Normal forms for matrices over uniserial rings of length two

Sebastian Jambor*†and Wilhelm Plesken‡§

Lehrstuhl B für Mathematik, RWTH Aachen University, Templergraben 64, 52062 Aachen, Germany

Abstract

This paper develops methods to describe the conjugacy classes of $\mathrm{GL}(n, R)$ on $R^{n\times n}$ for a serial ring R of length two. The main result is a reduction to a computation in the matrix algebra over the residue class field of R, which in some cases can be done theoretically without any actual computation.

1 Introduction

Whereas the normal forms of matrices over $\mathbb{F}_2$ of degree n are easily enumerated via Jordan or Frobenius normal forms (modulo the knowledge of irreducible polynomials of degree up to n over $\mathbb{F}_2$), there seems to be no classification available for normal forms of matrices over $\mathbb{Z}/4\mathbb{Z}$. On the other hand, A. Kerber pointed out to us that it is desirable to have access to the conjugacy classes of $\mathrm{GL}(n, \mathbb{Z}/4\mathbb{Z})$ for the enumeration of codes over $\mathbb{Z}/4\mathbb{Z}$ (cf. [BBF+06]). The present paper develops some methods to deal with these problems.
Since $\mathbb{Z}/4\mathbb{Z}$ can be replaced by any commutative uniserial ring R of length two, we formulate our results for that more general case.

Notation. Let R be a commutative uniserial ring of length two with generator π of the non-trivial ideal; $k := R/\pi R$ denotes the residue class field of R with natural epimorphism $\nu\colon R \to k$. Set $A := k^{n\times n}$ and $B := R^{n\times n}$ with the unit groups $A^* = \mathrm{GL}(n, k)$ and $B^* = \mathrm{GL}(n, R)$. The induced epimorphisms $B \to A$ and $B^* \to A^*$ are also denoted by ν.

Our main result is a reduction of the determination of B^*-conjugacy classes in B to a certain computation in the algebra A over the field k:

Theorem 1. *Let $a \in A$. Then the set of B^*-conjugacy classes in B intersecting $\nu^{-1}(\{a\})$ non-trivially is in 1-1 correspondence with $\mathrm{C}_A(a)^\# / \mathrm{C}_{A^*}(a)$, the set of orbits of $\mathrm{C}_A(a)^\# = \mathrm{Hom}_k(\mathrm{C}_A(a), k)$ under $\mathrm{C}_{A*}(a)$, where $\mathrm{C}_{A*}(a)$ acts on $\mathrm{C}_A(a)$ by conjugation and $\mathrm{C}_A(a)^\#$ is the dual module.*

In particular, the parameterization and the lengths of the $\mathrm{GL}(n, R)$-conjugacy classes of $R^{n\times n}$ depend only on the residue class field k of R, not on the ring R itself; cf. also Singla [Sin10], who proves that the number of conjugacy classes only depend on the residue class field, if it is finite.
Note, by general principles, the number of orbits of $\mathrm{C}_{A^*}(a)$ on $\mathrm{C}_A(a)$ is the same as the number of orbits of $\mathrm{C}_{A^*}(a)$ on $\mathrm{C}_A(a)^\#$, in case k is finite, although the orbits might differ in size. This follows from a well-known argument by R. Brauer, cf. [Hup67, Satz 13.5]: By Burnside's Lemma, the number of orbits is determined by the number of fixed points of the elements of $\mathrm{C}_{A^*}(a)$.

*Corresponding author
†Email address: sebastian@momo.math.rwth-aachen.de
‡Email address: plesken@momo.math.rwth-aachen.de
§This work was partially supported by the DFG priority program SPP 1388

Since $\mathrm{C}_{A^*}(a)$ acts linearly, the fixed points form the eigenspace to the eigenvalue 1. But the dimensions of the eigenspaces of a linear map and its dual are the same.
The 1-1 correspondence in Theorem 1 however is natural, modulo the choice of one fixed preimage $b \in B$ of a under ν.
Two special cases of our result are worthwhile to mention here already.

