The *MAGMA* Package *CommMatAlg*

Gabor Wiese*

April 13, 2003

Contents

1 Introduction

The *MAGMA* ([2]) package *CommMatAlg* provides various functions on commutative matrix algebras. It was written for the study of Hecke algebras, which are prominent examples coming from the theory of modular forms (see e.g. [4] and [5]).

Before describing the functions of the package, we shall summarize the underlying theory. A good reference is [1]. In a final section, the use of the package is demonstrated in a simple example.

2 Mathematical background

We fix a field k throughout this note. By a *representation* of a k-algebra A we understand a finite dimensional k-vector space V together with a k-algebra homomorphism $\rho : A \to \mathrm{End}_k(V)$. If

*Supported by the European Research Training Network Contract HPRN-CT-2000-00120 "Arithmetic Algebraic Geometry". Address: Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands; `http://www.math.leidenuniv.nl/~gabor/`, e-mail: `gabor@math.leidenuniv.nl`

the homomorphism is injective, the representation is said to be *faithful*. In the sequel, a subalgebra of $\mathrm{End}_k(V)$ will be called a *matrix algebra*. Hence an abstract k-algebra is isomorphic to a matrix algebra if and only if it has a faithful representation, which is the case if and only if A is finite dimensional as a k-vector space.

One can for instance consider the (left) *regular representation*, which is defined as follows. Given an (abstract) commutative Artinian k-algebra A with k-vector space basis $a_1, \ldots, a_n$, we let V be k^n, on which $a \in A$ acts by sending the standard basis vector $e_j = (0, \ldots, 0, 1, 0 \ldots, 0)$ of V to the vector $(c_{j,1}, \ldots, c_{j,n})$ satisfying $aa_j = \sum_{i=1}^n c_{j,i} a_i$.

Another faithful representation is the *dual representation*. We take $V = \mathrm{Hom}_k(A, k) = A^\vee$ and we let $(a.f)(\tilde{a}) = f(a\tilde{a})$ be the action. If we choose the same basis of A as above, the matrix representing a in the dual representation for the dual basis will be the transpose of the matrix for the regular one.

In this note we shall only be concerned with finite dimensional <u>commutative</u> k-algebras, which are assumed to have a 1, unless explicitly stated otherwise, in order to apply the general theory of commutative algebra. This we shall assume for the sequel.

Such a k-algebra A is *Artinian*, i.e. every descending chain of ideals becomes stationary. This is equivalent to the algebra being Noetherian and zero-dimensional. Consequently, all prime ideals are maximal, whence the Jacobson radical equals the nilradical $\mathcal{N}$, which is the set of all nilpotent elements in A. We number the necessarily finitely many maximal ideals of A by $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$. From general arguments we obtain

$$\{\text{ zero-divisors }\} = \bigcup_{i=1}^n \mathfrak{m}_i \quad \text{and} \quad \mathcal{N} = \{\text{ nilpotent el. }\} = \bigcap_{i=1}^n \mathfrak{m}_i.$$

Moreover, the primary decomposition of the zero ideal implies the existence of integers r_i such that $(0) = \mathfrak{m}_1^{r_1} \ldots \mathfrak{m}_n^{r_n}$. Application of the Chinese remainder theorem yields

$$A = A/(0) = A/\mathfrak{m}_1^{r_1} \ldots \mathfrak{m}_n^{r_n} \cong \prod_{i=1}^n A/\mathfrak{m}_i^{r_i} =: \prod_{i=1}^n A_i,$$

where A_i is a local Artinian quotient algebra of A. Equivalently, there exist idempotents $e_i \in A$ such that $A_i = A/(1 - e_i)A$. One also has that A_i is the localisation of A at $\mathfrak{m}_i$.

