Isomorphisms of $p$-adic group rings

By Klaus Roggenkamp and Leonard Scott*

A long-standing problem, first posed by Graham Higman [15] and later by Brauer [4] is the "isomorphism problem for integral group rings." Given finite groups $G$ and $H$, is it true that $\mathbb{Z}G \cong \mathbb{Z}H$ implies $G \cong H$? Many authors have worked on this question, but progress has been difficult [30]. Perhaps the best positive result was that of Whitcomb in 1968 [37], who showed that the implication $G = H$ holds for $G$ metabelian. Dade [9] showed there were counterexamples, even in the metabelian case, if $\mathbb{Z}$ were replaced by the family of all fields. Some mathematicians came to believe the problem was a kind of grammatical accident, that counterexamples for $\mathbb{Z}$ were surely there, if difficult to find.

We ourselves began this investigation looking for counterexamples, but found that they were indeed very difficult to find, much more difficult than we had anticipated. Slowly we began to believe that at least some exciting positive results were possible.

In this paper we answer the isomorphism problem for finite $p$-groups over the $p$-adic integers $\mathbb{Z}_p = \mathbb{Z}_{(p)}$, and in a very strong way: In the normalized units (augmentation 1) of $\mathbb{Z}_pG$ there is only one conjugacy class of groups of order $|G|$. This answers the isomorphism problem in the affirmative (for finite $p$-groups $G$, over $\mathbb{Z}$ or $\mathbb{Z}_p$) and in addition computes the entire Picard group [2] of the category of $\mathbb{Z}_pG$-modules in terms of automorphisms of $G$. Similarly we are able to settle the isomorphism problem for finite nilpotent groups and compute the associated semilocal Picard groups. We also treat more general coefficient domains: namely, integral domains $S$ of characteristic 0 in which no (rational) prime divisor of the group order is invertible, for the $SG$ isomorphism problem, and treat similar semilocal Dedekind domains for the Picard group computations. The Zassenhaus conjecture concerning the rational behavior of group ring automorphisms is verified for the nilpotent case in this general setting (cf. Corollary 3 below). Over $\mathbb{Z}$, we announce a positive answer to the isomorphism

*The authors gratefully acknowledge the support of NSF, DFG, Thyssen Stiftung, SERC, Queen Mary College, and the Center for Advanced Studies at the University of Virginia, while writing this paper.
problem for finite groups which are abelian by nilpotent, and give the proof in a special case (Corollary 5).

One general context of the isomorphism problem is the theory of isomorphisms and automorphisms of the general arithmetic or $p$-adic group, such as the group of units of an order. Though some critical ingredients of our proof, described below, naturally depend on the special context of group rings, the philosophy and some techniques could be of use in other situations. In particular, we prove a general result, Theorem 2, cf. Chapter 5, in the spirit of research begun by Fröhlich [12, Thm. 9] on automorphisms of $\mathbb{Z}_p$-orders (asserting that an automorphism trivial on an apparently "small" quotient of the order must in fact be inner).

The proof of the main result really begins with the observation (1.4.1) that $H^1(G, SG) = 0$ for the conjugation action of $G$ on $SG$, if $G$ is a finite group and $S$ an integral domain of characteristic 0. As a consequence, all derivations of the associative $S$-algebra $SG$ to itself are inner. Now questions about isomorphisms tend to reduce to questions about automorphisms, either inductively, cf. Chapter 2, or by looking at products ([20], as mentioned after Corollary 3 below). The above property of derivations, however, suggests a recipe for showing a given automorphism $\alpha$ of $SG$ is inner: First take the logarithm of $\alpha$, if possible, and show $\log \alpha$ is a derivation. Then apply the above property to obtain $\log \alpha = \text{ad} \ a$ (the map $x \mapsto ax - xa$) for some $a \in SC$. Then form $\exp a$, if possible, and try to show $\alpha$ is conjugation by $\exp a$.

If $S = \mathbb{Z}_p$, for example, then infinite series make sense, but there is no reason for $\log \alpha$ to exist or stabilize $SG$. For $G$ a finite $p$-group we can arrange inductively that $\alpha$ is trivial modulo $(c - 1)SG$ for $c$ a central element of order $p$ in $G$. One could form $\log \alpha$ at this point and write $\log \alpha = \text{ad} \ a$, but $\exp a$ need not exist, and efforts to get around this are hampered in particular by the fact that $c - 1$ is a zero divisor. So in Chapter 2 we translate the whole question into a problem concerning an automorphism $\alpha$ of a quotient order $\Lambda$ in which the image $\pi$ of $c - 1$ is not a zero divisor. The crucial derivation property is partially retained, in that $\pi$ multiples of derivations are inner. To get an idea where matters sit at this point, we have (after a small modification, in the spirit of Higman [15]) that

$$\alpha = 1 + \pi \phi,$$

where $\phi \in \text{End}_S \Lambda$ satisfies $\phi(\Lambda) \subseteq \text{rad} \ \Lambda$ (in the basic $S = \mathbb{Z}_p$ case). If one knew $\phi(\Lambda) \subseteq \text{rad}^2 \Lambda$, or even $\phi^n(\Lambda) \subseteq \text{rad}^2 \Lambda$ for some $n > 0$, then a general argument with logarithms (see Theorem 2 and its self-contained proof in Chapter 5) would complete the proof in spite of the difficulties with the exponential.

Some time before obtaining the general $p$-group case we were able to treat a class 2 $p$-group case (cf. [27], and the remarks following Corollary 4 for a
ISOMORPHISMS OF $p$-ADIC GROUP RINGS

by exhibiting the close connection between the Lie $p$-algebra structure of (a grading of) $G$ and a nondegenerate bilinear form associated naturally to critical sections of $\text{rad } \Lambda / \text{rad}^2 \Lambda$. The idea here is to work modulo $\pi \text{ rad}^2 \Lambda$ and find sufficiently strong conditions satisfied by the automorphism in question to force it into an obvious family of inner automorphisms. Using the natural induced module structure on a related section of the group ring, we were also able to use transfer. These arguments, slightly generalized, now comprise Chapter 4. To be in a position to apply them, however, one must know $\alpha$ is trivial on a large subgroup of $G$. This is the task of the very hard induction in Chapter 3. Essentially, one picks carefully an element just above the part of $G$ fixed by $\alpha$ and analyzes $\phi$ as an additive 1-cocycle on sections of $\Lambda$ natural with respect to $t$. The goal, of course, is to make $\alpha$ very slowly look more like the identity on $t$. The connection (on sections) between multiplicative and additive 1-cohomology for a group acting on a ring is a key theme.

Another general context of the isomorphism problem is the theory of conjugacy classes of finite subgroups in arithmetic and $p$-adic groups. Unfortunately, beyond the case $|H| = |G|$, we know very little about the finite subgroups of the normalized units of $\mathbb{Z}_p G$ for $G$ a finite $p$-group. Results of Quillen [24] describe the cohomology variety of this unit group in terms of the conjugacy classes of its finite elementary abelian $p$-subgroups, but we have been unable to formally identify this variety to that associated with $G$.\footnote{Recently, however, we have obtained some evidence for such an identification in case $G$ is a finite 2-group. Added in revision: In fact for $p = 2$ we have proved ([38], [39]) every finite $p$-subgroup of normalized units in $\mathbb{Z}_p G$ is conjugate to a subgroup of $G$, and have conjectured this is true for all $p$ [40]. An appendix to [40] suggests a proof in this generality, though we have not felt ready to claim the full result. Added in proof: Indeed A. Weiss of the University of Alberta has independently proved this subgroup theorem for all $p$. His work will appear in this journal.} If our result for $|H| = |G|$ could be explained by some kind of geometric “fixed-point” theorem, then one would expect every finite $p$-subgroup of normalized units would be conjugate to a subgroup of $G$. This is an important question, deserving further study. We point out that at least one has $H^1(H, \mathbb{Z}_p G) = 0$ under the conjugation action, for $H$ any subgroup of $G$. With $\mathbb{Z}_p G$ as a kind of integral form for a Lie algebra, this is analogous to the rigidity condition of Weil for discrete subgroups of Lie groups, a condition which does indeed restrict the conjugacy classes of these discrete groups. There is some potential here for a general theory.

The main results are all stated below, and some standard results are collected in Chapter 1. In some cases a useful commutative algebra result (see the appendix) simplifies the proofs. We also prove all the corollaries in this chapter. The remainder of the paper has been summarized above, but it should be pointed out that this paper evolved from a basic version treating the $\mathbb{Z}_p$ case.
for $p$-groups. The changes required for the general case were not easy to find, and even more difficult to incorporate unobtrusively into the original manuscript. A number of remarks on the basic $\mathbb{Z}_p$-case have been included to help keep the paper recognizable to those who checked through parts of the original version, and we hope they will provide other readers with some insight regarding the architecture of the proof.

We would in particular like to take this opportunity to thank Bob Sandling for reading the first version of the critical Chapter 3. We would also like to thank David Carter and Wolfgang Kimmerle for helpful comments, and Everett Dade and John Alperin for relevant conversations. Special thanks are also due to Everett Dade for many corrections and useful remarks concerning the final manuscript.

This paper is dedicated to Donald Coleman, who introduced the second author as an undergraduate to the study of finite group rings many years ago, and to Irving Reiner, who patiently supervised the first author's thesis on integral representations.

**Statements of the main results**

The main theorem is:

**Theorem 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, $S = \mathbb{Z}_p$). 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 $SG$.

The special case (to which the proof reduces inductively), where $H = \alpha(G)$ for an augmentation preserving $S$-algebra automorphism $\alpha$ of $SG$, is stated as Corollary 1 in Chapter 2 and not further restated here.

Examples based on Corollary 4 below show that the assumption in Theorem 1 regarding a unique maximal ideal containing $p$ is necessary (though of course always satisfied in the local case).

Apparently the first mathematicians to even speculate about a result like Theorem 1 were Berman and Rossa [3]. Our suspicions were first voiced in [32]. Whitcomb [37] was aware in a basic case that the theorem was implied by Corollary 1 [19, p. 341]. According to [30], he attributes the philosophy to his thesis advisor, John Thompson. Some special cases of the corollary, dealing with

---

2 We regret to report that Professor Reiner passed away on October 28, 1986, and that S. D. Berman died on February 22, 1987.
metacyclic $p$-groups, had been proved by Sekiguchi and his collaborators [10], [35], following up on Fröhlich [12].

Any Noetherian integral domain of characteristic 0 in which $p$ is not invertible is contained in a local domain satisfying the hypothesis of the theorem. (See the appendix to this paper.) Consequently, the theorem implies an affirmative answer to the isomorphism problem for finite $p$-groups over the original domain. For example, we might start with $\mathbb{Z}$ and note $\mathbb{Z} \subseteq \mathbb{Z}_p$. The $p$-group case for $\mathbb{Z}$ was known to imply an affirmative answer as well to the isomorphism problem over $\mathbb{Z}$ for finite nilpotent groups. We prove a very general version of this:

**Corollary 2.** Let $G$ be a finite nilpotent group and $S$ an integral domain of characteristic 0 in which no prime divisor of $|G|$ is invertible. Let $H$ be a finite group for which the category of $SG$-modules is $S$-linearly equivalent to the category of $SH$-modules (as occurs if $SC \sim SH$ as $S$-algebras, or if a full matrix algebra over $SG$ is $S$-isomorphic to a full matrix algebra over $SH$). Then $G \cong H$.

In the proof we show $SG \cong \tilde{SH}$ where $\tilde{S}$ is a semilocal Dedekind domain containing the subring of $S$ generated by the relevant coefficients, satisfying the same hypotheses. This reduction works for any finite group $G$ in the presence of an equivalence of categories.

The next result has been conjectured by Zassenhaus to hold for all finite groups (for $S = \mathbb{Z}$). It was verified for class 2 groups by Sehgal [33]. The same result is in Whitcomb [37], and Saksonov [29] proved the class 2 result for $p$-groups with $S$ as below. This conjecture has been central to our thinking about the isomorphism problem, at first as a tempting target for counterexamples, but later as a guide in the formulation of Theorem 1. Note that for $G$ a $p$-group and $S$ local, the theorem is just a strong reformulation of the Zassenhaus conjecture, though much more suitable for induction, as this paper demonstrates.

**Corollary 3 (Zassenhaus conjecture in the nilpotent case).** Let $G$ be a finite nilpotent group and $S$ an integral domain of characteristic 0 in which no prime divisor of $|G|$ is invertible. Let $H$ be a finite group of normalized units in $SG$ for which $|H| = |G|$. Then $H$ is conjugate to $G$ by a unit in $KG$, where $K$ is the quotient field of $S$.

W. Kimmerle has observed [20] that it is not really weaker in the Zassenhaus conjecture to consider the cases when $H$ is known to be isomorphic to $G$, since in any event one knows $H \times G$ is isomorphic to $G \times H$, and one can then argue that a suitable unit in $K(G \times H) \cong KG \otimes KKH$ carries $G$ into a copy of $H$. The same philosophy was very useful in guiding us to the “equivalence” formulation of Corollary 2, since the argument applies well to matrices.
over $SG$. The method also gives an alternate approach to the reduction in
Chapter 2 of Theorem 1 to Corollary 1.

Also, it makes no difference to assume $S$ is semilocal Dedekind (and thus, of
course, a principal ideal domain), because of the reduction afforded by the
appendix.

In the next corollary we describe the Picard group of $SG$ under the
hypotheses of Corollary 3 and the additional assumption that $S$ is semilocal
Dedekind. We view this as one of the main achievements of this paper.

We recall that, in such a semilocal situation,

$$\text{Pic}_SG \equiv \text{Out}_SG,$$

the outer automorphism group of $SG$. (See (1.2.9) in Chapter 1 below.) Follow-
ing Sandling [30] we define $n\text{Out}_SG$ to be the image in $\text{Out}_SG$ of the
normalized (augmentation-preserving) automorphisms of $SG$, and $n\text{Pic}_SG$ the
corresponding subgroup of $\text{Pic}_SG$. As is well-known, it is very easy to describe
$\text{Out}_SG$ in terms of $n\text{Out}_G(G)$: For each group homomorphism $\nu: G \to S^\times$ (the
units in $S$) there is an automorphism of $SG$ sending $g \in G$ to $\nu(g)$; such an
automorphism is normalized (or inner) if and only if it is trivial. Moreover, every
automorphism $\alpha$ of $SG$ can be written as the product of a normalized
automorphism and an automorphism associated with $\nu$ (namely, $\nu = \varepsilon \circ \alpha$
where $\varepsilon$ is the augmentation, cf. (1.1.1)). In this way we get a product
decomposition

$$\text{Out}_SG \equiv \text{Hom}_{\text{group}}(G, S^\times) \cdot n\text{Out}_SG.$$  

Multiplication can easily be given explicitly using (1.1.1). Neither factor is
obviously normal. (However, for nilpotent groups, Corollary 3 implies the left
factor is normal and centralized by the term Outcent $SG$ in (0.3).)

Now, following Fröhlich [12], put Outcent $SG = \text{Out}_{Z(SG)}SG$, regarding $SG$
as an algebra over its center $Z(SG)$. The group Outcent $SG$ is normal in $\text{Out}_SG$
(since it is the kernel of the action of the latter on $Z(SG)$) and contained in
$n\text{Out}_SG$. In fact any automorphism representing an element of Outcent $SG$ is
inner on $KG$, where $K$ is the quotient field of $S$, by the Skolem-Noether theorem.
Conversely, the automorphisms of $SG$ arising from inner automorphisms of $KG$
are all central (represent elements of Outcent $SG$).

So far, the discussion of $\text{Out}_SG$ is valid for an arbitrary finite group $G$. For
$G$ nilpotent, however, Corollary 3 (the Zassenhaus conjecture) tells us now that

$$n\text{Out}_SG = (\text{Outcent } SG)(\text{Out } G)$$

where $\text{Out } G$ is the outer automorphism group of $G$, viewed as a subgroup of
$\text{Out}_SG$. It is a consequence of a theorem of Fröhlich [12, Thm. 9] and Donald
Coleman’s fundamental result [6] for modular p-group algebras, that the natural
map $\text{Out } G \to \text{Out}_SG$ is indeed an embedding in the nilpotent case. (The question for general finite groups is apparently open.)

The intersection $\text{Outcent } G = (\text{Outcent } SG) \cap \text{Out } G$ is, modulo inner automorphisms of $G$, the group of automorphisms of $G$ stabilizing the conjugacy classes of $G$. (Cf. for instance Sah [28] for examples. The group $\text{Outcent } G$ is denoted there and elsewhere in the literature as $\text{Out}_G$. Hence to achieve our original goal of describing $\text{Pic}_SG \cong \text{Out}_SG$, we need only describe $\text{Outcent } SG$.

**COROLLARY 4.** Let $G$ be a finite nilpotent group, $S$ a semilocal Dedekind domain of characteristic 0 in which no prime divisor of $|G|$ is invertible. For each maximal ideal $\mathfrak{p}$ of $\mathbb{Z}(SG)$, let $B(\mathfrak{p})$ denote the localization (as a $\mathbb{Z}(SG)$-algebra) of $SG$ at $\mathfrak{p}$, and $D(\mathfrak{p})$ the Sylow $p$-subgroup of $G$ for the unique rational prime $p \in \mathfrak{p}$. (One knows the $\mathfrak{p}$'s and $B(\mathfrak{p})$'s explicitly, cf. below.) Then

a) $\text{Outcent } SG \cong \prod_{\mathfrak{p}} \text{Outcent } B(\mathfrak{p})$, via the natural projections, and

b) $\text{Outcent } B(\mathfrak{p}) \cong \text{Outcent } D(\mathfrak{p})$ for each $\mathfrak{p}$, and so depends only on $p \in \mathfrak{p}$. The inverse of the isomorphism is the natural composite

$\text{Outcent } D(\mathfrak{p}) \to \text{Outcent } G \to \text{Outcent } SG \to \text{Outcent } B(\mathfrak{p})$.

In particular

$$\text{Outcent } SG \cong \prod_{\mathfrak{p} \in \text{Max } \mathbb{Z}(SG)} \text{Outcent } D(\mathfrak{p}).$$

Also

$$n \text{Out}_SG = (\text{Outcent } SG)(\text{Out } G),$$

with the intersection of the last two factors equal to the natural "diagonal" copy of $\text{Outcent } G$ in the product.

The maximal ideals $\mathfrak{p}$ of $\mathbb{Z}(SG)$ are easy to describe: The nonzero ideal $\mathfrak{p} \cap \mathbb{Z}$ is prime, hence of the form $p\mathbb{Z}$ for some rational prime $p$. Let $D$ be a Sylow $p$-subgroup of $G$, and write $G = D \times D'$ where $D'$ is a $p'$-group. Since the augmentation ideal $I(SD)$ of $SD$ is nilpotent modulo $p$, the intersection $\mathbb{Z}(SG) \cap I(SD)SG$ is contained in $\mathfrak{p}$. Hence $\mathfrak{p}$ is determined by its image in $\mathbb{Z}(SG)/\mathbb{Z}(SG) \cap I(SD)SG \cong \mathbb{Z}(SD')$. Let $S(p) = \mathbb{Z}_{(p)}$, $S$ be the Dedekind domain obtained from $S$ by inverting the elements of the latter which are prime to $p$. The maximal ideals above $p$ in $\mathbb{Z}(SD')$ are determined by the quotient $\mathbb{Z}(SD')/p\mathbb{Z}(SD')$, which remains the same if $S$ is replaced by $S(p)$. However, $S(p)D'$ is a maximal order in the semisimple $K$-algebra $KD$, where $K$ is the quotient field of $S$, as is well-known. (The group order $|D'|$ is invertible in $S(p)$.) Hence $Z(S(p)D')$ is also a maximal order in $Z(KD')$, and so may be simply

---

3According to a result of J. Krempa, the kernel is at worst an elementary abelian 2-group when $S = \mathbb{Z}$. This result appears in a preprint "Group automorphisms inducing the identity map on cohomology" by S. Jackowski and Z. Marcinials of the University of Warsaw.
described as the integral closure of $S(p)$ in the latter (or equivalently, as a suitable localization of the integral closure of $S$). The center $Z(KD')$ of a finite group algebra over a field $K$ of characteristic 0 may be regarded as relatively well-understood: It is a direct product $\prod Z(M)$ of the centers of the simple components $M$ of $KD'$, with $Z(M)$ generated over $K$ by the traces (character values) of the elements of $D'$ in the matrix algebra

$$M \otimes_{Z(M)} \bar{K},$$

where $\bar{K}$ is an algebraic closure of $K$ (cf. [8]).

