Noncommutative Algebras in MAGMA

https://www.maths.usyd.edu.au/u/don/presentations.html

Don Taylor

The University of Sydney

13 November 2023

Algebras

From the MAGMA Handbook:

In MAGMA a *finitely-presented algebra* (FPA) is a quotient of a free associative algebra by an ideal of relations.

To compute with these ideals of relations, one constructs noncommutative Gröbner bases, which have many parallels with commutative Gröbner bases.

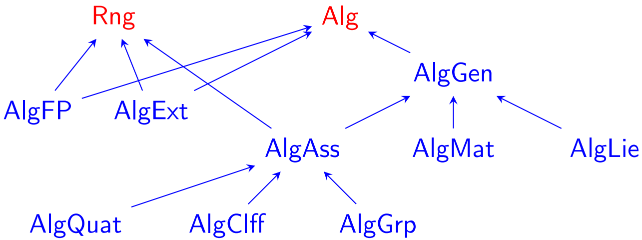
At the heart of the theory is a noncommutative version of the Buchberger algorithm which computes a Gröbner basis of an ideal of an algebra starting from an arbitrary basis (generating set) of the ideal.

One significant difference with the commutative case is that a noncommutative Gröbner basis may not be finite for a finitely-generated ideal.

The type hierarchy: varieties and categories

There are many types of algebras in MAGMA. For example

```
> M := MatrixAlgebra(GF(5),4); Type(M), IsAssociative(M);
 AlgMat true
```




```
> ISA(AlgMat,AlgAss), ISA(AlgClff,AlgAss), ISA(AlgAss,Rng);
 false true true
```

Other types: Heck algebras, universal enveloping algebras (AlgUE), quantized universal enveloping algebras (AlgQUE) and many more.

Clifford Algebras

Quadratic forms and Clifford algebras

Let V be a finite-dimensional vector space over a field $\mathbb{F}$ and let $Q : V \to \mathbb{F}$ be a quadratic form with *polar form* β; i.e., $\beta(u,v) = Q(u+v) - Q(u) - Q(v)$.

The *Clifford algebra* of Q is an $\mathbb{F}$-algebra C with identity $\mathbf{1}$ and a linear map $f : V \to C$ such that

$$f(v)^2 = Q(v)\mathbf{1} \quad \text{for all } v \in V.$$

Then $f(u)f(v) + f(v)f(u) = \beta(u,v)\mathbf{1}$.

For example:

```
> Q := StandardQuadraticForm(4,GF(11));
> C, V, f := CliffordAlgebra(Q);
> Dimension(C), One(C);
16 ( 1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0)
```

The dimension of a Clifford algebra is 2^n, where $n = \dim V$.

Exterior algebras

An *exterior algebra* is the Clifford of a quadratic form that is identically zero. MAGMA returns a *structure constant algebra* of type `AlgClff`.

However, MAGMA's intrinsic `ExteriorAlgebra` returns a quotient of a free algebra and even though `AlgExt` does not inherit from `AlgFP` most of the operations applicable to *finitely presented algebras* can be used. The Gröbner basis machinery applies to algebras of type `AlgExt`.

```
> E<w,x,y,z> := ExteriorAlgebra(GF(11),4);
> I := ideal< E | w*x + y*z >;
> B := quo< E | I>; B;
Affine Algebra of rank 4 over GF(11)
Graded Reverse Lexicographical (exterior algebra) Order
Variables: w, x, y, z
Quotient relations:
[
    w*x + y*z
]
```

Homomorphisms

To construct a homomorphism from an exterior algebra of type `AlgExt` to another algebra we only need to supply the images of the basis elements.

```
> C := CliffordAlgebra( ZeroMatrix(GF(11),4,4) );
> E<w,x,y,z> := ExteriorAlgebra(GF(11),4);
```

The vector space V and the embedding $f : V \to C$ can be obtained as attributes of C; namely `C‘space` and `C‘embedding`.

```
> h := hom< E -> C | [C‘embedding(v) : v in Basis(C‘space)] >;
```