For every element $a \in A$ we have its *minimal polynomial* $g_a \in k[X]$. Using the theory above we find for an element $a \in A$ the following equivalences

$$a \text{ is a non-unit } \Leftrightarrow a \text{ is a zero-divisor } \Leftrightarrow g_a(0) = 0.$$

In particular, an element a, which is invertible in A, is already a unit in the algebra generated by a. We call an element $a \in A$ *diagonalisable* if the minimal polynomial g_a is a product of pairwise coprime separable irreducible polynomials and *primary* if g_a is the power of an irreducible separable polynomial. The algebra A is said to be *diagonalisable* resp. *primary* if all its elements are.

If k is perfect, we dispose of the *(additive) Jordan decomposition*. It asserts that any element $a \in A$ is uniquely the sum $d + n$ with $d \in A$ diagonalisable and $n \in A$ nilpotent. This result can be derived from the Jordan decomposition over a separable closure by taking Galois invariants.

Lemma 2.1 *A commutative Artinian k-algebra A is local if and only if it is primary.*

Proof. We assume first that A is primary and we let a be a non-unit of A. Hence $g_a(0) = 0$ and consequently $g_a(X) = X^r f(X)$ with $f(0) \neq 0$. As g_a is a power of an irreducible polynomial it can only be equal to X^r, whence a is nilpotent. Consequently, A is local.

Conversely, we have to show that in a local algebra A every element is primary. Since this is trivial for nilpotent elements, let $a \in A$ be a unit and $\overline{a}$ be its image in the k-algebra $A/\mathfrak{m}$, which is a field extension of k. Thus the minimal polynomial $g_{\overline{a}} \in k[X]$ of $\overline{a}$ is irreducible. Moreover we have that $g_{\overline{a}}(a)$ is in the maximal ideal and thus nilpotent. As consequently the minimal polynomial of a divides a power of $g_{\overline{a}}$, the result follows. □

A decomposition of the k-algebra A into a product $\prod_{i=1}^n A_i$ together with a representation $\rho : A \to \mathrm{End}_k(V)$, yields a corresponding decomposition $V = \bigoplus_{i=1}^n V_i$ by putting $V_i := \rho(e_i)V$, where the $e_i \in A$ are the natural idempotents. More precisely, we have the natural homomorphisms $A_i = A/(1-e_i)A \to \mathrm{End}(V_i), a \mapsto \rho(a)|_{V_i}$, which provide a factorisation of ρ:

$$\rho : A \cong \prod_{i=1}^n A_i \to \prod_{i=1}^n \mathrm{End}(V_i) \hookrightarrow \mathrm{End}(V).$$

In other words, after a suitable choice of basis all matrices will be zero except for blocks on the diagonal corresponding to $A_i \to \mathrm{End}(V_i)$.

Such a decomposition of V can for instance be calculated by considering for each maximal ideal $\mathfrak{m}$ the sequence

$$V[\mathfrak{m}] \subset V[\mathfrak{m}^2] \subset \cdots \subset V[\mathfrak{m}^r],$$

where $V[\mathfrak{m}^i]$ is defined to be the subvector space of those $v \in V$ satisfying $\rho(m)v = 0$ for all $m \in \mathfrak{m}^i$. By looking at the natural idempotent $e_i \in A$ corresponding to the maximal ideal $\mathfrak{m} = \mathfrak{m}_i$, one immediately sees that $V_i = \rho(e_i)V$ equals $V[\mathfrak{m}_i^r]$, where r can be chosen as the minimal integer such that the sequence of inclusions above becomes stationary. Explicitly, one has $V_i = \bigcap \mathrm{Ker}(\rho(g))$, where g runs through a set of ideal generators of $\mathfrak{m}_i^r$.

If one chooses a basis of $V[\mathfrak{m}]$, extends it to a basis of $V[\mathfrak{m}^2]$ and so on, one finds that the blocks of the matrices corresponding to $\mathfrak{m}$ are (lower) triangular, provided that $k = A/\mathfrak{m}$ and that k is perfect.

