Research Article

On Finite Nilpotent Matrix Groups over Integral Domains

Dmitry Malinin

Department of Mathematics, UWI, Mona Campus, Kingston 7, Jamaica

Correspondence should be addressed to Dmitry Malinin; dmalinin@gmail.com

Received 31 October 2013; Accepted 19 November 2013

Academic Editors: I. Cangul and N. Jing

Copyright © 2013 Dmitry Malinin. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

We consider finite nilpotent groups of matrices over commutative rings. A general result concerning the diagonalization of matrix groups in the terms of simple conditions for matrix entries is proven. We also give some arithmetic applications for representations over Dedekind rings.

1. Introduction

In this paper we consider representations of finite nilpotent groups over certain commutative rings. There are some classical and new methods for diagonalizing matrices with entries in commutative rings (see [1, 2]) and the classical theorems on diagonalization over the ring of rational integers originate from the papers by Minkowski; see [3–5]. We refer to [6–8] for the background and basic definitions. First we prove a general result concerning the diagonalization of matrix groups. This result gives a new approach to using congruence conditions for representations over Dedekind rings. The applications have some arithmetic motivation coming back to Feit [9] and involving various arithmetic aspects, for instance, the results by Bartels on Galois cohomologies [10] (see also [11–14] for some related topics) and Bürgisser [15] on determining torsion elements in the reduced projective class group or the results by Roquette [16].

Throughout the paper we will use the following notations. C, R, Q, Q_p, Z, Z_p, and O_K denote the fields of complex and real numbers, rationals and p-adic rationals, the ring of rational and p-adic rational integers, and the ring of integers of a local or global field K, respectively. GL_n(R) denotes the general linear group over R. [E : F] denotes the degree of the field extension E/F. I_n denotes the unit m × m matrix. diag(d_1, d_2, ..., d_m) is a diagonal matrix having diagonal components d_1, d_2, ..., d_m. |G| denotes the order of a finite group G.

Theorem 1. Let A be a commutative ring, which is an integral domain, and let G ⊆ GL_n(A) be a finite nilpotent group indecomposable in GL_n(A). Let one suppose that every matrix g ∈ G is conjugate in GL_n(A) to a diagonal matrix. Then any of the following conditions implies that G is conjugate in GL_n(A) to a group of diagonal matrices:

(i) every matrix g = [g_{ij}] in G has at least one diagonal element g_{ij} ≠ 0,

(ii) −I_n is not contained in G, where I_n is the identity n × n matrix, and for any matrix g = [g_{ij}] in G, there are 2 indices i, j such that g_{ij} ≠ 0 and g_{ji} ≠ 0.

For the proof of Theorem 1 we need the following.

Proposition 2. If the centre of a finite subgroup G ⊆ GL_n(A) for a commutative ring A, which is an integral domain, contains a diagonal matrix d ≠ I_n then G is decomposable.

Proof. After a conjugation by a permutation matrix we can assume that

\[ d = \text{diag}(d_1, d_2, ..., d_k) \]

where d_i ≠ d_j for i ≠ j and d contains t_j elements that equal d_i, i = 1, ..., k. For a matrix g = [g_{ij}] ∈ G consider the system of linear equations determined by the conditions gd = dg; this immediately implies that g_{ij} = 0 for i ≤ t_1, j > t_1, and g_{k,m} = 0 for m ≤ t_1, k > t_1. Therefore, G is decomposable. This completes the proof of Proposition 2.
Proof of Theorem 1. Let us denote by $D$ the subgroup of all scalar matrices in $G$, and let $Z$ be the centre of $G$.

If $D \neq Z$, we use Proposition 2 and induction on $n$.

Let $D = Z$, and let the exponent of the group $Z$ be equal to $t$. Let $g_0 \in G$ be any element not contained in the centre $Z$ of $G$ such that the image of $g_0$ in the factor group $G/Z$ is contained in the centre of $G/Z$. Then we consider the homomorphism
\[
\psi : G' \to GL_n(A), \tag{2}
\]
given by $\psi(g) = g^{\psi}$. The kernel of $\psi$ is the set $D$ of all scalar matrices contained in $G$. This kernel is not trivial since $G$ is nilpotent. The image $\psi(G)$ is isomorphic to the factor group $G/D$. Let $g_0 = \text{diag}(d_1, \ldots, d_n)$. Then $\psi(g_0)$ is a non-scalar diagonal matrix in the centre of $\psi(G)$. $g_0$ is also not a scalar matrix, and for any $g \in G$ we have $gg_0 = g_0g\zeta$ for some root of $1 - \zeta = \zeta(g)$. If for the matrix $g = [g_{ij}]_{n \times n}$, the elements $g_{ii}$ and $g_{ij}$ are not zero, we obtain $d_i = d_i\zeta$ and $d_i = d_i\zeta$, which implies immediately that $\zeta = 1$ if $i = j$ (as in case (i) of Theorem 1). In case (ii) of Theorem 1, if $i \neq j$, we obtain $\zeta = 1$ and $\zeta = \pm 1$, but $\zeta = -1$ is impossible in the virtue of the condition that $-\zeta$ is not contained in $G$. Hence we have $\zeta = 1$, and $g_0$ is contained in $Z$, the centre of $G$. This contradiction completes the proof of Theorem 1. 