The constructor `hom` returns a linear map but MAGMA makes no attempt to check whether it preserves multiplication. But we can check directly.

```
> forall{ <s,t> : s, t in [w,x,y,z] | h(s*t) eq h(s)*h(t) };
true
```

Clifford algebras of forms in dimension 2

```
> I := IdentityMatrix(Rationals(),2);
> C1<e1,e2>, V1, f1 := CliffordAlgebra(I);
> C2<i,j>, V2, f2 := CliffordAlgebra(-I);
> J := Matrix(Rationals(),[[1,0],[0,-1]]);
> C3<u1,u2>, V3, f3 := CliffordAlgebra(J);
```

C1 is the algebra of 2×2 *matrices* over the rationals.
C2 is the algebra of *quaternions* with rational coefficients.

```
> U := [e1,e1*e2];
> Matrix(2,2,[ (U[s]*U[t] + U[t]*U[s])[1]/2 : s,t in [1,2] ]);
[ 1  0]
[ 0 -1]

> phi := hom< C3 -> C1 | [One(C1),e1,e1*e2,e2 ] >;
> forall<s,t> : s,t in Basis(C3) | phi(s*t) eq phi(s)*phi(t) ;
true
```

Therefore C3 is isomorphic to C1.

Finitely presented algebras

The *free associative algebra* of rank n over a field K is the set of K-linear combinations of noncommutative polynomials in n indeterminates. This is the *tensor algebra* of the vector space K^n.

A *finitely presented algebra* is the quotient of a free algebra by an ideal.

The Clifford algebra `C1` of the previous slide can be constructed as a finitely presented algebra.

```
> F<x1,x2> := FreeAlgebra(Rationals(),2);
> I := ideal< F | x1^2 - 1, x2^2 - 1, x1*x2 + x2*x1 >;
> C<e1,e2> := quo< F | I >;
> Rank(C), Dimension(C), Type(C);
2 4 AlgFP

> f := e1 + 3*e2 + 4 *e1*e2 + 6;
> LeadingTerm(f);
-4*e2*e1
```

Reflections

Suppose that $f : V \to C$ is the Clifford algebra of a quadratic form Q.

If $a \in f(V)$ is invertible, the map $f(V) \to f(V) : b \mapsto -a^{-1}ba$ is the reflection in the hyperplane orthogonal to a.

The reflections generate the orthogonal group of Q.

```
> F<z> := GF(9);
> Q := StandardQuadraticForm(4,F);
> C,V,f := CliffordAlgebra(Q);
> I := IsometryGroup(V);
> a := f(z*V.2 + V.3);
> M := -Matrix([(a^-1*f(b)*a) @@ f : b in Basis(V)]);
> M in I, IsReflection(M);
true
true (   0    z    1    0)    (   0 z^7    1    0)
```

The Clifford Group

The *Clifford group* of the Clifford algebra $f : V \to C$ is

$$\Gamma = \{ s : s \in C \mid s \text{ is invertible and } s^{-1} f(v) s \in f(V) \text{ for all } v \in V \}.$$

The map $\chi : \Gamma \to \mathrm{GL}(V)$ such that $f(v\chi(s)) = s^{-1} f(v) s$ is the *vector representation* of Γ. If $s \in \Gamma \cap f(V)$, then $-\chi(s)$ is a reflection.

If $\dim V$ is even, the image of χ is an orthogonal group (the isometry group of the quadratic space V).

```
> H := sub<GL(4,F)|
>     [VectorAction(f(g)) : g in V | QuadraticNorm(g) in {1,z}] >;
> H eq I;
true
```

Exercise. Suppose that $a, b \in f(V)$ and a is invertible. Show that $a^{-1} b a \in f(V)$.

Exercise. Find the image of χ when $\dim V$ is odd.

The main involution

Let C_+ (resp. C_-) be the subspace spanned by products of an even (resp. odd) number of basis elements. Then C_+ is a subalgebra and $C = C_+ \oplus C_-$.