We also note that $V[\mathfrak{m}]$ is the biggest subspace of $V[\mathfrak{m}^r]$, on which A acts diagnonalisably, i.e. if $\overline{\rho} : A \to \mathrm{End}_k(V[\mathfrak{m}])$ denotes the restriction, then $g_{\overline{\rho}(a)}$ is irreducible for all $a \in A$. We shall call $V[\mathfrak{m}]$ the *generalised eigenspace* corresponding to the maximal ideal $\mathfrak{m}$.

A local commutative k-algebra A is said to be *Gorenstein* if the annihilator $\mathfrak{a}$ of the maximal ideal is a simple A-module. This is the case if and only if $\mathfrak{a}$ is a 1-dimensional $A/\mathfrak{m}$-vector space. Accordingly, we define the *Gorenstein defect* of the local algebra to be this dimension minus 1. A commutative algebra is called *Gorenstein* if all its localisations are. Hence we define its *Gorenstein defect* to be the supremum of the Gorenstein defects of the localisations.

The algorithms implemented are easy consequences of the theory outlined above.

3 Documentation of *CommMatAlg*

If `PATH` is the directory in which `CommMatAlg.mg` is stored, type

```
Attach("PATH/CommMatAlg.mg");
```

in order to use the package. We remark that vectors in *MAGMA* are *row vectors*. This convention is adopted below.

3.1 Creation functions

- `intrinsic MatrixAlgebra ( L :: SeqEnum ) -> AlgMat`
  `intrinsic MatrixAlgebra ( L :: SeqEnum, S :: Tup ) -> AlgMat`
  `intrinsic MatrixAlgebra ( A :: AlgMat, S :: Tup ) -> AlgMat`

  Creates the matrix algebra generated by the given data:

  - the (commuting) matrices in the list `L`.
  - the restrictions to the stable subspace `S` (see section on algebra decompositions) of the (commuting) matrices in the list `L`.
  - the restriction to the stable subspace `S` of the matrix algebra `A`.

- `intrinsic Transpose ( A :: AlgMat ) -> AlgMat`

  Given a matrix algebra `A`, this function creates the transposed matrix algebra.

3.2 Algebra decompositions

Let us assume that we have a matrix algebra A of degree d, i.e. $A < \mathrm{End}(k^d)$. A *decomposition* $\prod_{i=1}^n A_i$ of A corresponds to a direct sum $k^d = \bigoplus_{i=1}^n V_i$, where each k-vector space V_i is stabilised by A.

Such a decomposition is represented gives rise to a tuple $\mathtt{T},\mathtt{S}$ as follows. `S` is a tuple `<C,D>`, where $\mathtt{D} = \mathtt{C}^{-1}$ and `C` is the base change matrix from the standard basis to a basis $\{v_{1,1}, \dots, v_{1,n_1}, v_{2,1}, \dots, v_{2,n_2}, \dots, v_{n,1}, \dots, v_{n,n_n}\}$ of V s.t. $\{v_{i,1}, \dots, v_{i,n_i}\}$ is a basis of V_i. `T` is an n-tuple $<< \mathtt{C}_1, \mathtt{D}_1 >, \dots, < \mathtt{C}_n, \mathtt{D}_n >>$ with $\mathtt{C}_i$ resp. $\mathtt{D}_i$ corresponding to the rows of `C` resp. the columns of $\mathtt{C}^{-1}$ belonging to the i-th subspace V_i. In other words, given an element of A considered as a matrix `M` w.r.t. to the standard basis of V, then $\mathtt{C}_i\mathtt{M}\mathtt{D}_i$ is the block of `M` corresponding to the restriction of `M` to V_i. V_i resp. $< \mathtt{C}_i, \mathtt{D}_i >$ are both called *stable subspaces*.

Moreover, $\mathtt{C}_i\mathtt{D}_i$ is the identity matrix of size the dimension of V_i and $\mathtt{D}_i\mathtt{C}_i$ is the idempotent in $\mathrm{End}(V)$ corresponding to V_i in the given decomposition, i.e. V_i is the image of the idempotent $\mathtt{D}_i\mathtt{C}_i$.