Corollary 2 (The semi-simple case)**.** *Let $a \in A$ such that its minimal polynomial μ is irreducible of degree d. Set $F := k[x]/\langle\mu\rangle$. Then $\mathrm{C}_A(a)^\# / \mathrm{C}_{A^*}(a)$ can be identified with $F^{m\times m}/\mathrm{GL}(m, F)$ for $m = n/d$, which again can be enumerated by Jordan normal forms.*

In concrete terms: Let $\Gamma \in k^{d\times d}$ be the companion matrix of μ; then the representation $F = k[x]/\langle\mu\rangle \to k^{d\times d}: x \mapsto \Gamma$ induces a representation $\rho: F^{m\times m} \to k^{n\times n}$. For $X \in F^{m\times m}$ denote an arbitrary preimage of $\rho(X)$ in $R^{n\times n}$ again by $\rho(X)$. Then if $b \in B$ is an arbitrary preimage of a, the conjugacy classes of B^* on B intersecting $\nu^{-1}(\{a\})$ non-trivially are represented by the elements

$$b + \pi\rho(J),$$

where J runs through all Jordan normal forms of $F^{m\times m}$.
The following corollary has also been proved by Nechaev in [Nec83] for a more general class of rings.

Corollary 3 (The cyclic case)**.** *Let $a \in A$ such that the minimal polynomial is the characteristic polynomial, denoted by χ. Then the relevant B^*-conjugacy classes on B are represented by the companion matrices in $R^{n\times n}$ of all possible monic lifts of χ to $R[x]$.*

For square matrices over a field, the classification of conjugacy classes can be reduced to matrices where the characteristic polynomial is a power of an irreducible polynomial; for the general case one takes block diagonal matrices of this form. The next remark shows that we can assume block diagonal form for the matrices in B as well, cf. also [Nec83].

Remark 4. *Let $a \in A$ be in block diagonal form $a = \mathrm{diag}(a_1, \ldots, a_\ell)$ with $a_i \in k^{m_i\times m_i}$, such that the characteristic polynomials are pairwise coprime, and let $\widetilde{b} \in \nu^{-1}(\widetilde{a})$. Then there exists a conjugate b of $\widetilde{b}$ in block diagonal form $b = \mathrm{diag}(b_1, \ldots, b_\ell)$ with $\nu(b_i) = a_i$. Furthermore, every element $c \in \mathrm{C}_B(b)$ is of block diagonal form $c = \mathrm{diag}(c_1, \ldots, c_\ell)$ with $c_i \in \mathrm{C}_{R^{m_i\times m_i}}(b_i)$.*

Several authors studied the similarity classes of matrices in $(\mathbb{Z}/p^\ell\mathbb{Z})^{n\times n}$ or, more generally, of matrices in $R^{n\times n}$, where R is a commutative uniserial ring of length ℓ with residue class field k, for various n and ℓ: Pomfret [Pom73] decides similarity for matrices in a special class, namely for those matrices $b \in R^{n\times n}$ where R is finite and the order of $\nu(b) \in k^{n\times n}$ is coprime to the characteristic of k. Nobs [Nob77] classifies the similarity classes for $n = 2$ and arbitrary ℓ, and Pizarro [Piz83] and Avni et. al. [AOPV09] do the same for $n = 3$ and arbitrary ℓ. Nechaev [Nec83] and Appelgate and Onishi [AO83] treat the problem to decide whether two given matrices in $R^{n\times n}$ or $\mathrm{SL}(n, R)$ are conjugate, respectively.
The present paper focuses on the case of $\ell = 2$ and arbitrary n. Theorem 1 gives a structural description of the decomposition of the conjugacy classes and is of theoretical interest in itself, but it also provides means to efficiently compute representatives and lengths of all conjugacy classes for moderately sized n (cf. Section 4).

2 Proof of the theorem

We will prove the theorem in several steps by a series of lemmas. First note that, instead of considering the whole action of B^* on B, it is enough to consider the action of the full preimage of the centralizer of a in A^* under ν on the full preimage of a in B under ν, i.e., the action of $\widetilde{C} := \nu^{-1}(\mathrm{C}_{A^*}(a))$ on $\nu^{-1}(\{a\})$.

As usual, the calculation of the orbits can be done in two steps: First, calculate the orbits of a normal subgroup N of $\widetilde{C}$, and second, act on these orbits with the factor group $\widetilde{C}/N$. In our case, we will choose $N := \ker(\nu) \trianglelefteq B^*$.

