CONTEMPORARY MATHEMATICS

264

Combinatorial and Computational Algebra

International Conference on Combinatorial and Computational Algebra
May 24–29, 1999
The University of Hong Kong
Hong Kong SAR, China

Kai Yuen Chan
Alexander A. Mikhalev
Man-Keung Siu
Jie-Tai Yu
Efim I. Zelmanov
Editors

American Mathematical Society

CONTEMPORARY MATHEMATICS

264

Combinatorial and Computational Algebra

International Conference on Combinatorial
and Computational Algebra
May 24–29, 1999
The University of Hong Kong
Hong Kong SAR, China

Kai Yuen Chan
Alexander A. Mikhalev
Man-Keung Siu
Jie-Tai Yu
Efim I. Zelmanov
Editors

American Mathematical Society
Providence, Rhode Island

2000 *Mathematics Subject Classification.* Primary 05–06, 08–06, 12–06, 13–06, 14–06, 17–06, 20–06, 26–06, 68–06, 94–06.

Library of Congress Cataloging-in-Publication Data

Combinatorial and computational algebra : a conference on combinatorial and computational algebra, May 24–29, 1999, Hong Kong / Kai Yuen Chan... [et al.], editors.

p. cm. — (Contemporary mathematics ISSN 0271-4132 ; 264)

International Conference on Combinatorial and Computational Algebra, held at the University of Hong Kong.

Includes bibliographical references.

ISBN 0-8218-1984-4 (alk. paper)

1. Algebra—Congresses. 2. Combinatorial analysis—Congresses. I. Chan, Kai-Yuen. II. International Conference on Combinatorial and Computational algebra (1999 : University of Hong Kong) III. Contemporary mathematics (American Mathematical Society); v. 264.

QA150.C64 2000

512—dc21 00-059345

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.
Visit the AMS home page at URL: `http://www.ams.org/`

10 9 8 7 6 5 4 3 2 1 05 04 03 02 01 00

Preface

This volume contains the refereed proceedings of the International Conference on Combinatorial and Computational Algebra which was held at the University of Hong Kong, Hong Kong Special Administrative Region, China from May 24 to 29, 1999. The conference was a part of the Algebra Program at the Institute of Mathematical Research and the Department of Mathematics of the University of Hong Kong.

The following topics were covered during the conference:

- Combinatorial and Computational Aspects of Group Theory
- Combinatorial and Computational Aspects of Associative and Nonassociative Algebras
- Automorphisms of Polynomial Algebras and the Jacobian Conjecture
- Combinatorics and Coding Theory.

In this volume the readers will find several excellent survey papers as well as research papers containing many significant new results on the subject. The emphasis was made on connections with other areas of mathematics. We hope that this volume will serve as an introductory guide for graduate students and as a good reference for further research in Combinatorial and Computational Algebra. We would like to thank all invited speakers for their beautifully presented motivating lectures and articles. We express our sincere gratitude to all the referees for their invaluable help. We are grateful to the American Mathematical Society for the help in the production of this volume. In particular we thank Christine M. Thivierge for her patient work in putting this volume together.

Finally, we want to express our special gratitude to the Department of Mathematics and the Institute of Mathematical Research of the University of Hong Kong for their warm hospitality, stimulating atmosphere and financial support.

Kai Yuen CHAN
Alexander A. MIKHALEV
Man-Keung SIU
Jie-Tai YU
Efim I. ZELMANOV

June 2000
New Haven – Hong Kong

Contents

Part III. Automorphisms of Polynomial Algebras and the Jacobian Conjecture

Part IV. Combinatorics and Coding Theory

Part I

Combinatorial and Computational Aspects of Group Theory

Contemporary Mathematics
Volume **264**, 2000

DEFORMATIONS AND LIFTINGS OF REPRESENTATIONS

ELI ALJADEFF AND ANDY R. MAGID

Technion (E.A.) and University of Oklahoma (A.R.M.)

ABSTRACT. k is an algebraically closed field of characteristic zero. A finitely generated group Γ is n rigid if there are only finitely many isomorphism classes of irreducible representations $\Gamma \to GL_n(k)$. Γ is not n rigid if and only if there exists a simple representation $\rho_0 : \Gamma \to GL_n(k)$ which lifts non-trivially to $\rho_t : \Gamma \to GL_n(k[[t]])$. Call ρ_t a deformation of ρ_0. The existence of ρ_t is equivalent to a consistent family of non-trivial lifts $\rho_a : \Gamma \to GL_n(k[t]/t^{a+1})$. We show that for Γ a reductive extension of a class r nilpotent if ρ_0 lifts to level $r+1$ then ρ_0 deforms.