The *main involution* of C is the linear map $J : C \to C$ such that $J(u) = u$ for $u \in C_+$ and $J(u) = -u$ for $u \in C_-$. It is an automorphism.

```
> J := MainInvolution(C);
> Cplus := EvenSubalgebra(C);
> forall{<u,v> : u,v in Basis(V) |
>     J(f(u)*f(v)) eq J(f(u))*J(f(v))};
```

Exercise. Suppose that $f : V \to C$ is a Clifford algebra over $\mathbb{F}$. Write a MAGMA function `derivation(C,lambda)` that takes a linear functional $\lambda : V \to \mathbb{F}$ and returns a derivation $d : C \to C$ such that $d(f(v)) = \lambda(v)\mathbf{1}$ and $d(xy) = d(x)y + J(x)d(y)$ for all $x, y \in C$.

More exercises

Exercise 1

```
> F := RationalField();
> Q := DiagonalMatrix(F,[1,-2,-5]);
> C,V,f := CliffordAlgebra(Q);
> E, h := EvenSubalgebra(C);
```

Show that E is a generalised quaternion algebra.

Exercise 2

```
> Q := StandardQuadraticForm(4,GF(25));
> C := CliffordAlgebra(Q);
> E := EvenSubalgebra(C);
```

Show that `E` is not simple. Find orthogonal central idempotents that generate its ideals. (Hint. Check out `DirectSumDecomposition`.)

Exercise 3

```
> F<w> := GF(25);
> Q := StandardQuadraticForm(5,F);
> C := CliffordAlgebra(w*Q);
```

Show that `C` is the algebra of 4×4 matrices over the field F_{625}.

The Spin group

The mapping that reverses the multiplication is the *main antiautomorphism* of C; its square is the identity.

The *special Clifford group* is $\Gamma^+ = \Gamma \cap C_+$.

The *spin group* is $\mathrm{Spin}(V,Q) = \{\, s \in \Gamma^+ \mid \alpha(s)s = 1 \,\}$, where α is the main antiautomorphism of C.

Suppose that $s = f(u)$ and $t = f(v)$ where $u, v \in V$ are orthogonal and $Q(u) = 0$. Then $st - 1 \in \mathrm{Spin}(V,Q)$ and $\chi(uv - 1)$ is a Siegel transformation.

```
> s := f(V.1);
> t := f(V.2);
> VectorAction(s*t - One(C)) eq SiegelTransformation(V.1,V.2);
true
```

The Siegel transformations generate the group $\Omega(V,Q)$.

Spin representations

If the dimension of V is even, the Clifford algebra C of Q is simple. A minimal right ideal of C is a *spin representation* and its elements are *spinors*. The minimal right ideals of C_+ are the *half spin* spaces.

The restrictions to the groups Γ, Γ^+ and $\mathrm{Spin}(V, Q)$ are also called spin representations.

```
> F<z> := GF(9);
> Q := StandardQuadraticForm(6,F);
> C,V,f := CliffordAlgebra(Q);
> S := MinimalRightIdeals(C : Limit := 1)[1];
> Dimension(S);
8
> s := f(V.1); t := f(V.2); g := s*t - One(C);
> m := VectorAction(g); n := ActionMatrix(S,g);
> IsUnipotent(m), IsUnipotent(n), IsUnipotent(-n);
true 2
false
true 2
```

$\mathrm{Spin}^+(6,9)$

Collect 6 random Siegel elements of $\mathrm{Spin}^+(6,9)$ and find the group they generate in the spin representation.

```
> X := { };
> for random u in V do
>   if u eq 0 or QuadraticNorm(u) ne 0 then continue; end if;
>   for random v in V do
>     if v ne 0 and DotProduct(u,v) eq 0 then Include(~X,<u,v>);
>       break;
>     end if;
>   end for;
>   if #X ge 6 then break; end if;
> end for;
> H := sub<GL(Dimension(S),F) | [ActionMatrix(S,f(u)*f(v) - One(C))
>        : p in X | true where u,v is Explode(p) ]>;
>   LMGFactoredOrder(H), FactoredOrder(OmegaPlus(6,F));
[ <2, 12>, <3, 12>, <5, 2>, <7, 1>, <13, 1>, <41, 1> ]
[ <2, 11>, <3, 12>, <5, 2>, <7, 1>, <13, 1>, <41, 1> ]
```