2.1 Action of the kernel

In this first step we describe the orbits of $N := \ker(\nu) \trianglelefteq B^*$ on $\nu^{-1}(\{a\})$.

Lemma 5. *For $a \in A$ define $\delta_a \colon k^{n\times n} \to k^{n\times n} \colon x \mapsto xa - ax$. Then there is a 1-1 correspondence between* $\operatorname{coker}(\delta_a)$ *and the orbits of N on $\nu^{-1}(\{a\})$.*

Proof. Fix $b \in \nu^{-1}(\{a\})$. Then $\nu^{-1}(\{a\}) = \{b + \pi x \mid x \in B\}$. For $b + \pi x \in \nu^{-1}(\{a\})$ and $1 + \pi y \in \widetilde{C}$, the conjugation action gives

$$(1 + \pi y)(b + \pi x)(1 - \pi y) = b + \pi(x + yb - by),$$

and since x and y can be chosen arbitrarily in B, there is a 1-1 correspondence between $\nu^{-1}(\{a\})/N$ and $\operatorname{coker}(\delta_b)$, where $\delta_b \colon \pi B \to \pi B$ is defined analogously to δ_a. Note that the R-module πB can be regarded as k-vector space, since $\pi \in R$ is in the kernel of the action; the vector space isomorphism $\pi B \to A \colon \pi x \mapsto \nu(x)$ induces an isomorphism $\operatorname{coker}(\delta_b) \cong \operatorname{coker}(\delta_a)$. □

2.2 Action of the factor group

For the second step, we have to study the action of $C := \mathrm{C}_{A^*}(a) = \widetilde{C}/N$ on $\nu^{-1}(\{a\})/N$. The bijection in the last lemma gives an induced action of C on $\operatorname{coker}(\delta_b)$, so we can study this action instead. This action however depends on the chosen preimage b of a. The main observation in this section is that we can assume that C acts linearly on $\operatorname{coker}(\delta_b)$ by conjugation. This relies on the fact that we can construct preimages b such that $\mathrm{C}_{B^*}(b)$ is well-behaved:

Lemma 6. *Let $a \in A$. Then there exists a lift $b \in B$ of a, such that the map $\mathrm{C}_B(b) \to \mathrm{C}_A(a)$ induced by ν is an epimorphism.*
In particular, any element in $\mathrm{C}_{A^*}(a)$ has a preimage in $\mathrm{C}_{B^*}(b)$.

Proof. We can assume that a is given in Frobenius normal form, so a is in block diagonal form, where the blocks are companion matrices of polynomials $\mu_1, \ldots, \mu_\ell \in k[x]$ with $\mu_i | \mu_{i+1}$. Choose monic lifts $\widetilde{\mu}_1, \ldots, \widetilde{\mu}_\ell \in R[x]$ with $\widetilde{\mu}_i | \widetilde{\mu}_{i+1}$ and $\deg \widetilde{\mu}_i = \deg \mu_i$, and let b be the block diagonal matrix where the blocks are the companion matrices of the $\widetilde{\mu}_i$. The result now follows by the usual argument to describe the endomorphism ring of a finitely generated module over a principal ideal domain: Let $M_i := R[x]/\langle \widetilde{\mu}_i \rangle$. Then $R^{n\times 1}$ is an $R[x]$-module via the action of b isomorphic to $M := M_1 \oplus \cdots \oplus M_\ell$, and $\mathrm{C}_B(b) \cong \operatorname{End}_{R[x]}(M) \cong \bigoplus_{i,j} \operatorname{Hom}_{R[x]}(M_i, M_j)$. Similarly, set $N_i := k[x]/\langle \mu_i \rangle$. Then $k^{n\times 1}$ is a $k[x]$-module via the action of a, isomorphic to $N := \nu(M) = N_1 \oplus \cdots \oplus N_\ell$, and $\mathrm{C}_A(a) \cong \operatorname{End}_{k[x]}(\nu(M)) \cong \bigoplus_{i,j} \operatorname{Hom}_{k[x]}(N_i, N_j)$. It therefore suffices to show that the induced map $\operatorname{Hom}_{R[x]}(M_i, M_j) \to \operatorname{Hom}_{k[x]}(N_i, N_j)$ is surjective. So let $\alpha \in \operatorname{Hom}_{k[x]}(N_i, N_j)$; then α is induced by a homomorphism $k[x] \to k[x] \colon 1 \mapsto f$ for some $f \in k[x]$ such that $\mu_j | \mu_i f$. We construct a preimage of α as follows: If $\mu_j | \mu_i$, take any preimage $\widetilde{f} \in R[x]$ of f. Then the map $R[x] \to R[x] \colon 1 \mapsto \widetilde{f}$ induces a homomorphism $\widetilde{\alpha} \in \operatorname{Hom}_{R[x]}(M_i, M_j)$, and $\widetilde{\alpha}$ is a preimage of α. If $\mu_i | \mu_j$, set $g := \mu_i f / \mu_j$ and let $\widetilde{g} \in R[x]$ be a preimage of g. Define $\widetilde{f} := \widetilde{g}\widetilde{\mu}_j / \widetilde{\mu}_i$. Then $\widetilde{\alpha}$ is a preimage of α again. □