INTRODUCTION

We work throughout over an algebraically closed field k of characteristic zero, which can be taken to be the complex numbers $\mathbb{C}$.

This paper is the first of a series of planned investigations of deformations and liftings of representations of finitely generated groups. In its first four sections, we present the background definitions, results, and constructions on which the future work will lie. In the final section, we analyze the special case of nilpotent by reductive groups.

To accurately describe the contents of the paper requires the precise definitions and formulations given below. Loosely speaking, however, we can say the following: some groups, such as finite groups and arithmetic groups in simple algebraic groups, have the property that they have only finitely many isomorphism classes of irreducible complex representations in any given degree. For those that don't, the infinitely many isomorphism classes of simple representations in any given degree can be given the structure of an algebraic variety, and the geometric properties of that variety (for example, its dimension) can be used to understand the collection of classes of representations. Actually all finitely generated groups have such representation varieties: for those with finitely many isomorphism classes of representations in each degree, the varieties are just finite sets of isolated points.

An isolated point in a variety of classes of representations is the class of a representation which has the property that all representations in a neighborhood of it are isomorphic to it. Such a representation is called rigid. Representations without this property, that is, ones with non-isomorphic representations arbitrarily close to

1991 *Mathematics Subject Classification.* 20C18.

Andy Magid was partially supported by NSA grant MDA904-98-1-0024. This work was done while Andy Magid was Lady Davis Fellow and Visiting Professor at the Technion-Israel Institute of Technology, whose support is gratefully acknowledged.

it, call called deformable. This notion of deformation is, by definition, geometric, but it turns out that it also has a completely algebraic description: a representation $\rho_0 : \Gamma \to GL_n(k)$ is deformable if it lifts non-trivially to $\rho_t : \Gamma \to GL_n(k[[t]])$. Such a lift exists if and only if for every level a there are liftings $\rho_a : \Gamma \to GL_n(k[t]/t^{a+1})$ compatible with ρ_0 and each other.

Extending representations of the finitely generated group Γ to level a, or from level a to level $a+r$, is analogous to extending modular representations of the finite group F from $\mathbb{Z}/p$ to $\mathbb{Z}/p^a$, or from $\mathbb{Z}/p^a$ to $\mathbb{Z}/p^{a+r}$: in both cases the obstruction lies in an appropriate H^2 of Γ or G. Maranda's Theorem for finite groups exploits the fact that $H^2(G,\cdot)$ is annihilated by a power of p depending only on G to show that a modular representation which extends to a sufficiently high level, again depending only on G, can be lifted to representation to $\hat{\mathbb{Z}}_p$. One of our main motivations for undertaking this investigation was to look at whether such a "Maranda-type" theorem holds for deformations of representations of finitely generated groups, namely whether there is a level a, depending only on the group Γ and (possibly) the integer n , such that all simple representations $\rho_0 : \Gamma \to GL_n(k)$ which extend to level a have a non-trivial deformation.

In section four below, we analyze the cohomological foundations of such a theorem, and in section five we establish such a theorem for the special case of a nilpotent by linearly reductive group.

To prepare for the subsequent planned publications, and for the convenience of readers, much of this paper is devoted to exposition and background. We have tried to make it self-contained.

A general reference for the basic facts to be cited in this section, and for other information about representation varieties, is [LM1]. Also, the expository article [M2] additionally explains deformations.

We now establish conventions and notations:

Throughout, Γ denotes a finitely generated group with presentation

$$\Gamma = \langle x_1, \dots, x_d \mid s_a \quad a \in \mathcal{A} \rangle.$$

An n–dimensional representation of Γ is a homomorphism

$$\rho : \Gamma \to GL_n(k)$$

and we denote the set of all such $R_n(\Gamma)$ and call it the *variety of representations* of Γ of degree n. It is indeed a variety: we can identify $R_n(\Gamma)$ with the d–tuples (A_i) of elements of $GL_n(k)$ satisfying $s_a(A_1, \dots, A_n) = I_n$ for all $a \in \mathcal{A}$. One can also view $R_n(\Gamma)$ as the k points of the scheme $\mathrm{Hom}(\Gamma, GL_n(\cdot))$. We denote this scheme by $\mathcal{R}_n(\Gamma)$.