The following proposition is an easy consequence of the above discussion, and summarizes most of it. The reader may also find (1.2.12) and the discussion preceding it informative.

\begin{proposition}
Each maximal ideal of $Z(SG)$ contains a unique rational prime $p$. For any prime $p$, write $G = D \times D'$ where $D$ is a $p$-group and $D'$ is a group of order prime to $p$. Then the maximal ideals $\mathfrak{p}$ of $Z(SG)$ above $p$ are parameterized by the simple components $M$ of $KD'$, where $K$ is the quotient field of $S$, and by the maximal ideals $\mathfrak{p}'$ above $p$ in the integral closures $S'$ of $S$ in $Z(M)$. Explicitly, $\mathfrak{p}$ is the inverse image of $\mathfrak{p}'$ under the natural map $Z(SG) \to S'$. Moreover, $D = D(\mathfrak{p})$, and

$$B(\mathfrak{p}) \cong SD \otimes S'_p(M \cap SD'),$$

where $S'_p$ denotes the localization of $S'$ at $\mathfrak{p}'$, and the tensor product is over $S$.
\end{proposition}

The last isomorphism follows, because every primitive idempotent of $Z(SG)_{(p)}$ outside $M$ kills the central idempotent of $M$ (which is in $Z(SG)_{(p)}$ but not in $Z(SG)_{(p)}$) and so becomes zero in the localization $Z(SG)_{\mathfrak{p}}$ of $Z(SG)_{(p)}$. The expression for $B(\mathfrak{p})$ becomes even more manageable in the completion, where $S'_p(M \cap SD')$ is a full matrix algebra over $\hat{S}'_p$. (There are no division algebras in the simple components of group algebras over $p$-adic fields, if $p$ does not divide the order of the group [11, Cor. 9.5].) Thus $\hat{S}'_pD' = [\prod \hat{S}'_i]_{n_i}$, where $\hat{S}'_i$ are unramified extensions of $\hat{S}'_p$ representing the various $\hat{S}'_p$ and $(\hat{S}'_pD)_n$ is the corresponding $B(\mathfrak{p})$. Because of this, the proof of Corollary 4 does indeed formally reduce to Theorem 1; cf. (1.3.3). Note that much of the generality of that theorem is needed for the corollary, even for $S$ a semilocalization of $Z$.

The $S'_p$-algebra $S'_p(M \cap SD')$ is, in fact, a full matrix algebra over $S'_p$, as may be argued with a lattice giving the Morita equivalence with $S'_p$ over the completion.

We take this opportunity to mention that the conjugacy part of our preliminary announcement at the Korea conference [24] for class two groups was inaccurate. The correct version is given by Corollary 4.

If the hypothesis that $S$ be semilocal is dropped in Corollary 4, then the Picard group $\text{Picent}SG$ (still the main ingredient in $\text{Pic}_SG$) can still be
determined, up to Picent $Z(SG)$, using Fröhlich's exact sequence [12, Theorem 6]. Here $Z(SG)$ denotes the center of $SG$, and a definition of Picent may be found in the discussion preceding (1.2.10) below. This determination is interesting even for $S = Z$ and $G$ a $p$-group, and we note (without proof) for this case that

i) Picent $ZG ≅$ Picent $Z(ZG) \times \text{Outcent}(G)$, where $\text{Outcent}(G) = \text{Out}(G)$ is as above.

ii) Every invertible $ZG$-bimodule $M$ over $Z(ZG)$ has the form $M = aZGa$ where $a$ is an invertible ideal in $Z(ZC)$ and $a$ is a unit in $QG$ normalizing $ZG$. In particular $M ≅ aZG$ as a left $ZG$-module. (The latter holds even if $M$ is not "over $Z(ZG)$", in the sense that $Z(ZG)$ has the same action on both sides.)

It is also interesting to note (from Corollary 1) that every central automorphism of $Z_pG$ (even every augmented automorphism) is, modulo an inner automorphism, liftable to an automorphism of $ZG$.

In our last corollary we content ourselves with $S = Z$ (or a suitable semilocalization). We intend to remove the single block hypothesis in a later paper. Notice that the hypothesis is at least automatically satisfied if $G/N$ is a $p$-group.

**Corollary 5.** Let $G$ be a finite group and $N$ an abelian normal subgroup with $G/N$ nilpotent. (Assume for each prime divisor $p$ of $G/N$ that the Sylow $p$-subgroup $N_p$ of $N$ belongs to a single $Z_pG/N$-block, where the group law in $N_p$ is written additively and viewed as a $Z_pG/N$-module with the action of $G/N$ induced by conjugation in $G$.) Then $ZG = ZH$ implies $G = H$, for any finite group $H$. The same is true if $Z$ is replaced by any of its semilocalizations in which no prime divisor of $G$ is invertible.

The proof (1.3.4) is a direct application of Corollary 4, by the small group ring method; cf. (1.1.8). See [30] for a further general discussion. Unfortunately, one can also easily use Corollary 4 to give examples of finite groups $G, G'$ and normal abelian subgroups $N, N'$ with the small group rings isomorphic, at least semilocally, but with $G$ and $G'$ nonisomorphic (even with $G/N$ nilpotent). For a time we expected that this might also lead to counterexamples to the isomorphism problem itself. However, it now appears that, with sufficient effort, the different factors appearing in Corollary 4 can be coordinated. It seems likely that the study of Picard groups will lead to further understanding of the isomorphism problem, though we are by no means yet ready to predict a positive answer.

1. Preliminaries and proofs of the corollaries

This section treats some standard results on group rings in a setting suitable for this paper, including a number of proofs for completeness. In (1.1.6) a
A commutative algebra result (cf. the appendix) enables an efficient general treatment of Berman's invariance of class sums. Unless otherwise noted, we assume throughout (1.1) that $G$ is a finite group, and $S$ is an integral domain of characteristic $0$ in which no prime divisor of $G$ is invertible.

Let $v$ be any homomorphism from $G$ to the units $S^\times$ of $S$. Then $g \mapsto v(g)g$ ($g \in G$) is a group homomorphism, even an isomorphism, and extends to an automorphism $\tau: SC \to SC$. We regard such automorphisms as trivial, but they are useful for adjusting other automorphisms or isomorphisms to an augmentation-preserving form. Note $\epsilon(\tau(g)) = v(g)$ where $\epsilon: SG \to S$ is the augmentation map $g \mapsto 1$. If $\alpha: SG \to SH$ is any isomorphism of $S$-group algebras, then the composition $\epsilon \circ \alpha$ induces a homomorphism $v$ from $G$ to the units of $S$. If $\tau$ is defined as above, then $\alpha \circ \tau^{-1}$ preserves the augmentation. To summarize, we have proved the following well-known result (valid in fact for any group $G$ and commutative ring $S$).

\begin{equation}
(1.1.1) \text{PROPOSITION. For any group } H, \text{ every } S\text{-algebra isomorphism } \alpha: SG \to SH \text{ has the form } \alpha' \circ \tau, \text{ where } \alpha' \text{ is an augmentation-preserving isomorphism, and } \tau \text{ is an automorphism of } SG \text{ with } \tau(g) = \nu(g)g \text{ (} g \in G \text{) for a suitable (and unique) homomorphism } \nu: G \to S^\times.
\end{equation}

Define a unit or group of units in $SG$ to be normalized if it has image 1 under the augmentation. Any subgroup $H$ of units of $SG$, if it contains no elements of $S^\times$, is isomorphic to a normalized subgroup via $h \mapsto \epsilon(h)^{-1}h$ ($h \in H$). In view of this fact and the proposition above, it is standard practice to restrict attention to normalized units and augmentation-preserving group algebra maps.

The following result is due in its original form to G. Higman [15] as are most of its corollaries. A proof in the present context may be found in Sehgal [34, II, Corollary 1.5], or in Karpilovsky [19, Theorem 2.1], where the version stated here is attributed to Saksonov.

\begin{equation}
(1.1.2) \text{PROPOSITION. Let } u \text{ be a normalized unit of finite order in } SG. \text{ If } u \neq 1 \text{ then the coefficient of } 1 \text{ in the expression of } u \text{ as an } S\text{-linear combination of elements of } G \text{ is zero.}
\end{equation}

\begin{equation}
(1.1.3) \text{COROLLARY. If } H \text{ is a finite subgroup of the normalized units of } SG, \text{ then the elements of } H \text{ are } S\text{-linearly independent, and } SH \subseteq SG \text{ is a pure } S\text{-submodule. In particular } |H| \leq |G|, \text{ with equality if and only if } SH = SG.
\end{equation}

\textbf{Proof}: First of all, the elements of $H$ are $S$-independent. Otherwise we could arrange a relation $s.1 = \sum_{h \in H} s_h h$ with $s_h \in S$ ($h \in H$), not all zero, and $s \in S$ not zero. This clearly contradicts (1.1.2).
If $SH$ is not $S$-pure, we can arrange (multiplying by a suitable element of $H$) to have an expression $\Sigma_h k_h h$ in $SG$, with the $k_h$ belonging to the quotient field $K$ of $S$, but with $k_1 \notin S$. Again (1.1.2) gives a contradiction. (Gary Thompson points out that, similarly, $SG/SH$ is flat, a stronger purity.)

One can show that $|H|$ divides $|G|$ (Berman, cf. [31]) though we do not need this here. Note when $|H| = |G|$ that the equality $SH = SG$ is in particular an isomorphism of $S$-group algebras, and that all augmentation-preserving isomorphisms essentially arise this way.

(1.1.4) **Corollary.** Let $H$ be a normalized unit group in $SG$ with $SH = SG$. Then there is an equality of centers $Z(H) = Z(G)$.

Proof: The set $GZ(H)$ is a finite subgroup of normalized units, and so must be $G$. This gives $Z(H) \subseteq Z(G)$, and similarly $Z(G) \subseteq Z(H)$. Thus $Z(H) = Z(G)$. Q.E.D.

Note from (1.1.2) that any normalized unit of finite order not in $Z(G)$ has a zero coefficient at any element of $Z(G)$. (Multiply by the inverse of the latter.) We also have the following corollary, due to Jackson [16], though it is no longer needed in the present version of this paper.

(1.1.5) **Corollary.** Let $C = \langle c \rangle$ be a cyclic central subgroup of $G$. Then any normalized unit of finite order in $SC + (c - 1)SG$ belongs to $C$.

Proof: Write $u = u_1 + u_2$ with $u_1 \in SC$ and $u_2 \in (c - 1)S(G - C)$, where $S(G - C)$ denotes all $S$-linear combinations of $G - C$, the set of elements of $G$ not in $C$. Let $\epsilon$ denote the augmentation map. Then $\epsilon(u_2) = 0$, and so $\epsilon(u_1) = 1$, since $u$ is normalized. In particular $u_1 \neq 0$, so that $u \in C$ by the remark above. Q.E.D.

If $X$ is a subset of $G$, write $X$ for the sum in $SG$ of the elements of $X$. (To avoid later confusion, we mention that the same notation is used also in the image ring $A$ discussed in Chapter 3.) When $SG = SH$ as above, we can certainly use the same notation for subsets of $H$. A class sum for $G$ is a set $K$ where $K$ is a conjugacy class of $G$. The following result is due, apparently, to Berman in its original form and to Saksonov in full generality, cf. [19], though other authors as well proved fairly general versions. We reduce the proof to a familiar case treated by Glauberman and Passman [22].

(1.1.6) **Proposition.** Suppose $H$ is a finite subgroup of normalized units with $SH = SG$. Then $H$ and $G$ have the same class sums.

Proof. Replacing $S$ with the ring generated over $Z$ by the coefficients appearing in the expressions for elements of $H$ in terms of $G$ and vice versa, we
may assume $S$ is Noetherian. By the appendix we can assume without loss of
generality that $S$ is a principal ideal domain in which it is still the case that no
prime divisor of $|G|$ is invertible. Let $K$ be the quotient field of $S$, and embed $K$
in a field $\Omega$ containing $C$. Let $K_0$ be the intersection in $\Omega$ of $K$ with the field of
$|G|^{th}$ roots of unity. Observe that $K_0$ is normal as an extension of $Q$, and that
complex conjugation $x \mapsto x^*$ makes sense in $K_0$ and commutes with the action
of its Galois group $\mathcal{G}$. Let $S_1$ be the ring consisting of all elements of $S$ which
have the form $a/n$ where $a$ is an algebraic integer in $K_0$ and $n$ is an integer all
of whose prime factors divide $|G|$. In fact, the elements of $S_1$ must be algebraic
integers: Any $s \in S_1$ is a root of the polynomial $p(t) = \prod_{\sigma \in \mathcal{G}} (t - s^\sigma)$, whose
coefficients lie in $S_1 \cap Q = \mathbb{Z}$. (Let $a/n$ as above lie in $S_1 \cap Q$. Then the term $a$
must be a rational integer, which may be taken prime to $n$; thus $a = (a/n)n$
has no prime of $S$ in common with $n$, which visibly forces $n$ to be a unit. So
$n = \pm 1$, since prime divisors of $|G|$ are not invertible in $S$.)

Using standard character-theoretic formulae for class sums and central
idempotents, we see that the class sums of $G$ can be written as $S_1$-linear
combinations of those of $H$. (See [34, p. 891; however, it is not accurate to assert
yet that the coefficients are rational. Indeed, they might well be roots of unity
without the normalization assumption.)

Since the elements of $S_1$ are algebraic integers, the result now follows from
Theorem C of [19] and the discussion there on p. 567 of normalization. (The
method, essentially, is to consider the coefficient of $1$ in $\sum_{\sigma \in \mathcal{G}} (K\mathbb{K}^*)^\sigma$. It should
be noted that one needs the fact that the coefficients mentioned above are
algebraic integers in the well-behaved field $K_0$, hence satisfy the arithmetic-geo-
metric mean inequality $\sum_{\sigma \in \mathcal{G}} (x^\sigma)^n \geq |\mathcal{G}|$, if $x \neq 0$. This completes the proof
of the proposition.

We remark that the proposition of course generalizes Corollary (1.1.4).
Actually, we need only the corollary in the proof of Theorem 1, though the
proposition is used in the proof of the corollaries to the theorem.

One standard consequence of the proposition is the following: Let $I(SG)$
denote the augmentation ideal of $SG$, the kernel of $SG \to S$. This notation is
used throughout this paper, and we abbreviate $I(SG) = I(G)$ when $S$ is
understood from context. Note if $N \triangleleft G$, then $I(N)SG = I(N)G$ is the kernel of
the natural map $SG \to SG/N$. Sandling [30] attributes the following result to a
number of authors, including Cohn-Livingston (1963).

(1.1.7) COROLLARY. Suppose $H$ is a finite subgroup of normalized units in
$SG$ with $SG = SH$. Then there is an inclusion-preserving bijection between the
normal subgroups of $G$ and those of $H$ such that, if $N$ corresponds to $M$, then
$I(N)G = I(M)H$. In particular, there is a natural isomorphism $SG/N \simeq SH/M$. 

Proof. The bijection is just the natural one arising from the equality of class sums. Note that the group-theoretic kernel of any characteristic 0 linear representation of $SG$ consists precisely of the classes $K$ which map to $|K|$. The corollary follows immediately.

It is also true that the correspondence preserves commutator groups, cf. [34, III, Section 4], and one can also show, using the argument below in (1.1.8), that $N/[N, N] \cong M/[M, M]$. Also, the $SG = SH$-module structures on the tensor product with $S$ over $\mathbb{Z}$ with these abelian groups, resulting from the respective conjugation actions, are isomorphic. There are also naturally isomorphic $S$-algebra extensions associated with these modules. In more detail:

(1.1.8) Discussion. We will concentrate attention on abelian normal subgroups. If $N < G$ is abelian, we let $s_s(G, N) = s(G, N)$ denote the ring $SG/I(SN)I(SG)$. We have called $s(G, N)$ the small group ring over $S$ associated with $G$ and $N$. Its ancestry dates back to Higman's thesis [15] and it was the focal point of Whitcomb's methods [37]. Crowell [7] and Gruenberg-Roggenkamp [13] used it to give a natural realization of the isomorphism $H^2(H, N) \cong \text{Ext}_H^1(I(ZH), N)$ for $H$ a group (like $G/N$ above) acting on an abelian group $N$.

There is a natural surjection $s(G, N) \rightarrow SG/N$ with kernel

$$I(N)G/I(N)I(G) \cong S \otimes_{\mathbb{Z}} N$$

as left $SG$-module (cf., for example, [34, III, 1.15, ii], taking $m = 0$ there and tensoring with $S$ over $\mathbb{Z}$). The inverse of the isomorphism is obtained from the map sending $n$ in $N$ to the coset of $n - 1$. It seems natural to write the image of $N$ as $N - 1$. In this way $S(N - 1)$ is an ideal in $s(G, N)$, with square zero, additively isomorphic to the abelian group $S \otimes_{\mathbb{Z}} N$, and with quotient $s(G, N)/S(N - 1) \cong SG/N$. The action of $SG/N$ on the left of $S(N - 1)$ is induced by the conjugation action of $G/N$ on $N$, and the action on the right is trivial (that is, obtained from the augmentation $SG/N \rightarrow S$).

All elements of $s(G, N)$ which map to units in $SG/N$ are themselves units in $s(G, N)$, and the kernel of the resulting surjection $s(G, N)^\times \rightarrow (SG/N)^\times$ of unit groups is $1 + S(N - 1)$. The latter contains a natural copy $N = 1 + (N - 1) = 1 + \mathbb{Z}(N - 1)$ of the group $N$. One difficulty, when one works with rings more general than $\mathbb{Z}$ or its related semilocalizations or completions, is that this copy of $N$ is not easily distinguished, ring-theoretically, in $1 + S(N - 1)$. It is true, however, that the $S$-module $S(N - 1) \cong S \otimes_{\mathbb{Z}} N$ determines $N$ up to isomorphism as an abelian group. (Using the appendix, we may assume $S$ is a
Dedekind domain. $S \otimes \mathbb{Z} N$ is then a finitely generated torsion-module, whose $S$-invariants clearly determine the $\mathbb{Z}$ invariants of $N$.)

(1.2) **Automorphisms, isomorphisms, and Picard groups.**

Let $S$ be a commutative ring and $\Lambda$ an $S$-algebra. (All rings and algebras are associative with identity unless otherwise specified, and all modules are unital.) There is a very general procedure, which we first learned from [14; proofs of the Noether theorems], for converting automorphism questions on $\Lambda$ to questions about bimodules. To illustrate, let $\alpha$ be an $S$-automorphism of $\Lambda$. Form the $\Lambda\Lambda$ bimodule $\Lambda^{(\alpha,1)}$ which is $\Lambda$ as a right $\Lambda$-module, but in which the new left action $\lambda . x$ is $\alpha(\lambda)x$ for $\lambda, x \in \Lambda$. (All bimodules are understood to be $S$-linear.) Then it is easily seen that

(1.2.1) $\alpha$ is inner iff $\Lambda^{(\alpha,1)} = \Lambda$ as $\Lambda\Lambda$ bimodules.

More generally, if $\alpha, \beta$ are $S$-automorphisms of $\Lambda$, then $\alpha$ is the composition of $\beta$ with an inner automorphism if and only if $\Lambda^{(\alpha,1)} = \Lambda^{(\beta,1)}$. These results may also be found in [2, II, 5.2], placed in the broader context of the Morita theory.

For another generalization (also found in [14]), let $\Gamma, \Gamma'$ be $S$-subalgebras of $\Lambda$, and suppose $\alpha : \Gamma' \to \Gamma$ is an $S$-isomorphism. We can repeat the above procedure to define a new $\Gamma\Gamma'$ bimodule $\Lambda^{(\alpha,1)}$, and we have:

(1.2.2) $\alpha$ is the restriction to $\Gamma'$ of an inner automorphism of $\Lambda$ if and only if $\Lambda^{(\alpha,1)} = \Lambda$ as $\Gamma\Gamma'$ bimodules.

Of course the map $\alpha$ on $\Gamma'$ may well be the restriction of an automorphism $\alpha$ on $\Lambda$, in which case we can use (1.2.2) to modify the automorphism on $\Lambda$ (composing it with an inner automorphism). It is desirable to know just how much of a modification has been made, in terms of the isomorphism in (1.2.2); so we spell out the correspondence explicitly.

(1.2.3) Suppose $\phi : \Lambda^{(\alpha,1)} \to \Lambda$ is an isomorphism as in (1.2.2). Then $u = \phi(1)$ is a unit in $\Lambda$, and $\phi(x) = u^{-1}xu$ ($x \in \Gamma'$).

The straightforward verification is left to the reader.

We apply this as follows, in the spirit of Fröhlich [12]. The term "$S$-order" below abbreviates "$S$-order in a semisimple algebra". The hypothesis on $\pi$ is chosen to make the proof constructive as well as sufficiently general.

(1.2.4) **Proposition.** Suppose $S$ is a discrete valuation domain of characteristic 0, and $\mathfrak{p}$ is its maximal ideal. Suppose $\Lambda$ is an $S$-order (in a semisimple algebra), and $\Gamma' \subseteq \Lambda$ is an $S$-pure $S$-subalgebra which is also an order. Let $\pi$ be any nonzerodivisor in the center of $\Lambda$ such that some power of $\pi$ lies in $\mathfrak{p}\Lambda$, and let $M > 0$ be any given integer. Then there exists an integer $N > 0$ such
that, if $\alpha$ is an $S$-automorphism of $\Lambda$ fixing $\pi$ whose restriction to $\Gamma'$ is the identity modulo $\pi^n\Lambda$, then there is a unit $u$ of $\Lambda$ in $1 + \pi^m\Lambda$ with

$$\alpha(x) = u^{-1}xu \quad \text{for } x \in \Gamma'.$$

**Proof.** Note $\Delta = \Gamma' \otimes \Lambda^\alpha$ is also an $S$-order. By a well-known result of Donald Higman [5, Thm. 75.11], there is an integer $N_0 > 0$ such that $\pi^{N_0}$ kills all higher cohomology for the order $\Delta$, and if $N > N_0$, then any two of its lattices isomorphic modulo $\pi^N\Delta$ are isomorphic. Moreover, the isomorphism may be chosen to agree modulo $\pi^{N-N_0}\Delta$ with the original isomorphism (given modulo $\pi^N\Delta$). If we interpret this in terms of (1.2.3), the proposition follows.

In particular, the question as to whether $\alpha$ is inner on $\Gamma'$ in (1.2.4) is totally an issue for the completion. We mention that, when $S$ is already complete, semisimple algebra hypotheses such as found above (guaranteeing the existence of the Higman ideal) can often be eliminated in applications by instead using limit arguments.