Minkowski space

```
> Q := DiagonalMatrix(Rationals(),[1,1,1,-1]);
> C<e1,e2,e3,e4>, V, f := CliffordAlgebra(Q);
> IsSimple(C), Dimension(Centre(C));
true 1
```

C is the central simple algebra of 4×4 matrices over $\mathbb{Q}$.

```
> E, h := EvenSubalgebra(C);
> Z := Centre(E); i := Z.2;
> IsSimple(E), Dimension(E), Dimension(Z), i^2;
true 8 2 (-1  0)
> AsPolynomial(h(i));
e1*e2*e3*e4
```

E is the central simple algebra of 2×2 matrices over $\mathbb{Q}[i]$.

```
> ee := (1/2)*(1 - e1*e4);
> ff := (1/2)*(1 + e1*e4);
> R, r := rideal< E | ee >;
> S, s := rideal< E | ff >;
> Dimension(R), Dimension(S);
4 4
```

Exercise: Pauli matrices

Let `E` be the even subalgebra of the Clifford algebra of the quadratic form `Q` over the rationals with signature $(3,1)$.

```
> Q := DiagonalMatrix(Rationals(),[1,1,1,-1]);
> C<e1,e2,e3,e4>, V, f := CliffordAlgebra(Q);
> E, h := EvenSubalgebra(C);
> Z := Centre(E);
```

Let `R` be the right ideal

```
> R, r := rideal< E | (1/2)*(1 - e1*e4) >;
```

Observe that `Z` is isomorphic to the Gaussian field $\mathbb{Q}[i]$
and that `R` is a vector space of dimension 2 over `Z`. Check that `{-e1*e2*e3*e4+e2*e3, e1*e2-e2*e4}` is a `Z`-basis for `R`.

Identifying `Z` with $\mathbb{Q}[i]$, write a MAGMA function that returns the matrix in $\mathbb{M}_2(\mathbb{Q}[i])$ of an element of `E` acting on `R`.

Show that the matrices of `e4*e3`, `e4*e2` and `e4*e1` are the *Pauli* matrices.

Group Algebras

Representations

The *group algebra* of a finite group G with coefficients from a field (or ring) K is the K-space $K[G]$ of formal sums $\sum_{g\in G} a_g g$ with coefficients $a_g \in K$ and multiplication inherited from G.

Let χ_j $(1 \le j \le m)$ be the irreducible complex characters of G, let $\rho_j : G \to \mathrm{GL}(W_j)$ be a representation corresponding to χ_j and put $n_j = \dim(W_j)$.

Define $\widetilde{\rho}_j : \mathbb{C}[G] \to \mathrm{End}(W_j) : \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g \rho_j(g)$. The family $(\widetilde{\rho}_j)_{1\le j\le m}$ defines the *Fourier transform*

$$\widetilde{\rho} : \mathbb{C}[G] \to \prod_{j=1}^{m} \mathrm{End}(W_j) \simeq \prod_{j=1}^{m} \mathbb{M}_{n_j}(\mathbb{C}).$$

The group algebra $\mathbb{C}[G]$ is semisimple and $\widetilde{\rho}$ is an isomorphism.

Splitting the regular representation

In MAGMA $\mathbb{C}$ is not an 'exact field'. However, the irreducible representations of G can always be written over the field of nth roots of unity, where n is the exponent of G (Richard Brauer).