For example, if Γ is the free group on d generators F_d, we have

$$R_n(F_d) = GL_n(k)^{(d)}.$$

Both variety and scheme of representations are affine; we denote their respective coordinate rings $A_n(\Gamma)$ $(= k[R_n(\Gamma)])$ and $\mathcal{A}_n(\Gamma)$ $(= k[\mathcal{R}_n(\Gamma)])$. The matrix coordinate functions x_{ij}^{γ}, where $x_{ij}^{\gamma}(\rho)$ is the i,j entry of $\rho(\gamma)$ clearly belong to $A_n(\Gamma)$, and in fact generate it as a k algebra.

The quotient of $\mathcal{A}_n(\Gamma)$ by its nilradical is isomorphic to $A_n(\Gamma)$, and this nilradical can be non zero.

There is a representation

$$\mathcal{P} : \Gamma \to GL_n(\mathcal{A}_n(\Gamma))$$

which is universal with respect to representations

$$\rho : \Gamma \to GL_n(B)$$

in commutative k algebras B: for any such ρ there is a unique k algebra homomorphism $f_\rho : \mathcal{A}_n(\Gamma) \to B$ such that $\rho = GL_n(f_\rho) \circ \mathcal{P}$.

There is a representation

$$P : \Gamma \to GL_n(A_n(\Gamma))$$

which has a similar universal property with respect to representations in reduced commutative k algebras.

We can apply this universal property to a representation $\rho \in R_n(\Gamma)$. Then there is a unique homomorphism $f_\rho : \mathcal{A}_n(\Gamma) \to \mathbb{C}$ such that $\rho = GL_n(f_\rho) \circ \mathcal{P}$; the kernel M_ρ of f_ρ is a maximal ideal and the corresponding point in the variety $R_n(\Gamma)$ is ρ itself. When ρ is understood from context, we can denote M_ρ just by M alone.

More generally, if F is any closed affine subset of $R_n(\Gamma)$, the canonical map $A_n(\Gamma) \to k[F]$ produces, on composition with P, a representation

$$P_F : \Gamma \to GL_n(A_n(\Gamma)) \to GL_n(k[F]))$$

which has the property that $P_F(\gamma)(\rho) = \rho(\gamma)$ for $\rho \in F$ and $\gamma \in \Gamma$.

Two representations ρ and ρ' in $R_n(\Gamma)$ are *equivalent* (isomorphic) if there is $A \in GL_n(k)$ with $A^{-1}\rho A = \rho'$. Since scalar matrices act trivially, this conjugation action defines an action of $PGL_n(k) = GL_n(k)/k^*$ on $R_n(\Gamma)$; we denote the orbit of ρ under the action by $\mathcal{O}(\rho)$. (Thus $\mathcal{O}(\rho)$ is the isomorphism class of ρ.) Every orbit $\mathcal{O}(\rho)$ is of course a quasi–affine subvariety of $R_n(\Gamma)$. It is closed exactly when ρ is semisimple and has trivial $PGL_n(k)$ stabilizer exactly when ρ is simple.

The closure of the orbit of a representation ρ contains its "semi-simplification" ρ_{ss} (in module terms, the direct sum of the quotients in a composition series of ρ). There are GL_n invariant functions (characters) which separate non-isomorphic semi-simple representations. It follows that orbits of semi-simple representations are closed, and hence that every closed orbit is the class of a semi-simple representation. We denote $R_n(\Gamma)//GL_n$ by $SS_n(\Gamma)$; by the above $SS_n(\Gamma)$ parameterizes the classes of semi-simple representations and we can describe the map $R_n(\Gamma) \to SS_n(\Gamma)$ as $\rho \mapsto [\rho_{ss}]$, using $[\cdot]$ to stand for isomorphism class.

A representation $\rho \in R_n(\Gamma)$ is simple if and only if its image spans $M_n(k)$, and it can be seen from this characterization that the subset $R_n(\Gamma)^s$ of simple representations forms an open subvariety of $R_n(\Gamma)$: $R_n(\Gamma)^s$ is covered by affine open GL_n stable subsets given by the non-vanishing of certain determinants asserting that a particular set of elements $\{\rho(\gamma_i)\}$ form a basis of $M_n(k)$). Thus we obtain a geometric quotient variety

$$R_n(\Gamma)^s \to R_n(\Gamma)^s/PGL_n(\mathbb{C}) = S_n(\Gamma)$$

where the quotient map is locally trivial for the étale topology. The points of $S_n(\Gamma)$ correspond to the equivalence classes of simple representations, the class of the simple representation ρ being denoted $[\rho]$. The fibre over $[\rho]$ is the orbit $\mathcal{O}(\rho)$.

