Algebras and Reductive Groups in Magma

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

Don Taylor

The University of Sydney

23 October 2023

Outline

Day 1

- MAGMA overview
- The read-evaluate-print-loop (REPL)
- Interactive programming
  - A simple word game
  - The Catalan numbers
  - Projective planes, graphs, automorphism groups
  - Exploring small groups: the Small Groups Database

Day 2

- The type system and coercion
- Group theory examples
  - Constructing the Hall–Janko group
  - Group algebras and the group determinant
  - Central extensions of symmetric groups

Day 3

- Structure constant algebras
- Lattices, root systems
- Root data, reductive groups

Structure Constant Algebras

Octonions

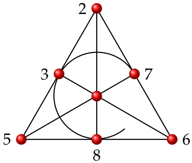
The octonions

Let R be a ring. The (non-associative) algebra $\mathbb{O}(R)$ of *octonions* over R has a basis $1 = e_1, e_2, \ldots, e_8$, such that

$$e_i^2 = -1 \quad \text{for } i \geqslant 2 \text{ and}$$
$$e_i e_j = \pm e_k \quad \text{for } i, j \geqslant 2 \text{ and } i \neq j,$$

where the triples $\{i, j, k\}$ form the lines of a 7-point projective plane on the set $\{2, 3, \ldots, 8\}$. The signs are determined by setting $e_2 e_3 = e_5 = -e_3 e_2$ and using the fact that for $i, j \geqslant 2$ and $i \neq j$, the elements e_i and e_j generate an associative algebra (quaternions) such that $e_i e_j = e_k$ implies $e_{i+1} e_{j+1} = e_{k+1}$ (subscripts modulo 7).

For all things octonion see (1) Conway and Smith. (2003), *On quaternions and octonions: their geometry, arithmetic, and symmetry*. (2) Papers of Robert A. Wilson




```
> fano := {@ <2 + n, 2 + (n+1) mod 7, 2 + (n+3) mod 7> : n in [0..6] @};
```

The octonions in MAGMA

`Algebra< R, n | T >` creates a *structure constant algebra* with a basis $e_1, \ldots, e_n$ satisfying $e_i e_j = \sum_k a_{ij}^k e_k$, where the sequence `T` contains the 4-tuples $\langle i, j, k, a_{ij}^k \rangle$ such that $a_{ij}^k \neq 0$.

The structure constant 4-tuple corresponding to $e_2 e_3 = e_5$ is `<2,3,5,1>` and from this we get five more by applying the symmetric group $\mathrm{Sym}(3)$ to the first three indices, taking account of the sign.

```
> T := [<f[1^g],f[2^g],f[3^g],Sign(g)> : g in Sym(3), f in fano];
```

Next add $e_i^2 = -1$ (for $2 \leqslant i \leqslant 8$), then the relations $e_1 e_i = e_i e_1 = e_i$.

```
> T cat:= [ <i,i,1,-1> : i in [2..8] ];
> T cat:= [ <1,i,i,1> : i in [1..8] ] cat [<i,1,i,1> : i in [2..8] ];
```

The octonions over the ring `R`:

```
> octonions := func< R | Algebra< R, 8 | T > >;
```

Note. MAGMA has an intrinsic `OctonionAlgebra(K,a,b,c)`, where `K` is a field (of odd or zero characteristic) and `a`, `b` and `c` are parameters.

Printing the multiplication table

```
> OZ := octonions(Integers());
> PA<e1,e2,e3,e4,e5,e6,e7,e8> := PolynomialAlgebra(Integers(),8);
> print Matrix(PA,8,8,
>   [&+[Eltseq(OZ.i*OZ.j)[h] * PA.h : h in [1..8]]: i,j in [1..8]]);
```

```
[ e1  e2  e3  e4  e5  e6  e7  e8]
[ e2 -e1  e5  e8 -e3  e7 -e6 -e4]
[ e3 -e5 -e1  e6  e2 -e4  e8 -e7]
[ e4 -e8 -e6 -e1  e7  e3 -e5  e2]
[ e5  e3 -e2 -e7 -e1  e8  e4 -e6]
[ e6 -e7  e4 -e3 -e8 -e1  e2  e5]
[ e7  e6 -e8  e5 -e4 -e2 -e1  e3]
[ e8  e4  e7 -e2  e6 -e5 -e3 -e1]
```

For each line of the Fano plane there is a *quaternion* subalgebra. For example, the quaternion algebra $\mathbb{H}$ of the triple $[2,3,5]$ is the linear span of 1, e_2, e_3 and e_5 and the octonion algebra is $\mathbb{H} \oplus e_8\mathbb{H}$.

Trace, norm and conjugate

The linear span of $e_2, \ldots, e_8$ is the space of *pure* octonions.