For central automorphisms of an order (those which fix the center) it is often possible to go in the reverse direction, that is, to construct desired local or even semilocal $S$-algebra automorphisms from those over local completions. The natural context here is definitely Morita theory and Picard groups, where the constructions are made in terms of appropriate modules, then re-interpreted in terms of automorphisms. We outline some of this theory below. General references are [2, III] and especially [12]. The results we describe are somewhat technical at points, and are not needed for the proof of Theorem 1, but are used in proving its corollaries.

Let $S$ be a commutative ring and $\Lambda, \Lambda'$ $S$-algebras. All $\Lambda$-$\Lambda'$ bimodules will be understood to have the same $S$-module structure on both sides. Every $S$-linear equivalence between the category of $\Lambda$-modules and that of $\Lambda'$ has (up to natural isomorphism) the form $X \mapsto M \otimes_\Lambda X$ where $M$ is an invertible $\Lambda'$-$\Lambda$ bimodule. (That is, there is a $\Lambda$-$\Lambda'$ bimodule $N$ with $M \otimes_\Lambda N \approx \Lambda'$ and $N \otimes_{\Lambda'} M \approx \Lambda$. Equivalently, $M$ is a finitely generated projective generator as right $\Lambda$-module, and $\Lambda' \approx \text{End}(M)$. An analogous equivalence holds with $\Lambda, \Lambda'$ interchanged.) Conversely, any invertible bimodule $M$ gives an equivalence. Isomorphic bimodules give naturally isomorphic equivalences, and conversely.

If $\alpha: \Lambda' \rightarrow \Lambda$ is an isomorphism then we can define a $\Lambda'$-$\Lambda$ bimodule $\Lambda^{(\alpha)}$ as in (1.2.1) and (1.2.2), which is easily seen to be invertible. The associated equivalence of categories is naturally isomorphic to $X \mapsto X^\alpha$, where, if $X$ is a $\Lambda$-module, $X^\alpha$ is the $\Lambda'$ module obtained by letting $\Lambda'$ act on $X$ through $\alpha$.

When does an ($S$-linear) equivalence of categories arise from an $S$-algebra isomorphism? The answer is very reasonable in terms of bimodules. Observe
that:

(1.2.5) Assume all elements of Λ which have a left inverse are invertible. (This holds, for example, if Λ is finitely generated as an S-module.) Then a bimodule M for Λ'-Λ (with the same S-action on both sides) is of the form Λ(α,1) for some S-linear isomorphism α: Λ' → Λ if and only if M is free of rank one on each side.

The verification is based on the fact that End_Λ(M) = Λ, if M is a right Λ-module isomorphic to Λ: Indeed, identifying the Λ-module M with Λ, we obtain λ'.m = (λ'.1) = α(λ')m (λ' ∈ Λ, m ∈ M) for some S-algebra homomorphism α: Λ → Λ'. The map α is clearly injective, and, if m ∈ M = Λ is chosen with α(Λ')m = Λ, then m is a unit by hypothesis, and so α is an isomorphism. (We are grateful to the referee for pointing out that some invertibility hypothesis was indeed necessary here.)

(1.2.6) Corollary. Suppose G, H are finite groups and S is a semilocal Dedekind domain of characteristic 0 in which no prime divisor of |G| is invertible. Then every S-linear equivalence of the category of SG-modules with the category of SH-modules is induced by an S-algebra isomorphism SH = SG.

Proof. Let the equivalence be given by an invertible SH-SG-module M with inverse N, and let K denote the quotient field of S. By Swan's theorem, cf. [25, (9.3)], we know that

(1.2.7) If S, G are as in (1.2.6), then every finitely generated projective SG-module is free.

Suppose now that some prime divisor p of |H| was invertible in S. Choose then a subgroup P of H with order p, and note SP = S ⊕ I(SP). Correspondingly SH = S|^H ⊕ I(SP)|^H decomposes as a left SH-module. The summand I(SP)|^H is projective, but over K it contains no copy of a certain KH-module (namely, the trivial module). But its corresponding SG-module would be free, so over K it intertwines with all KG-modules. This contradiction shows all prime divisors of H are also not invertible in S.

Consequently, we can apply (1.2.7) to both G and H. Let M be isomorphic as a right SG-module to a direct sum of m copies of SG. Then SH = M ⊕_{SG} N has S-rank m times that of N, which is free on the right as an SH-module. This forces m = 1, and similarly M has rank 1 on the left as an SH-module. The result now follows from (1.2.5).

(1.2.8) Remark. Observe that, if the assumption in (1.2.6) that S be semilocal Dedekind is dropped, it can be recovered by enlarging (a suitable Noetherian subring of) S, using the appendix. Any S-linear categorical equiva-
lence (as exhibited by an invertible bimodule) produces a corresponding categorical equivalence over the enlarged ring, to which (1.2.6) then applies.

In the way of a converse, we note (but do not include the proof) that, if $S$ is a Dedekind domain of characteristic 0, and $\tilde{S}$ is a semilocalization of $S$ in which no prime divisor of $|G|$ is invertible, and $G$, $H$ are finite groups with $\tilde{S}H \cong \tilde{S}G$, then the category of $SG$-modules is equivalent to that of $SH$ modules.

If $S$ is a commutative ring and $\Lambda$ is an $S$-algebra then $\text{Pic}_S\Lambda$ is defined (as in [2, III] and [12]) to be the group of isomorphism classes of invertible $\Lambda$-$\Lambda$ bimodules (with the same action of $S$ on both sides). The group law is given by tensoring over $\Lambda$. As we have seen, it is naturally isomorphic to the group of $S$-linear auto-equivalences of the category of $SG$-modules.

(1.2.9) Corollary (see also (1.2.12) below). Suppose $G$ is a finite group and $S$ is a semilocal Dedekind domain of characteristic 0 in which no prime divisor of $|G|$ is invertible. Let $\Lambda$ be $SG$, or, more generally, the $S$-algebra of all $n \times n$ matrices over $SG$ for some positive integer $n$. Then $\text{Pic}_S\Lambda \cong \text{Out}_SSG$, the group of $S$-algebra automorphisms of $SG$ modulo inner automorphisms.

Proof. In any event $\text{Pic}_S\Lambda \cong \text{Pic}_SG$, since the category of $\Lambda$-modules is $S$-linearly equivalent to that of $SG$ (the equivalence for $n \times n$ matrices given by the classical invertible bimodule of $1 \times n$ row vectors). However, (1.2.6) shows that the natural map $\text{Aut}_SSG \to \text{Pic}_SG$ is surjective. We have already noted in (1.2.1) that the kernel consists of inner automorphisms. Q.E.D.

We do not know, incidentally, if one can always find, for a non-inner $S$-algebra automorphism of $SG$, or of any order $\Lambda$, a left $\Lambda$-module $X$ with $X^* \neq X$. All one knows from (1.2.1) is that there is no natural isomorphism for all $X$.

We now come to a main point in our outline: Even if one starts out primarily interested in automorphisms of orders, it is desirable to study the Picard group, because an important piece of it behaves well (in terms of other Picard groups) with respect to recovering semilocal or local information from localizations or completions.

Let $S$ be an integral domain with quotient field $K$, and $\Lambda$ an $S$-order in a semisimple $K$-algebra. (Thus $\Lambda$ is torsion-free of finite rank over $S$, and $KA = K \otimes_\Lambda \Lambda$ is semisimple.) As in [12] we define $\text{Pic}_{\gamma(\Lambda)}\Lambda$ to be $\text{Pic}_{\gamma(\Lambda)}\Lambda$, where $Z(\Lambda)$ denotes the center of $\Lambda$. Then classical Wedderburn theory applied to $KA \otimes_{\text{tr}(\Lambda)} KA^\text{op}$ shows that $\text{Pic}_{\gamma(\Lambda)}\Lambda$ is precisely the kernel of the map $\text{Pic}_S\Lambda \to \text{Pic}_KKA$. (This kernel could be used in place of $\text{Pic}_{\gamma(\Lambda)}\Lambda$ for more general $\Lambda$'s.) Equivalently, the bimodules of $\text{Out}_{\gamma(\Lambda)}\Lambda = \text{Out}_S\Lambda \cap \text{Pic}_{\gamma(\Lambda)}\Lambda$
are those represented by a fractional ideal of the form $u \Lambda$ where $u$ is a unit in $K\Lambda$ normalizing $\Lambda$. See Fröhlich [12, Cor. 2 to Thm. 4] for further details.

The following proposition combines a number of results of [12], specializing them to the semilocal case.

(1.2.10) **Proposition.** Let $S$ be a semilocal Dedekind domain with quotient field $K$, and $\Lambda$ an $S$-order in a semisimple $K$-algebra. Then

$$\text{Picent } \Lambda \cong \prod_{\mathfrak{p}} \text{Picent } \Lambda_{\mathfrak{p}} \cong \text{Picent } \hat{\Lambda}_{\mathfrak{p}}$$

where $\mathfrak{p}$ runs over all the maximal ideals of $S$, and $\hat{\Lambda}_{\mathfrak{p}}$ denotes the completion of $\Lambda$ at $\mathfrak{p}$. Analogous isomorphisms hold for Outcent.

**Proof.** We give the proof in the context of [12], though our semilocal situation is much simpler; the experienced reader can easily construct his own arguments here (and in (1.2.11) below), using bimodules over the center of $\Lambda$ and the inclusion of Outcent in Picent.

Note that $Z(\Lambda)$ is a semilocal commutative ring. A standard argument with Nakayama's lemma shows any projective generator for it has the ring itself as a summand. Therefore Picent $Z(\Lambda) = 1$, and the first isomorphism follows from Theorem 6 of [12]. The second isomorphism, for Picent and Outcent, is Corollary 3 to Theorem 4 in [12]. The first isomorphism for Outcent follows from Corollary 1 to Theorem 6 in [12], and the observation that units may be approximated in our semilocal case with the Chinese Remainder Theorem. (Suppose for each maximal ideal $\mathfrak{p}$ of $S$ we have a unit $u_{\mathfrak{p}}$ of $K\Lambda$ stabilizing $\Lambda_{\mathfrak{p}}$. Let $u$ be an element of $K\Lambda$ congruent to $u$ modulo $u_{\mathfrak{p}}$ for each $\mathfrak{p}$ and some large $n$. If $n$ is sufficiently large, then, for each $\mathfrak{p}$, $u$ is the multiple of $u_{\mathfrak{p}}$ by a unit of $\Lambda_{\mathfrak{p}}$. In particular $u$ stabilizes each $\Lambda_{\mathfrak{p}}$, and hence $\Lambda_{\mathfrak{p}}$ and gives rise to the same element of Outcent $\Lambda_{\mathfrak{p}}$ as $u_{\mathfrak{p}}$.)

This completes the proof of the proposition. We mention that Fröhlich's proofs of the results involved show the advantages of working with Picent even if one is interested more in Outcent. Also, if $S$ is not semilocal, then there is at least a surjection to the right-hand local terms when using Picent, though there need not be for Outcent. (Note Picent $\Lambda_{\mathfrak{p}} = \text{Picent } \hat{\Lambda}_{\mathfrak{p}} = 1$ for almost all $\mathfrak{p}$ [12, Theorem 6].)

(1.2.11) **Corollary.** Let $S$ and $\Lambda$ be as above in (1.2.10); then the same conclusions hold:

$$\text{Picent } \Lambda \cong \prod_{\mathfrak{p}} \text{Picent } \Lambda_{\mathfrak{p}} \cong \prod_{\mathfrak{p}} \text{Picent } \hat{\Lambda}_{\mathfrak{p}}$$

with $\mathfrak{p}$ ranging instead over the maximal ideals of $Z(\Lambda)$. Analogous isomorphisms hold for Outcent.
Proof. Let $\mathfrak{p}$ be a maximal ideal of $S$. Then $\hat{\mathbb{Z}}(\Lambda)_\mathfrak{p}$ is a direct sum of finitely many local $\hat{\mathbb{Z}}_\mathfrak{p}$-algebras, by the well-known lifting of idempotents. The intersections of their maximal ideals with $\mathbb{Z}(\Lambda)$ are distinct, and clearly give the complete set of maximal ideals $\mathfrak{p}$ of $\mathbb{Z}(\Lambda)$ above $\mathfrak{p}$. (The quotient of $\mathbb{Z}(\Lambda)$ modulo $\mathfrak{p}$ is unaffected by the completion.) Observe also that the factor giving $\mathfrak{p}$ is indeed $\hat{\mathbb{Z}}(\Lambda)_\mathfrak{p}$, since it has the correct quotients modulo powers of $\mathfrak{p}$, and is complete. Similarly, the product of this factor with $\hat{\Lambda}_\mathfrak{p}$ is $\hat{\Lambda}_\mathfrak{p}$. Clearly the functor Picent on $S$-algebras commutes with finite direct products [12, Theorem 3]; so

$$\text{Picent} \hat{\Lambda}_\mathfrak{p} \cong \prod_{\mathfrak{p} \not\supset \mathfrak{p}} \text{Picent} \hat{\Lambda}_\mathfrak{p}.$$ 

Finally, note that $\Lambda_\mathfrak{p}$ is an $S_\mathfrak{p}$-order to which (1.2.11) applies. Its completion with respect to $\mathfrak{p}$ is clearly the same as its completion with respect to $\mathfrak{p}$. Consequently,

$$\text{Picent} \Lambda_\mathfrak{p} \cong \text{Picent} \hat{\Lambda}_\mathfrak{p}.$$ 

The corollary now follows for Picent, and the argument for Outcent is analogous.

Q.E.D.

The decomposition $\hat{\Lambda}_\mathfrak{p} \cong \prod_{\mathfrak{p} \not\supset \mathfrak{p}} \hat{\Lambda}_\mathfrak{p}$ can be seen to be the familiar decomposition of $\hat{\Lambda}_\mathfrak{p}$ into “blocks.” In case $\Lambda$ is the group ring over $S$ of a finite group $G$ as in (1.2.9) then one obtains $\text{Picent} B \cong \text{Outcent} B$ for each block $B$ of $S^G$. This in fact follows more directly from the fact that $B$ is “clean”: Every finitely generated projective $B$-module which is free for $KIB$ is free for $B$.

Consequently (1.2.9) may be supplemented as follows.

(1.2.12) Proposition. If $S$ is any semilocal Dedekind domain of characteristic 0, and $G$ is a finite group, then $\text{Picent} SG \cong \text{Outcent} SG$. The same isomorphism holds for any ring direct factor of $SG$ (a block, for example, if $S$ is local and complete).

This is immediate from our observation about blocks and (1.2.11), or, alternately, the analogous observation for $S^G$ itself, and (1.2.10). As previously noted, the functors Picent and Outcent commute with finite direct products.

Finally we point out:

(1.2.13) Proposition. If $G$ is a finite group and $S$ is a semilocal Dedekind domain in which $|G|$ is invertible, then

$$\text{Picent} SG = \text{Outcent} SG = 1.$$ 

Proof. Let $M$ be an invertible bimodule representing an element of Picent $SG$. Then $KM = KG$ as bimodules, or, equivalently, as $K(G \times G)$-modules where $K$ is the quotient field of $S$.  

Of course \(|G \times G|\) is also invertible in \(S\). Changing notation, one just needs to know in general that \(SG\)-lattices \(M, N\) which are isomorphic over \(KG\) are isomorphic over \(SG\). This fact is well-known in case \(S\) is semilocal Dedekind, and the proof is complete.

(1.3) Proofs of the corollaries to Theorem 1.

In this section we prove Corollaries 2, 3, 4, and 5, as stated in the introduction. For the statement and initial discussion of Corollary 1, see Chapter 2.

(1.3.1) Proof of Corollary 2. By (1.2.8) and the appendix, we can assume \(S\) is a semilocal Dedekind domain in which no prime divisor of \(|G|\) is invertible, and \(SG = SH\) as \(S\)-algebras. By (1.1.1) we may assume \(H\) is a normalized subgroup of the units of \(SG\) with \(SG = SH\). From (1.1.7) we obtain easily for the \(p\)-Sylow subgroups that \(SG_p = SH_p\) for any given prime \(p\) dividing \(|G|\). Now localize \(S\) at a prime divisor of \(p\) in \(S\), then apply Theorem 1 to obtain \(G_p = H_p\). Of course (1.1.6) also shows \(H\) is nilpotent. Since \(p\) was arbitrary dividing \(|G| = |H|\), we have \(G = H\). Q.E.D.

(1.3.2) Proof of Corollary 3. By (1.1.3) we have \(SG = SH\). By the appendix we can assume \(S\) is a semilocal Dedekind domain, as above. Localizing further if necessary, we may assume \(S\) has a unique maximal ideal containing \(p\), for any divisor \(p\) of \(|G|\). Writing \(G = G_p \times G_p\) for such a \(p\), with a similar decomposition for \(H\), we clearly have from (1.1.7) that \(I(SG_p)SG = I(SH_p)SH\). In this way we may identify \(SG_n = SH_n\) as quotient (factor) rings of \(SG = SH\). (We must be a little careful here with this notation, since momentarily we will want also to regard \(SG_p \subseteq SG\) in the natural way.) In the quotient rings the hypothesis of Theorem 1 is satisfied for each \(p\). Consequently, there is a unit \(u_p\), which we may assume is normalized, which conjugates \(H_p\) to \(G_p\) in the quotient. Let \(v_p \in SG_p \subseteq SG\) be the unit in the internal \(SG_p\) which maps to \(u_p\) in the quotient. Note \(v_p\) maps to 1 in any quotient \(SG_q\) with \(q \neq p\). Conjugating \(H\) by \(v = \prod v_p\), we may assume \(G_n = H_n\) in the quotient \(SG_n\), for each \(p\) dividing \(|G|\).

Let \(\alpha\) be any isomorphism \(G \to H\) and regard \(\alpha\) as an automorphism of \(SG\). Clearly \(\alpha\) induces an automorphism \(\alpha_p\) on the quotient ring \(SG_p\), which, by the above paragraph, must be induced by an automorphism of \(G_p\). Let \(\beta_p\) be the corresponding automorphism of the internal \(G_p \subseteq G\), and note \(\beta = \prod_p \beta_p\) is an automorphism. Replacing \(\alpha\) with \(\alpha \beta^{-1}\), we may assume to start that \(\alpha\) induces the identity on the quotient ring \(SG_p\), for each \(p\) dividing \(|G|\).

Next observe that each conjugacy class \(K\) of the nilpotent group \(G = \prod G_p\) is a product \(K = \prod K_p\) of conjugacy classes \(K_p \subseteq G_p\), and correspondingly the class sum is a product \(K = \prod K_p\). The class sum \(K\) is characterized among class
sums by the fact that its image in the quotient ring $SG_p$ is a positive integer multiple of $K_p$ for each $p$. (The reader, by now, we hope, takes the latter confusion of notation in good humor.) However, $a(K)$ also has this property. Since $a(K)$ is a class sum, by (1.1.6), it must be that $a(K) - K$. It now follows from the Skolem-Noether theorem that $a$ becomes inner over the quotient field of $S$.

Q.E.D.

(1.3.3) Proof of Corollary 4. Part a) is immediate from (1.2.11). For part b) note that $\text{Outcent } B(\hat{\mu}) \cong \text{Outcent } \hat{B}(\hat{\mu})$, where $\hat{B}(\hat{\mu})$ is the completion of $B(\hat{\mu})$ with respect to $\hat{\mu}$. This follows again by (1.2.11) and the definition of $B(\hat{\mu})$.

By the remark following (0.4), $\hat{B}(\hat{\mu})$ is a full matrix algebra over the group algebra of $D(\hat{\mu})$, over a local Dedekind domain in which $p$ is not invertible. By Theorem 1 (or Corollary 1), and (1.2.9), every central automorphism of $\hat{B}(\hat{\mu})$ is induced modulo inner automorphisms by an automorphism of $D(\hat{\mu})$. A similar statement holds for $B(\hat{\mu})$ by the above isomorphism. We leave to the reader the straightforward task of checking that there is an induced surjection $\text{Outcent } D(\hat{\mu}) \to \text{Outcent } B(\hat{\mu})$ via the map in the statement of part b). Such a map is injective, as remarked following (0.3).

The last part of the corollary follows, by way of (0.3) and the surrounding discussion, from Corollary 3. This completes the proof.

(1.3.4) Proof of Corollary 5. Without loss of generality we may assume $N$ is the smallest normal subgroup of $G$ with $G/N$ nilpotent. Consequently, $[N, G] = N$, and, more precisely, $[N_p, (G/N)_p] = N_p$. Here $N = N_p \times N_p$, with $N_p$ a Sylow $p$-subgroup, and a similar notation is used for $G/N$. It follows that the module $N$ for $G/N$ has vanishing cohomology, since $N_p$ does not lie in the principal $p$-block, and, in particular, the extension $G$ of $N$ is split.

Take $S$ to be the semilocalization of $\mathbb{Z}$ at the prime divisors of $|G|$ (the intersection of the localizations). In view of (1.1.1) we may assume $H$ is a normalized group of units of $SG$, and $SG = SH$. Let $M$ be the normal subgroup of $H$ corresponding to $N$ as in (1.1.7). Then $M$ is abelian, $H/M$ is nilpotent, and $[M, H] = M$. (Cf. (1.1.8) and remarks preceding it.) It follows as above that $H$ is a split extension of $M$. Of course $G/M = H/N$ by Corollary 2 applied to $SG/N \cong SG/1(SN)G \cong SH/M$. To show $G \cong H$ it is now necessary and sufficient that there be an isomorphism $\alpha: G/N \to H/M$ such that the resulting module $M^\alpha$ is isomorphic to $N^\beta$ as $G/N$-module for some group automorphism $\beta$ of $G/N$.