We will focus primarily on simple representations in this work. We have already noted that isomorphism classes semi-simple representations are separated by characters, which are global invariant functions. For simple representations, the argument for this is elementary and we present it here, beginning with the definition of character.

Definition. Let $\rho \in R_n(\Gamma)$ be a representation. Then $\chi(\rho) : \Gamma \to k$ by $\gamma \mapsto \mathrm{Trace}(\rho(\gamma))$ is the *character* of ρ.

Note that $\chi(\rho)$ is constant on the orbit $\mathcal{O}(\rho)$. Now we can show that simple representations are determined by their characters:

Proposition. *Let ρ_1 and ρ_2 in $R_n(\Gamma)^s$ be simple representations such that $\chi(\rho_1) = \chi(\rho_2)$. Then ρ_1 and ρ_2 are isomorphic.*

Proof. We use P_i to denote the k algebra homomorphism $k[\Gamma] \to M_n(k)$ from the group algebra of Γ to the matrix ring by $\sigma a_\gamma \gamma \mapsto \sigma a_\gamma \rho(\gamma)$. This is a surjective map since ρ_i is simple. Let I_i be its kernel. Suppose $I_1 = I_2$ and denote this common kernel I. Then using the maps induced from the P_i we have k algebra isomorphisms $M_n(k) \to k[\Gamma]/I \to M_n(k)$. The composite, being a k algebra automorphism of $M_n(k)$, must be given by conjugation by some $A \in GL_n(k)$ and this A produces an isomorphism of ρ_1 with ρ_2. So to prove the proposition it will be enough to show that representations with the same character have the same kernel ideal. For this, we fix a single simple representation $\rho \in R_n(\Gamma)^s$ with corresponding algebra homomorphism P and kernel ideal I

Then $a = \Sigma a_\gamma \gamma \in I$; that is, $P(a) = 0$, if and only if $\mathrm{Trace}(P(a)B) = 0$ for all $B \in M_n(k)$. Since $\rho(\Gamma)$ spans $M_n(k)$, it is enough to take $B \in \rho(\Gamma)$, so that $a \in I$ if and only if $0 = \mathrm{Trace}(P(a)\rho(\tau)) = \Sigma a_\gamma \chi(\rho)(\gamma\tau)$ for all $\tau \in \Gamma$.

It is clear from this formula that if two simple representations have the same character then they have the same kernel ideal and hence are isomorphic.

We use characters to construct functions on $R_n(\Gamma)$ as follows: for each $\gamma \in \Gamma$ let $\chi_\gamma : R_n(\Gamma) \to k$ be given by $\rho \mapsto \chi(\rho)(\gamma)$. It is clear that the functions χ_γ belong to $A_n(\Gamma)$ (they are sums of matrix coordinate functions) and that they are $GL_n(k)$ invariant and hence belong to $k[SS_n(\Gamma)]$. Moreover, their restriction to $S_n(\Gamma)$ separates points, as the proposition shows.

Unlike the situation for representation varieties, the geometry of the varieties of isomorphism classes of semi-simple or simple representations of the free group F_d are not known: $SS_n(F_d)$, for example, is the variety of closed simultaneous conjugacy classes of d tuples of invertible matrices.

Geometric and Formal Deformations

Definition. A representation $\rho \in R_n(\Gamma)$ is called *rigid* if representations close to ρ in $R_n(\Gamma)$ are isomorphic to it. More precisely, ρ is rigid if the orbit $\mathcal{O}(\rho)$ contains an open set in $R_n(\Gamma)$, and hence is open. A representation which is not rigid is *deformable.*

A simple representation ρ, whose orbit is then closed, is then rigid if and only if $[\rho]$ is an isolated point of $S_n(\Gamma)$. So a simple representation ρ deforms if and only if $[\rho]$ is not an isolated point; that is, if and only if there is a curve $C \subseteq S_n(\Gamma)$ passing through $[\rho]$.