If $\xi = ae_1 + \eta$, where a is a scalar, and η is a pure octonion, the *conjugate* of ξ is $\overline{\xi} = ae_1 - \eta$.

The *norm* of ξ is defined by $\xi\overline{\xi} = \overline{\xi}\xi = \mathsf{norm}(\xi)e_1$.
The *trace* of ξ is defined by $\xi + \overline{\xi} = \mathsf{trace}(\xi)e_1$.

Therefore $\xi^2 - \mathsf{trace}(\xi)\xi + \mathsf{norm}(\xi)e_1 = 0.$

```
> conj := func< xi | 2*xi[1]*One(Parent(xi))-xi>;
> norm := func< xi | (xi*conj(xi))[1] >;
> trace := func< xi | 2*xi[1] >;
> F<z1,z2,z3,z4,z5,z6,z7,z8> := FunctionField(Integers(),8);
> OF := octonions(F);
> x := OF![z1,z2,z3,z4,z5,z6,z7,z8];
> norm(x), trace(x), trace(x*OF.3);
z1^2 + z2^2 + z3^2 + z4^2 + z5^2 + z6^2 + z7^2 + z8^2
2*z1
-2*z3
```

Lattices

Root Systems

Lattices

A *lattice* in Magma is a free $\mathbb{Z}$-module contained in $\mathbb{Q}^n$ or $\mathbb{R}^n$, with a positive definite inner product taking values in $\mathbb{Q}$ or $\mathbb{R}$.

A subring of a finite dimensional algebra A over $\mathbb{Q}$ is an *order* if it is a lattice in A and contains a basis of A.

An order is *integral* over $\mathbb{Z}$ (i.e., every element is the root of polynomial with coefficients in $\mathbb{Z}$).

```
> B := Matrix([[1,2,3],[3,2,1]]);
> L := Lattice(B);
> AmbientSpace(L); // returns two objects
Full Vector space of degree 3 over Rational Field
Mapping from: Lat: L to Full Vector space of degree 3 over
                Rational Field given by a rule [no inverse]
> Rank(L);
2
```

Integrality

An element of $\mathbb{O}(\mathbb{Q})$ is *integral* if its trace and norm are integers.

A subring of $\mathbb{O}(\mathbb{Q})$ is an order if its elements are integral; e.g. $\mathbb{O}(\mathbb{Z})$.

There are seven maximal orders in $\mathbb{O}(\mathbb{Q})$ that contain $\mathbb{O}(\mathbb{Z})$; they are pairwise isomorphic.

An order containing $\mathbb{O}(\mathbb{Z})$ is spanned by e_i ($1 \leqslant i \leqslant 8$) and elements of the form $\frac{1}{2}(\pm e_{h_1} \pm e_{h_2} \pm e_{h_3} \pm e_{h_4})$.

Let $\mathbb{O}_{\mathbb{Z}}$ denote the lattice spanned by $\mathbb{O}(\mathbb{Z})$ and $\frac{1}{2}(e_{h_1} + e_{h_2} + e_{h_3} + e_{h_4})$, where $\{h_1, h_2, h_3, h_4\}$ or its complement in $\{1, \ldots, 8\}$ has the form $\{1, i, j, k\}$ and $\{i, j, k\}$ is a line of the Fano plane with 1 and 2 swapped.

```
> X := { Include( {h^pi : h in line}, 2 ) : line in fano }
>   where pi is Sym(8)!(1,2); X;
{1,2,3,5},{1,2,4,8},{1,2,6,7},{1,5,7,8},{1,3,6,8},{1,3,4,7},{1,4,5,6}
```

Conway calls $\mathbb{O}_{\mathbb{Z}}$ the *octavian integers*; it is a maximal order.

A Moufang loop

The units in $\mathbb{O}_Z$ are the elements of norm 1. They form a *Moufang loop* $\mathcal{M}$ of order 240.

```
> X join:= {{1..8} diff x : x in X };
> X := { SetToSequence(x) : x in X };
> OQ := octonions(Rationals());
> B := Basis(OQ);
> M := { a*x : x in B, a in {1,-1} };
> M join:= {(a*B[p[1]]+b*B[p[2]]+c*B[p[3]]+d*B[p[4]])/2 :
>     a,b,c,d in {1,-1}, p in X};
> #M, forall{ <x,y> : x,y in M | x*y in M };
240 true
```

Exercise. Show that the elements of $\mathcal{M}$ satisfy the alternative laws: $(xy)x = x(yx)$, $x(xy) = x^2y$, $(xy)y = xy^2$ but $\mathcal{M}$ is not associative.

Exercise. Show that every element of $\mathcal{M}$ has an inverse.

