Hindawi Publishing Corporation
ISRN Algebra
Volume 2013, Article ID 638623, 4 pages
http://dx.doi.org/10.1155/2013/638623

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

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. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Q}_p$, $\mathbb{Z}$, $\mathbb{Z}_p$, 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. $\mathrm{GL}_n(R)$ denotes the general linear group over R. $[E : F]$ denotes the degree of the field extension E/F. I_m denotes the unit $m \times m$ matrix. $\mathrm{diag}(d_1, d_2, \ldots, d_m)$ is a diagonal matrix having diagonal components $d_1, d_2, \ldots, d_n$. $|G|$ denotes the order of a finite group G.

Theorem 1. *Let A be a commutative ring, which is an integral domain, and let $G \subset GL_n(A)$ be a finite nilpotent group indecomposable in $GL_n(A)$. Let one suppose that every matrix $g \in G$ 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 $g = [g_{ij}]_{i,j}$ in G has at least one diagonal element $g_{ii} \neq 0$,*

(ii) *$-I_n$ is not contained in G, where I_n is the identity $n \times n$ matrix, and for any matrix $g = [g_{ij}]_{i,j}$ in G, there are 2 indices i, j such that $g_{ij} \neq 0$ and $g_{ji} \neq 0$.*

For the proof of Theorem 1 we need the following.

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

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

$$d = \mathrm{diag}\left(d_1, \ldots, d_1, d_2, \ldots d_2, \ldots, d_i, \ldots, d_i, \ldots, d_k, \ldots, d_k\right), \tag{1}$$

where $d_i \neq d_j$ for $i \neq j$ and d contains t_i elements that equal d_i, $i = 1, \ldots, k$. For a matrix $g = [g_{ij}]_{i,j} \in G$ consider the system of linear equations determined by the conditions $gd = dg$; this immediately implies that $g_{ij} = 0$ for $i \leq t_1$, $j > t_1$, and $g_{km} = 0$ for $m \leq t_1$, $k > t_1$. 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

$$\psi : G' \longrightarrow \mathrm{GL}_{n^t}(A), \tag{2}$$

given by $\psi(g) = g^{\otimes^t}$. The kernel of ψ 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 $g_0 = \mathrm{diag}(d_1, \ldots, d_n)$. Then $\psi(g_0)$ is a nonscalar diagonal matrix in the centre of $\psi(G)$, g_0 is also not a scalar matrix, and for any $g \in G$ we have $gg_0 = g_0 g\zeta$ for some root of $1\zeta = \zeta(g)$. If for the matrix $g = [g_{nk}]_{n,k}$ the elements g_{ij} and g_{ji} are not zero, we obtain $d_j = d_i\zeta$ and $d_i = d_j\zeta$, 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 $\zeta^2 = 1$ and $\zeta = \pm 1$, but $\zeta = -1$ is impossible in the virtue of the condition that $-I_n$ 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 χ, let $\{0\} \neq \mathcal{J} \neq S$, and let g be a $n \times n$ matrix of finite order congruent to $I_n (\mathrm{mod}\, \mathcal{J})$.*

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

(ii) *Let $\chi = 0$, and let $\mathcal{J} = \mathfrak{p}$ be a prime ideal having ramification index e with respect to p, let $g \equiv I_n (\mathrm{mod}\, \mathfrak{p}^r)$, and let*

$$\lambda p^{i-1}(p-1) \leqslant \frac{e}{r} < p^i (p-1), \quad i \geqslant 0, \ \lambda = \min\{1, i\}. \tag{3}$$

Then $g^{p^i} = I_n$; in particular, any finite group of matrices congruent to $I_n (\mathrm{mod}\, \mathfrak{p}^t)$ 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 $d = [K : \mathbb{Q}]$ 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 $N_{K/\mathbb{Q}}(\mathcal{J}) > p^{d/(p-1)}$.*

Remark 5. Earlier Bürgisser obtained a similar result for $N_{K/\mathbb{Q}}(\mathcal{J}) > 2^d$; see [18, Lemma 3.1].