So suppose ρ is a deformable simple representation. We are going to see first the geometric significance for $R_n(\Gamma)$ of such a curve C. By selecting an irreducible component of C containing $[\rho]$, we can assume that C is irreducible. Let U be an affine open $GL_n(k)$ stable subset of $R_n(\Gamma)^s$ containing ρ of the sort considered above: U is the set of representations ρ' in $R_n(\Gamma)$ where

$$s(\rho') = \det([\mathrm{Trace}(\rho'(\gamma_i\gamma_j)])$$

doesn't vanish, where $\{\rho(\gamma_i)\}$ is a k basis of $M_n(k)$.

Then $k[U] = A_n(\Gamma)[s^{-1}]$ and, since s is GL_n invariant, we also have that the image V of U in $S_n(\Gamma)$ is affine with $k[V] = k[U]^{GL_n}$. Let C also denote the affine curve $C \cap V$. Let F be the inverse image of C in $R_n(\Gamma)^s$ and let D be an irreducible affine curve in F which contains ρ and whose image in C is not a point. (Note that F is irreducible and affine, so any irreducible curve containing both ρ and a point not in $\mathcal{O}(\rho)$ works.) The image of D in C is then cofinite in C, so that the image contains an affine open subset to which ρ belongs. We replace C by this affine open subset and D by its intersection with the inverse image in $R_n(\Gamma)^s$ of C.

In this setup, then we have, for the deformable representation ρ, an irreducible closed affine curve D in $R_n(\Gamma)^s$, containing ρ, and such that the image C of D in $S_n(\Gamma)$ is an irreducible closed affine curve containing $[\rho]$.

Corresponding to D we have the representation $P_D : \Gamma \to GL_n(k[D])$. For $d \in D$, we will use ρ_d to denote d, so $\rho_d(\gamma) = P_D(\gamma)(d)$, and we will further denote ρ, as an element of D, by 0, so that $\rho = \rho_0$. For the corresponding characters $\chi(\rho_d)$, we have, in the obvious notation, that $\chi(\rho_d) = \chi(P_D)(d)$. The fact that the image C of D is not a point then can be phrased as saying that the characters $\chi(\rho_d)$ are not all the same, which is equivalent to the assertion that $\chi(P_D)(\Gamma)$ is not a subset of k.

We call this situation a geometric deformation of ρ:

Definition. Let $\rho \in R_n(\Gamma)^s$. A *geometric deformation* of ρ is a embedding $d \mapsto \rho_d$ of an irreducible affine curve D with base point 0 in $R_n(\Gamma)^s$ such that $\rho_0 = \rho$. The deformation is *non-trivial* if the map $d \mapsto \chi(\rho_d)$ is non-constant.

Our discussion above shows that deformable representations have non-trivial geometric deformations. The converse is obvious, and so we have

Proposition. *A simple representation is deformable if and only if it has a non-trivial geometric deformation.*

We resume the discussion with the same notation. Let M_0 be the maximal ideal of $k[D]$ corresponding to ρ. Since D is irreducible, $k[D]$ is an integral domain. Its normalization E is the irreducible affine curve whose coordinate ring $k[E]$ is the integral closure of $k[D]$ in its quotient field $k(D)$. Let M be a maximal ideal of $k[E]$ lying over M_0. E is nonsingular and the completion of $k[E]$ at M is a formal power series algebra $k[[t]]$ in any local generator of M. The k algebra injections $k[D] \to k[E] \to k[[t]]$ give, upon composition with P_D, a representation

$$\rho_t : \Gamma \to GL_n(k[[t]])$$

such that $\rho_t \equiv \rho \pmod{t}$. Since, in the obvious notation, $\chi(\rho_t) = \chi(P_D)$, we also have that $\chi(\rho_t)(\Gamma)$ is not a subset of k.

We call this situation a formal deformation of ρ:

Definition. Let $\rho \in R_n(\Gamma)^s$. A *formal deformation* of ρ is a representation $\rho_t : \Gamma \to GL_n(k[[t]])$ over formal power series such that the residual representation ρ_0 given by setting $t = 0$ coincides with ρ. The deformation is *non-trivial* if $\chi(\rho_t)$ is non-constant. The *non-triviality degree* of ρ_t is the smallest positive integer m such that there is $\gamma \in \Gamma$ so that the coefficient of t^m in $\chi(\rho_t)(\gamma)$ is non-zero.

