p-1} S(m_1, m_2, \dots, m_i) \\
&\quad = \sum_{m_i=0}^{p-1} (S'(m_1, m_2, \dots, m_i) - S(m_2, m_3, \dots, m_i)) \\
&\quad = \sum_{m_i=0}^{p-1} \left( \sum_{j_i=i-1}^{p-1} j_i \zeta^{j_i m_i} \dots \sum_{j_2=1}^{j_3-1} \zeta^{j_2 m_2} \left( \frac{(\zeta^{m_1})^{j_2} - 1}{\zeta^{m_1} - 1} \right) \right) \\
&\quad = \frac{1}{\zeta^{m_1} - 1} \sum_{m_i=0}^{p-1} (S(m_1 + m_2, m_3, \dots, m_i) - S(m_2, m_3, \dots, m_i)) \\
&\quad = 0.
\end{aligned}$$

*Case* 2. $m_1 = m_2 = \cdots = m_k = 0$, $1 \leq k \leq i-2$. In this case, we now have

$$\begin{aligned}
&\sum_{m_i=0}^{p-1} S(0, \dots, 0, m_{k+1}, \dots, m_i) \\
&\quad = \sum_{m_i=0}^{p-1} (S'(0, \dots, 0, m_{k+1}, \dots, m_i) - S(\underbrace{0, \dots, 0}_{k-1 \text{ 0's}}, m_{k+1}, \dots, m_i)) \\
&\quad = \sum_{m_i=0}^{p-1} \left( \sum_{j_i=i-1}^{p-1} j_i \zeta^{m_i j_i} \dots \sum_{j_{k+1}=k}^{j_{k+2}-1} \zeta^{m_{k+1} j_{k+1}} \binom{j_{k+1}}{k} \right).
\end{aligned}$$

The same argument involving the $S_{k,r}$'s used in the proof of Case 2 of Proposition 5.2 may now be applied to reduce the above expression to a sum of expressions, each of which satisfies the induction hypothesis. This completes the proof of Case 2.

*Case* 3. $m_1 = m_2 = \cdots = m_{i-1} = 0$. Referring to equation (5.8), we now have

$$\sum_{m_i=0}^{p-1} S(0, 0, \dots, 0, m_i) = 1/(i-1)! \sum_{m_i=0}^{p-1} \zeta^{i m_i} g_p^{(i)}(\zeta^{m_i}).$$

Since $g_p(x) = 1 + x + \cdots + x^{p-1}$, the $i$th derivative will be $\sum_{k=0}^{p-i-1} \frac{(i+k)!}{k!} x^k$. Thus

$$\begin{aligned}
1/(i-1)! \sum_{m_i=0}^{p-1} \zeta^{i m_i} g_p^{(i)}(\zeta^{m_i}) &= 1/(i-1)! \sum_{m_i=0}^{p-1} \zeta^{i m_i} \sum_{k=0}^{p-i-1} \frac{(i+k)!}{k!} \zeta^{m_i k} \\
&= \sum_{k=0}^{p-1-i} i \binom{k+i}{i} \sum_{m_i=0}^{p-1} \zeta^{(i+k) m_i}.
\end{aligned}$$

Note now that $\sum_{m_i=0}^{p-1} \zeta^{(i+k) m_i} = 0$ unless $i + k \equiv 0 \pmod{p}$. However, $2 \leq i + k \leq p-1$. The proof of Case 3 is now complete, which in turn completes the proof of Proposition 5.4. □

*A brief digression.* Much energy was spent in this chapter dissecting the expression

$$M = \sum_{i=2}^{p-1} \pi^{i-1} \sum_{i,p} \prod_{k=1}^{i} {}^{t^j k}(s^{p-1} + \cdots + 1)x.$$

Letting $\vec{m} = (m_1, \ldots, m_{i-1})$ and defining $\sigma_l = m_1 + m_2 + \cdots + m_l$, it was shown that the coefficient of $f(k, \vec{m}) = s^k s^{\sigma_{i-1}} x_{\sigma_{i-1}} x_{\sigma_{i-2}} \cdots x_{\sigma_1} x$ in the above expression is

$$\sum_{j_{i-1}=i-1}^{p-1} (1 + \zeta^{\sigma} + \cdots + \zeta^{\sigma(p-1-j_{i-1})}) \zeta^{m_{i-1} j_{i-1}} \sum_{j_{i-2}=i-2}^{j_{i-1}-1} \zeta^{m_{i-1} j_{i-1}} \cdots \sum_{j_1=1}^{j_2-1} \zeta^{m_1 j_1}$$

which we denote by $S(k, \vec{m})$. It is easy to see that

$$\mathrm{pr}_l(M) \equiv \sum_{i=2}^{p-1} \pi^{i-1} \sum_{\mathscr{E}} S(\rho_l(\vec{m}), \vec{m}) f(\rho_l(\vec{m}), \vec{m}) \qquad (\operatorname{mod} \pi^{p-1} \operatorname{rad} \Lambda_0)$$

where $\mathscr{E} = \{(m_1, m_2, \ldots, m_{i-1})\colon 0 \le m_1, \ldots, m_{i-1} \le p-1\}$ as before, and where $\rho_l(\vec{m})$ is defined to be the unique value of $k \in [0, p-1]$ such that $\sigma = \sigma_{i-1} + k \equiv l \pmod{p}$. Arguments similar to those used in the proofs of Propositions 5.2 and 5.4 can also be used to obtain the following results:

**Proposition 5.5.** *Assume* $p > 2$. *Then for any fixed* $i$ *with* $2 \le i \le p-1$, *the coefficients* $\sum(k, \vec{m})$ *are all congruent to* $0$ *modulo* $\pi^{p-i}\Lambda_0$.

**Proposition 5.6.** *Assume* $p > 2$. *Then for any* $l \ge 0$

$$\sum_{m_{i-1}=0}^{p-1} S(\mathrm{pr}_l(\vec{m}), \vec{m}) = p.$$

*Completion of the proof of Proposition* 4.5. The results in this chapter have been directed toward analyzing congruence (5.2),

$$0 \equiv px + \sum_{i=2}^{p} \pi^{i-1} \sum_{i,p} \prod_{k=1}^{i} {}^{t^j k}(s-1)^{p-1}x \qquad (\operatorname{mod} \pi^{p-1} \operatorname{rad} \Lambda^{\Omega}).$$

Proposition 5.4 allows us to deduce that the $0$ projection of the expression

$$\sum_{i=2}^{p} \pi^{i-1} \sum_{i,p} \prod_{k=1}^{i} {}^{t^j k}(s-1)^{p-1}x$$

is in fact congruent to $0$ modulo $\pi^{p-1} \operatorname{rad} \Lambda^{\Omega}$. We may immediately conclude that $x \in \operatorname{rad} \Lambda^{\Omega}$, thus completing the proof of Proposition 4.5. □

*Completion of the proof of Theorem* 1.2. Once we have $x \in \operatorname{rad} \Lambda^{\Omega}$, the argument used in §3 may be applied to complete the proof of the theorem. □

## 6. Future directions

I. Proposition 5.2 shows that if $\gamma(t) = (s-1)^{p-1}x + \pi^n y + \pi\lambda_f$ where $x \in \Lambda_0$, $y \in \Lambda_0 \oplus \Lambda_\zeta$, $n \ge p-1$, and $\mathrm{pr}_s(\lambda_f) \in \pi^{p-2}\Lambda_f$, then $x$ must be in $\operatorname{rad} \Lambda^{\Omega}$. Using this knowledge, it seems likely that one could show that $x$ is actually in some higher power of $\operatorname{rad}\Lambda^{\Omega}$. Just how far one can go in this direction will require additional analysis of the congruence

$$0 \equiv \operatorname{pr}_{0+\zeta}\left[px + \sum_{i=2}^{p} \pi^{i-1} \sum_{i,p} \prod_{k=1}^{i} {}^{t^j k}((s-1)^{p-1}x + \pi\lambda_f)\right] \quad (\operatorname{mod} \pi^{p-1} \operatorname{rad}^e \Lambda^{\Omega})$$

where $e$ would be 2 for starters. Once again one could replace $(s-1)^{p-1}$ with $1+s+\cdots+s^{p-1}$ and organize terms according to coefficients of $s^{\sigma}$ where $\sigma$ would be reduced $\operatorname{mod} p$. The most delicate part of this analysis would be controlling the long $\operatorname{pr}_0$ part of the product of two other long parts.

II. It is not to hard to show that $\Lambda/\pi\Lambda$ is a local Artinian ring. It follows that every normalized unit in $\Lambda$ is torsion modulo $\pi\Lambda$. If one lets $u = (1+\pi\gamma(u, g))g$ where $g \in G$ then one can show, as in §2, that

$$\gamma(uv, gh) = \gamma(u, g) + {}^{g}\gamma(v, h) + \pi\gamma(u, g){}^{g}\gamma(v, h).$$

It is possible now to apply some of the techniques and results of §§2 through 5 even to a nontorsion unit $u$, especially in the case of group rings $SG$ over groups of order $p^3$. In this particular case, it is possible much of the time to conjugate $u$ into a commutative subring of $SG$.

III. What other, more general, results can be developed with the proof of Theorem 1.2? What hypotheses can be relaxed? In light of Proposition 1.2.4 and the Appendix of [RS2] it seems likely that it suffices to assume $S$ is a local or semilocal Dedekind domain of characteristic zero with a unique maximal ideal containing $p$, as in the hypothesis of Theorem 1.1. Also, it is possible to define a different augmentation map $\varepsilon: \mathscr{A} \to S$ via $\sum_{i,j} s_{i,j}(y_i \otimes g_j) \mapsto \sum_{i,j} s_{i,j}$. This new choice for $\varepsilon$ gives more elements of augmentation $1$. It is necessary now to insure that there exists some $H \leq G$ and some unit $z \in \mathscr{A}$ such that ${}^{z}U \equiv H$ modulo $(c-1)\mathscr{A}$.