Proposition 3. Let $\mathcal{J}$ be an ideal of a Dedekind ring $S$ of characteristic $\chi$, let $\{0\} \neq \mathcal{J} \neq S$, and let $g$ be an $n \times n$ matrix of finite order congruent to $I_n(\text{mod } \mathcal{J})$.

(i) If $\chi = p > 0$, then $g^{p^i} = I_n$ for some integer $i$. If $\chi = 0$, then $1$ contains a prime number $p$ and $g^{p^i} = I_n$ for some integer $i$. In particular, a finite group of matrices congruent to $I_n(\text{mod } \mathcal{J})$ is a $p$-group.

(ii) Let $\chi = 0$, and let $\mathcal{J} = \mathcal{P}$ be a prime ideal having ramification index $e$ with respect to $p$, let $g \equiv I_n(\text{mod } \mathcal{P})$, and let
\[
\lambda \rho^{i-1} (p - 1) \leq e < \rho^i (p - 1), \quad i \geq 0, \quad \lambda = \min \{1, i\}. \tag{3}
\]

Then $g^{\rho^i} = I_n$; in particular, any finite group of matrices congruent to $I_n(\text{mod } \mathcal{P})$ is trivial if $e < r(p - 1)$.

See [17, Lemma 1] for the proof of Proposition 3.

The following corollary can be immediately obtained from Proposition 3.

Corollary 4. Let $K$ be a number field of degree $d = [K : Q]$ with the maximal order $O_K$. The kernel of reduction of $GL_n(O_K)$ modulo an ideal $\mathcal{J}$ of $O_K$, containing a prime number $p$, has no torsion if the norm $N_{K/Q}(\mathcal{J}) > \rho^{d(p-1)}$.

Remark 5. Earlier Bürgisser obtained a similar result for $N_{K/Q}(\mathcal{J}) > \rho^d$; see [18, Lemma 3.1].

Propositions 3 and 6 below can be used for estimating the orders of finite subgroups of $GL_n(O_K)$ using the reduction modulo some prime ideal $\mathcal{P} \subset O_K$. It is also possible to determine the structure of a $p$-subgroup of $GL_n(O_K)$ having the maximal possible order with some modifications in the case $p = 2$. The theorems describing the maximal $p$-subgroups of $GL_n(K)$ over fields can be found in [19]; in particular, it is proven that there is only one conjugacy class of maximal $p$-subgroups of $GL_n(K)$ for $p > 2$; see also [9, 20]. However, the equivalence of subgroups in $GL_n(O_K)$ over $O_K$ is a more subtle question. See [21, chapter 3], [22, 23] for the structure of finite linear groups (including the groups of small orders). See [15] for more details, proofs, and applications to determining torsion elements in the reduced projective class group.

As a corollary of Theorem 1 we can obtain the following proposition.

Proposition 6. Let $K/O_p$ be a finite extension, and let $\zeta_p \in O_K$. Let $p = \psi$, and let $e = p - 1$. Let $G$ be a finite subgroup of $GL_n(O_K)$ and $g \equiv I_n(\text{mod } p)$ for all $g \in G$. Then $G$ is conjugate in $GL_n(O_K)$ to an abelian group of diagonal matrices of exponent $p$.