A trivial deformation of ρ would be one in which $\chi(\rho_t)$ is constant. There always exists a trivial deformation of ρ: since $GL_n(k) < GL_n(k[[t]])$, we can simply set $\rho_t = \rho$. More generally, we could take this deformation and follow it by conjugation by an element of $GL_n(k[[t]])$. We will show below that these are the only trivial deformations.

Our discussion so far shows that representations with geometric deformations have formal deformations. We will also establish the converse:

Theorem. *A simple representation has a non-trivial formal deformation if and only if it has a geometric deformation.*

Proof. We need to prove "only if". So suppose ρ has a formal deformation $\rho_t : \Gamma \to GL_n(k[[t]])$. Because of the universal property of P, ρ_t comes from P and a k algebra map $A_n(\Gamma) \to k[[t]]$. To simplify notation, we now write A for $A_n(\Gamma)$ and M for M_ρ. Since ρ_t goes to ρ when $t = 0$, the image of M_ρ lands in $tk[[t]]$. Thus the k algebra map $A \to k[[t]]$ factors through A_M. We write P_M for the composite $\Gamma \to GL_n(A) \to GL_n(A_M)$ and f for the map $A_M \to k[[t]]$, so that $\rho_t = GL_n(f) \circ P_M$. Suppose further that ρ_t is nontrivial. Then there is $\gamma \in \Gamma$ such that $\mathrm{Trace}(\rho_t(\gamma)) \notin k$. Thus $f(\mathrm{Trace}(P_M(\gamma))) \notin k$, so $\mathrm{Trace}(P_M(\gamma)) \notin k$. Earlier, we introduced the notation χ_γ for $\mathrm{Trace}(P(\gamma))$ as a function on $R_n(\Gamma)$. Thus we see that the existence of a non-trivial formal deformation ρ_t of ρ implies the existence on a χ_γ non-constant in A_M. Now we want to show that this implies that ρ geometrically deforms.

If, on the contrary, ρ is rigid, then $\mathcal{O}(\rho)$ is open as well as closed, and hence is an irreducible and connected component of $R_n(\Gamma)$. Then A_M is an integral domain whose quotient field is the function field $k(\mathcal{O}(\rho))$. PGL_n acts on this field with field of invariants k, so the invariant function χ_γ would be constant in $k(\mathcal{O}(\rho))$ and hence in A_M. This contradiction implies that ρ is not rigid and completes the proof of the theorem.

Because of the theorem, we may unambiguously refer to representations as "deformable" to mean both geometrically and non-trivially formally deformable.

From a formal deformation $\rho_t : \Gamma \to GL_n(k[[t]])$ of a simple representation ρ we can produce a consistent family of representations

$$\rho_i : \Gamma \to GL_n(k[t]/(t^{i+1}))$$

from the k algebra surjections $k[[t]] \to k[t]/(t^{i+1})$. Each of these representations reduces to the original ρ when $t = 0$. and, for $i > j$, ρ_i reduces to ρ_j modulo t^{j+1}. Conversely, if we have such a consistent family then their inverse limit is a formal deformation of ρ. We introduce the following terminology for such representations:

Definition. Let $\rho \in R_n(\Gamma)^s$. A *lifting* of ρ to level i is a representation $\sigma : \Gamma \to GL_n(k[t]/t^{i+1})$ over such that the residual representation σ_0 given by setting $t = 0$ coincides with ρ. The lifting is *non-trivial* if the character $\chi(\sigma)$ is non-constant. The *non-triviality degree* of σ is the smallest positive integer m such that there is $\gamma \in \Gamma$ so that the coefficient of t^m in $\chi(\sigma)(\gamma)$ is non-zero.

A lifting is trivial if its character is constant. The following proposition will allow us to identify the trivial liftings.

Proposition. *Let A be a local k algebra with maximal ideal M and residue field k, and let $\sigma : \Gamma \to GL_n(A)$ be such that the residual representation $\rho : \Gamma \to GL_n(k)$ is simple. Suppose that Trace$(\sigma(\Gamma)) \subset k$. Then there is $\alpha \in GL_n(A)$ such that $\sigma = \alpha\rho\alpha^{-1}$.*

Proof. Using the inclusion $k \subset A$ we regard both ρ and σ as maps from Γ to $GL_n(A)$. We consider the two k algebra homomorphisms $f, g : k[\Gamma] \to M_n(A)$ coming from ρ and σ respectively. We are going to show that the kernels I and J of f and g are equal.