Let $\alpha: G/N \to H/M$ be any isomorphism, and view $\alpha$ as an augmentation-preserving automorphism of $SG/B$. By Corollary 4 we may assume $\alpha$ is central (by composing with an automorphism of $G/N$). Also, if $\hat{\mu}$ is a maximal ideal in $Z(SG/N)$, the projection $\alpha_{\hat{\mu}}$ of $\alpha$ on $B(\hat{\mu}) = (SG/N)_{\hat{\mu}}$ is (up to an inner
automorphism) the projection of a central group automorphism \( \beta_\phi \) of \( G/N \) on \( B(\phi) \) by Corollary 4. Moreover, \( \beta_\phi \) is trivial on \( (C/N)_p \), if \( p \in \phi \).

In the small group ring \( s(G, N) \), cf. (1.1.8), we have \( M = N \). Put \( N_\phi = 1 + (N - 1)_\phi \) in \( s(G, N) \), where the localization of \( N - 1 \) is with respect to the left action of \( Z(SG/B) \). Then \( N = \prod N_\phi \), and

\[
M^\alpha = \prod N_\phi^\alpha
\]

with \( \phi \) ranging over the maximal ideals of \( Z(SG/N) \).

Note that, so far, we have not used the parenthetic hypothesis, which implies for each prime \( p \) dividing \( |G| \) that \( N_p = N_{\phi} \) for some \( \phi \). We write \( \beta_p = \beta_\phi \) correspondingly, and put \( \beta = \prod \beta_p \), an automorphism of \( G/N \). Note \( N_{\phi}^p = N_p \), if \( p \neq q \), since \( \beta_q \) is central. (Apply (1.2.13) to \( Z_p(G/N)_q \).) Thus \( M^\alpha = N^\beta \) by (1.3.5), and the corollary follows.

(1.4) Cohomology. As mentioned in the introduction, the following result gives at least some heuristic reason for expecting the isomorphism problem to have a positive answer. It is used via (2.6) and Theorem 2 in Chapter 5 in proving the main theorem.

(1.4.1) Proposition. Let \( S \) be a commutative ring of characteristic 0, in the sense that no nonzero element of \( S \) has finite additive order. Let \( H \) be a finite group acting by permutations on a set \( X \), and form the permutation module \( SX \) for \( SH \). Then \( H'(H, SX) = 0 \).

In particular, if \( H \) is contained in a group \( G \), and \( H \) acts on \( SG \) by conjugation, then \( H'(H, SG) = 0 \). For \( G = H \) a finite group, this gives \( H'(SG, SG) = 0 \) in the sense of augmented algebras, or, in other words, every \( S \)-linear derivation from \( SG \) to itself is inner.

Proof. Without loss of generality we may assume \( H \) is transitive on \( X \). Thus \( SX \) is induced from the trivial module \( S \) for a subgroup \( L \) of \( H \). By the result of Eckmann which is well-known as Shapiro's lemma, we have \( H'(H, SX) \cong H'(L, S) \). The latter consists of group homomorphisms from \( L \) to the additive group of \( S \), since \( L \) acts trivially. However, our characteristic 0 assumption implies there are none of these, except for the trivial map, so that \( H'(H, SX) = 0 \).

When \( G = H \) the identification of \( H'(SG, M) \), for an \( SG \)-bimodule \( M \), with \( H'(G, M) \) for the corresponding "conjugation action" \( m \mapsto gmg^{-1} \) \((m \in M, g \in G)\) on \( M \) is well-known, and easy to describe: A derivation \( D: SG \to M \) gives a 1-cocycle \( \gamma: G \to M \) defined by \( \gamma(g) = D(g)g^{-1} \). Conversely, cocycles can be used to define \( S \)-linear derivations, and coboundaries correspond precisely to inner derivations. This concludes the proof of the proposition.
The following proposition is used in Chapter 4 in giving a thematic proof of (4.3) using induced modules. As we point out there, an alternate proof of (4.3) can be obtained by a more direct inspection of cocycles.

(1.4.2) **Proposition.** Let \( p \) be a fixed prime, \( F \) an \( F_v \)-vector space, and \( L \) a proper subgroup of a finite elementary abelian \( p \)-subgroup \( E \). Then, with \( F \) as a trivial \( E \)-module, the transfer map

\[
H^1(L, F) \to H^1(E, F)
\]

is zero.

**Proof.** If \( \gamma \in H^1(L, F) \), denote the transfer of \( \gamma \) to \( E \) by \( \gamma^E \). Since \( \gamma^E \) is just a group homomorphism \( E \to F \), to show it is zero it is sufficient to show its restriction to each subgroup \( T \subseteq E \) of order \( p \) is zero. By Tate's Mackey formula for transfer [5, XII, Prop. 9.1], we have

\[
\gamma^E|_T = \sum \gamma^E|_{L' \cap T}
\]

with \( x \) ranging over a set of \( L, T \) double coset representatives in \( E \), \( L^x = x^{-1}Lx \), and \( \gamma^x(y) = x^{-1}\gamma(xyx^{-1}) \) for \( y \in L^x \). Here we have \( L^x = L \) and \( \gamma^x = \gamma \). If \( L \cap T = 1 \), then clearly \( \gamma^E|_T = 0 \). On the other hand, if \( L \cap T \neq 1 \), then \( T \subseteq L \), and the number of \( L, T \) double coset representatives is a multiple of \( p \). Thus \( \gamma^E|_T \) is a multiple of \( p \) times \( \gamma|_{L \cap T} \), and thus equal to 0, since \( F \) is an \( F_v \)-space. Q.E.D.

(1.5) **Linear algebra (and classical Lie theory).**

The proposition below plays a key role in analyzing the Lie filtrations in Chapter 4.

(1.5.1) **Proposition.** Let \( V \) be a finite-dimensional vector space over a field \( F \), and suppose

\[
(\ ,\ ,) : V \times V \to F
\]

is a nondegenerate skew-symmetric form. If \( \text{char } F \neq 2 \), then every linear transformation \( \psi : V \to V \) satisfying

\[
(\psi(u), v) + (u, \psi(v)) = 0 \quad (u, v \in V)
\]

is an \( F \)-linear combination of linear transformations of the form

\[
u \mapsto (u, v)w + (u, w)v \quad (u \in V)
\]

where \( v, w \in V \). If \( \text{char } F = 2 \), then the same conclusion holds if \( \psi \) satisfies in addition

\[
(u, \psi(u)) = 0 \quad (u \in V).
\]
Proof. For any \( F \)-linear map \( \tau: V \rightarrow V \) and any \( v \in V \), define a vector \( \tau^*(v) \in V \) by the condition

\[
(\tau(u), v) + (u, \tau^*(v)) = 0 \quad (u \in V).
\]

There is a unique such vector, since \((\ ,\ )\) defines an isomorphism of \( V \) with its dual space, and \( u \mapsto (\tau(u), v) \) is certainly an \( F \)-linear map. It follows easily that \( \tau^* \) is \( F \)-linear as a map from \( V \) to itself, and that \( \tau^{**} = \tau \). Moreover, the involution \( * \) is \( F \)-linear in its action on the space \( \text{End}_F(V) \) of \( F \)-endomorphisms of \( V \).

For \( v, w \in V \), let \( \tau_{v, w} \) be the linear transformation

\[
\tau_{v, w}(u) = (u, v)w \quad (u \in V).
\]

Then \( (\tau_{v, w}(u), x) + (u, \tau_{v, w}(x)) = (u, v)(w, x) + (u, v)(x, w) = 0 \quad (u, x \in V) \); so \( \tau_{v, w}^* = \tau_{w, v} \). Since the \( \tau_{v, w} \)'s span \( \text{End}_F(V) \), the transformations \( \tau_{v, w} + \tau_{w, v} \) span the subspace of transformations of the form \( \tau + \tau^* \) with \( \tau \in \text{End}_F(V) \). When \( \text{char } F \neq 2 \), this is just the fixed point space of the involution \( * \), while the equation satisfied by \( \psi \) above says precisely \( \psi^* = \psi \). Thus \( \psi \) is indeed in the span of the linear transformations of the prescribed form in this case.

When \( \text{char } F = 2 \) we choose a basis \( B \) for \( V \). The involution \( * \) permutes the basis \( \{ \tau_{v, w}|v, w \in B\} \) of \( \text{End}_F(V) \). Its fixed points in \( \text{End}_F(V) \) are thus \( F \)-linear combinations of transformations \( \tau_{v, w} + \tau_{w, v} \) and \( \tau_{v, v} \) (\( v, w \in B \)). Write accordingly

\[
\psi = \tau + \tau^* + \sum_{v \in B} f_v \tau_{v, v} \quad (f_v \in F).
\]

For \( v \in B \) choose \( v^* \in V \) with \((v^*, u) = 1 \) if \( u = v \) and \((v^*, u) = 0 \) if \( u \in B \) and \( u \neq v \). Then

\[
0 = (v^*, \psi(v^*)) = (v^*, \tau(v^*)) + (v^*, \tau^*(v^*)) + \sum_{u \in B} f_v(v^*, u)u
\]

\[
= (v^*, \tau(v^*)) + (\tau(v^*), v^*) + f_v
\]

for each \( v \in V \). Thus \( \psi = \tau + \tau^* \) has the required form in this case as well, and the proposition is proved.

We remark in passing that the \( \psi \)'s in the proposition are precisely the elements of certain classical Lie algebras, the symplectic Lie algebra when \( \text{char } F \neq 2 \), and the orthogonal Lie algebra when \( \text{char } F = 2 \).

(1.6) An identity.

The following identity is used a number of times in Chapters 3, 4, and 5, sometimes without explicit reference.
(1.6.1) Proposition. 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

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

Proof. Just write $[z, x] = [1 + z, x] = (1 + z)x - x(1 + x)$, and the formula follows immediately.

Often this is used in conjunction with the expansion $(1 + z)^{-1} = 1 - z + z^2 - \cdots$ which holds modulo any ideal containing a power of $z$, and is literally true in many complete situations.

2. The main reduction

In this chapter we begin the proof of Theorem 1. An immediate special case of the latter is:

Corollary 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 $p$. If $\alpha$ is an augmentation-preserving automorphism of $SG$, then $\alpha$ is the composition of an automorphism of $SG$ induced by an automorphism of the group $G$ followed by an inner automorphism of $SG$.

(2.0) Conversely, we claim that the corollary implies the theorem:

By (1.1.3) we have $SH = SG$, and by (1.1.4) we have an equality $Z(G) = Z(H)$ of the centers of the two groups. Let $Z_1$ denote the subgroup of $Z(G)$ consisting of the elements whose $p^{th}$ power is the identity. By induction we may assume the theorem is true for all groups of order less than $|G|$, and, in particular, for $G/Z_1$. Thus in $SG/I(SZ_1)G \cong SG/Z_1$, the group $H/Z_1$ is conjugate to $G/Z_1$ by an inner automorphism, say $^u(H/Z_1) = G/Z_1$ where $\bar{u}$ is a unit in $SG/Z_1$. Let $u$ be a unit in the small group ring $s(G, Z_1)$ which maps onto $\bar{u}$. (See (1.1.8).) Thus

$$ ^u(H)(1 + S(Z_1 - 1)) = G(1 + S(Z_1 - 1)) \text{ in } s(G, Z_1)^{\times}. $$

Let $X$ be the group generated by $^uH$ and $G$ in $s(G, Z_1)^{\times}$. Since the group $1 + S(Z_1 - 1)$ is of exponent $p$ and central in $s(G, Z_1)^{\times}$, we clearly have $X = G \times W$ for some finite elementary abelian $p$-group $V$, and similarly $X = ^uH \times W$ with $W$ elementary abelian. Since $|G| = |H|$ by hypothesis, we have $|V| = |W|$. Hence $V \cong W$, and $G \simeq H$ by the Krull-Schmidt theorem. Any such isomorphism induces an augmentation-preserving automorphism of $SG$, and the theorem now follows by applying the corollary to $G$ itself. Q.E.D.
Furthermore, we have:

(2.1) Reduction. To prove Theorem 1 it suffices to prove Corollary 1 in the case where $S$ is local and complete. That is, we can and shall assume henceforth that $S$ is a complete discrete valuation domain of characteristic 0 with residue field $F = S/\mathfrak{p}$ of characteristic $p$.

Proof. Let $\mathfrak{p}$ be the unique maximal ideal of $S$ containing $p$, let $\hat{S}_{\mathfrak{p}}$ denote the completion of $S$ with respect to $\mathfrak{p}$. If we assume the result over $\hat{S}_{\mathfrak{p}}$, there is a group automorphism $\beta$ of $G$ such that $\alpha \beta^{-1}$ becomes inner in $\hat{S}_{\mathfrak{p}} G$. In particular $\alpha \beta^{-1}$ is certainly central on $SG$. If $\mathfrak{g}$ is a maximal ideal of $S$ not containing $p$, then $\text{Outcent } S G = \text{Picent } S G = 1$ by (1.2.13). Now it follows from (1.2.10) that $\alpha \beta^{-1}$ is inner. Q.E.D.

We can get more out of the argument for (2.0). Let $H = \alpha(G)$. Since $S$ is local, all units of $SG/Z_1$ pull back to units of $SG$. Observe that:

(2.1.1) The set of automorphisms $\alpha$ of the form described in the conclusion of Corollary 1—that is, compositions of inner and group automorphisms—is closed under multiplication. Thus we may assume by induction, as in the discussion of (2.0), that $C$ and $H = \alpha(C)$ have precisely the same image in $SG/Z_1$, and so the inverse image $Y = G(1 + S(Z_1 - 1))$ in $s(G, Z_1)$ is stable under $\alpha$. Clearly $Y = G \times E$, where $E$ is a (possibly infinite) elementary abelian subgroup of $1 + S(Z_1 - 1)$.

Let $\beta$ be the group endomorphism $G \rightarrow Y \rightarrow Y \rightarrow G$, where the first map is inclusion and the last is projection on $G$ with respect to $Y = G \times E$. Since $\alpha(Z(G)) = Z(H) = Z(G) \subseteq G$ the map $\beta$ agrees with $\alpha$ on $Z(G)$. In particular $\beta$ is an automorphism, since it is injective on $Z(G)$. (Every normal subgroup $\neq 1$ of a finite $p$-group intersects the center.) As usual, we may view it as an automorphism of $SG$, and replace $\alpha$ with $\alpha \beta^{-1}$. This proves the following statement:

(2.2) To prove Corollary 1 by induction on $|G|$, we can (and shall henceforth) assume $\alpha$ is the identity on $Z(G)$.

Continuing with our discussion, let $\text{Fr}(G)$ denote the Frattini subgroup of $G$, the smallest normal subgroup with an elementary abelian quotient. Certainly we may assume $\text{Fr}(G) \neq 1$, since otherwise $\alpha = 1$ by (2.2). Fix a subgroup $C$ of order $p$ in $Z(G) \cap \text{Fr}(G)$. Thus $\text{Fr}(G/C) = \text{Fr}(G)/C$. Among the many careful choices of subgroups that must be made in this paper, the choice of $C$ in the intersection, rather than just in $Z(G)$, is one of the least essential. However, it does somewhat ease our notational burden.

By (2.2), $\alpha$ is the identity on $C \subseteq Z(G)$ and hence induces automorphisms on $s(G, C)$ and $SG/C$. By induction, $\alpha$ can be modified by composition with an
inner automorphism of $SG$ so that $\alpha(G/C) = G/C$, with (2.2) still holding. Then the inverse image $Y = G(1 + S(C - 1))$ of $G/C$ in $s(G, C)$ is stable under $\alpha$. As before $Y = G \times E$ and we obtain an automorphism $\beta: G \to Y \to G$ agreeing with $\alpha$ on $Z(C)$ and on $C/C$. Replacing $\alpha$ with $\alpha\beta^{-1}$ gives:

(2.3) To prove Corollary 1 by induction on $|G|$, we can (and shall henceforth) assume in addition to (2.2) that $\alpha$ is the identity on $SG/C$.

Note if $S = \mathbb{Z}_p$, then $1 + S(C - 1) = C$ in $s(G, C)^\times$, so that in the discussion above $\beta = \alpha$ on $G$ in $s(G, C)$. We record:

(2.3.1) Remark. If $S = \mathbb{Z}_p$, it may be assumed in addition that $\alpha$ is the identity on $s(G, C)$.

(2.3.2) Notation. Continuing now with our general discussion, let $c$ be a generator for $C$, and let $C$ be the sum in $SG$ of all the elements of $C$. Then $CSG$ is an ideal in $SG$, and also is the full set of fixed points in $SG$ for multiplication by $c$. Thus

$$\Lambda = SG/CSG$$

is a torsion-free $S$-module. Indeed, since $SG$ is free for the multiplication action of $SC$, we see even that $\Lambda$ is free for the action of the image $R = SC/CS$ of $SC$ in $\Lambda$. We have

$$R = S[\pi]$$

where $\pi$ is the image of $c - 1$ in $\Lambda$. Note that $\pi$ is central and not a zero divisor in $\Lambda$. (After all, $\Lambda$ was defined by factoring out the fixed points of $c$, which are the zeros of $c - 1$, from an $S(c)$-lattice.) We sometimes write $\xi$ for the image of $c$ in $\Lambda$. Then

$$\mathbb{Z}_p[\xi] = \mathbb{Z}_p[\pi] \subseteq R$$

is isomorphic to $\mathbb{Z}_pC/CS\mathbb{Z}_pC$, the extension of $\mathbb{Z}_p$ by a primitive $p^{th}$ root of 1 (namely $\xi$). Note $R = S\mathbb{Z}_p[\pi] \cong S \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\pi]$. Also $\pi^{p - 1} = up$ where $u$ is a unit in $\mathbb{Z}_p[\pi] \subseteq R$, and $\pi R \cap S = pS$. It is an easy exercise to check that:

(2.3.3) The unit $u$ is congruent to $-1$ modulo $\pi \mathbb{Z}_p[\pi]$.

We think of $\Lambda$ as an $S$-order, and $R$ as a well-understood special subring of its center (which in general may not be a domain, though $\pi$ is not a zero divisor).

Finally, we write

$$k = S/pS \cong R/\pi R,$$

an Artinian commutative local ring. Its residue field

$$k/rad k \cong S/rad S \cong R/rad R \cong \Lambda/rad \Lambda$$

is $F = S/\not{\pi}S$. We also write $\not{\pi} = rad R = \not{\pi} + \pi R$. 

(2.3.4) Note that $\alpha$ in (2.3) induces an automorphism of $\Lambda$ trivial modulo $\pi\Lambda$. Before completing our reduction to $\Lambda$, we need a fairly well-known pull-back diagram, which in our context is especially useful.

(2.4) Lemma. There is a natural isomorphism $\Lambda/\pi\Lambda \cong kG/C$, which gives a pull-back diagram

$$
\begin{array}{ccc}
SG & \longrightarrow & \Lambda \\
\downarrow & & \downarrow \\
SG/C & \longrightarrow & kG/C.
\end{array}
$$

Proof. The ideals $I(C)G$ and $CSG$ intersect trivially in $SG$, and their sum $\Sigma = I(C)SG + CSG$ can be written alternately as $(c - 1)SG + CSG$, or as $I(C)SG + pSG$. (This is all clear from corresponding statements in $SC$, which are obvious, and the fact that $SG$ is free as an $SC$ module.) The first alternate description gives $SG/\Sigma \cong \Lambda/\pi\Lambda$, and the second gives $SG/\Sigma \cong SG/C/pSG/C \cong kG/C$. The lemma follows easily.

In general the reader will have to keep in mind the maps involved in this lemma, as described by its proof, though these are all the obvious choices. One useful and immediate consequence of the isomorphism $\Lambda/\pi\Lambda \cong kG/C$ is:

(2.4.1) The group $G$ maps bijectively onto its image in the units of $\Lambda$.

Accordingly, and with some abuse of notation, we identify $G$ with its image in $\Lambda$; in this identification we have $C \subseteq R$. Note that the elements of $G$ generate $\Lambda$ as an $S$-module.

(2.5) Proposition (reduction to $\Lambda$). Every $R$-linear automorphism $\alpha$ of the order $\Lambda$ which is the identity modulo $\pi\Lambda$ comes from a unique $S$-automorphism of $SG$ (denoted also by $a$) which fixes $C$ pointwise and induces the identity on $SC/C$ (hence automatically preserves augmentation). Conversely, any such automorphism $a$ of $SG$ induces an $R$-automorphism of $\Lambda$ which is the identity modulo $\pi\Lambda$. Moreover

a) $\alpha$ is inner on $SG$ if and only if $\alpha$ is inner on $\Lambda$.

b) $\alpha$ stabilizes $G \subseteq SG$ (that is, $\alpha$ is induced by a group automorphism) if and only if $\alpha$ stabilizes $G \subseteq \Lambda$.

c) In fact, $\alpha$ stabilizes setwise (or pointwise) any given subset of $G \subseteq SG$ if and only if $\alpha$ stabilizes setwise (or pointwise) the corresponding subset of $G \subseteq \Lambda$. 


Proof. The first part of the proposition follows formally from the pull-back lemma (2.4), as do b) and c), and the converse property is immediate. (Keep in mind that \( R \) is the image in \( \Lambda \) of \( SC \).) To prove a), suppose \( \alpha \) is inner on \( \Lambda \), equal to conjugation by a unit \( x \), say. Let \( \bar{x} \) be the image in \( kG/C \cong \Lambda/\pi\Lambda \) of \( x \). Since \( \alpha \) induces the identity on \( \Lambda/\pi\Lambda \) by hypothesis, it follows that the unit \( \bar{x} \) in \( kG/C \) is central. Since the centers of \( kG/C \) or \( SG/C \) just consist of linear combinations of class sums, there is an element \( y \) in the center of \( SG/C \) with image \( x \) in \( kG/C \). Since \( S \) is local, \( y \) is automatically a unit and a) follows easily. The reverse implication in a) is trivial, so the proof of the proposition is complete.