Proof of Proposition 6. Let us prove that $G$ is abelian of exponent $p$. Let $\pi$ be a prime element of $O_K$. Let $g_1 = I_n + \pi B_1$, $g_2 = I_n + \pi B_2$ for some $g_1, g_2 \in G$. Then $g_1^{-1} = I_n - \pi B_1(\text{mod } \pi^2)$, $i = 1, 2$, and $h = g_1 g_2^{-1} \equiv I_n(\text{mod } \pi^2)$. It follows from Proposition 2 that $h = I_n$ and the same proposition shows that $g^{\pi} = I_n$ for any $g \in G$. First of all, $G$ is conjugate over $O_K$ to a group of triangular matrices, since $G$ is abelian and $O_K$ is a local ring; see [6, Theorem 73.9] and the remarks in [6, on page 493]. Following Theorem 1, let us prove that every $g \in G$ is diagonalizable. We can describe explicitly the matrix $M$ such that
\[
M^{-1} g M = \text{diag} (\lambda_1, \lambda_2, \ldots, \lambda_n) \tag{4}
\]
diagonal matrix for a triangular matrix $g$ of order $p$ which is congruent to $I_n(\text{mod } p)$. Indeed, let $g \in G$ and
\[
g = \begin{bmatrix}
\zeta(1) I_{t_1} & P_1^1 & \cdots & 0 \\
0 & \zeta(2) I_{t_2} & \cdots & P_2^1 \\
\vdots & \vdots & \ddots & \vdots \\
0 & \cdots & \cdots & \zeta(k) I_{t_k}
\end{bmatrix}, \tag{5}
\]
and let
\[
S = \begin{bmatrix}
I_{t_1} & 0 \ldots & A_1 \\
0 & I_{t_2} & \ldots & A_2 \\
\vdots & \vdots & \ddots & \vdots \\
0 & \cdots & \cdots & I_{t_k}
\end{bmatrix}, \tag{6}
\]
for $t_1 + t_2 + \cdots + t_k = n$ and $t_1 \leq t_2 \leq \cdots \leq t_k$, $\zeta(\phi), i = 1, 2, \ldots, k$ are appropriate $p$-roots of $1$. We consider
\[
S^{-1} g S = \begin{bmatrix}
\zeta(1) I_{t_1} & * & \cdots & M_{t_1}^k \\
0 & \zeta(2) I_{t_2} & \cdots & M_{t_2}^k \\
\vdots & \vdots & \ddots & \vdots \\
0 & \cdots & \cdots & \zeta(k) I_{t_k}
\end{bmatrix}, \tag{7}
\]
and we find the system of conditions for providing $M_k^t = 0_t \times t_k$ matrix. We have the following system of conditions:

\[
\begin{align*}
\zeta_{(1)} (1 - \zeta_{(k)} \zeta_{(1)}^{-1}) A_1 + P_{k-1} A_{k-1} + P_k &= 0_{t_1 \times t_k}, \\
\vdots \\
\zeta_{(k-2)} A_{k-2} (1 - \zeta_{(k)} \zeta_{(k-2)}^{-1}) + P_k^{k-2} A_{k-1} + P_k^{k-2} &= 0_{t_{k-2} \times t_k}, \\
\zeta_{(k-1)} A_{k-1} (1 - \zeta_{(k)} \zeta_{(k-1)}^{-1}) + P_k^{k-1} &= 0_{t_{k-1} \times t_k}.
\end{align*}
\]

(8)

The condition $g \equiv l_n(\text{mod } p)$ implies that $P_i^t = 0_{t_i \times t_i}$, and we can find a matrix $M$ that transforms $g$ to a diagonal form as required.

The condition $g \equiv l_n(\text{mod } p)$ of Proposition 6 implies that the condition (i) of Theorem 1 holds true. Since $G$ is an abelian group of exponent $p$, this allows us to prove our claim over the ring $O_K$.

Remark 7. Using the same argument for an algebraic number fields $K/Q$ we can prove a similar result. Let $O$ be a Dedekind ring in $K$, and let $\zeta_p \in O$. Let $p = \mathfrak{p}^e$, $e = p - 1$. Let $G$ be a finite subgroup of $\text{GL}_n(O)$ and $g \equiv l_n(\text{mod } p)$ for all $g \in G$. Then $G$ is conjugate in $\text{GL}_n(O)$ to an abelian group of diagonal matrices of exponent $p$.

In this situation we can use the statement (8.1.20) in [CR] for proving the above result for the given Dedekind ring $O$ (compare also the proof of (8.1.20) and (75.27) in [6]).

However, in Proposition 6 the ramification index $e = p - 1$. Below there are two examples giving constructions of local field extensions $K/Q_p$ and finite subgroups $G \subset \text{GL}_n(O_K)$ which are contained in the kernel of reduction of $\text{GL}_n(O_K)$ modulo ideals having ramification indices $e > p - 1$.