Corollary 7. *For $a \in A$ choose a preimage $b \in B$ as in Lemma 6, so that every centralizer element in $C = \mathrm{C}_{A^*}(a)$ lifts to an element of $\mathrm{C}_{B^*}(b)$. Then the action of C on* $\operatorname{coker}(\delta_a)$ *induced by the bijection in Lemma 5 is the linear action induced by conjugation of C on A.*

Proof. Let $c \in \mathrm{C}_{A^*}(a)$, and choose a preimage $\widetilde{c} \in \mathrm{C}_{B^*}(b)$. Then

$$\widetilde{c}(b + \pi x)\widetilde{c}^{-1} = b + \pi \widetilde{c} x \widetilde{c}^{-1}.$$

As in Lemma 5, we can identify $\operatorname{coker}(\delta_b)$ with $\operatorname{coker}(\delta_a)$, and under this identification the representative $\pi \widetilde{c} x \widetilde{c}^{-1}$ maps onto the representative cxc^{-1}. □

2.3 Intrinsic description of the orbits

The previous two steps give a 1-1 correspondence between the conjugacy classes of B^* on B intersecting $\nu^{-1}(\{a\})$ non-trivially, and the orbits $\operatorname{coker}(\delta_a)/\,\mathrm{C}_{A^*}(a)$. The final step is to replace $\operatorname{coker}(\delta_a)$ by an object with an intrinsic connection to $\mathrm{C}_{A^*}(a)$:

Lemma 8. *Let $a \in A$ and $C := \mathrm{C}_{A^*}(a)$. Then $(\ker \delta_a)^\#$ and $\operatorname{coker} \delta_a$ are isomorphic as kC-modules, where C acts by conjugation on $\ker \delta_a$ and $\operatorname{coker} \delta_a$, and $(\ker \delta_a)^\#$ denotes the dual module.*

Proof. Let $\delta_a^{\mathrm{tr}} \colon (k^{n\times n})^\# \to (k^{n\times n})^\# \colon \varphi \mapsto \varphi \circ \delta_a$ denote the dual map of δ_a. Then

$$\alpha_1 \colon \operatorname{coker}(\delta_a) \to \ker(\delta_a^{\mathrm{tr}})^\# \colon X + \operatorname{im} \delta_a \mapsto (\varphi \mapsto \varphi(X))$$

is an isomorphism of k-vector spaces, as can be seen using the standard pairing of $k^{n\times n}$ and $(k^{n\times n})^\#$ (cf. e.g. [Coh82, Section 8.2]). Furthermore, the pairing $T \colon k^{n\times n} \times k^{n\times n} \to k \colon (X, Y) \mapsto \operatorname{trace}(XY^{\mathrm{tr}})$ gives a natural isomorphism $k^{n\times n} \cong (k^{n\times n})^\#$, which restricts to the isomorphism

$$\alpha_2 \colon \ker(\delta_a) \to \ker(\delta_a^{\mathrm{tr}}) \colon X \mapsto T(-, X^{\mathrm{tr}}).$$

Thus $\operatorname{coker}(\delta_a)$ and $\ker(\delta_a^{\mathrm{tr}})^\#$ are isomorphic as k-vector spaces. But $\ker(\delta_a^{\mathrm{tr}})$ is a kC-module via ${}^c\varphi = (X \mapsto \varphi(c^{-1}Xc))$ for $c \in C$ and $\varphi \in \ker(\delta_a^{\mathrm{tr}})$, and it is easy to verify that the maps α_1 and α_2 are isomorphisms of kC-modules, which proves the lemma. □