(2.51) Discussion. This essentially completes the reduction to \( \Lambda \), though (2.6) will be needed in Chapter 5. For \( \alpha \) an automorphism of \( \Lambda \) as obtained from (2.3) we can write

\[
\alpha(g) = \mu(g)g \quad (g \in G)
\]

where \( \mu(g) \in 1 + \pi\Lambda \). The automorphism condition \( \alpha(gh) = \alpha(g)\alpha(h) \) gives the cocycle condition \( \mu(gh) = \mu(g)\mu(h)(g, h \in G) \), where \( \mu(h) = g\mu(h)g^{-1} \). Write \( \mu(g) = 1 + \pi\gamma(g) \) where \( \gamma(g) \in \Lambda \). As we will see in the next chapter, some of the multiplicative cocycle properties of \( \mu \) are inherited additively by \( \gamma \). If \( \gamma \) were in fact an additive cocycle, then (2.6) below would make \( \pi\gamma \) inner, and if this property were inherited by \( \alpha \), then \( \alpha \) would be inner on \( SC \) by (2.5), and we would be done. This reasoning cannot be followed exactly, but it is a guide for what follows (especially Chapter 5) and the reader may at least view it as encouraging.

We begin instead by trying to enlarge the subgroup, call it \( \Omega \), on which \( \alpha \) is known to be the identity (equivalently, on which \( \gamma \) is known to vanish). To start, we have \( Z(G) \subseteq \Omega \). For technical reasons we will restrict our search for enlargements to subgroups of \( C_G(Z(G, C)) \), where we define \( Z(G, C) \) to be the inverse image of \( Z(C/C) \) in \( C \).

If \( \Omega \) is not all of \( C_G(Z(G, C)) \), we try to enlarge it by the addition of an element \( t \) of \( C_G(Z(G, C)) \) which has order \( p \) modulo \( \Omega \) and centralizes \( G/\Omega \). Such a choice is possible, since \( C_G(Z(G, C))/\Omega \) is normal in \( G/\Omega \).

Now we try inductively to "push down" \( \gamma(t) \) toward 0 by making modifications on \( \alpha \). That is, to force \( \gamma(t) \) into \( \pi^n\Lambda \) for successively larger values of \( n \). Once \( n \) is large enough we can take \( \gamma(t) = 0 \) by applying (1.2.4). Unfortunately, this philosophy serves only to isolate a very hard problem, and considerable effort is needed to pass from \( n \) to \( n + 1 \). This is the critical situation studied in the next chapter, which requires some very technical arguments. Once it has been handled, though, the way is opened to more conceptual approaches in Chapters 4 and 5.
The case \( S = \mathbb{Z}_p \) was the original one treated, and is somewhat easier because of (2.3.1). The following proposition translates this into the language of \( \Lambda \). The proposition is no longer needed for the general argument, though it certainly inspired several parts of the latter. It still may be used to avoid the proof of (4.0.1) and simplify the first part of (3.6), in the \( S = \mathbb{Z}_p \) case.

\[(2.5.2)\] **Proposition.** If \( S = \mathbb{Z}_p \) it may be assumed that \( \alpha \) in (2.3) induces a map on \( \Lambda \) which is the identity modulo \( \pi \text{ rad } \Lambda \). (For arbitrary \( S \) and \( \alpha \) as in (2.1) and (2.3), the induced map on \( \Lambda \) is the identity modulo \( \pi \Lambda \), as noted in (2.3.4).)

**Proof.** If \( S = \mathbb{Z}_p \), the image in \( \Lambda \) of the ideal \( I(SG)I(SG) \) whose quotient is \( s(G, C) \), is \( \pi \text{ rad } \Lambda \). (Note \( p = p - C \) in \( \Lambda \) is in the image of \( I(SG) \); so the quotient of \( \Lambda \) by the latter is \( \mathbb{F}_p \), if \( S = \mathbb{Z}_p \).)

Finally, the proposition below (for arbitrary \( S \)) is needed in Chapter 5.

\[(2.6)\] **Proposition.** \( \pi H^1(\Lambda, \Lambda) = 0 \); that is, all \( \pi \)-multiples of \( S \)-linear derivations from \( \Lambda \) to itself are inner.

**Proof.** The homomorphism \( SG \to \Lambda \) determines a natural map \( H^1(\Lambda, \Lambda) \to H^1(SG, \Lambda) \) which is easily seen to be injective. Since \( H^1(SG, SG) = 0 \) by (1.4.1) the connecting homomorphism \( H^1(SG, \Lambda) \to H^2(SG, \mathbb{C}SG) \), arising from the defining sequence \( 0 \to \mathbb{C}SG \to SG \to \Lambda \to 0 \), is also injective. However, multiplication by \( c - 1 \) obviously kills \( \mathbb{C}SG \), hence kills \( H^2(SG, \mathbb{C}SG) \) and \( H^1(SG, \Lambda) \). But on the latter it is just multiplication by \( \pi \). The proposition follows immediately.

### 3. The critical situation

In this chapter we are concerned with the critical situation below, introduced in (2.5.1).

- \( G \) is a finite \( p \)-group for some prime \( p > 0 \).
- \( C = \langle c \rangle \) is a central subgroup of \( G \) of order \( p \) contained also in the Frattini subgroup \( \text{Fr}(G) \).
- \( S \) is a complete discrete valuation domain of characteristic 0 with residue field of characteristic \( p \). (The completeness is not used in this chapter or the next.)
- \( F = S/\mathbb{F} \) is the residue field of \( S \).
- \( \Lambda = SG/\mathbb{C}SG \), where the notation \( X \) means the sum of the elements in the set \( X \). The map \( SG \to \Lambda \) is injective on \( G \), and we will by abuse of notation regard \( G \) as both a subset of \( SG \) and of \( \Lambda \), the exact meaning determined by context. We will, however, usually write
\[ \zeta = \text{the image of } c \text{ in } \Lambda. \text{(But sometimes we just write } c). \text{ Thus} \\
\pi = S[\zeta] \text{ is central in } \Lambda. \text{ Moreover} \\
\pi = \zeta - 1 \text{ is not a zero divisor in } R \text{ or } \Lambda, \quad \pi^{n-1}R = pR, \text{ and } \Lambda/\pi\Lambda \cong (SG/C)/\pi(SG/C). \\
\hat{\mu} = \mu + \pi R \text{ where } \mu \text{ is the maximal ideal of } S. \text{ Thus } \hat{\mu} = \text{rad } R = R \cap \text{rad } \Lambda, \\
\text{and } \Lambda/\hat{\mu}\Lambda \cong FG/C. \text{ (For } S = \mathbb{Z}_p, \text{ the ideal } \hat{\mu} \text{ is just } pR.\) \\
\alpha \text{ is an automorphism of } \Lambda \text{ which is the identity modulo } \pi\Lambda \text{ and} \\
\mu : G \rightarrow 1 + \pi\Lambda \text{ is the associated multiplicative } 1\text{-cocycle given by} \\
\alpha(g) = \mu(g)g \text{ on } g \in G. \\
\gamma : G \rightarrow \lambda \text{ is the function defined by } \mu = 1 + \pi\gamma. \\
\Omega \text{ is a normal subgroup of } G \text{ containing } Z(G) \text{ and contained in} \\
C_G(Z(G, C)), \text{ and on which } \gamma \text{ is identically } 0. \text{ Here } Z(G, C) \text{ denotes the} \\
\text{inverse image in } G \text{ of the center } Z(G/C) \text{ of } G/C. \\
t \text{ is an element of } C_G(Z(G, C)) \text{ which centralizes } G/\Omega \text{ and has order } p \\
\text{modulo } \Omega. \\
n \text{ is a nonnegative integer for which } \gamma(t) \in \pi^n\Lambda. \\
\text{Any automorphism } \beta \text{ of the group } G \text{ which fixes } C \text{ (we use "fix" in the} \\
\text{pointwise sense) induces through its action on } SG \text{ an } R\text{-automorphism of the} \\
R\text{-algebra } \Lambda. \text{ We shall refer to such automorphisms of } \Lambda \text{ as "group automor-} \\
\text{phisms". If in addition } \beta \text{ fixes } G/C, \text{ then the induced } \beta \text{ fixes } \Lambda/\pi\Lambda. \text{(The} \\
\text{reader might wish to review (2.5) at this point.)} \\
\text{(3.0) Goal: To show the automorphism } \alpha \text{ can be composed with inner} \\
\text{automorphisms of } \Lambda \text{ together with "group automorphisms" of } \Lambda, \text{ with all} \\
\text{automorphisms the identity modulo } \pi\Lambda, \text{ so that} \\
1) \text{The condition that } \mu \text{ map } G \text{ into } 1 + \pi\Lambda \text{ is retained.} \\
2) \text{The new } \gamma \text{ still vanishes on } \Omega. \\
3) \text{The new } \gamma \text{ satisfies } \gamma(t) \in \pi^{n+1}\Lambda. \\
\text{The rest of the chapter is devoted entirely to establishing this goal. It is} \\
\text{necessary to approach the proof very slowly and carefully, taking full advantage} \\
of the details of structure created by the hypotheses. We begin with} \\
\text{(3.1) Lemma. The cocycle } \mu, \text{ and thus the function } \gamma, \text{ take values in the} \\
\text{fixed points } \Lambda^\Omega \text{ of } \Omega \text{ in } \Lambda. \text{ These fixed points are the image in } \Lambda \text{ of } (SG)^\Omega. \\
\text{Proof. The first statement is a well-known property of cocycles trivial on a} \\
\text{normal subgroup; a proof may be given as follows: For } x \in \Omega \text{ and } g \in G, \text{ put} \\
xg = gx' \text{ where } x' \in \Omega. \text{ Then } \mu(x)(\mu(g)) = \mu(g)(\mu(x')), \text{ and so } \mu(g) = \mu(g), \\
\text{since } \mu \text{ is trivial on } \Omega.
For the statement regarding \((SG)\bigcirc\), note the exact sequence
\[(SG)\bigcirc \to \Lambda^u \to H^1(\Omega, \mathbb{C}SG)\]
and observe that \(\mathbb{C}SG \cong \mathbb{C}G/C\) is a permutation module for \(\Omega\) under the conjugation action. By (1.4) the cohomology group above is zero, and the lemma follows immediately.

(3.1.1) A basis for \(\Lambda^u\). As is well-known, a standard \(S\)-basis for \((SG)\bigcirc\) is obtained from the sums \(X\), where \(X\) is an orbit of some element \(x\) of \(G\) under \(\Omega\). As noted above, the images of these orbit sums in \(\Lambda\) generate \(\Lambda^u\) as an \(S\)- or \(R\)-module. In fact the situation is even nicer. Some of the sums \(X\) go to zero in \(\Lambda\). These are the ones with an \(x\) in \(X\) for which \(cx\) is also in \(X\). The images of the other orbit sums almost form an \(S\)-basis, in that the dependence relations they satisfy are all obtained \(S\)-linearly from those of the form
\[\sum_{i=0}^{p-1} c^i X = 0 \quad \text{in } \Lambda.\]
Of course \(\sum_{i=0}^{p-1} c^i\) is already zero in \(R\). If \(y \in G\) we will denote the sum in \(\Lambda\) of the elements of the \(\Omega\)-orbit \(\Omega(y)\) of \(y\) by \(\Omega(y)\). (To avoid possible confusion, we agree in the following not to use this exact notation \(\Omega(y)\) in \(SG\).) An \(R\)-basis for \(\Lambda^u\) is obtained by choosing one such orbit sum from each nonzero set \(\{c^i\Omega(y)\}_{i \geq 0}\) of \(C\)-translates. It is worth noting that such choices lead to the same elements modulo \(\pi\Lambda^u\).

(3.1.2) The decomposition of \(\Lambda^u\) with respect to \(t\). Given an orbit sum \(\Omega(y) \neq 0\) in \(\Lambda\) there are three possibilities for the action of \(\langle t \rangle\):

0) \(\Omega(y) = \Omega(y)\).

f) \(\Omega(y), t\Omega(y), \ldots, t^{p-1}\Omega(y)\) are \(R\)-independent.

j, i) \(\Omega(y) = \xi^i\Omega(y)\) for an 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.

Note that if \(\Omega(y)\) fits a given case above, then so does \(c^j\Omega(y)\) for any \(j\).

Hence these conditions are well-behaved with respect to the \(R\)-bases discussed above.

We define \(\Lambda^u_0\) to be the \(R\)-submodule of all \(R\)-linear combinations of \(\Omega(y)\)'s satisfying condition 0), and define \(\Lambda^u_{\xi, i}\) and \(\Lambda^u_{\xi, i}\) similarly. Also we put
\[\Lambda^u_\xi = \sum_{0 < i < p} \Lambda^u_{\xi, i}.\]
The sum \(\Lambda^u_0 + \Lambda^u_{\xi, 1} + \Lambda^u_{\xi, 1}\) is then direct, as is the above decomposition of \(\Lambda^u_{\xi, 1}\).
Taking projections with respect to these decompositions, we write
\[ Y = Y_0 + Y_f + Y_i \]
and
\[ Y_i = \sum_{0 < i < p} Y_{i, i}. \]

(3.2) **Lemma.** The free \( R \)-spaces \( \Lambda_0^0, \Lambda_f^0, \Lambda_i^0, \Lambda_{i, i}^0 \) are all \( G \)-stable under conjugation and \( R \)-pure in \( \Lambda \). (Thus, the corresponding quotients of \( \Lambda \) have no \( R \)-torsion.) The functions \( \gamma_0, \gamma_f, \gamma_i, \gamma_{i, i} \) take values in \( \Lambda^0 \) and are, modulo \( \pi \Lambda^0 \), all additive 1-cocycles on \( G \). Their values on \( t \) lie in \( \pi^n \Lambda^0 \). (Here \( n \) is the integer given just above (3.0).)

**Proof.** Since \( \Lambda^0 \) is obviously \( R \)-pure in \( \Lambda \) (this is clear for \( R = \mathbb{Z}_p \)), and the general case follows by tensoring with \( S \) over \( \mathbb{Z}_p \), the \( R \)-purity of the spaces above follows from the direct sum decompositions we have discussed for \( \Lambda_0^0 \) and \( \Lambda_i^0 \). The spaces are all \( G \)-stable, since they can be described back in \( (SG)^0 \) in terms of the conjugation action of \( t \) on \( \Omega \)-orbit sums, and \( t \) is centralized by \( G \) modulo \( \Omega \).

It suffices now to show \( \gamma \) is a cocycle on \( G \) modulo \( \pi \Lambda^0 \), as the rest follows from the direct sum decompositions. Since \( \mu \) is a multiplicative 1-cocycle, we have that
\[ (1 + \pi \gamma(x))(1 + \pi^* \gamma(y)) = 1 + \pi \gamma(xy), \]
so that
\[ \gamma(x) + \gamma(y) + \pi \gamma(x) \gamma(y) = \gamma(xy) \quad (x, y \in G). \]
Since the term \( \pi \gamma(x) \gamma(y) \) lies in \( \pi \Lambda^0 \), the result follows.

We could have also noted above that the restrictions of the functions to \( (t) \) are cocycles modulo \( \pi \Lambda^0 \). This turns out not to be a useful observation at this point, essentially because the parameter \( n \) loses its uniform significance for \( \gamma_0(t), \gamma_f(t), \gamma_i(t) \) in the arguments that now begin to develop.

(3.3) **Main Lemma.** Let \( m \geq n \) be an integer such that \( \gamma_f(t) \) and \( \gamma_i(t) \) belong to \( \pi^m \Lambda \). (Note that \( \gamma_0 \) is not mentioned.) Then the automorphism \( \alpha \) can be composed with inner automorphisms of \( \Lambda \) and "group automorphisms" of \( \Lambda \), all automorphisms the identity modulo \( \pi \Lambda \), so that conditions 1) and 2) of (3.0) remain satisfied, and each of the following hold:

a) The new \( \gamma_0(t) \) is still in \( \pi^n \Lambda \).
b) The new \( \gamma_f(t) \) is still in \( \pi^m \Lambda \).
c) The new \( \gamma_i(t) \) is in \( \pi^{m+1} \Lambda \).
d) If the old \( \gamma(t) \) is in \( \text{rad} \Lambda \), then so is the new \( \gamma(t) \).
We remark that later (3.5) will give a way of pushing down \( y(t) \) into a higher power of \( \pi \Lambda \) while keeping a) and c) above satisfied, for \( m \) in a suitable range. The two lemmas (3.3) and (3.5) together provide a "see-saw" mechanism for pushing down both \( y_\xi(t) \) and \( y(t) \). Once these two are down far enough, we can force \( y_\xi(t) \) down as well, cf. (3.6), reaching the goal of this chapter and creating what is in effect a "triple see-saw," albeit one in which the eventual movement of the participants is inevitably downward.

**Proof.** We have a lot of work to do on \( y_\xi \), most of it relevant mainly to the case \( m = 0 \). First we note:

**Claim 1.** Each \( y_{\xi, i}(t) \) is centralized by \( G \) modulo \( \pi \Lambda \).

This claim is in fact true for all \( i \), though we need it only for \( 0 < i < p \). The proof can be given by elementary calculations, but here is a more conceptual argument: Recall (3.2), and let \( g \in G \). Then, modulo \( \pi \Lambda^2 \), \( \xi(\gamma_{\xi,i}(s^{-1}t)) - (s\gamma_{\xi,i})(t) \) is the value of the \( G \)-conjugate of the cocycle \( \gamma_{\xi,i} \) on \( t \). This \( G \)-conjugate is equivalent to the original cocycle on \( G \), as is well-known. Now note that, since \( \xi = 1 \) (mod \( \pi \)), the original cocycle is taking values in fixed points, namely \( (L^0_{\xi,i} + \pi \Lambda^2) / \pi \Lambda^2 \subseteq (L^0 / \pi \Lambda^2)^{(G,t)} \), for the subgroup of \( G \) generated by \( \Omega \) and \( t \). Thus equivalence on this subgroup means equality, and the claim follows.

Next,

**Claim 2.** If \( 0 < i < p \), then \( y_{\xi, i}(t) \in \text{rad } A \).

The argument has nothing to do with whether or not \( y(t) \) is in \( \text{rad } A \). It depends on our hypothesis that \( t \) be in \( C_\xi(Z(G,C)) \), and, moreover, is our only need for this assumption: By the first claim, the image of \( y_{\xi, i}(t) \) in \( \Lambda / \pi \Lambda \cong FG/C \) must be a linear combination of \( G/C \)-class sums. The image must also be expressible using the \( R \)-basis for \( \Lambda^0_{\xi,i} \), as described in (3.1.1) and (3.1.2). If a coset \( xc \) lies in the center of \( G/C \), then \( t \) centralizes \( x \) by the hypothesis \( t \in C_\xi(Z(G,C)) \); thus \( \Omega(x) \) is in \( \Lambda^0_0 \) and so does not contribute to \( y_{\xi, i}(t) \). Therefore all \( G/C \) classes whose sums appear with a nonzero coefficient in the expression for the image of \( y_{\xi, i}(t) \) in \( FG/C \) have cardinality greater than one. The corresponding sums thus lie in the radical of \( FG/C \) (even in the square of the radical). The claim follows.

(3.3.1) The trace ideal \( I \), its graded quotient, and the projection operators \( pr_j \). Before proceeding with the proof of (3.3), we take note of some further important facts related to the action of \( t \) on \( \Lambda^0 \). For \( x \in \Lambda^0 \) define \( T(x) \) to be the sum of the conjugates of \( x \) under the group \( \langle \Omega, t \rangle \) of order \( p \). Then \( T(\Lambda^0) = p \Lambda^0_0 + T(\Lambda^0_0) \), and so \( I = \pi \Lambda^0 + T(\Lambda^0) = \pi \Lambda^0 + T(\Lambda^0_0) \) is an ideal in the ring \( L \) of points in \( \Lambda^0 \) fixed by \( t \) modulo \( \pi \Lambda^0 \). Note \( I \) is \( \alpha \)-stable, being
the preimage in $\Lambda^G$ of a submodule of $\Lambda^G/\pi\Lambda^G$, and $I \subseteq \text{rad } \Lambda^G$, since obviously $T(x) = 0$ in $\Lambda/\text{rad } \Lambda$. We can write the $R$-module $L$ as

$$L = I + \Lambda^G_0 + \Lambda^G_1,$$

a sum decomposition which becomes direct modulo $\pi\Lambda^G$. We claim that the quotient $E = L/I$ is a $\mathbb{Z}/p\mathbb{Z}$-graded ring, with $j$th grade $E_j = L_j/I$, where $L_j = I + \Lambda^G_{j,k}$, for any integer $j$. Equivalently, $L_jL_k \subseteq L_{j+k}$ for any integers $j$, $k$. (The ring $k$ of the previous chapter is not used here; there should be no confusion.) To see this, think in terms of eigenspaces of $t$: the product of the $\xi^j$ and $\xi^k$ eigenspaces is contained in the $\xi^{j+k}$ eigenspace. Note, however, that the $\xi^j$ eigenspace of $t$ in $\Lambda^G$ contains $\Lambda^G_{j,0}$ and is contained in $I + \Lambda^G_{j,k} = L_j$ for each $j$, whence $L_jL_k \subseteq L_{j+k}$ as we claimed.

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, we put $M_j = (I + M) \cap L_j = I + (M \cap L_j)$. (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 (apply the “image” definition), and we write $M^k$ for $(M^k)_j$.