Example 8. For the following finite extension $K/Q_p$ of local fields obtained via adjoining torsion points of elliptic curves, let $O_K$ be the ring of integers of $K$ with the maximal ideal $\mathfrak{p}$. Consider an elliptic curve $E$ over $\mathbb{Z}_p$ with supersingular good reduction (see [24, Section 1.11]). Let $K/Q_p$ be the field extension obtained by adjoining $p$-torsion points of $E$; then the formal group associated with $E$ has a height of 2; its Hopf algebra $O_A$ is a free module of rank $p^2$ over $\mathbb{Z}_p$ and for the kernel $E_p$ of multiplication by $p$, $|E_p| = p^2$ (see [25, L3 and Section 2]). Note that for some $E$ the ramification index $e = e(K/Q_p) = p^2 - 1$ ([24, page 275, Proposition 12]).

We can consider the group $G$ of $p$-torsion points as $\mathbb{Z}_p^G$-

isomorphism $E$ of the Hopf algebra $O_A$ to the $\mathbb{Z}_p^G$-algebra $O_K$; then $G = \text{Hom}_{\mathbb{Z}_p^G}(O_A, O_K)$, and the algebra $O_A$ is isomorphic to $\mathbb{Z}_p[X]/(\zeta_p X + \zeta_2 X^2 + \cdots + X^p)$; see [25, Section 2] and [26]. So there is a representation $r : G \rightarrow \text{GL}_n(O_K)$, and since $E$ is supersingular, the image of $r$ is contained in the kernel of reduction modulo $p$.

The following example shows that the reduction of $\text{GL}_n(O_K)$ modulo a prime divisor of $p$ may contain $p$-groups of any prescribed nilpotency class $l > 1$ for extensions $K/Q_p$ with large ramification; these groups are not abelian, and they are not diagonalizable in $\text{GL}_n(O_K)$.

Example 9. Let us consider the following $p$-group of nilpotency class $l$ determined by generators $a, b_1, b_2, \ldots, b_l$ and relations $b_i^p = 1$, $b_i b_j = b_j b_i$, $i = 1, 2, \ldots, l$; $a b_i = b_i a$, $b_i b_j = b_i a b_j^{i - 1} a^{-1}$, $i = 1, 2, \ldots, l$; $a^p = 1$, where $n = p^2 > 1 > p^2 - 1$ and $t$ is a suitable positive integer. Let $H$ be the abelian subgroup of $G$ generated by $b_1, \ldots, b_l$, and let $\chi$ denote the character of $H$ given on the generators as follows: $\chi(b_i) = \zeta_p$, $\chi(a) = a$.

A character $\chi$ together with the decomposition of $G$ into cosets with respect to $H$: $G = 1 \cdot H + a \cdot H + \ldots + a^{n-1} \cdot H$ gives rise to an induced representation $R = \text{Ind}_H^G \chi$ of $G$. For the $n \times n$ matrices $e_{ij}$ having precisely one nonzero entry in the position $(i, j)$ equal to 1 we can define a $n \times n$ matrix using the binomial coefficients \[ C = \sum_{n \geq i \geq j \geq 1} (-1)^{i-j} \binom{n}{i-j} e_{ij}. \]

(10)

Theorem 10. Let $Q_p(\zeta_{p^n})$ denote the extension of $Q_p$ obtained by adjoining all roots $\zeta_{p^n}$, $i = 1, 2, \ldots, p$-primary orders of $1$, let $p$ be the uniformizing element of a finite extension $K/Q_p$ such that $K \subset Q_p(\zeta_{p^n})$, and let $D = \text{diag}(1, \pi, \pi^2, \ldots, \pi^{n-1})$. Then for $g \in G$ the representation $R_n(g) = \text{Ind}_H^G \chi(g)D^{-1}C^{-1}R(g)CD$ of $G$ is a faithful, absolute, irreducible representation in $\text{GL}_n(O_K)$ by matrices congruent to $I_n(\text{mod } p)$. Moreover, such representations are pairwise nonequivalent over $O_{Q_p(\zeta_{p^n})}$ and for the lower central series $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$ of $G$ all elements of $R_n(G_{i+1})$ are congruent to $I_{n}(\text{mod } p^i)$ if the elements of $R_n(G)$ are congruent to $I_{n}(\text{mod } p^{n-i})$.

For the proof of Theorem 10 (which is constructive) see [17, 27]. Remark that the construction of Theorem 10 can be realized also over the integers of cyclotomic subextensions $K \subset Q(\zeta_{p^n}) = \bigcup_{i=1}^{\infty} Q(\zeta_{p^i})$ of $Q$ and other global fields.

Acknowledgment

The author is grateful to the referees for useful suggestions.
References