For example, $\mathbb{Q}[w]$, where $w^3 = 1$ is a splitting field for $\mathrm{Alt}(4)$.

```
> G := AlternatingGroup(4);
> F<w> := CyclotomicField(3 : Sparse);
> A := GroupAlgebra(F,G);
> R, rho := RegularRepresentation(A);
> V := GModule(sub<GL(#G,F) | [rho(G.i) : i in [1..Ngens(G)]]>);
> dsd := DirectSumDecomposition(V);
> [Dimension(X) : X in dsd];
[ 1, 1, 1, 3, 3, 3 ]
> ActionGenerators(dsd[4]);
[
    [-1  0  0]     [ 0  1  1]
    [ 0  0  1]     [ 1  0 -1]
    [ 0  1  0],    [ 0  1  0]
]
```

Fourier inversion

Collect the representations $G \to \mathrm{GL}(W_j)$.

```
> irreps := IrreducibleModules(G,F); // intrinsic
> sigma := [hom< G -> GL(Dimension(W),F) | ActionGenerators(W) >
>    : W in irreps];
```

Let $\widetilde{\rho}_j$ $(1 \le j \le m)$ be the irreducible representations of $F[G]$. Suppose that $U = [u_1, \ldots, u_m]$ where $u_j \in \operatorname{im} \widetilde{\rho}_j$. The following function returns $u \in F[G]$ such that $\widetilde{\rho}_j(u) = u_j$ for all j.

```
> fourierInv := func< A,sigma,U | // A is the group algebra
>    &+[ &+[Nrows(u)*Trace(sigma[i](s^-1)*u) : i -> u in U]*A!s
>       : s in Group(A) ] >;
```

Check.

```
> U := < rho(Random(G)) : rho in sigma >;
> fourierInv(A,sigma,U);
```

```
(-w + 1)*Id(G) + (-w + 1)*(1, 2)(3, 4) + (-w + 1)*(1, 3, 2) + (-w + 1)*(1, 4, 3)
+ (-w + 1)*(2, 3, 4) + (-w + 1)*(1, 2, 4) + (2*w - 2)*(1, 3, 4) + (2*w - 2)*(1, 4, 2)
+ (2*w + 10)*(2, 4, 3) + (2*w - 2)*(1, 2, 3) + (-w + 1)*(1, 3)(2, 4) + (-w + 1)*(1, 4)(2, 3)
```

Matrix Algebras

Groups, modules and algebras

The MAGMA function `PermutationModule(G,H,F)` creates the G-module over the field F from the action of the group G on the cosets of a subgroup H. The function `Action` returns the matrix algebra giving the action on the module. The group itself is returned by `MatrixGroup`.

```
> G := Sym(7);
> H := YoungSubgroup([3,3,1]);
> M := PermutationModule(G,H,GF(2));
> A := Action(M);
> W := MatrixGroup(M);
> Type(W), #W, #G, Index(G,H); A:Minimal;
GrpMat 5040 5040
Matrix Algebra of degree 140 and dimension 2124
       with 2 generators over GF(2)
```

Records

MAGMA is capable of generating a considerable amount of information about an algebra. In many cases the data is returned as a *record* or as a sequence of records. To access the data in a field `xxx` in a record `r`, use `r‘xxx`.

For example, if `A` is the action algebra of the permutation module from the previous example we have

```
> r := AlgebraGenerators(A);
> Names(r);
[ FieldGenerators, PermutationMatrices, PrimitiveIdempotents,
RadicalGenerators,SequenceRadicalGenerators,
GeneratingPolynomialsForCenters, StandardFormConjugationMatrices ]
> #r‘PrimitiveIdempotents;
5
```

This implies that A modulo its Jacobson radical is the direct sum of five simple algebras. We can check this directly.

```
> J := JacobsonRadical(A);
> dd := DirectSumDecomposition(A/J); #dd;
5
```

Simple quotients

There is a faster way to find the decomposition of A and it returns a lot more information.

```
> sq := SimpleQuotientAlgebras(A);
> Names(sq);
[ SimpleQuotients, DegreesOverCenters, DegreesOfCenters,
  OrdersOfCenters ]
> sq`DegreesOverCenters;
[ 20, 14, 8, 6, 1 ]
> sq`DegreesOfCenters;
[ 1, 1, 1, 1, 1 ]
> sq`OrdersOfCenters;
[ 2, 2, 2, 2, 2 ]
```

Generators, idempotents, presentations

Suppose that K is a finite field. The quotient $A/J(A)$ of a K-algebra A by its Jacobson radical is a direct sum of full matrix algebras A_i over extension fields K_i of K.