For each integer $j$ define $\text{pr}_j: \Lambda^G \to \Lambda^G_{j,0}$ to be the projection with respect to the decomposition of $\Lambda^G$ discussed in (3.1.2), reducing $j$ modulo $p$, and using $\Lambda^G_{j,0} = \Lambda^G_0$. Note that $\text{pr}_j(\Lambda^G) = \Lambda^G_{j,0} \subseteq L_j$, and moreover $L_j = I + \text{pr}_j(\Lambda^G) = I + \text{pr}_j(L)$. In fact the equation $M_j = I + \text{pr}_j(M)$ holds for all graded $R$-submodules $M$ of $L$. In more detail: $\text{pr}_j(I) \subseteq \text{pr}_j(\pi\Lambda^G + \Lambda^G_0) = \pi\Lambda^G$—a fact we will use again later—and so $\text{pr}_j(I) \subseteq L_j$. In particular, it follows for all $j$ that $\text{pr}_j(x) = x$ modulo $I$ when $x \in L_j$, and $\text{pr}_j(x) = 0$ modulo $I$ when $x \in L_k$ for some $k \equiv j$ (mod $p$). (Note that the $\text{pr}_j$'s are orthogonal idempotent projections.) Since $I \subseteq M_k \subseteq L_k$ for each $k$, the equation for $M_j$ now follows from $M + I = \sum_k M_k$ by applying $\text{pr}_j$ to both sides and adding $I$.

We return now to the proof of (3.3). For any integer $j$, let $D_j = L_j \cap \text{rad } L = L_j \cap \text{rad } \Lambda$, which contains $I$, and put $D = \sum D_j$, a graded submodule of $L$, with $D_j$ in agreement with the subscript notation above. $D$ is an ideal in $L$, nilpotent modulo $\pi\Lambda^G$, and thus nilpotent modulo $I$. Note that $\gamma_j, i(t) \in D_j$ by Claim 2, if $0 < i < p$. Observe that $D$, like $I$ above, is $a$-stable.

Claim 3. Suppose $k > 0$ is an integer such that $\gamma_{j, i}(t) \in D_j^k$ for all $i$ with $0 < i < p$. Then the automorphism $a$ can be composed with inner automorphisms and “group automorphisms” of $\Lambda$ so that conditions 1) and 2) of (3.0) remain satisfied, and in addition $\gamma_{j, i}(t) \in D_j^{2k}$ when $0 < i < p$. Furthermore, if the old $\gamma(t)$ is in $\text{rad } \Lambda$, then so is the new $\gamma(t)$.

Repeated application of this claim will treat the case $m = 0$ of the lemma we are trying to prove, since eventually $D^k \subseteq I$, and $\text{pr}_i(I) \subseteq \pi\Lambda^G$ if $0 < i < p$. 

(Of course p_*(\gamma_{i,t}(t)) = \gamma_{i,t}(t).) We will also use parts of the proof below to deal with the remaining (easier) case m > 0. In that case we ignore k and work instead with the hypotheses of the lemma on m. The necessary modifications this entails are noted in parenthetic remarks.

Consider the element
\[ d = \sum_{i=1}^{n-1} \frac{1}{i} \gamma_{i,t}(t) \]
which is in $D^k + I$ (in $\pi^m \Lambda^\Omega$ for the $m > 0$ case). We have $\xi d \equiv d$ modulo $\pi \Lambda^\Omega$ by Claim 1, for each $g \in C$. In particular $(1 + d)g(1 + d)^{-1} \equiv g$ modulo $\pi \Lambda$.

Let $\delta$ be the map $\text{conj}(1 + d)$, the automorphism of $\Lambda$ sending $x \in \Lambda$ to $(1 + d)x = (1 + d)x(1 + d)^{-1}$. Since $\Omega$ centralizes $d$, the group $\Omega$ is fixed by $\delta$.

Let $\alpha'$ be the composite automorphism $\alpha \circ \delta$. The above paragraph shows that, as a replacement for $\alpha$, the automorphism $\alpha'$ satisfies conditions 1) and 2) of (3.0). Next, we have to examine $\alpha'(t)$. By construction $\alpha' - d$ is congruent to $\pi \gamma_{i,t}(t)$ modulo $\pi^{m+2} \Lambda^\Omega$, because $\xi - 1 = \pi (c^i - 1)/(c - 1)$ is congruent to $\pi i$ modulo $\pi^2$ in $R$. It follows from (1.6.1) that $\delta(t)t^{-1}$ may be written
\[
\begin{align*}
\delta(t)t^{-1} &= 1 + [d, t](1 + d)^{-1}t^{-1} \\
&= (1 + (d - t)(1 - d + t^2 + \ldots)) \\
&\equiv 1 - \pi \gamma_{i,t}(t)
\end{align*}
\]
modulo $\pi^{m+2} \Lambda^\Omega + \pi(D^k + I)$. (If $m > 0$ we can drop the $\pi(D^k + I)$ term, since it comes from elements in $\pi(\pi^m \Lambda^\Omega)^2$.) Now apply $\alpha$. Since $\gamma_{i,t}(t) \in \pi^m \Lambda^\Omega$, and $\alpha$ on $\Lambda^\Omega$ is the identity modulo $\pi \Lambda^\Omega$, we have $\alpha(\gamma_{i,t}(t)) = \gamma_{i,t}(t)$ modulo $\pi^{m+1} \Lambda^\Omega$. Thus $\alpha'(t)t^{-1} = \alpha(\delta(t)t^{-1})\alpha(t)t^{-1}$ is congruent to $(1 - \pi \gamma_{i,t}(t))\alpha(t)t^{-1} = (1 - \pi \gamma_{i,t}(t))(1 + \pi \gamma(t))$ modulo
\[
(\pi(\pi^{m+1} \Lambda^\Omega) + \alpha(\pi^{m+2} \Lambda^\Omega + \pi(D^{2k} + I)))(1 + \pi \gamma(t))
\]
\[\subseteq (\pi^{m+2} \Lambda^\Omega + \pi(D^{2k} + I))(L + \pi^{m+1} \Lambda^\Omega) \subseteq (\pi^{m+2} \Lambda^\Omega + \pi(D^{2k} + I)).\]

If $m > 0$ we can again drop the $\pi(D^{2k} + I)$ terms here and in the next sentence. Consequently, the new $\mu(t)$, which is $\alpha'(t)t^{-1}$, is congruent modulo $\pi^{m+2} \Lambda^\Omega + \pi(D^{2k} + I)$ to $1 - \pi \gamma_{i,t}(t)$ or $\pi \gamma(t) = 1 + \pi \gamma_0(t) + \pi \gamma_1(t)$, applying $p_{*, t}$, it follows for $0 < i < p$ that the new $\gamma_{i,t}(t)$ lies in $D_i^{2k}$ as claimed. (If $m > 0$, we obtain $\gamma_{i,t}(t) \in \pi^{m+1} \Lambda^\Omega$ for the new $\gamma$.)

Also, since the new $\gamma(t)$ differs from the old only by $\gamma_{i,t}(t)$, modulo $\pi^{m+1} \Lambda^\Omega + D^{2k} + I \subseteq \text{rad } \Lambda$, the new $\gamma(t)$ is in $\text{rad } \Lambda$, if the old $\gamma(t)$ was in $\text{rad } \Lambda$. 
Completion of the proof of (3.3). If \( m > 0 \) then we obtain, as indicated, the above congruences for the new \( \mu(t) \) with the \( \sigma(D^{2k} + 1) \) term dropped—that is, we obtain \( \gamma_{\ell,i}(t) \in \pi^{m+1}\Lambda^\Omega \). Condition d) of (3.3) is retained as indicated. This gives all four conditions a), b), c), d), and completes the proof of the lemma.

(3.4) Lemma. Assume the hypothesis of (3.3) and in addition that \( p - 1 + n > m \). Then \( T(\gamma_i(t)) \) is in \( \pi^{m+1}\Lambda^\Omega \), where \( T \) is the trace function defined in (3.3.1).

Proof. Let \( s = \gamma_i(t) + \gamma_0(t) \) and \( z = \gamma_0(t) \). Then it suffices to show \( T(s) \) is in \( \pi^{m+1}\Lambda^\Omega \), since the G-module sum \( \Lambda^\Omega_f + \Lambda^\Omega_i \) is direct (to mention just one of several possible arguments here; in fact, \( T(s) = T(\gamma_i(t)) \)). Put \( u = \mu(t) = 1 + \pi(t) \). Since the multiplicative 1-cocycle \( \mu \) vanishes on \( t^p \in \Omega \), we have the norm condition

\[
u(tu) \cdots (t^{p-1}u) = 1
\]

which, equivalently, is a consequence of the fact that \( \alpha(t^p) = t^p \). Note \( \pi(z) = z \) by definition of \( \Lambda^\Omega_0 \). Hence the contribution of the product of the conjugates of \( 1 + \pi \) (thinking of \( u \) as \( (1 + \pi) + \pi s \)) to the above product is just \( (1 + \pi)^p \). The latter is congruent to 1 modulo \( \pi^{p+n}\Lambda^\Omega \), since \( z \in \pi^n\Lambda^\Omega \) by the hypothesis of this chapter, and \( \pi^p \) is a unit \( w \) times \( p \sigma \) in \( R \). Continuing the expansion of the rest of the product, we obtain a sum of factors, each a product of conjugates of \( 1 + \pi \) times a product of conjugates \( \pi s \), the latter product nonempty. The sum of factors where the latter product contains only one conjugate of \( \pi s \) contributes \( \pi T(s) \), plus terms having \( \pi \) times a conjugate of \( \pi s \) as a factor.

So the rest of the product is \( \pi T(s) \) plus terms involving a conjugate of \( \pi s \) or \( \pi \) times a conjugate of \( \pi s \). This gives \( \pi T(s) \) modulo \( \pi^{2+n+m}\Lambda^\Omega \).

Consequently, \( T(s) \) is congruent to 0 modulo \( \pi^n\Lambda^\Omega \), where \( n \) is the smaller of the exponents \( p - 1 + n \) and \( 1 + n + m \). If \( n = 1 + n + m \), then the lemma follows, because \( n \geq 0 \). And if \( n = p - 1 + n \) then the lemma follows from our hypothesis on \( m \). Thus the lemma is proved.

It is useful to note what happens in the above argument if the condition on \( m \) is replaced by \( m = p - 1 + n \). The product \( (1 + \pi) \sigma \) is congruent to \( 1 + \pi(z + wz^p) \) modulo \( \pi^{p+1+n}\Lambda^\Omega \), where \( w \) is the unit in \( R \) mentioned above, and of course, \( 2 + n + m \geq p + 1 + n \). Thus:

(3.4.1) Under the hypothesis of (3.3) and the condition \( m = p - 1 + n \), we have a congruence

\[
p(z + wz^p) = -T(s) \pmod{\pi^{p+n}\Lambda^\Omega}
\]
where \( z = \gamma_0(t), \ s \in \pi^{p-1+n} \Lambda^\Omega \) is \( \gamma_f(t) + \gamma_i(t) \), and \( w \) is a unit in \( R \) congruent to \(-1\) modulo \( \pi R \).

The congruence on \( w \), obtained from (2.3.3), will be used in (3.6).

(3.5) LEMMA. Assume the hypothesis of (3.3) and in addition that \( p - 1 + n > m \), as in (3.4). Assume also that the automorphism \( \alpha \) has been modified in accordance with the conclusion of (3.3) to satisfy conditions a), b), c), d) of that lemma. Then the automorphism \( \alpha \) can be further modified (composed with inner automorphisms and "group automorphisms" of \( \Lambda \) (the latter are not actually needed in this step), all the identity modulo \( \pi \Lambda \)) so that conditions 1) and 2) of (3.0) remain satisfied, conditions a), c), and d) of (3.3) remain satisfied, and in addition the following stronger form b') of condition b) holds:

b') The new \( \gamma_f(t) \) is in \( \pi^{m+1} \Lambda \).

Proof. Since \( T(\gamma_f(t)) \equiv 0 \) modulo \( \pi^{m+1} \Lambda^\Omega \), and \( \Lambda^\Omega_f \) is free for the cyclic group \( \langle \Omega, t \rangle / \Omega \), we have \( \gamma_f(t) = \gamma - \gamma \) modulo \( \pi^{m+1} \Lambda^\Omega \), for some \( \gamma \in \pi \pi \Lambda_f \). (In particular, it follows that \( \gamma_f(t) \in \text{rad } \Lambda \).) Thus

\[
\text{conj}(1 + \pi y)(t) = (1 + \pi y)t(1 + \pi y)^{-1} = \left(1 + \pi [y, t]t^{-1}(1 + \pi (t y)^{-1})t \right) \text{ (use (1.6.1))} \equiv (1 - \pi \gamma_f(t))t \pmod{\pi^{m+2} \Lambda}.
\]

Applying \( \alpha \) we obtain, for \( \alpha' = \alpha \circ \text{conj}(1 + \pi y) \), that

\[
\alpha'(t) = \alpha(1 + \pi \gamma_f(t)) \alpha(t) - (1 + \pi \alpha(\gamma_f(t))(t + \pi \gamma(t))t) \\
\equiv (1 - \pi \gamma_f(t))(1 + \pi \gamma(t))t, \text{ since } \gamma_f(t) = \pi^m \lambda \text{ for some } \lambda \in \Lambda, \text{ and } \alpha(\lambda) \equiv \lambda \pmod{\pi \Lambda}, \\
\equiv (1 + \pi \gamma_0(t) + \gamma_i(t))t \pmod{\pi^{m+2} \Lambda}.
\]

Consequently, conditions a), c), and b') are satisfied. As noted above, the old \( \gamma_f(t) \) is in \( \text{rad } \Lambda \) here, so the above congruence gives d). One sees easily that 1) and 2) of (3.0) are satisfied as well, and the proof of the lemma is complete.

(3.6) The concluding argument for achieving (3.0). Repeatedly applying (3.3) and (3.5) in turn, we may assume that \( \gamma_f(t) \) and \( \gamma_i(t) \) belong to \( \pi^{n+1} \Lambda^\Omega \). (In particular they belong to \( \pi^n + 1 \Lambda \).) Now (3.4.1) gives \( \gamma(t) + w \gamma(t)^p \equiv 0 \) modulo \( \text{rad } \Lambda \). Indeed, for \( s \) in (3.4.1) we have \( T(s) = T(\gamma_f(t)) \equiv 0 \) modulo \( \pi^{m+1} \Lambda^\Omega \) by (3.4), and here \( m + 1 = p + n \). Thus \( p(z + wz^p) \equiv 0 \) modulo \( \pi^p \Lambda^\Omega \), and so \( z + wz^p \equiv 0 \) modulo \( \pi \Lambda^\Omega \subset \text{rad } \Lambda \). However, \( \gamma(t) = z + \gamma_f(t) + \gamma_i(t) \), and the terms \( \gamma_f(t), \gamma_i(t) \) lie in \( \pi \Lambda^\Omega \subset \text{rad } \Lambda \) by (3.3), (3.5). Hence \( \gamma(t) + w \gamma(t)^p \) lies in \( \text{rad } \Lambda \).
Since \( w \equiv -1 \pmod{\pi} \) the image of \( \pi(t) \) in \( \Lambda/\text{rad} \Lambda \equiv F \) belongs to the prime field \( F_p \), say \( \gamma(t) \equiv i \cdot 1 \) modulo \( \text{rad} \Lambda \), where \( i \in \mathbb{Z} \). Choose a homomorphism \( \nu: G \to C \) with \( \Omega \) in the kernel and with \( \nu(t) = c^i \), and let \( \beta \) be the automorphism \( \beta(g) = g \nu(g) \) (\( g \in G \)) of \( C \). Then
\[
\beta(t) t^{-1} - 1 = (c - 1)((c^i - 1)/(c - 1)) = \sigma \gamma(t) \quad \text{modulo} \quad \pi \text{ rad} \Lambda.
\]
Replacing \( \alpha \) with \( a \beta^{-1} \) we now have \( \gamma(t) \in \text{rad} \Lambda \).

This condition is retained in (3.3) and (3.5), by d) of (3.3), so the first line of this part (3.6) of the proof may be repeated, this time with \( \gamma(t) \in \text{rad} \Lambda \).

Since \( p - 1 > 0 \), and \( \gamma(t) \in \text{rad} \Lambda \) at this point, by the above discussion, we now know that \( \gamma_0(t) = \gamma(t) - \gamma_f(t) - \gamma_f(t) \) lies in \( \text{rad} \Lambda \), thus in \( \text{rad} \Lambda^2 \).

In particular \( 1 + wz^{p-1} \) is a unit, if \( z = \gamma_0(t) \) and \( w \in R \). However, (3.4.1) shows for \( z = \gamma_0(t) \) and some \( w \in R \) that \( z(1 + wz^{p-1}) \) belongs to \( T(\pi^n\Lambda^\Omega) + \pi^{n+1}\Lambda^\Omega \subseteq \pi^n I \), where \( I \) is the trace ideal in the ring \( L \), both described in (3.3.1). Recall that the ring \( L \) is just the space of elements of \( \Lambda^2 \) fixed by \( t \) modulo \( \text{rad} \Lambda^2 \). So \( z, 1 + wz^{p-1}, \) and \( (1 + wz^{p-1})^{-1} \) all belong to \( L \), and we have
\[
z \in \pi^n I.
\]

Applying the projection operator \( pr_0 \) to this expression, we obtain from (3.3.1) that
\[
z \in \pi^{n+1}\Lambda^\Omega,
\]
and so certainly \( \gamma_0(t) = z \) belongs to \( \pi^{n+1}\Lambda \), along with \( \gamma_f(t) \) and \( \gamma_f(t) \). Thus \( \gamma(t) \in \pi^{n+1}\Lambda \), which was our goal. This concludes the chapter.

4. Transfer and Lie filtrations

We continue with most of the notation of the previous chapter: \( G \) is a finite \( p \)-group, \( C = \langle c \rangle \) is a central subgroup of order \( p \) contained in the Frattini subgroup \( \text{Fr}(G) \), \( S \) is a complete discrete valuation domain of characteristic 0 with residue field \( F = S/\mathfrak{m} \) of characteristic \( p \), \( \Lambda \) is the ring \( SC/CSC \) where \( C \) is the sum of the elements of \( C \), \( R \) is the ring \( S[\pi] \) where \( \pi = c - 1 \) in \( \Lambda \), and \( \mathfrak{m} = \mathfrak{m} + \pi R \). \( Z(G, C) \) is the inverse image in \( G \) of \( Z(G/C) \). Finally, \( \alpha \) is an \( R \)-algebra automorphism of \( \Lambda \) which is the identity modulo \( \pi \Lambda \).

Temporarily let \( t \) and \( \Omega \) be as in Chapter 3. Repeatedly applying (3.0), and thus repeatedly modifying \( \alpha \) by inner and group automorphisms trivial on \( \Lambda/\pi \Lambda \), we can obtain, in the terminology of Chapter 3, that \( \gamma(t) \in \pi^n \Lambda \) for any given large integer \( N \). By (1.2.4) we can further compose \( \alpha \) with an inner automorphism, conjugation by \( 1 + \pi^M \lambda \) for some \( \lambda \in \Lambda \) and large \( M \) (depending on \( N \)), so that the new \( \alpha \) is the identity on \( \langle \Omega, t \rangle \). Repeating this whole
procedure with further $t$'s, we may enlarge $\Omega$ until it is all of $C_G(Z(G, C))$. Thus:

(4.0) We may assume $\alpha$ is the identity on $\Omega$ for $\Omega = C_G(Z(G, C))$.

It should be noted that $\Omega = C_G(Z(G, C))$ is a huge subgroup of $G$, in particular it contains the Frattini subgroup.

We now fix the above notation for $\Omega$.

Condition (4.0) on $\alpha$ is, of course, in addition to our condition that $\alpha$ be the identity modulo $\pi\Lambda$. If $S = C_p$, then we can quickly arrange at the same time that $\alpha$ be the identity modulo $\pi\Lambda$. Fortunately, this is implied as well by (4.0) in the general case:

(4.0.1) We may assume as well that $\alpha$ is the identity modulo $\pi\Lambda$.

Proof of (4.0.1). We will show that $\alpha$ may be modified to satisfy (4.0.1). That is, the map $\alpha$ may be composed with inner automorphisms of $\Lambda$ trivial on $\Lambda/\pi\Lambda$ and on $\Omega = C_G(Z(G, C))$ so that the new $\alpha$ is the identity modulo $\pi\Lambda$.

If $H$ is a subgroup of $C$ containing $C$, we let $J(H)$ denote the image, plus $\mathfrak{f} \cdot 1$, of the augmentation ideal of $sH$ in $A$. (The notation is discussed more fully in (4.2) below.) Let $\nu$ denote the $S$-linear map

$$A \to \nu A/\nu A \oplus A/\nu A \oplus F$$

induced by $\pi \gamma$ (where $\alpha(g) = (1 + \pi \gamma(g))g$ for $g \in G$), and let $\tilde{\nu}$ denote the induced linear functional on $J(G)/(J(G)^2 + \mathfrak{f} A) \cong F \otimes_{\mathfrak{f} p} (G/\text{Fr}(G))$. (The isomorphism is a standard one; cf. (4.2) below). To see that $\tilde{\nu}$ defined on $J(G)$ does indeed vanish on $J(G)^2 + \mathfrak{f} A$, one can use the fact that $\gamma$ vanishes on $\Omega \cong \text{Fr}(G)$, though it also follows from cocycle equations; cf. (3.2).) Since $\alpha$ is the identity on $\Omega = C_G(Z(G, C))$ by (4.0), $\tilde{\nu}$ vanishes on $\Omega$ and so induces a map which we also denote by $\tilde{\nu}$, on $V = J(G)/(J(G)^2 + J(\Omega) + \mathfrak{f} A) \cong F \otimes_{\mathfrak{f} p} (C/\Omega)$.