We remark for computational purposes that the isomorphism $\operatorname{coker} \delta_a \to (\ker \delta_a)^\#$ is given by

$$\gamma \colon \operatorname{coker} \delta_a \to (\ker \delta_a)^\# \colon X + \operatorname{im} \delta_a \mapsto (Y \mapsto \operatorname{trace}(XY)).$$

Proof of Theorem 1. Choose a preimage $b \in B$ of a as in Lemma 6 so that $\mathrm{C}_B(b) \to \mathrm{C}_A(a)$ is surjective, and for each orbit ${}^{\mathrm{C}_{A^*}(a)}c \in \mathrm{C}_A(a)^\#/\,\mathrm{C}_{A^*}(a)$ let $x_c + \operatorname{im} \delta_a = \gamma^{-1}(c) \in \operatorname{coker} \delta_a$, and denote a preimage of x_c in B again by x_c. Then the B^*-conjugacy classes in B intersecting $\nu^{-1}(\{a\})$ non-trivially are represented by the elements $b + \pi x_c$, where c runs over a system of representatives of the orbits $\mathrm{C}_A(a)^\#/\,\mathrm{C}_{A^*}(a)$. □

Note that it is in fact not important which preimage b of a we choose: each choice will give a 1-1 correspondence. However, if we want to calculate the centralizers, then the choice is important (see Corollary 9).

2.4 Proof of the corollaries

Proof of Corollary 2. The $k[x]$-module $k^{n\times 1}$ is semi-simple, isomorphic to $F \oplus \cdots \oplus F$. Hence $\mathrm{C}_A(a) \cong F^{m\times m}$, which is self-dual as $\mathrm{GL}(m, F)$-module. □

Proof of Corollary 3. In this case, the $k[x]$-module $k^{n\times 1}$ is isomorphic to $k[x]/\langle \chi \rangle$. The endomorphism ring is commutative, so the unit group acts trivially by conjugation, and the orbits are parameterized by $\operatorname{coker} \delta_a$. We can assume that a is the companion matrix of χ. Then the elementary matrices $e_{i,n} \in k^{n\times n}$ with 1 in position (i, n) and zero everywhere else are a system of representatives of $\operatorname{coker} \delta_a$. This can be seen for example by using the isomorphism γ above together with the fact that the powers of a form a k-basis of $\ker \delta_a$. □

Proof of Remark 4. Let $k^{n\times 1} = k^{m_1\times 1} \oplus \cdots \oplus k^{m_\ell \times 1}$ be the decomposition of $k^{n\times 1}$ corresponding to the block diagonal form of a, and let $\delta_1, \ldots, \delta_\ell \in \mathrm{End}_k(k^{n\times 1})$ be the corresponding idempotents, which can be written as polynomials in a. These idempotents can be lifted to idempotents $\varepsilon_1, \ldots, \varepsilon_\ell \in \mathrm{End}_R(R^{n\times 1})$ as polynomials in $\widetilde{b}$ such that $\overline{\varepsilon_i} = \delta_i$ (cf. [Jac80, Proposition 7.14]), yielding a decomposition $R^{n\times 1} = R^{m_1\times 1} \oplus \cdots \oplus R^{m_\ell\times 1}$. Choose a basis of $R^{n\times 1}$ adjusted to this decomposition which maps onto the standard basis of $k^{n\times 1}$, then the desired b can be chosen to be $\widetilde{b}$ with respect to this basis.
The statement about the centralizer is immediate, since the ε_i can also be written as polynomials in b, which shows that the $R^{m_i\times 1}$ are invariant under every $c \in \mathrm{C}_B(b)$. □

3 Centralizers

The description of the orbits of a group on a set is not complete without a description of the stabilizers.