For each i there is a primitive idempotent e_i such that $e_i A_i e_i \simeq K_i$.

The algebra A_i can be generated by elements b_i and t_i such that $b_i^{n_i} = e_i$ and t_i is conjugate to a permutation matrix of degree n_i, were $n_i = |K_i|$. If $e = \sum_i e_i$, then eAe is the *condensed algebra* of A; it is Morita equivalent to A.

```
> G := Sym(7);
> H := DirectProduct(Sym(3),Sym(3));
> M := PermutationModule(G, G !! H, GF(3));
> A := Action(M);
> pp := PrimitiveIdempotents(A);
> P, J, mu := Presentation(A);
> C := CondensedAlgebra(A);
> #pp, "|", Dimension(A), Degree(A), "|", Dimension(C), Degree(C);
7 | 2319 140 | 30 18
```

Basic Algebras

Definition

From the Chapter 92 (by Jon Carlson) of the Handbook:

A *basic algebra* is a finite dimensional algebra over a field, all of whose simple modules have dimension one.

In the literature such an algebra is known as a “split” basic algebra.

Every algebra is Morita equivalent to a basic algebra, though a field extension may be necessary to obtain the split basic algebra.

MAGMA has several functions that create the basic algebras corresponding to algebras of different types.

The type `AlgBas` in Magma is optimized for the purposes of doing homological calculations.

Example

Continuing the previous example of a permutation module of $\mathrm{Sym}(7)$.

```
> B := BasicAlgebraOfMatrixAlgebra(A);
> B;
Basic algebra of dimension 30 over GF(3)
Number of projective modules: 7
Number of generators: 17
```

Compare this with the condensed algebra.

```
> C := CondensedAlgebra(A);
> C;
Matrix Algebra of degree 18 with 17 generators over GF(3)
> R := JacobsonRadical(C);
> C/R;
Associative Algebra of dimension 7 with base ring GF(3)
> IsCommutative($1);
true
```

Idempotents and projective modules

Suppose A is a finite dimensional algebra over a field F. If $e_1, \ldots, e_s$ are primitive orthogonal idempotents such that $1 = e_1 + \cdots + e_s$, then A is the direct sum of the indecomposable (a.k.a. projective) right A-modules $e_i A$. If A is basic, then $e_i A \simeq e_j A$ iff $i = j$.

Number the e_i so that $e_1 A, \ldots, e_t A$ represent the isomorphism classes of projective indecomposable modules. Then eAe is a basic algebra for A.

```
> P := PermutationGroup(ATLASGroup("2A7"));
> M := PermutationModule(P,Stabiliser(P,1),GF(2));
> A := Action(M);
Matrix Algebra of degree 240 with 2 generators over GF(2)
> C := CondensedAlgebra(A); C;
Matrix Algebra of degree 36 with 15 generators over GF(2)
> CartanMatrix(A);
[3 2 0 0 0 4]
[2 3 0 0 0 4]
[0 0 7 4 4 0]
[0 0 4 4 2 0]
[0 0 4 2 4 0]
[4 4 0 0 0 8]
```

Basic algebras of blocks

Here is an example from Jon Carlson showing that the basic algebra of the *principal* block of the double cover of $\mathrm{Alt}(7)$ is isomorphic to the basic algebra of the *second* block of the double cover of $\mathrm{Alt}(9)$.

```
> A := BasicAlgebraFromGroup("2A7",2,1); A;
Basic algebra of dimension 38 over GF(2)
Number of projective modules: 3
Number of generators: 8
> B := BasicAlgebraFromGroup("2A9",2,2); B;
Basic algebra of dimension 38 over GF(2)
Number of projective modules: 3
Number of generators: 8
> IsIsomorphic(A,B);
true Mapping from: AlgBas: A to AlgBas: B
```