The above considerations now suggest the following environment in which it seems the methods of §§2 through 5 may be applied:

(1) $S$ is a commutative local ring of characteristic zero with unique maximal ideal $\wp$ containing $p$.
(2) $\mathscr{A}$ is a local, $S$-algebra that is finitely generated as an $S$-module with basis $\mathscr{B}_1$.
(3) There are groups $H$ and $\Omega$ such that $H \subseteq \mathscr{B}_1$, $H$ is a $p$-group, $[H, \Omega] = p$, and there exists some $c \in H \cap Z(\mathscr{A})$ such that $c^p = 1$.
(4) $H$ acts on $\mathscr{B}_1$ by multiplication on both the left and the right.

**Wishful thought 6.3.** Let $\mathscr{A}$, $S$, $H$, ... be given as above. Suppose that there is a group $U \subseteq \mathscr{A}$ such that

(i) $\Omega \leq U$;
(ii) There exists a function $\gamma: H \to \Lambda$ such that $g \mapsto (1+\pi\gamma(g))g$ defines an isomorphism between $H$ and $U$;
(iii) $\gamma|_{\Omega} = 0$.

Then $U$ is conjugate to $H$ in $\mathscr{A}$.

**Conjecture 6.4.** Let $S$ be a complete, discrete valuation ring of characteristic 0 having maximal ideal $\wp$ containing $p$. Let $\mathscr{A}$ be a local $S$-algebra that is also finitely generated as an $S$-module. Let $\mathscr{B}_1$, $H$, $\Omega$, $c$, be given as in the list above. Finally, let $U$ be a subgroup of $\mathscr{A}^*$ such that $|U| = |H|$, $\Omega \trianglelefteq U$, and $U \equiv H$ modulo $(c-1)\mathscr{A}$. Then $U$ is conjugate to $H$ in $\mathscr{A}$.

*A brief comment on Conjecture* 6.4. Some progress has been made on Conjecture 6.4. The arguments in §§1, 2, and 3 all seem to hold. However, there is now some difficulty taking proper advantage of the multiplicative relationships hidden in the module decomposition $\Lambda^{\Omega} = \Lambda_0 \oplus \Lambda_{\zeta} \oplus \Lambda_f$. It is likely that some more hypotheses will be needed to generate the identity $\Lambda_i = s^i\Lambda_0$ and to retain the conclusions of Lemmas 4.1 and 4.2. Theorem 1.2, of course, provides a setting where these difficulties can be overcome.

## References

[CR1] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Wiley Interscience, 1962.

[CR2] ——, *Methods of representation theory*, vol. 1, Wiley Interscience, 1962.

[D] E. C. Dade, *Deux groups finis ayant le même algèbre de groupe sur tout corps*, Math. Z. **119** (1971).

[Hi] G. Higman, *Units in group rings*, D. Phil. thesis, Oxford Univ., 1940.

[Hu] T. W. Hungerford, *Algebra*, Holt, Rhinehart, and Winston, 1974.

[K] G. Karpilovsky, *Unit groups of classical rings*, Oxford Univ. Press, 1988.

[M] H. Matsumura, *Commutative ring theory*, Cambridge Univ. Press, 1986.

[R1] K. W. Roggenkamp, *Picard groups of integral group rings of nilpotent groups*, Proc. Sympos. Pure Math., vol. 47, Amer. Math. Soc., Providence, R.I., 1987, pp. 477–486.

[R2] ——, *Subgroup rigidity of p-adic group rings*, preprint, June, 1989.

[RS1] K. W. Roggenkamp and L. L. Scott, *The isomorphism problem for integral group rings of finite nilpotent groups*, Proc. of Groups-St. Andrews 1985, Cambridge Univ. Press, 1986.

[RS2] ——, *Isomorphisms of p-adic group rings*, Ann. of Math. (2) **126** (1987), 593–647.

[RS3] ——, *On a conjecture of Zassenhaus for finite group rings*, preprint (submitted).

[S] L. L. Scott, *Recent progress on the isomorphism problem*, Proc. Sympos. Pure Math., vol. 47, Amer. Math. Soc., Providence, R.I., 1987, pp. 259–274.

[Se] S. K. Sehgal, *Topics in group rings*, Marcel Dekker, 1978.

[T] G. Thompson, *Subgroup rigidity in group rings*, Ph.D. thesis, Univ. of Virginia, 1990.

[W] A. Weiss, *Rigidity of p-adic p-torsion*, Ann. of Math. (2) **127** (1988), 317–332.

[We] E. Weiss, *Algebraic number theory*, McGraw-Hill.

[Wh] A. Whitcomb, *The group ring problem*, Ph.D. thesis, Univ. of Chicago, 1968.

Virginia Commonwealth University, Box 2014, Richmond, Virginia 23284-2014
*E-mail address*: gthompso@cabell.vcu.edu