Propositions 3 and 6 below can be used for estimating the orders of finite subgroups of $\mathrm{GL}_n(\mathbb{O}_K)$ using the reduction modulo some prime ideal $\mathfrak{p} \subset O_K$. It is also possible to determine the structure of a p-subgroup of $\mathrm{GL}_n(O_K)$ having the maximal possible order with some modifications in the case $p = 2$. The theorems describing the maximal p-subgroups of $\mathrm{GL}_n(K)$ over fields can be found in [19]; in particular, it is proven that there is only one conjugacy class of maximal p-subgroups of $\mathrm{GL}_n(K)$ for $p > 2$; see also [9, 20]. However, the equivalence of subgroups in $\mathrm{GL}_n(O_K)$ 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 $K/\mathbb{Q}_p$ be a finite extension, and let $\zeta_p \in O_K$. Let $p = \mathfrak{p}^e$, and let $e = p - 1$. Let G be a finite subgroup of $GL_n(O_K)$ and $g \equiv I_n (\mathrm{mod}\, \mathfrak{p})$ 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 π 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 $g_i^{-1} \equiv I_n - \pi B_i (\mathrm{mod}\, \pi^2)$, $i = 1, 2$, and $h = g_1 g_2 g_1^{-1} g_2^{-1} \equiv I_n (\mathrm{mod}\, \pi^2)$. It follows from Proposition 2 that $h = I_n$ and the same proposition shows that $g^p = I_n$ 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

$$M^{-1} g M = \mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n) \tag{4}$$

is a diagonal matrix for a triangular matrix g of order p which is congruent to $I_n (\mathrm{mod}\, \mathfrak{p})$. Indeed, let $g \in G$ and

$$g = \begin{vmatrix} \zeta_{(1)} I_{t_1} & P_2^1 \ldots & P_k^1 \\ 0 & \zeta_{(2)} I_{t_2} \ldots & P_k^2 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \zeta_{(k)} I_{t_k} \end{vmatrix}, \tag{5}$$

and let

$$S = \begin{vmatrix} I_{t_1} & 0 \ldots & A_1 \\ 0 & I_{t_2} \ldots & A_2 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & I_{t_k} \end{vmatrix}, \tag{6}$$

for $t_1 + t_2 + \cdots + t_k = n$ and $t_1 \leq t_2 \leq \cdots \leq t_k, \zeta_{(i)}$, $i = 1, 2, \ldots, k$ are appropriate p-roots of 1. We consider

$$S^{-1} g S = \begin{vmatrix} \zeta_{(1)} I_{t_1} & * \ldots & M_k^1 \\ 0 & \zeta_{(2)} I_{t_2} \ldots & M_k^2 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \zeta_{(k)} I_{t_k} \end{vmatrix}, \tag{7}$$

and we find the system of conditions for providing $M_k^i = 0_{t_i,t_k}$, the zero $t_i \times t_k$ matrix. We have the following system of conditions:

$$\zeta_{(1)}\left(1-\zeta_{(k)}\zeta_{(1)}^{-1}\right)A_1 + P_2^1 A_2 + \cdots + P_{k-1}^1 A_{k-1} + P_k^1 = 0_{t_1,t_k},$$

$$\cdots$$

$$\zeta_{(k-2)}A_{k-2}\left(1-\zeta_{(k)}\zeta_{(k-2)}^{-1}\right) + P_{k-1}^{k-2}A_{k-1} + P_k^{k-2} = 0_{t_{k-2},t_k},$$

$$\zeta_{(k-1)}A_{k-1}\left(1-\zeta_{(k)}\zeta_{(k-1)}^{-1}\right) + P_k^{k-1} = 0_{t_{k-1},t_k}. \tag{8}$$

The condition $g \equiv I_n(\mathrm{mod}\,\mathfrak{p})$ implies that $P_i^j \equiv 0_{t_j t_i}(\mathrm{mod}\,\mathfrak{p})$, and we can find A_i, $1 \le i \le k-1$ sequentially using the results of the previous steps:

$$A_{k-1} = -\frac{P_k^{k-1}}{\zeta_{(k-1)}\left(1-\zeta_{(k)}\zeta_{(k-1)}^{-1}\right)},$$

$$A_{k-2} = -\frac{\left(P_k^{k-2} + P_{k-1}^{k-2}A_{k-1}\right)}{\zeta_{(k-2)}\left(1-\zeta_{(k)}\zeta_{(k-2)}^{-1}\right)}, \tag{9}$$

$$A_{k-3} = -\frac{\left(P_k^{k-3} + P_{k-1}^{k-3}A_{k-1} + P_{k-2}^{k-3}A_{k-2}\right)}{\zeta_{(k-3)}\left(1-\zeta_{(k)}\zeta_{(k-3)}^{-1}\right)},$$

and so on. Now, using the induction on the degree n we can find a matrix M that transforms g to a diagonal form as required.

The condition $g \equiv I_n(\mathrm{mod}\,\mathfrak{p})$ 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 $K/\mathbb{Q}$ 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 $\mathrm{GL}_n(O)$ and $g \equiv I_n(\mathrm{mod}\,\mathfrak{p})$ for all $g \in G$. Then G is conjugate in $\mathrm{GL}_n(O)$ to an abelian group of diagonal matrices of exponent p.