We allow also that $\bigoplus_{i=1}^n V_i$ is a proper subspace of k^d. Those may occur in the program for instance as common eigenspaces. Internally, some complement is used in order to make the computations work.

- `intrinsic Idempotents ( D :: Tup ) -> SeqEnum, Tup`

  Given a tuple of stable subspaces $D =<< \mathtt{C}_1, \mathtt{D}_1 >, \ldots, < \mathtt{C}_n, \mathtt{D}_n >>$, this function returns a list of the idempotents corresponding to the subspaces and a tuple $< \mathtt{C}, \mathtt{C}^{-1} >$, where C is the base change matrix from the standard basis to a basis for the sum of the stable subspaces (plus some complement, if necessary).

- `intrinsic CommonLowerTriangular ( A :: AlgMat ) -> Tup,Tup`
  `intrinsic LocalDecomposition ( A :: AlgMat ) -> Tup,Tup`

  Given a matrix algebra A of degree d, which decomposes into n local factors $\prod_{i=1}^{n} A_i$, these two identical functions decompose k^d into $\bigoplus_{i=1}^{n} V_i$ such that A stablilizes each V_i and such that $A_i < \mathrm{End}(V_i)$. More precisely, the decomposition is obtained by for each maximal ideal $\mathfrak{m}_i$ taking a basis of $k^d[\mathfrak{m}_i]$, extending it to a basis of $k^d[\mathfrak{m}_i^2]$ and so on. If the algebra is defined over the field $A/\mathfrak{m}_i$, one obtains by this a basis with respect to which the blocks of the matrices corresponding to $\mathfrak{m}_i$ are lower triangular.

- `intrinsic CommonGeneralizedEigenspaces ( A :: AlgMat ) -> Tup`

  Given a matrix algebra A of degree d, which decomposes into n local factors $\prod_{i=1}^{n} A_i$, this function computes the subspace $\bigoplus_{i=1}^{n} k^d[\mathfrak{m}_i]$ of k^d. The vector space $k^d[\mathfrak{m}_i]$ is called a *generalised eigenspace*. If A is defined over $A/\mathfrak{m}_i$, then $k^d[\mathfrak{m}_i]$ is the simultaneous eigenspace corresponding to $\mathfrak{m}_i$.

- `intrinsic CommonEigenspaces ( A :: AlgMat ) -> Tup`

  Given a matrix algebre A of degree d, this function computes the direct sum of all simultaneous eigenspaces.

- `intrinsic Eigenspaces ( M :: Mtrx ) -> Tup`

  This function is the same as `CommonEigenspaces` for the algebra generated by the matrix M.

- `intrinsic RestrictMatrix ( M :: Mtrx, P :: Tup ) -> Mtrx`

  Given a tuple $\mathtt{P} =< \mathtt{C}, \mathtt{D} >$, calculates the matrix CMD. For instance, P could correspond to a stable subspace.

- `intrinsic RestrictList ( L :: SeqEnum, P :: Tup ) -> SeqEnum`

  Applies the function `RestrictMatrix` to all matrices in the list L.

3.3 Other functions

- `intrinsic JordanDecomposition ( M :: Mtrx ) -> Mtrx, Mtrx`

  Calculates the decomposition $\mathtt{M} = \mathtt{D} + \mathtt{N}$ with D diagonalisable and N nilpotent.

- `intrinsic GorensteinDefect ( A :: AlgMat ) -> RngIntElt`

  Returns the Gorenstein defect of the commutative matrix algebra `A`.

- `intrinsic IsGorenstein ( A :: AlgMat ) -> BoolElt`

  Returns whether the commutative matrix algebra `A` is Gorenstein, that is has Gorenstein defect 0.

- `intrinsic IsLocalAlgebra ( A :: AlgMat ) -> BoolElt`

  Returns whether the algebra `A` is local.

- `intrinsic CommonResidueField ( A :: AlgMat ) -> Any`

  Returns the field generated by the residue fields of the matrix algebra `A`.