Corollary 9. *Let the orbit of $x \in B$ in the 1-1 correspondence of Theorem 1 be represented by the orbit of an element $c \in \mathrm{C}_A(a)^\#$, where $a = \nu(x)$. Then the centralizer of x in B^* is an extension of $\mathrm{C}_A(a)$ by $\mathrm{Stab}_{\mathrm{C}_{A^*}(a)}(c)$, that is, an extension of the additive group of the centralizer of a in A by the stabilizer of c in $\mathrm{C}_{A^*}(a)$ under the transposed conjugation.*

4 Examples

We first describe the conjugacy classes of $R^{2\times 2}$, where R is a finite uniserial ring of length two. This has been done in [Nob77] and [AOPV09] in greater generality for rings of arbitrary lengths. We will however use this example to show how to apply Theorem 1 purely theoretically. Furthermore, we will give the extension type of the centralizers of each conjugacy class.

Example 10 (Conjugacy classes of $\mathrm{GL}(2, R)$)**.** We assume that $k = \mathbb{F}_q$ is a finite field with q elements in order to determine the number and sizes of conjugacy classes.
Every element of $A = k^{2\times 2}$ is either a scalar matrix or a cyclic element. If a is cyclic, then the centralizer $\mathrm{C}_A(a)$ is isomorphic to $\mathbb{F}_{q^2}$, $\mathbb{F}_q[x]/\langle x^2\rangle$, or $\mathbb{F}_q \oplus \mathbb{F}_q$, depending on whether the minimal polynomial has zero, one, or two distinct roots in $\mathbb{F}_q$. The conjugacy classes are parameterized by the companion matrices (cf. Corollary 3), and since the stabilizers are abelian, the action of their unit groups is trivial. Hence the centralizers are extensions of $\mathrm{C}_A(a)$ by $\mathrm{C}_{A^*}(a)$ (cf. Corollary 9). Note that there are $(q^2 - q)/2$ choices for monic polynomials with zero or two roots in $\mathbb{F}_q$, and q choices for monic polynomials with one root.
If $a \in A$ is scalar, then the orbits are parameterized by Jordan normal forms α of $k^{2\times 2}$ (cf. Corollary 2). The stabilizers are extensions of A by $\mathrm{C}_{A^*}(\alpha)$.
In total, there are seven different types of conjugacy classes, which are listed in Table 1.

number	size	extension type of centralizer
$q^2(q^2-q)/2$	$q^2(q^2-q)$	$\mathbb{F}_{q^2}$ by $\mathbb{F}_{q^2}^*$
$q^2(q^2-q)/2$	$q^2(q^2+q)$	$\mathbb{F}_q \oplus \mathbb{F}_q$ by $(\mathbb{F}_q \oplus \mathbb{F}_q)^*$
q^3	$q^2(q^2-1)$	$\mathbb{F}_q[x]/\langle x^2\rangle$ by $(\mathbb{F}_q[x]/\langle x^2\rangle)^*$
q^2	1	$\mathrm{GL}(2, R)$
$q(q^2-q)/2$	q^2-q	$\mathbb{F}_q^{2\times 2}$ by $\mathbb{F}_{q^2}^*$
$q(q^2-q)/2$	q^2+q	$\mathbb{F}_q^{2\times 2}$ by $(\mathbb{F}_q \oplus \mathbb{F}_q)^*$
q^2	q^2-1	$\mathbb{F}_q^{2\times 2}$ by $(\mathbb{F}_q[x]/\langle x^2\rangle)^*$

Table 1: Size and type of conjugacy classes in $\mathrm{GL}(2, R)$

Our initial motivation was the description of the conjugacy classes of $\mathrm{GL}(n,\mathbb{Z}/4\mathbb{Z})$, so we give another examples in this context. But note that it is just as simple to construct the conjugacy classes of $\mathrm{GL}(n,\mathbb{Z}/4\mathbb{Z})$ on $(\mathbb{Z}/4\mathbb{Z})^{n\times n}$, or to replace $\mathbb{Z}/4\mathbb{Z}$ by an arbitrary uniserial ring R of length two.