In this situation we can use the statement (81.20) in [CR] for proving the above result for the given Dedekind ring O (compare also the proof of (81.20) 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 $K/\mathbb{Q}_p$ and finite subgroups $G \subset \mathrm{GL}_n(O_K)$ which are contained in the kernel of reduction of $\mathrm{GL}_n(O_K)$ modulo ideals having ramification indices $e > p-1$.

Example 8. For the following finite extension $K/\mathbb{Q}_p$ 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 $K/\mathbb{Q}_p$ 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, 1.3 and Section 2]). Note that for some E the ramification index $e = e(K/\mathbb{Q}_p) = p^2-1$ ([24, page 275, Proposition 12]).

We can consider the group G of p-torsion points as $\mathbb{Z}_p$-algebra homomorphisms from the Hopf algebra O_A to the $\mathbb{Z}_p$-algebra O_K; then $G = \mathrm{Hom}_{\mathbb{Z}_p}(O_A, O_K)$, and the algebra O_A is isomorphic to $\mathbb{Z}_p[X]/(c_1X + c_2X^2 + \cdots + X^{p^2})$; see [25, Section 2] and [26]. So there is a representation $\nu : G \to \mathrm{GL}_{p^2}(O_K)$, and since E is supersingular, the image of ν is contained in the kernel of reduction modulo $\mathfrak{p}$.

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

Example 9. Let us consider the following p-group of nilpotency class l, determined by generators $a, b_1, \ldots, b_l$ and relations $b_i^p = 1$, $b_ib_j = b_jb_i$, $i = 1, 2, \ldots, l$; $ab_1 = b_1a$, $b_{i-1} = b_iab_1^{-1}a^{-1}$, $i = 1, 2, \ldots, l$; $a^n = 1$, where $n = p^t \ge l > p^{t-1}$ and t is a suitable positive integer. Let H be the abelian subgroup of G generated by $b_1, \ldots, b_l$, and let χ denotes the character of H given on the generators as follows: $\chi(b_1) = \zeta_p - a$ primitive p-root of 1, $\chi(b_i) = 1$, $i = 2, \ldots, l$. The character χ together with the decomposition of G into cosets with respect to H: $G = 1 \cdot H + a \cdot H + \cdots + a^{n-1} \cdot H$ gives rise to an induced representation $R = \mathrm{Ind}_H^G\chi$ 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 $\binom{n-j}{i-j}$:

$$C = \Sigma_{n \ge i \ge j \ge 1}(-1)^{i-j}\binom{n-j}{i-j}e_{ij}. \tag{10}$$

Theorem 10. *Let $\mathbb{Q}_p(\zeta_{p^\infty})$ denote the extension of $\mathbb{Q}_p$ obtained by adjoining all roots ζ_{p^i}, $i = 1, 2, 3, \ldots$ of p-primary orders of 1, let π be the uniformizing element of a finite extension $K/\mathbb{Q}_p$ such that $K \subset \mathbb{Q}_p(\zeta_{p^\infty})$, and let $D = \mathrm{diag}(1, \pi, \pi^2, \ldots, \pi^{n-1})$. Then for $g \in G$ the representation $R_\pi(g) = D^{-1}C^{-1}R(g)CD$ of G is a faithful, absolute, irreducible representation in $GL_n(O_K)$ by matrices congruent to $I_n(\mathrm{mod}\,\pi)$. Moreover, such representations are pairwise nonequivalent over $O_{\mathbb{Q}_p(\zeta_{p^\infty})}$, and for the lower central series $G = G_l \supset G_{l-1} \supset \cdots \supset G_0 = \{I_n\}$ of G all elements of $R_\pi(G_{l-i+1})$ are congruent to $I_n(\mathrm{mod}\,\pi^{iw})$ if the elements of $R_\pi(G)$ are congruent to $I_n(\mathrm{mod}\,\pi^w)$.*

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 $K \subset \mathbb{Q}(\zeta_{p^\infty}) = \bigcup_{i=1}^{\infty}\mathbb{Q}(\zeta_{p^i})$ of $\mathbb{Q}$ and other global fields.

Acknowledgment

The author is grateful to the referees for useful suggestions.

References

[1] W. C. Brown, *Matrices Over Commutative Rings*, vol. 169 of *Monographs and Textbooks in Pure and Applied Mathematics*, Marcel Dekker, New York, NY, USA, 1993.

[2] D. Laksov, "Diagonalization of matrices over rings," *Journal of Algebra*, vol. 376, pp. 123–138, 2013.

[3] H. Minkowski, "Überber den arithmetischen Begriff der Äquivalenz und über die endlichen Gruppen linearer ganzzahliger Substitutionen," *Journal für Die Reine und Angewandte Mathematik*, vol. 100, pp. 449–458, 1887.