A root system

The *reflection* r_α in the hyperplane orthogonal to a non-zero vector α in a vector space V with inner product (u, v) is given by

$$vr_\alpha = v - [\![v, \alpha]\!]\alpha \text{ where } [\![v, \alpha]\!] = \frac{2(v, \alpha)}{(\alpha, \alpha)}.$$

In $\mathbb{O}(\mathbb{Q})$ we have $(u, v) = u\bar{v} + v\bar{u}$ and so $vr_\alpha = -\alpha\bar{v}\alpha/\alpha\bar{\alpha}$.

```
> ref := func< a, v | -a*conj(v)*a / norm(a) >;
> refmat := func< a | MatrixRing(BaseRing(P),Dimension(P))!
>                  [ref(a,x) : x in Basis(P)] where P is Parent(a) >;
```

Claim. The Moufang loop $\mathcal{M}$ is a root system. That is

- $0 \notin \mathcal{M}$.
- For all $\alpha \in \mathcal{M}$ the reflection r_α leaves $\mathcal{M}$ invariant.
- For all $\alpha, \beta \in \mathcal{M}$ the *Cartan coefficient* $[\![\alpha, \beta]\!]$ is an integer.

Exercise. Use MAGMA to check the claim.

Simple roots

First find a set of positive roots (i.e., the roots on one side of a hyperplane)

```
> z := 0Q![2^i : i in [1..8]];
> P := {@ v : v in M | InnerProduct(z,v) gt 0 @}; #P;
120
```

A *simple root* is a positive root that is not the sum of positive roots.

```
> S := P diff {@ u+v : u,v in P | u+v in P @};
> for s in S do print s; end for;
(-1/2 -1/2 -1/2    0   1/2    0    0    0)
(   0    0    1    0    0    0    0    0)
(   0    1    0    0    0    0    0    0)
(   1    0    0    0    0    0    0    0)
(   0    0    0 -1/2    0 -1/2 -1/2  1/2)
(   0    0    0    1    0    0    0    0)
(-1/2    0    0 -1/2 -1/2  1/2    0    0)
(   0    0 -1/2    0 -1/2 -1/2  1/2    0)
```

Root systems, Coxeter groups, Dynkin diagrams

The *Cartan matrix* of a root system is $(\llbracket \alpha_i, \alpha_j \rrbracket)$.

```
> V := VectorSpace(OQ);
> SV := ChangeUniverse(S,V);
> C := Matrix(Integers(),8,8,[2*(a,b)/(b,b) : a,b in SV]);
> C; // Cartan matrix
[ 2 -1 -1 -1  0  0  0  0]
[-1  2  0  0  0  0  0 -1]
[-1  0  2  0  0  0  0  0]
[-1  0  0  2  0  0 -1  0]
[ 0  0  0  0  2 -1  0  0]
[ 0  0  0  0 -1  2 -1  0]
[ 0  0  0 -1  0 -1  2  0]
[ 0 -1  0  0  0  0  0  2]
```

The octavian ring $\mathbb{O}_{\mathbb{Z}}$ is the E_8 root lattice.

```
> W := CoxeterGroup(C);
> DynkinDiagram(W);
E8    8 - 2 - 1 - 4 - 7 - 6 - 5
              |
              3
```

The automorphism group of $\mathbb{O}_{\mathbb{Z}}$

$w \in \mathbb{O}_{\mathbb{Z}}$ has order 3 if and only if its norm is 1 and trace is -1.

```
> M3 := [ x : x in M | trace(x) eq -1 ];
> forall{ w : w in M3 | w^3 eq 1 };
true
```

If w has order 3, the map $x \mapsto \overline{w}xw$ is an automorphism of $\mathbb{O}_{\mathbb{Z}}$.

```
> aut := func< a, v | a^3 eq 1 select a^2*v*a else 0 >;
> autmat := func< a | MatrixRing(BaseRing(P),Dimension(P))!
>               [aut(a,x) : x in Basis(P)] where P is Parent(a) >;
> forall <s,t,w> : s,t in S, w in M3 | aut(w,s*t) eq aut(w,s)*aut(w,t);
true
```

```
> reps := [ Rep(Q) : Q in {{x,x^-1} : x in M3}];
> gens := [ autmat(w) : w in reps ];
> G := sub<GL(8,Rationals()) | gens >;
> CompositionFactors(G); #G;
    G
    |  2A(2, 3)                    = U(3, 3)
    1
6048
```

Exercises

Exercise. Show that the elements `gens` are involutions and that `G` can be generated by three of them.

Exercise. Find the orbits of `G` on $\mathcal{M}$ and their lengths.