Suppose this has been done. Because ρ is irreducible, the image of f is $M_n(k)$, which freely generates $M_n(A)$ as A module. Let B denote the image of g. If $I = J$, $M_n(k)$ and B are isomorphic. Under the composition

$$k[\Gamma] \to M_n(A) \to A/M \otimes_A M_n(A) = M_n(k)$$

the images of f and g coincide, so that B generates $M_n(A)$ as A module as well. Thus the isomorphism $M_n(k) \to B$ extends to an A automorphism

$$M_n(A) = A \otimes_k M_n(k) \to A \otimes_k B = M_n(A)$$

which is inner since A is local [B1.5.3, p.74]. If the inner automorphism is given by conjugation by $\alpha \in GL_n(A)$, then it follows that $\alpha g \alpha^{-1} = f$, and hence the proposition results.

Next we note that for any $z \in k[\Gamma]$, since $f(z)$ and $g(z)$ agree modulo M, so do Trace$(g(z))$ and Trace$(f(z))$. Since both traces belong to k, the traces coincide in A.

It remains to show that I and J coincide. To begin, we note that for $X \in M_n(A)$, $X = 0$ if and only if Trace$(XY) = 0$ for all $Y \in M_n(k)$. More precisely, if $E_{ij} \in$

$M_n(k)$ has 1 in the i, j position and 0 elsewhere then $\text{Trace}(XE_{ij})$ is the j,i entry of X.

As noted above, the image B of g, as well as the image $M_n(k)$ of f, both generate $M_n(A)$ as an A module. Since the trace is linear, this implies that $X = 0$ if and only if $\text{Trace}(XY) = 0$ for all $Y \in B$ as well.

Thus $g(x) = 0$ if and only if $\text{Trace}(g(x)g(y)) = 0$ for all $y \in k[\Gamma]$, and $f(x) = 0$ if and only if $\text{Trace}(f(x)f(y)) = 0$ for all $y \in k[\Gamma]$ as well. But $\text{Trace}(f(x)f(y)) = \text{Trace}(f(xy)) = \text{Trace}(g(xy)) = \text{Trace}(g(x)g(y))$, and it follows that the kernels of f and g are equal.

Suppose that ρ_a is a lifting of the simple representation $\rho = \rho_0$ to level $a \geq 1$. We say that ρ_a *extends* to level $a+1$ if there is a lifting ρ_{a+1} of ρ which reduces to ρ_a modulo t^{a+1}. If there is no such ρ_{a+1}, we say that ρ_a is *obstructed.* We can also talk about extensions of more than a single level at a time.

We are going to see that extension and obstruction can have interpretations in group cohomology. Extending a lifting ρ_a to level $b = a + r$ means going from a representation $\Gamma \to GL_n(k[t]/t^{a+1})$ to a representation $\Gamma \to GL_n(k[t]/t^{b+1})$ which reduces to it modulo t^{a+1}. The kernel of the surjection $GL_n(k[t]/t^{b+1}) \to GL_n(k[t]/t^{a+1})$ is $I + t^{a+1}M_n(k[t]/t^{b+1})$. If $a > r$, this is an abelian group, isomorphic to the vector space $t^{a+1}M_n(k[t]/t^{b+1})$. Also

$$t^{a+1}M_n(k[t]/t^{b+1}) = M_n(t^{a+1}k[t]/t^{b+1}).$$

As a $k[t]$ module, $k[t]/t^r$ is isomorphic to $t^{a+1}k[t]/t^{b+1}$, the isomorphism being given by multiplication by t^{a+1}. So $t^{a+1}M_n(k[t]/t^{b+1})$ is isomorphic to $M_n(k[t]/t^r)$.

Since matrices over $k[t]$ modulo the c power of t are uniquely representable as sums of powers of t up to $c-1$ times matrices over k, this last isomorphism can be made explicit.

In summary, we have the following group extension exact sequence:

For $a > r \geq 1$,

$$0 \to M_n(k[t]/t^r) \to GL_n(k[t]/t^{a+r+1}) \to GL_n(k[t]/t^{a+1}) \to 1$$

$$A = \sum_{i=0}^{r-1} t^i A_i \mapsto t^{a+1}A_0 + \cdots + t^{a+r}A_{r-1} \quad A_i \in M_n(k).$$

As with all group extensions with abelian kernel, the above extension corresponds to a certain cocycle in $c_{a,r} \in Z^2(GL_n(k[t]/t^{a+1}), M_n(k[t]/t^r))$ (which we will make explicit shortly). A representation $\rho_a : \Gamma \to GL_n(k[t]/t^{a+1})$ extends to $GL_n(k[t]/t^{a+r+1})$ if and only if the cocycle $c_{a,r} \circ \rho_a \in Z^2(\Gamma, M_n(k[t]/t^r)$ is a coboundary.