However, the group commutator map

$$G/C_G(Z(G, C)) \times Z(G, C)/Z(G) \to C \cong F_p$$

is clearly a nondegenerate pairing of $F_p$ vector spaces. If $x \in G$ and $y \in Z(G, C)$, then $(x - 1)(y - 1) - (y - 1)(x - 1) = xy - yx = (xy^{-1}y^{-1} - 1)yx = xy^{-1}y^{-1} - 1$ modulo $\pi\Lambda$, since $xy^{-1}y^{-1} - 1$ is in $\pi\Lambda$. Consequently, the ring theoretic commutator $[\ , \ ]$ gives a nondegenerate pairing

$$V \times W \to F$$

with $V$ as above, $W = J(Z(G, C))/(J(Z(G, C))^2 + J(Z(G)) + \mathfrak{f} S(Z(G, C))$ and
$F$ is identified with $\pi \Lambda / \pi \text{rad} \Lambda$. The term $SZ(G, C)$ is of course understood as
the image in $\Lambda$ of the group algebra of $Z(G, C)$.

Thus we can choose $w \in W$ such that $\tilde{\rho}(v) = (v, w)$ for all $v \in V$, using
the above form. If $z \in J(Z(G, C))$ represents $w$, then (noting $\rho(1) = 0$) we have

$$\rho(x) \equiv [x, z] \mod \pi \text{rad} \Lambda$$

for all $x \in \Lambda$. Observe $z \in \text{rad} \Lambda$, so $1 + z$ is a unit. The reader may now easily
check using (1.6.1), that multiplying $\alpha$ on the right with conjugation by
$(1 + z)^{-1}$ results in a new $\alpha$ which is the identity modulo $\pi \text{rad} \Lambda$. Of course,
$1 + z$ centralizes $\Omega$ and $\Lambda / \pi \Lambda$; so the proof is complete.

Now define $\phi: \Lambda \to \text{rad} \Lambda \subseteq \Lambda$ by

$$\alpha(x) = x + \pi \phi(x) \quad (x \in \Lambda).$$

The goal of this chapter is to establish the following:

(4.1) Goal. The automorphism $\alpha$ may be composed with inner automor-
phisms of $\Lambda$ so that the new $\alpha$ still is the identity modulo $\pi \text{rad} \Lambda$, and in
addition the new $\phi$ satisfies

$$\phi^2(\Lambda) \subseteq \text{rad}^2 \Lambda.$$ 

We also will maintain the condition that $\alpha$ is the identity on $\Omega$, which is
useful for the proof, though it is not necessary for the application of (4.1) in
Chapter 5.

Just to keep notation as simple as possible, it is useful to note that
(4.1.1) $\pi \subseteq \text{rad}^2 \Lambda$,
which follows from $C \subseteq \text{Fr}(G)$. Thus \text{rad}^2 \Lambda + \mu \Lambda = \text{rad}^2 \Lambda + \mu \Lambda$. It is also
useful to note $\text{rad}^2 \Lambda + \mu \Lambda = \text{rad}^2 \Lambda + \mu \cdot 1$, since $\mu \Lambda = \mu(\text{rad} \Lambda + S)$.

(4.2) Notation. If $H$ is a subgroup of $G$ containing $C$, we let $J(H)$ denote
the image, plus $\mu \cdot 1$, of the augmentation ideal of $SH$ in $\Lambda$. (This augmentation
ideal, incidentally, contains $\mu \cdot 1$, if $S = \mathbb{Z}_p$, since $p = p - C$ in $\Lambda$.) Note that
the image of $J(H)$ in $FG/C$ identifies naturally with the augmentation ideal of
$FH/C$. It also is useful to note that $J(H) + \text{rad}^2 \Lambda \supseteq \mu \cdot 1 + \text{rad}^2 \Lambda \supseteq \mu \Lambda$ is
the full inverse image in $\Lambda$ of $I(FH/C) + I^2(FG/C)$. We will freely use the
standard identification of $I(F \mu G/C)/I^2(F \mu G/C)$ with the Frattini quotient
$G/\text{Fr}(G)C$, which here is $G/\text{Fr}(G)$, of $G/C$.

Another useful consequence of $\mu \cdot 1 \supseteq J(H)$ is that $J(H)$ is the radical of
the image of $SH$ in $\Lambda$. We will sometimes just denote this image also by $SH$
when it is clear we are working in $\Lambda$. In particular, $SH \cap \text{rad} \Lambda = J(H)$, since
the radical of any $S$-subalgebra of $\Lambda$ is its intersection with $\text{rad} \Lambda$. 
The argument establishing the next lemma can be rephrased without transfer, and perhaps even shortened, by quoting previous discussions, as we indicate. However, we think it is instructive, and have retained the argument in its original form.

(4.3) Lemma. \( \phi(\Lambda) \subseteq J(Z(G, C)) + \text{rad}^2\Lambda \).

Proof. It suffices, of course, to show \( \phi(G) \subseteq J(Z(G, C)) + \text{rad}^2\Lambda \). For \( g \in G \), write \( \alpha(g) = \mu(g)g \) and \( \mu(g) = 1 + \pi\gamma(g) \). Thus \( \phi(g) = \gamma(g)g \), and so it suffices to show \( \gamma(G) \subseteq J(Z(G, C)) + \text{rad}^2\Lambda \), since the latter module is contained in \( \text{rad} \Lambda \), and \( G \) acts trivially on \( \Lambda/\text{rad}^2\Lambda \) by right multiplication.

Note that

\[
\text{rad}(SZ(G, C) + \text{rad}^2\Lambda) = (\text{rad}A \cap SZ(G, C)) + \text{rad}^2\Lambda
\]

so it suffices to show \( \gamma(G) \subseteq SZ(G, C) + \text{rad}^2\Lambda \), since we already know \( \gamma(G) \subseteq \text{rad} \Lambda \). The reader understands, of course, that the notation \( SZ(G, C) \) means in this context the \( S \)-span in \( \Lambda \) of \( Z(G, C) \).

Observe that

\[
SZ(G, C) + \text{rad}^2\Lambda \supseteq SZ(G, C) + \frac{1}{2} \Lambda + [\Lambda, \Lambda]
\]

where \([x, y]\) means \( xy - yx \) \( (x, y \in \Lambda) \). Thus it suffices to show \( \gamma(G) \subseteq SZ(G, C) + \frac{1}{2} \Lambda + [\Lambda, \Lambda] \). The latter is the full inverse image of \( FZ(G, C) + [FG/C, FG/C] \) under the natural homomorphism \( \Lambda \to FG/C \).

Put \( \Lambda = FG/C \) and let \( \tilde{\gamma} \) denote the function obtained by composing \( \gamma \) with the above map \( \Lambda \to \Lambda \). At this point we simply want to show \( \tilde{\gamma} \) takes values in \( FZ(G, C) + [\Lambda, \Lambda] \). (The alternate proof of (4.3) is to read this off from the proofs of Claim 1 and Claim 2 in (3.3), noting \( \tilde{\gamma}(t) \) is a coboundary and allowing \( i = 0 \) in the discussion of \( \gamma_i(t) \) in terms of class sums. In our context here, \( t \) is an element of \( G \), perhaps not in \( C_\mathbb{F}(Z(G, C)) \), though this only indicates possible \( FZ(G, C) \) terms in \( \tilde{\gamma}(t) \).) As argued in (3.2), the function \( \tilde{\gamma} \) is a cocycle, and thus defines a class \( [\tilde{\gamma}] \in H^1(G, \Lambda) \). Consider now the cohomology group \( H^1(G, \Lambda/[\Lambda, \Lambda]) \) and the natural map \( H^1(G, \Lambda) \to H^1(G, \Lambda/[\Lambda, \Lambda]) \). Since \( C \) acts trivially in its conjugation action on \( \Lambda/[\Lambda, \Lambda] \), the \( G \)-cohomology classes with coefficients in the latter consist each of single cocycles. Thus we can work at the cohomology level and show that the image of \( [\tilde{\gamma}] \) in \( H^1(G, \Lambda/[\Lambda, \Lambda]) \) lies in the image of \( H^1(G, FZ(G, C)) \) under the map on cohomology induced by the natural map

\[
FZ(G/C) \subseteq FG/C = \Lambda \to \Lambda/[\Lambda, \Lambda].
\]
To do this we recall that $\overline{\Lambda}$ is a direct sum of induced modules

$$\overline{\Lambda} = \bigoplus_i F|_{H_i}^G$$

according to the decomposition of $G/C$ into conjugacy classes. Here $H_i/C$ is the centralizer in $G/C$ of an element $x_i \in G/C$, and the $x_i$'s together form a complete system of representatives for the conjugacy classes of $G/C$. Each $FG$-module $F|_{H_i}^G$ has a unique quotient isomorphic to $F$, and it is the quotient by a submodule lying in $[\Lambda, \Lambda]$. This was first discovered by Ward [36]; essentially, the point is that $y x_i - x_i = (yx_i)y^{-1} - y^{-1}(yx_i)$ if $y \in G/C$. Conversely, $[\Lambda, \Lambda]$ is contained in and thus equal to, the sum of these submodules. Hence we have a commutative diagram

$$\begin{array}{ccc}
\Lambda & \longrightarrow & \overline{\Lambda}/[\overline{\Lambda}/\Lambda] \\
\uparrow & & \uparrow \\
\bigoplus_i F|_{H_i}^G & \longrightarrow & \bigoplus_i F
\end{array}$$

where the vertical maps are natural isomorphisms. It is easy to identify $FZ(G/C)$ in this picture. It is precisely the direct sum of all terms $F|_{H_i}^G$ where $x_i \in Z(G/C)$, or in other words $H_i = G$. Thus we are reduced to showing that the projection of $[\gamma]$ on $H^1(G, F|_{H_i}^G)$ has zero image in $H^1(G, F)$ when $H_i \neq G$.

However, we know $\gamma$ vanishes on $\Omega$, hence on $Fr(G)$. Since $H_i \neq G$, we have also $H_i Fr(G) \neq G$. Thus by (1.4.2) the transfer map

$$H^1(H_i, Fr(G)/Fr(G), F) \rightarrow H^1(G/Fr(G), F)$$

is zero. Consider now the diagram

$$\begin{array}{ccc}
H^1(H_i, F) & \longrightarrow & H^1(G, F) \\
\downarrow & & \downarrow \\
H^1(H, Fr(G), F) & \longrightarrow & H^1(G/Fr(G), F)
\end{array}$$

where the top triangle is obtained from the isomorphism $H^1(H_i, F) \cong H^1(G, F|_{H_i}^G)$ of Shapiro's lemma, the map $H^1(G, F|_{H_i}^G) \rightarrow H^1(G, F)$ discussed above, and transfer $H^1(H_i, F) \rightarrow H^1(G, F)$. An easy dimension shift shows this triangle is commutative. The lower triangle consists entirely of transfer maps,
and is also commutative. The inverse of the Shapiro lemma map is a simple projection (a fact which may also be obtained by dimension-shifting), and so the image of $[\gamma]$ in the left-hand term $H^1(H, F)$ vanishes on restriction to $H \cap Fr(G)$. By Tate's Mackey formula for transfer [5, XII, Prop. 9.1], the image of $[\gamma]$ in the bottom term vanishes on restriction to $H^1(Fr(G), F)$, hence is inflated from $H_1 Fr(G)/Fr(G)$. Since inflation commutes with transfer, the lemma follows.

Returning to the map $\phi$, we note

\[(4.4.1) \quad \phi(xy) = \phi(x)y + \alpha(x)\phi(y) \quad (x, y \in \Lambda)\]

as follows immediately from $\alpha(xy) = \alpha(x)\alpha(y)$ and the definition of $\phi$. In particular $\phi(rad^2 \Lambda) \subseteq rad^2 \Lambda$. Since $\phi(\Omega) = 0$, and $Z(Z(G, C)) = Z(G, C) \cap C(Z(G, C)) = Z(G, C) \cap \Omega$, we have also $\phi(Z(Z(G, C))) = 0$. In particular $\phi$ stabilizes $J(Z(Z(G, C))) + rad^2 \Lambda$, and by (4.3), $\phi$ certainly stabilizes $J(Z(G, C)) + rad^2 \Lambda$. Define

\[\text{(4.4.2)} \quad V = \frac{J(Z(G, C)) + rad^2 \Lambda}{J(Z(Z(G, C))) + rad^2 \Lambda} \cong F \otimes \frac{Z(G, C)Fr(G)}{Z(Z(G, C))Fr(G)}\]

the tensor products taken over $F_\ell$. The first isomorphism here is standard, and the second follows from the fact that

\[Z(G, C) \cap (Z(ZG, C))Fr(G) = Z(Z(G, C))(Z(G, C) \cap Fr(G)) \]

\[= Z(Z(G, C)),\]

since $Z(G, C) \cap Fr(G) \subseteq Z(G, C) \cap \Omega - Z(ZG, C)$. As follows from the remarks above,

\[\text{(4.4.3)} \quad \text{The map } \phi \text{ induces a map } \bar{\phi}: V \to V.\]

Because $\phi(G) \subseteq J(Z(G, C)) + rad^2 \Lambda$ and $\phi(Z(Z(G, C))) = 0$, to get $\phi^3(G) \subseteq rad^2 \Lambda$ we need only modify $\phi$ so that $\bar{\phi}$ becomes 0 on $V$. We record this below.

\[\text{(4.4.4) Reduction. To achieve the goal (4.1) it is enough to compose } \alpha \text{ with inner automorphisms which are the identity modulo } \pi \text{ rad } \Lambda \text{ and are the identity on } \Omega \text{ so that the new } \bar{\phi} \text{ is 0 on } V.\]

The condition regarding $\Omega$ is necessary to insure the validity of the reduction to $V$. We do indeed have a supply of such inner automorphisms with which to modify $\alpha$ and $\phi$. 

(4.5) Proposition. Let \( I \) be a finite index set and suppose for each \( i \in I \) there are elements \( r_i \in R \) and \( y_i, z_i \in Z(G, C) \). Put \( b = \sum r_i(y_i - 1)(z_i - 1) \). Let \( \beta \) be the inner automorphism of \( \Lambda \) which is conjugation by \( 1 + b \). Then

i) \( \beta \) is the identity modulo \( \pi \rad \Lambda \);

ii) \( \beta \) is the identity on \( \Omega \);

iii) If \( \phi' \) denotes the new function \( \phi \) associated with the automorphism \( \alpha' = \alpha \circ \beta \), then

\[
\phi'(x) = \phi(x) + \frac{1}{\pi} [b, x] \mod \pi \rad^2 \Lambda \quad (x \in \Lambda).
\]

Proof. We have for \( x \in \Lambda \),

\[
\beta(x) = x + [1 + b, x] (1 + b)^{-1} \equiv x + [b, x] \mod ([b, x] \rad^2 \Lambda),
\]

since \( b \in \rad^2 \Lambda \).

Now \( [b, x] = \sum r_i((y_i, x)(z_i - 1) + (y_i - 1)(z_i, x)) \) lies in \( \pi \rad \Lambda \), since for \( y \in Z(G, C) \) and \( x \in G \)

\[
[y, x] = yx - xy = (y'x - x)y = (c'y - x)y
\]

for some integer \( j \). However, \( (c'^{j} - 1)xy = ((c'^{j} - 1)/(c' - 1))\tau xy \) is clearly in \( \pi \Lambda \). Thus i) holds, and we also get

\[
\beta(x) \equiv x + [b, x] \mod \pi \rad^2 \Lambda \quad \text{(even \( \pi \rad^3 \Lambda \)).}
\]

Note that \( \alpha(\pi \lambda) = \pi \alpha(\lambda) = \pi \lambda \mod \pi^2 \rad \Lambda \subseteq \pi \rad^2 \Lambda \), for any \( \lambda \in \Lambda \). This applies in particular to \( \pi \lambda - [b, x] \), and so

\[
(\alpha \circ \beta)(x) \equiv x + \pi \phi(x) + [b, x] \mod \pi \rad^2 \Lambda.
\]

We now obtain iii) from the definition of \( \phi' \) by dividing by \( \pi \). Since each \( y_i \) and \( z_i \) defining \( b \) lies in \( Z(G, C) \), the element \( b \) centralizes \( \Omega \), and so ii) is clear. This completes the proof of the proposition.

(4.6) A bilinear form on \( V \). To analyze the term \( 1/\pi [b, x] \) above, it is useful to introduce a bilinear form on \( V \). Of course \( V \cong F \otimes (Z(G, C)/Z(Z(G, C))) \) carries the nondegenerate group commutator form \( V \times V \to F \otimes C \cong F \), but we need to relate this to the ring commutator. If \( x, y \in G \), let \( \{ x, y \} \) denote the group commutator \( xyx^{-1}y^{-1} \). Thus \( [x, y] = ((x, y) - 1)yx = (x, y) - 1 + ((x, y) - 1)(yx - 1) \). So if \( x \) or \( y \) belongs to \( Z(G, C) \) then

\[
[x, y] \in \pi \Lambda,
\]

and

\[
[x, y] = (x, y) - 1 \mod \pi \rad \Lambda.
\]
Hence we can define a *nondegenerate skew-symmetric bilinear form* 
\[( , ): V \times V \to \Lambda/\text{rad} \Lambda \cong F\]
by identifying \(\pi\Lambda/\pi \text{rad} \Lambda \cong \Lambda/\text{rad} \Lambda \cong F\), and setting \((v, w) - [x, y] - [x - 1, y - 1]\) modulo \(\pi \text{rad} \Lambda\), if \(x, y \in Z(G, C)\) and \(v, w\) are the cosets in \(V\) containing \(x - 1, y - 1\):

\[v = x - 1 + (J(Z(Z(G, C)))) + \text{rad}^2 \Lambda,\]
\[w = y - 1 + (J(Z(Z(G, C)))) + \text{rad}^2 \Lambda.\]

Equivalently,

\[(v, w) = \frac{1}{\pi} [x - 1, y - 1] \mod \text{rad} \Lambda.\]

Observe that \([x - 1, J(Z(Z(G, C)))) + \text{rad}^2 \Lambda] \subseteq [x - 1, \text{rad} \Lambda]\text{rad} \Lambda + \text{rad} \Lambda [x - 1, \text{rad} \Lambda] \subseteq \pi \text{rad} \Lambda\) by (4.6.1). A similar statement holds for \(y - 1\). This gives the useful generalization:

\[(4.6.3)\] If \(x, y, v, w\) are as above, and \(s \in v, t \in w\), then

\[(v, w) = \frac{1}{\pi} [x - 1, t] \mod \text{rad} \Lambda,\]

and also

\[(v, w) = \frac{1}{\pi} [s, y - 1] \mod \text{rad} \Lambda.\]

Next we interpret the term \(\frac{1}{\pi} [b, x]\) of (4.5 iii) in terms of the form \(( , )\).

\[(4.6.4)\] **Proposition.** Let \(b = \sum \tau_i (y_i - 1)(z_i - 1)\) as in (4.5), and let \(v_i, w_i\) be the elements of \(V\) which \(y_i - 1, z_i - 1\) represent. Let \(\tilde{r}_i\) be the element of \(F \cong R/\mu R\) represented by \(r_i\). Again denote by \(\beta\) the inner automorphism of \(\Lambda\) which is conjugation by \(1 + b\), and let \(\tilde{\phi}'\) denote the new function \(\tilde{\phi}\) (cf. (4.4.3)) associated with the automorphism \(\alpha' = \alpha \circ \beta\). Then

\[\tilde{\phi}'(u) = \tilde{\phi}(u) + \sum \tilde{r}_i ((v_i, u) w_i + (w_i, u) v_i) \quad (u \in V).\]

**Proof.** The space \(V\) is spanned by those \(u\) represented by an element \(x - 1\) with \(x \in Z(G, C)\); so it suffices to prove the formula for one of these. From (4.5) we have

\[\phi'(x - 1) \equiv \phi(x - 1) + \frac{1}{\pi} [b, x - 1] \mod \text{rad}^2 \Lambda\]

\[- \phi(x - 1) + \sum \tau_i ([y_i, 1, x - 1] (z_i - 1))\]

\[+ (y_i - 1)[z_i - 1, x - 1]).\]
Now \((1/\pi)[z, -1, x - 1]\) is \((w, u)\) modulo \(\Lambda\) and certainly commutes with \(z, -1\) modulo \(\pi^2\Lambda\). Also \((1/\pi)[y, -1, x - 1]\) is \((v, u)\) modulo \(\Lambda\). The proposition follows immediately.

(4.7) Classical Lie algebras; concluding the proof of (4.1).

In view of (4.6.4) our job now is to show \(\phi\) lies in the span of the set of linear transformations \(V \rightarrow V\) of the form \(u \rightarrow (v, u)w + (w, u)v, u, v, w \in V\). Not all linear transformations from \(V\) to itself lie in this span, but fortunately \(\phi\) is not arbitrary.

(4.7.1) Proposition. The map \(\overline{\phi}\) of (4.4.3) satisfies
\[
(\overline{\phi}(u), v) + (u, \overline{\phi}(v)) = 0 \quad (u, v \in V).
\]
Also, if \(p = 2\),
\[
(u, \overline{\phi}(u)) = 0 \quad (u \in V).
\]

Proof. Without loss of generality we may assume \(u, v\) are represented by \(x - 1, y - 1\) where \(x, y \in Z(G, C)\). From (4.4.1) we have
\[
\phi((x - 1)(y - 1)) = \phi(x - 1)(y - 1) + \alpha(x - 1)\phi(y - 1)
\]
\[
= \phi(x - 1)(y - 1) + (x - 1)\phi(y - 1)
\]
modulo \(\pi\) rad \(\Lambda\) (even modulo \(\pi\) rad \(\pi^2\Lambda\)).