Example 11 (Conjugacy classes of $\mathrm{GL}(6,\mathbb{Z}/4\mathbb{Z})$)**.** There are 60 conjugacy classes of $\mathrm{GL}(6,2)$, giving 60 possibilities for the element a. After decomposition into blocks, there are only 15 elements left which have a block which is neither semi-simple nor cyclic. We will take a closer look at those elements; the other 45 elements can be dealt with theoretically, as in the last example (they give 3386 conjugacy classes in $\mathrm{GL}(6,\mathbb{Z}/4\mathbb{Z})$).
For an irreducible polynomial $\mu\in\mathbb{F}_2[x]$ of degree d and a partition $\lambda=(\lambda_1,\dots,\lambda_\ell)$ of $m\in\mathbb{N}$, let $\Phi(\mu,\lambda)\in\mathbb{F}_2^{md\times md}$ be the Frobenius normal form with elementary divisors $\mu^{\lambda_1},\dots,\mu^{\lambda_\ell}$ (so the semi-simple case corresponds to the partition $\lambda=(1,\dots,1)$, while the cyclic case corresponds to the partition $\lambda=(m)$). Furthermore, let $\Gamma(\mu):=\Phi(\mu,(1))$ be the companion matrix of μ. The 15 elements are then the matrices

- $\mathrm{diag}(\Phi(x-1,(2,1)),\Gamma(\mu_3))$, where μ_3 is one of the two irreducible polynomials of degree 3, (here, $\mathrm{diag}(M_1,M_2)$ means the block diagonal matrix with the matrices M_i on the diagonal),
- $\mathrm{diag}(\Phi(x-1,\lambda),\Gamma(x^2+x+1))$, where λ is one of the three non-trivial partitions of 4, (that is, $\lambda\neq(1,1,1,1),(4)$),
- $\Phi(x-1,\lambda)$, where λ is one of the nine non-trivial partitions of 6, and
- $\Phi(x^2+x+1,(2,1))$.

We use GAP ([GAP08]) to compute the orbits $\mathrm{C}_A(a)^\#/\,\mathrm{C}_{A^*}(a)$, where a runs through the 15 matrices. For example, the preimage of $\Phi(x-1,(2,1,1,1,1))$ gives 300 conjugacy classes in $\mathrm{GL}(6,\mathbb{Z}/4\mathbb{Z})$.
In total, $\mathrm{GL}(6,\mathbb{Z}/4\mathbb{Z})$ has 6018 conjugacy classes.

The algorithm mentioned in the last example is implemented in GAP and can be downloaded from [Jam11]. We give here a rough outline of the main task of the algorithm, namely to compute the orbits of $\mathrm{C}_{A^*}(a)$ on $\mathrm{C}_A(a)^\#$ for a given $a\in A$. By Remark 4 we are reduced to the case where the characteristic polynomial of a is a power of an irreducible polynomial $\mu\in k[t]$, so we have to compute the orbits of $\mathrm{Aut}_{k[x]}(M)$ on $\mathrm{End}_{k[x]}(M)$, where $M\cong k[x]/\langle\mu^{d_1}\rangle\oplus\cdots\oplus k[x]/\langle\mu^{d_\ell}\rangle$, for some $d_1\leq\cdots\leq d_\ell$. This reduces to the case $N\cong K[x]/\langle x^{d_1}\rangle\oplus\cdots\oplus K[x]/\langle x^{d_\ell}\rangle$, where K is the field $k[t]/\langle\mu(t)\rangle$ as follows: Each $M_i:=k[x]/\langle\mu^{d_i}\rangle$ is an algebra with factor algebra K. Since K is finite, it is in particular separable, so by Wedderburn's Principal Theorem (cf. [Alb61, Theorem 3.23]), K is a subfield of M_i. This shows that M_i is a K-algebra isomorphic to $K[x]/\langle x^{d_i}\rangle$. Furthermore, every element of $\mathrm{Hom}_{k[x]}(M_i,M_j)$ is induced by right multiplication with an element of M_j (cf. proof of Lemma 6), which proves that $\mathrm{Hom}_{k[x]}(M_i,M_j)$ is a $K[x]$-module isomorphic to $\mathrm{Hom}_{K[x]}(K[x]/\langle x^{d_i}\rangle,K[x]/\langle x^{d_j}\rangle)$. Finally note that

$$\mathrm{End}_{k[x]}(M)\cong\bigoplus_{i,j}\mathrm{Hom}_{k[x]}(k[x]/\langle\mu^{d_i}\rangle,k[x]/\langle\mu^{d_j}\rangle),$$