For later use, we recall explicitly how the cocycle $c_{a,r} \circ \rho_a$ arises. For notational simplicity, we will write

$$0 \to M \to E \to G \to 1$$

for the sequence

$$0 \to M_n(k[t]/t^r) \to GL_n(k[t]/t^{a+r+1}) \to GL_n(k[t]/t^{a+1}) \to 1$$

and write $f : M \to E$ for $M_n(k[t]/t^r) \to GL_n(k[t]/t^{a+r+1})$ and $\rho : \Gamma \to G$ for ρ_a. Then from the sequence and ρ we have the sequence

$$0 \to M \to E \times_G \Gamma \to \Gamma \to 1$$

where $A \in M$ maps to $(f(A), e)$ and $(A, \gamma) \in E \times_G \Gamma$ maps to γ. Extending ρ to E is the same as finding a homomorphic section $\Gamma \to E \times_G \Gamma$.

The extension problem depends on the structure of $M_n(k[t]/t^r)$ as a Γ module, a topic to which we will turn below. First, we want to make the cocycle $c_{a,r}$ explicit. To do so, it is first convenient to write the group $GL_n(k[t]/t^{a+1})$ in a different form.

We let $U_n(k[t]/t^{a+1}) = I + tM_n(k[t]/t^{a+1})$, a subgroup of $GL_n(k[t]/t^{a+1})$. We also consider $GL_n(k)$ as a subgroup of $GL_n(k[t]/t^{a+1})$ in the obvious way. Then there is an isomorphism:

$$U_n(k[t]/t^{a+1})GL_n(k) \to GL_n(k[t]/t^{a+1})$$

$$(I + A = \sum_{i=0}^{a} t^i A_i)(B) \mapsto \sum_{i=0}^{a} t^i A_i B \quad A_i, B \in M_n(k), A_0 = I.$$

expressing $GL_n(k[t]/t^{a+1})$ as a semi-direct product.

Then we can define a section from $GL_n(k[t]/t^{a+1}) = U_n(k[t]/t^{a+1})GL_n(k)$ to $GL_n(k[t]/t^{a+r+1}) = U_n(k[t]/t^{a+r+1})GL_n(k)$ by

$$s_{a,r} : U_n(k[t]/t^{a+1})GL_n(k) \to U_n(k[t]/t^{a+r+1})GL_n(k)$$

$$(\sum_{i=0}^{a} t^i A_i)(B) \mapsto (\sum_{i=0}^{a} t^i A_i)(B).$$

We define $c_{a,r}(X, Y) \in M_n(k[t]/t^r)$ so that

$$s_{a,r}(X)s_{a,r}(Y)s_{a,r}(XY)^{-1} = t^{a+1}c_{a,r}(X, Y).$$

This also says that $s_{a,r}(X)s_{a,r}(Y) = t^{a+1}c_{a,r}(X, Y)s_{a,r}(XY)$.

We can write $X = UC$ and $Y = VD$ where $U, V \in U_n(k[t]/t^{a+1})$ and $C, D \in GL_n(k)$. Then $XY = (U^C V)CD$, where $^C V = CVC^{-1}$. Writing s for $s_{a,r}$ and c for $c_{a,r}$ we then have $s(X) = s(U)C$, $s(Y) = s(V)D$, $^C s(V) = s(^C V)$, and $s(XY) = s(U^C V)CD$ so that $s(X)s(Y) = s(U)^C s(V)CD = s(U)s(^C V)CD$ and hence

$$\begin{aligned} t^{a+1}c(X, Y) &= s(U)Cs(V)D(s(U^C V)CD)^{-1} \\ &= s(U)s(^C V)CD(CD)^{-1}s(U^C V)^{-1}. \end{aligned}$$

This says that

$$t^{a+1}c_{a,r}(UC, VD) = s_{a,r}(U)s_{a,r}(^C V)s_{a,r}(U^C V)^{-1}$$

and that

$$s_{a,r}(U)s_{a,r}(^C V) = t^{a+1}c_{a,r}(UC, VD)s_{a,r}(U^C V).$$