Interchanging the roles of \(x\) and \(y\) gives a second congruence, which when subtracted from the first gives
\[
\phi([x - 1, y - 1]) = [\phi(x - 1), y - 1] + [x - 1, \phi(y - 1)]
\]
modulo \(\pi\) rad \(\Lambda\).

Since \([x - 1, y - 1] \in \pi\Lambda \cap SZ(G, C) = \pi SZ(G, C)\) by (4.6.1), and since \(\phi(SZ(G, C)) \subseteq \pi \phi(SZ(G, C)) \subseteq \pi \text{ rad } \Lambda\), the left-hand term of the above congruence is zero modulo \(\pi\) rad \(\Lambda\). Dividing by \(\pi\), we have
\[
0 = \frac{1}{\pi} [\phi(x - 1), y - 1] + \frac{1}{\pi} [x - 1, \phi(y - 1)] \quad \text{modulo rad } \Lambda.
\]

However, by (4.6.3) we have that
\[
(\overline{\phi}(u), v) = \frac{1}{\pi} [\phi(x - 1), y - 1] \quad \text{modulo rad } \Lambda,
\]
and
\[
(u, \overline{\phi}(v)) = \frac{1}{\pi} [x - 1, \phi(y - 1)] \quad \text{modulo rad } \Lambda.
\]

This gives the first equation of the proposition.
For the second, when \( p = 2 \), note that the \( Z(G, C)/Z(Z(G, C)) \) is elementary abelian, so that in particular \( x^2 \subset Z(Z(G, C)) \subseteq \Omega \), giving \( \alpha(x^2) = x^2 \). Expanding \( \alpha(x^2) = \alpha(x)^2 = (x + \pi\phi(x))^2 \), we get

\[
0 = \pi(x\phi(x) + \phi(x)x) + \pi^2\phi(x)^2 \equiv \pi[x, \phi(x)] \mod \pi^2 \text{rad} \Lambda.
\]

(Note \( \pi\phi(x)x = -\pi\phi(x)x + 2\pi\phi(x)x \). Since \( \phi(x) = \phi(x - 1) \) and \( [x, \phi(x - 1)] = [x - 1, \phi(x - 1)] \), we have

\[
0 = \frac{1}{\pi}[x - 1, \phi(x - 1)] \mod \text{rad} \Lambda.
\]

Again applying (4.6.3), we get \( 0 = (u, \phi(u)) \), and the proof of the proposition is complete.

(4.7.2) Concluding arguments for achieving (4.1). By (1.5.1) the linear transformations \( \phi \) satisfying the conclusion of (4.7.1) do indeed lie in the span of the set of linear transformations \( V \rightarrow V \) of the form \( u \rightarrow (v, u)w + (w, u)v - ((u, v)w + (u, w)v) \). Hence we may assume \( \phi = 0 \) by (4.6.4). Now (4.1) is obtained from (4.4.4). This achieves the goal of this chapter.

It is interesting to note that Lazard, in his comprehensive treatment of \( p \)-adic analytic groups [21], defined two kinds of Lie algebra structures on such a group. The first was in characteristic \( p \), and, for the case of units in \( p \)-adic group rings of \( p \)-groups, essentially equivalent to that of Jennings [17], also studied later by Quillen [23]. The present chapter may be viewed as having achieved its aims through analyzing this characteristic \( p \) structure. Similarly the next chapter is philosophically near Lazard's characteristic zero Lie structure, though the arguments involved here are more delicate.

5. Logarithms and Theorem 2; Conclusion

(5.0) Notation. In this chapter \( p \) is a fixed prime, \( S \) is a complete discrete valuation domain of characteristic 0 with \( p \) belonging to the maximal ideal \( \mathfrak{p} \) of \( S \), and \( \Lambda \) is an \( S \)-free \( S \)-algebra of finite rank over \( S \).

We assume also that we have an element \( \pi \) in the center of \( \Lambda \) which is not a zero divisor in \( \Lambda \) and which satisfies \( \pi^{p-1} \in p\Lambda \).

Our condition on \( \pi \) ensures that, if \( \phi \in \text{End}_S \Lambda \) commutes with (multiplication by) \( \pi \), then

\[
\log(1 + \pi\phi) = -\sum_{i=1}^{\infty} \frac{(-1)^i}{i} (\pi\phi)^i = -\pi \sum_{i=1}^{\infty} (-1)^i \left( \frac{\pi^{i-1}}{i} \right) \phi^i = \pi D
\]
for some $D \in \text{End}_S \Lambda$, since $\pi^{-1}/i$ belongs to $\text{End}_S \Lambda$ and converges to 0 in the
$p$-adic topology.

(5.1) **Lemma.** Suppose $\alpha$ is an $S[\pi]$-automorphism of $\Lambda$ which is the
identity modulo $\pi \Lambda$, and put $\alpha = 1 + \pi \phi$ for some $\phi \in \text{End}_S \Lambda$. (Note that this
can be done, since $\pi$ is not a zero divisor.) Then $\log \alpha = \pi D$ where $D$ is an
$S[\pi]$-linear derivation from $\Lambda$ to itself.

**Proof.** As noted, we have $\log \alpha = \log(1 + \pi \phi) = \pi D$ for some $D \in \text{End}_S \Lambda,$
and $D$ clearly commutes with $\pi$.

Using differentiation with respect to $t$, observe the formal identity

$$\log(1 + xt)(1 + yt) = \log(1 + xt) + \log(1 + yt)$$

in $K[x, y][[t]]$, where $x, y, t$ are commuting indeterminates and $K$ is the
quotient field of $S$. Apply this in the $K$-algebra $B = K \otimes_S (\text{End}_T \Lambda \otimes_T \text{End}_T(\Lambda)),$
where $T = S[\pi]$ and $x$ is specialized to $1 \otimes (\phi \otimes 1)$, $y$ to $1 \otimes (1 \otimes \phi)$, and $t$ to
$1 \otimes (\pi t 1) = 1 \otimes (1 \otimes \pi)$. 

To interpret the result, let $F = 1 \otimes (\pi \phi \otimes 1 + 1 \otimes \pi \phi + \pi \phi \otimes \pi \phi)$ be the
image of $(1 + xt)(1 + yt) - 1$, and let $\omega: K \otimes_S (\Lambda \otimes_T \Lambda) \rightarrow K \otimes_S \Lambda$ be the
map induced by multiplication. The domain $M = K \otimes_S (\Lambda \otimes_T \Lambda)$ of $\omega$ is of
course a natural $B$-module, and we let $b \in \text{End}_K M$ denote the transformation
induced by a given $b \in B$.

Since $\alpha$ is an automorphism, we have for $u, v \in \Lambda$, that

$$\pi \phi(u) + \pi \phi(v) + \pi \phi(u) \pi \phi(v) = \pi \phi(uv).$$

This says precisely that $\pi \phi \omega = \omega \Phi$ as maps $M \rightarrow K \otimes_S \Lambda$. Consequently,
$(\pi \phi)^i \omega = \omega \Phi^i$ for all $i \geq 0$, and so

$$(\log(1 + \pi \phi)) \omega = \omega \log(1 + \Phi) = \omega \log(1 + \Phi)$$

However, our identity gives

$$\log(1 + \Phi) = \log(1 \otimes (1 + \pi \phi \otimes 1)) + \log(1 \otimes (1 + 1 \otimes \pi \phi))$$

$$= 1 \otimes (\log(1 + \pi \phi) \otimes 1) + 1 \otimes (1 \otimes \log(1 + \pi \phi)),$$

the last step obtained by expanding the log terms and rewriting. (Or note that
$f \mapsto f \otimes 1$ is a continuous homomorphism $\text{End}_T \Lambda \rightarrow \text{End}_T \Lambda \otimes_T \text{End}_T \Lambda$, as is
$f \mapsto 1 \otimes f$, for $f \in \text{End}_T \Lambda$.) Substituting in the above equation and applying
both sides to $1 \otimes (u \otimes v) \in M$ give

$$\log(1 + \pi \phi)(uv) = (\log(1 + \pi \phi)(u))v + u(\log(1 + \pi \phi)(v)).$$

Thus $\pi D$, and hence $D$, is a derivation, and the proof is complete.
We remark that our hypothesis \( \pi^{p-1} \in p\Lambda \) was used only to get \( D \in \text{End}_{S}\Lambda \). For the fact that it is a derivation (of \( K \otimes_{S} \Lambda \)) we used only the convergence of \( \pi^{i-1}/i \) to 0, which follows if \( \pi^{e} \in p\Lambda \) for any particular \( e > 0 \).

We will now state the main result of this chapter. Put \( \tilde{\rho} = \rho + \pi S[\pi] \), where \( \rho \) is the maximal ideal of \( S \).

**Theorem 2.** Assume, in addition to the notation of (5.0), that \( \pi D \) is inner for every \( S[\pi] \)-linear derivation \( D \) from \( \Lambda \) to itself, and that \( \Lambda = Z(\Lambda) + \text{rad} \Lambda \) (which holds, for example, if \( \Lambda \) is local). Let \( \alpha \) be an \( S[\pi] \)-automorphism of \( \Lambda \), and put \( \alpha = 1 + \pi \rho \) for some \( \rho \in \text{End}_{S}\Lambda \). Assume also that

\[
\phi^{n}(\Lambda) \subseteq \text{rad}^{2}\Lambda + \tilde{\rho}\Lambda \quad \text{(some } n > 0) 
\]

or, equivalently (cf. 5.2 below), that \( \phi^{m} \to 0 \) in the \( p \)-adic topology as \( m \to \infty \). Then the automorphism \( \alpha \) of \( \Lambda \) is inner.

**(5.2) Lemma.** Let \( \alpha \) be an \( S[\pi] \)-algebra automorphism of \( \Lambda \) of the form \( \alpha = 1 + \pi \rho \) where \( \rho \in \text{End}_{S}\Lambda \) satisfies

\[
\phi^{n}(\Lambda) \subseteq \text{rad}^{2}\Lambda + \tilde{\rho}\Lambda 
\]

for some \( n > 0 \). Then \( \phi^{m} \to 0 \) in the \( p \)-adic topology of \( \text{End}_{S}\Lambda \), as \( m \to \infty \).

**Proof.** First observe the identity

\[
\phi(xy) = \phi(x)\alpha(y) + x\phi(y) \quad (x, y \in \Lambda)
\]

which follows from \( \pi \phi = \alpha - 1 \) and the fact that \( \alpha \) is an automorphism.

In other words, if \( \Phi \) is the operator \( \phi \otimes \alpha + 1_{\Lambda} \otimes \phi \) on \( \Lambda \otimes_{S} \Lambda \), and \( \omega: \Lambda \otimes_{S} \Lambda \to \Lambda \) is the multiplication, then \( \phi \omega = \omega \Phi \). Thus \( \phi^{q} \omega = \omega \Phi^{q} \) for each \( q \geq 0 \). If \( q \) is a power of \( p \), then the binomial theorem gives \( \Psi^{q} = \phi^{q} \otimes \alpha^{q} + 1_{\Lambda} \otimes \phi^{q} \) modulo \( p \text{End}_{S}\Lambda \otimes \text{End}_{S}\Lambda \); hence

\[
(5.2.1) \quad \phi^{q}(xy) = \phi^{q}(x)\alpha^{q}(y) + x\phi^{q}(y) \quad (q \text{ a power of } p),
\]

the congruence being modulo \( p\Lambda \).

Choosing also \( q \geq n \), we have

\[
\phi^{n}(\Lambda) = \phi^{n}\phi^{q-n}(\Lambda) \subseteq \phi^{n}(\Lambda) \subseteq \text{rad}^{2}\Lambda + \tilde{\rho}\Lambda.
\]

Taking \( x \in \text{rad} \Lambda \) and \( y \in \text{rad}^{4}\Lambda \), we deduce by induction on \( k \)

\[
\phi^{q}(\text{rad}^{k+1}\Lambda) \subseteq \text{rad}^{k+2}\Lambda + \tilde{\rho}\Lambda \quad (k \geq 0).
\]

Consequently, \( \phi^{q} \) is nilpotent on \( \Lambda/\tilde{\rho}\Lambda \). Thus \( \phi \) is certainly nilpotent on \( \Lambda/\tilde{\rho}\Lambda \), as well as \( \Lambda/p\Lambda \) and \( \Lambda/p^{e}\Lambda \) for any \( e \geq 0 \). (Note \( \phi(\rho\Lambda) = \rho\phi(\Lambda) \), and \( \rho \) is
nilpotent modulo $p \Lambda$ or $p' \Lambda$.) This gives $\phi^m \in p^r \text{End}_S \Lambda$ for all large $m$, and so $\phi^m \to 0$ as $m \to \infty$.

Q.E.D.

We are now ready for the proof of Theorem 2.

(5.3) **Proof of Theorem 2.** We want to show $\alpha$ is inner. We will successively modify $\alpha$ by inner automorphisms (composing it with them) until it is congruent to the identity modulo an arbitrarily large power of $\pi \Lambda$, then argue that we can take a limit. The inner automorphism we use on any (possibly modified) $\alpha = \gamma + \pi \phi$ will have the form

$$\beta = 1 + \pi \phi$$

as endomorphisms, where $\psi$ is an $S[\pi]$-linear endomorphism of $\Lambda$ which commutes with $\phi$. For fixed $\phi$, the set of such automorphisms $\beta$ is closed under multiplication (and inverses) and contains $\alpha$. We have $(\phi \psi)^n(\Lambda) \subseteq \text{rad}^n \Lambda + p \Lambda$ (and so $(\phi \psi)^m \to 0$ as $m \to \infty$, by (5.2)) for each of these automorphisms; so the hypotheses of the theorem will be maintained throughout the modifications.

The modification is done as follows, always the same way:

$$\log \alpha = \pi \phi \left(1 - \frac{\pi \phi}{2} + \cdots + \frac{(-1)^{p-1}}{p} \phi^{p-1} + \cdots\right) = \pi D$$

where $D$ is an $S[\pi]$-linear derivation on $\Lambda$, by (5.1). Thus $\pi D$ is inner and we may write $(\pi D)(x) = [a, x]$ $(x \in \Lambda)$ for some $a \in \Lambda$. Since $\Lambda = Z(\Lambda) + \text{rad} \Lambda$, we may take $a \in \text{rad} \Lambda$. Let $\beta$ be the inner automorphism which is conjugation by $1 - a$. Then (1.6.1) gives

$$\beta(x) = x - [a, x](1 - a)^{-1}$$

$$= x - \pi D(x)(1 - a)^{-1} \quad (x \in \Lambda).$$

Note $D(a) = (1/\pi)[a, a] = 0$. Hence the derivation $D$ commutes with multiplication by $a$. The equation for $\log \alpha$ shows $D$ has the form $\phi \eta$ where $\eta$ commutes with $\phi$ and lies in $1 + \phi E$, where $E$ is the closure of $S[\pi, \phi]$ in $\text{End}_{S[\pi]} \Lambda$. Actually, $S[\pi, \phi]$ is already closed as is $S[\pi]$, since $\Lambda$ (and thus $\text{End}_{S[\pi]} \Lambda$) is a finite rank $S$-algebra. Thus the powers of $\phi \eta$ span the same $S[\pi]$-submodule modulo $\phi^m E$ as the powers of $\phi$, if $m$ is any positive integer. (Use induction on $m$.) It follows that multiplication by $a$ commutes with $\psi$, as does multiplication by $(1 - a)^{-1}$, and so $\beta$ has the form mentioned at the beginning of the proof.

The equation for $\log \alpha$ shows

$$\pi D(x) \equiv \pi \phi(x) \pmod{\pi \phi^2(\Lambda)} \quad (x \in \Lambda).$$
Thus

\[
\alpha \beta(x) = \alpha(x - \pi D(x)(1 - a)^{-1})
\]

\[
\equiv x + \pi \phi(x) - \pi D(x)(1 - a)^{-1} \text{ modulo } \pi^2 \phi(\Lambda),
\]

since \(\alpha(y) = y + \pi \phi(y) \equiv y \text{ modulo } \pi \phi(\Lambda)\)

for every \(y \in \Lambda\),

\[
\equiv x + \pi \phi(x) - \pi D(x) \text{ modulo } \pi \phi(\Lambda)a + \pi^2 \phi(\Lambda),
\]

since \(D(\Lambda) \subseteq \phi(\Lambda)\) and \(\phi\) commutes with multiplication by \(a\),

\[
\equiv x \text{ modulo } \pi \phi^2(\Lambda) + \pi \phi(\Lambda)a + \pi^2 \phi(\Lambda),
\]

a congruence which has many consequences.

Put \(\alpha' = \alpha \beta\) and write \(\alpha' = 1 + \pi \phi'\). Then

\[
\phi'(\Lambda) \subseteq \phi^2(\Lambda) + \phi(\Lambda)a + \pi \phi(\Lambda), \quad \text{and}
\]

\[
(\phi')^m(\Lambda) \subseteq \phi^{m+1}(\Lambda) + \phi^m(\Lambda)a + \pi \phi^m(\Lambda) \quad (m > 0),
\]

since \(\phi' = \phi \psi\) for some \(S[\pi]\)-linear endomorphism \(\psi\) of \(\Lambda\) commuting with \(\phi\).

In particular, since \(a \in \text{rad } \Lambda\), if \(\phi^{m+1}(\Lambda) \subseteq \text{rad } \Lambda\), then \((\phi')^m(\Lambda) \subseteq \text{rad } \Lambda\).

Successively applying the construction, we can assume to start that \(\phi(\Lambda) \subseteq \text{rad } \Lambda\).

The same argument can now be repeated with \(\text{rad}^{N+1}(\Lambda)\) whenever we know \(\phi(\Lambda) \subseteq \text{rad}^N(\Lambda)\). (For the above argument, \(N = 0\).) Hence we can modify \(\alpha\) so that it is congruent to the identity modulo an arbitrarily large power of \(\text{rad } \Lambda\), and thus an arbitrarily large power of \(\pi \Lambda\). (If \(\Lambda\) is an \(S\)-order in a semisimple algebra, this is sufficient, by (1.2.4), to complete the proof.)

Actually, once we get \(\psi(\Lambda) \subseteq \pi \Lambda\), then the element \(\alpha\) can be chosen in \(\pi \Lambda\), and the power of \(\pi \Lambda\) to which \(\alpha\) approximates the identity now increases with every iteration. The product of the \(\beta\)'s used clearly converges in \(\text{End}_S \Lambda\) to an inner automorphisms of \(\Lambda\) equal to \(\alpha\).

Q.E.D.

(5.4) **Remark.** The difference between \(\text{rad } \Lambda\) and \(\text{rad}^2 \Lambda\) is critical, and we do have examples where \(\phi(\Lambda) \subseteq \text{rad } \Lambda\) for a central automorphism \(\alpha = 1 + \pi \phi\) of an order \(\Lambda\) satisfying the remaining hypotheses of the theorem, but with \(\alpha\) not inner.

(5.5) **Conclusion.** By (2.6) the order \(\Lambda\) in the reduction of Chapter 2 satisfies the hypothesis of Theorem 2, which has just been proved. To prove
Theorem 1, it is enough by Chapter 2 to prove Corollary 1, and (2.3), (2.5) reduce this to proving the corollary when the automorphism $\alpha$ induced on $\Lambda$ is of the form $1 + \pi \phi$ for some $\phi \in \text{End}_S \Lambda$, with $S$, $\Lambda$ and $\pi$ as in (5.0). Chapters 3 and 4, cf. (4.1), show $\alpha$ may be modified by suitable inner and “group automorphisms” which are the identity on $C$ and $G/C$ so that the condition $\phi^n(\Lambda) \subseteq \text{rad}^2 \Lambda \setminus \beta \Lambda$ required in Theorem 2 is satisfied (with even $\phi^n(\Lambda) \subseteq \text{rad}^2 \Lambda$). Thus $\alpha$ is now inner, and application of (2.3), (2.5) shows the original automorphism of $SG$ is the composition of inner and “group” automorphisms, which is Corollary 1.

The remaining corollaries were proved in Chapter 1. This concludes the paper.

Appendix

**Lemma.** Let $S$ be a Noetherian integral domain and $P \subseteq S$ a finite subset, no element of which is invertible in $S$. Then $S$ is contained in a principal ideal domain in which no element of $P$ is invertible.

**Proof.** For each $x \in P$ choose a prime ideal $p(x)$ of $S$ containing $x$ and minimal with that property. By the Krull Hauptidealsatz [1, 11.17], $p(x)$ has height 1. Let $\tilde{S}$ be the localization of $S$ at the multiplicative set $S - \bigcup_{x \in P} p(x)$. By [1, 3.11] the only nonzero prime ideals of $\tilde{S}$ are the extensions of the $p(x)$'s. Also, $\tilde{S}$ is Noetherian. Replacing $S$ by $\tilde{S}$, we may assume that $S$ is a Noetherian semilocal domain of dimension 1.

By [18, 2-3, ex. 13] the integral closure $\tilde{S}$ of $S$ in its quotient field is a Dedekind domain. It remains semilocal by [18, 2-2, ex. 21], hence is a principal ideal domain. Q.E.D.

For a somewhat more involved kind of reduction, which, however, gets specializations inside number fields, see the Geyer method treated in Roggenkamp [26].

University of Virginia, Charlottesville

References


(Received April 6, 1986)