hence $\mathrm{End}_{k[x]}(M)\cong\mathrm{End}_{K[x]}(N)$.
The remaining problem is a technical one, namely to represent $\mathrm{End}_{K[x]}(N)$ and $\mathrm{Aut}_{K[x]}(N)$ on the computer. For $f\in K[x]$ with $x^{d_j}|x^{d_i}f$ let $\alpha_f\in\mathrm{Hom}_{K[x]}(K[x]/\langle x^{d_i}\rangle,K[x]/\langle x^{d_j}\rangle$ denote the induced homomorphism. Set $e:=\max(0,d_j-d_i)$, then $(\alpha_{x^e},\alpha_{x^{e+1}},\dots,\alpha_{x^{d_j-1}})$ is a basis of $\mathrm{Hom}_{K[x]}(N_i,N_j)$. This gives a basis of $\mathrm{End}_{K[x]}(N)$, and each of these basis elements can easily be described by matrices over K.

As for $\mathrm{Aut}_{K[x]}(N)$, note that $\alpha \in \mathrm{End}_{K[x]}(M)$ is invertible if and only if it is invertible modulo the radical. But $\mathrm{End}_{K[x]}(M)/\operatorname{rad}(\mathrm{End}_{K[x]}(M))$ is isomorphic to a direct sum of matrix algebras over K, and its unit group is isomorphic to a direct product of general linear groups. Generators of general linear groups can be easily computed, and lifting generators of this group together with generators of the kernel gives generators of $\mathrm{Aut}_{K[x]}(M)$, again as matrices over K.
The representation $\mathrm{Aut}_{K[x]}(M) \to \mathrm{GL}(\mathrm{End}_{K[x]}(M))$ can be computed by choosing the generators of $\mathrm{Aut}_{K[x]}(M)$ and a basis of $\mathrm{End}_{K[x]}(M)$; transposing gives the contragredient representation. Now the GAP functions can be used to compute the orbits of $\mathrm{Aut}_{K[x]}(M)$ on $\mathrm{End}_{K[x]}(M)^{\#}$ together with their stabilizers.

References

[Alb61] A. Adrian Albert. *Structure of algebras.* Revised printing. American Mathematical Society Colloquium Publications, Vol. XXIV. American Mathematical Society, Providence, R.I., 1961.

[AO83] H. Appelgate and H. Onishi. Similarity problem over $\mathrm{SL}(n, \mathbf{Z}_p)$. *Proc. Amer. Math. Soc.*, 87(2):233–238, 1983.

[AOPV09] Nir Avni, Uri Onn, Amritanshu Prasad, and Leonid Vaserstein. Similarity classes of 3×3 matrices over a local principal ideal ring. *Comm. Algebra*, 37(8):2601–2615, 2009.

[BBF+06] Anton Betten, Michael Braun, Harald Fripertinger, Adalbert Kerber, Axel Kohnert, and Alfred Wassermann. *Error-correcting linear codes*, volume 18 of *Algorithms and Computation in Mathematics.* Springer-Verlag, Berlin, 2006.

[Coh82] P. M. Cohn. *Algebra. Vol. 1.* John Wiley & Sons Ltd., Chichester, second edition, 1982.

[GAP08] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008.

[Hup67] B. Huppert. *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin, 1967.

[Jac80] Nathan Jacobson. *Basic algebra. II.* W. H. Freeman and Co., San Francisco, Calif., 1980.

[Jam11] Sebastian Jambor. Source files. `http://wwwb.math.rwth-aachen.de/~sebastian`, 2011.

[Nec83] A. A. Nechaev. Similarity of matrices over a commutative local Artinian ring. *Trudy Sem. Petrovsk.*, (9):81–101, 1983.

[Nob77] Alexandre Nobs. Die irreduziblen Darstellungen von $\mathrm{GL}_2(Z_p)$, insbesondere $\mathrm{GL}_2(Z_2)$. *Math. Ann.*, 229(2):113–133, 1977.

[Piz83] Antonio Pizarro. Similarity classes of 3×3 matrices over a discrete valuation ring. *Linear Algebra Appl.*, 54:29–51, 1983.

[Pom73] J. Pomfret. Similarity of matrices over finite rings. *Proc. Amer. Math. Soc.*, 37:421–422, 1973.

[Sin10] Pooja Singla. On representations of general linear groups over principal ideal local rings of length two. *J. Algebra*, 324(9):2543–2563, 2010.