- `intrinsic ChangeRingList ( L :: SeqEnum , F :: Rng ) -> SeqEnum`

  Changes the coefficient ring of all the matrices in the list `L` to the ring `F`.

- `intrinsic IdealTorsion ( m :: AlgMat ) -> ModTupFld`

  Given an ideal `m` in a matrix algebra of degree d over a field F, calculate the sub vector space of F^d consisting of those elements killed by every element of `m`.

- `intrinsic UPO ( A :: AlgMat ) -> RngIntElt`

  Computes the unipotency order of the matrix algebra `A`. That is by (my personal) definition the number $\max_{\mathfrak{m} \lhd A \text{ maximal}} \left(\min_{n \geq 0} \left(\mathfrak{m}^n = (0) \right) \right)$.

4 An example session

We assume that the package is stored in the folder `PATH`. First we attach the package:

```
> Attach("PATH/CommMatAlg.mg");
```

We create the full matrix algebra of 4 by 4 matrices over `GF(2)`.

```
> alg := MatrixAlgebra (GF(2),4);
```

Next, we create the following three matrices:

```
> id := alg!1; id;
[1 0 0 0]
[0 1 0 0]
[0 0 1 0]
[0 0 0 1]
> x := alg![1,1,1,1,0,0,0,0,1,1,0,1,0,0,1,0]; x;
[1 1 1 1]
[0 0 0 0]
```

```
[1 1 0 1]
[0 0 1 0]
> y := alg![1,0,1,1,0,0,0,0,1,1,0,1,0,1,1,0]; y;
[1 0 1 1]
[0 0 0 0]
[1 1 0 1]
[0 1 1 0]
```

Now we take the matrix algebra generated by these matrices:

```
> A := MatrixAlgebra([id,x,y]); A;
Matrix Algebra of degree 4 with 3 generators over GF(2)
```

Let us check whether the algebra is commutative.

```
> Centre(A) eq A;
true
```

Its dimension is:

```
> Dimension(A);
4
```

Now we generate its local factors.

```
> L,S := LocalDecomposition(A); #L;
2
```

There are two of them. The first one is just a copy of $\mathbb{F}_2$:

```
> A1 := MatrixAlgebra(A,L[1]); A1;
Matrix Algebra of degree 1 with 3 generators over GF(2)
```

The second is more interesting.

```
> A2 := MatrixAlgebra(A,L[2]); A2;
Matrix Algebra of degree 3 with 3 generators over GF(2)
> Basis(A2);
[
  [1 0 0]
  [0 1 0]
  [0 0 1],

  [0 0 0]
  [0 0 0]
  [1 0 0],

  [0 0 0]
  [0 0 0]
  [0 1 0]
]
```

We see that the algebra consists of lower triangular matrices, as it ought to, since the residue field is the ground field and the algebra was generated by choosing such a basis.

We can also base change the whole algebra to the lower triangular basis:

```
> B := MatrixAlgebra(A,S); Basis(B);
[
    [1 0 0 0]
    [0 0 0 0]
    [0 0 0 0]
    [0 0 0 0],

    [0 0 0 0]
    [0 1 0 0]
    [0 0 1 0]
    [0 0 0 1],

    [0 0 0 0]
    [0 0 0 0]
    [0 0 0 0]
    [0 1 0 0],

    [0 0 0 0]
    [0 0 0 0]
    [0 0 0 0]
    [0 0 1 0]
]
```

References

[1] Atiyah, M. F., Macdonald, I. G.: *Introduction to Commutative Algebra*, Addison-Wesley

[2] Bosma, W., Cannon, J. J., Playoust, C.: *The Magma Algebra System I: The User Language,* J. Symbolic Comput. **24** (1997), pp. 235-265

[3] Edixhoven, S. J.: *Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod* 2 *of weight* 1.

[4] Wiese, G.: *Computing Hecke algebras of weight* 1 *in* MAGMA, Appendix to [3]

[5] Wiese, G.: *The* MAGMA *package* Hecke1, documentation and source are available from the author's homepage