[4] H. Minkowski, "Zur Theorie der positiven quadratischen Formen," *Journal für Die Reine und Angewandte Mathematik*, vol. 101, no. 3, pp. 196–202, 1887.

[5] H. Minkowski, *Geometrie der Zahlen*, Teubner, Berlin, Germany, 1910.

[6] C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Interscience Publishers, New York, NY, USA, 1962.

[7] C. W. Curtis and I. Reiner, *Methods of Representation Yheory. Vol. I*, John Wiley & Sons, New York, NY, USA, 1981.

[8] C. W. Curtis and I. Reiner, *Methods of Representation Theory. Vol. II*, vol. 2, John Wiley & Sons, New York, NY, USA, With applications to finite groups and orders, 1987.

[9] W. Feit, "Finite linear groups and theorems of Minkowski and Schur," *Proceedings of the American Mathematical Society*, vol. 125, no. 5, pp. 1259–1262, 1997.

[10] H.-J. Bartels, "Zur Galoiskohomologie definiter arithmetischer Gruppen," *Journal für die Reine und Angewandte Mathematik*, vol. 298, pp. 89–97, 1978.

[11] J. Rohlfs, "Arithmetisch definierte Gruppen mit Galoisoperation," *Inventiones Mathematicae*, vol. 48, no. 2, pp. 185–205, 1978.

[12] H.-J. Bartels and D. A. Malinin, "Finite Galois stable subgroups of GL_n," in *Noncommutative Algebra and Geometry*, C. de Concini, F. van Oystaeyen, N. Vavilov, and A. Yakovlev, Eds., vol. 243 of *Lecture Notes in Pure and Applied Mathematics*, pp. 1–22, 2006.

[13] H.-J. Bartels and D. A. Malinin, "On finite Galois stable subgroups of GL_n in some relative extensions of number fields," *Journal of Algebra and its Applications*, vol. 8, no. 4, pp. 493–503, 2009.

[14] D. A. Malinin, "Galois stability for integral representations of finite groups," *Rossiĭskaya Akademiya Nauk: Algebra i Analiz*, vol. 12, no. 3, pp. 106–145, 2000 (Russian).

[15] B. Bürgisser, "On the projective class group of arithmetic groups," *Mathematische Zeitschrift*, vol. 184, no. 3, pp. 339–357, 1983.

[16] P. Roquette, "Realisierung von Darstellungen endlicher nilpotenter Gruppen," *Archiv der Mathematik*, vol. 9, pp. 241–250, 1958.

[17] D. A. Malinin, "Integral representations of p-groups over local fields," *Doklady Akademii Nauk SSSR*, vol. 309, no. 5, pp. 1060–1063, 1989 (Russian).

[18] B. Bürgisser, "Finite p-periodic quotients of general linear groups," *Mathematische Annalen*, vol. 256, no. 1, pp. 121–132, 1981.

[19] C. R. Leedham-Green and W. Plesken, "Some remarks on Sylow subgroups of general linear groups," *Mathematische Zeitschrift*, vol. 191, no. 4, pp. 529–535, 1986.

[20] J.-P. Serre, "Bounds for the orders of the finite subgroups of $G(k)$," in *Group Representation Theory*, pp. 405–450, EPFL Press, Lausanne, Switzerland, 2007.

[21] A. E. Zalesskii, "Linear groups," *Russian Mathematical Surveys*, vol. 36, pp. 63–128, 1981.

[22] A. E. Zalesskiĭ, "Linear groups," in *Algebra. Topology. Geometry*, vol. 21 of *Itogi Nauki i Tekhniki*, pp. 135–182, Moscow, Russia, 1983.

[23] P. H. Tiep and A. E. Zalesskii, "Some aspects of finite linear groups: a survey," *Journal of Mathematical Sciences*, vol. 100, no. 1, pp. 1893–1914, 2000.

[24] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques," *Inventiones Mathematicae*, vol. 15, no. 4, pp. 259–331, 1972.

[25] F. Destrempes, "Deformations of Galois representations: the flat case," in *Seminar on Fermat's Last Theorem*, vol. 17, pp. 209–231, American Mathematical Society, Providence, RI, USA, 1995.

[26] V. A. Kolyvagin, "Formal groups and the norm residue symbol," *Izvestiya Akademii Nauk SSSR*, vol. 43, no. 5, Article ID 10541120, 1979.

[27] D. A. Malinin, "Integral representations of p-groups of a given class of nilpotency over local fields," *Rossiĭskaya Akademiya Nauk: Algebra i Analiz*, vol. 10, no. 1, pp. 58–67, 1998 (Russian).