The map $x \mapsto \overline{x}$ is an anti-automorphism of $\mathbb{O}_{\mathbb{Z}}$; its matrix is

```
> conjmat := MatrixRing(Rationals(),8)![ conj(b) : b in Basis(OQ) ];
> #sub<GL(8,Rationals()) | G, conjmat >;
12096
```

Exercise* Find the full automorphism group of $\mathbb{O}_{\mathbb{Z}}$.

Root Data
Groups of Lie Type

Root data

A reductive group is defined by a *root datum* and a field.

A *root datum* is a 4-tuple $\mathcal{R} = (X, \Phi, Y, \Phi^\star)$ where X and Y are lattices in duality with respect to a pairing $\langle -, - \rangle : X \times Y \to \mathbb{Z}$, and $\Phi \subset X$ and $\Phi^\star \subset Y$ are root systems with a bijection $\Phi \to \Phi^\star : \alpha \mapsto \alpha^\star$ such that $\langle \alpha, \alpha^\star \rangle = 2$. For $\alpha \in \Phi$, the *reflections*

$$s_\alpha : X \to X : x \mapsto x - \langle x, \alpha^\star \rangle \alpha \quad \text{and}$$
$$s_\alpha^\star : Y \to Y : y \mapsto y - \langle \alpha, y \rangle \alpha^\star$$

satisfy $\Phi s_\alpha = \Phi$ and $\Phi^\star s_\alpha^\star = \Phi^\star$.

The *Weyl group* of $\mathcal{R}$ is $\langle s_\alpha \mid \alpha \in \Phi \rangle$.

The root datum is completely determined by its *simple roots* and *simple coroots*.

```
> RD := RootDatum("E7" : Isogeny := "SC"); RD;
RD: Simply connected root datum of dimension 7 of type E7
```

Simple roots, Cartan matrices, isogeny

Let $e_1, e_2, \ldots, e_d$ be a basis for X, let $f_1, f_2, \ldots, f_d$ be the dual basis for Y and use these bases to identify X and Y with the standard lattice $\mathbb{Z}^d$.

Choose a base of simple roots $\alpha_1, \ldots, \alpha_\ell$ for Φ.
Then $\alpha_i = \sum_{j=1}^d a_{ij} e_j$ and $\alpha_i^\star = \sum_{j=1}^d b_{ij} f_j$ and $C = \langle \alpha_i, \alpha_j^\star \rangle = AB^\top$, where $A = (a_{ij})$ and $B = (b_{ij})$.

Conversely, a pair of $\ell \times d$ matrices A and B such that $AB^\top$ is a Cartan matrix determines a root datum $\mathcal{R}$. The rows of A are the simple roots and the rows of B are the corresponding coroots.

The *semisimple rank* of $\mathcal{R}$ is ℓ, the number of simple roots; the *reductive rank* is d, the rank d of X.

Isogeny: the root datum is *semisimple* if $\ell = d$; it is *adjoint* if $X = \mathbb{Z}\Phi$; it is *simply connected* if $Y = \mathbb{Z}\Phi^\star$.

Adjoint and simply connected root data are necessarily semisimple.

A Magma example

```
> RD := RootDatum("G2");
> A := SimpleRoots(RD); A;
[1 0]
[0 1]
> B := SimpleCoroots(RD); B;
[ 2 -3]
[-1  2]
> CartanMatrix(RD) eq A*Transpose(B);
true
> RD eq RootDatum(A,B);
true
```

Exercise. Find all semisimple root data (up to isomorphism) of type A_3. (Hint: Let C be a Cartan matrix of type A_3 and consider factorisations $C = AB^\top$.)

Groups of Lie type

Suppose that RD is a root datum $(X, \Phi, Y, \Phi^\star)$

If A is a ring, GroupOfLieType(RD,A) creates a group of *Lie type*.

The generators are *root elements* $x_\alpha(a)$ and *torus elements* $y \otimes t$, where $\alpha \in \Phi$, $a \in A$, $y \in Y$ and $t \in A$ ($t \neq 0$).

```
> RD := RootDatum("G2");
> F := GaloisField(5);
> G := GroupOfLieType(RD,F);
> Random(G);
x2(2) x3(2) x6(1) x4(4) x5(3) x1(3)
(2 1)
n1 n2 n1 n2 n1
x3(2) x6(3) x4(3) x5(3) x1(1)
```

$(2, 1)$ is the torus element $(f_1 \otimes 2)(f_2 \otimes 1)$; `elt<G | Vector(F,[2,1])>`.

`n1 n2 n1 n2 n1` is the Weyl group element corresponding to the product of reflections $s_{\alpha_1}s_{\alpha_2}s_{\alpha_1}s_{\alpha_2}s_{\alpha_1}$; `elt<G | 1,2,1,2,1 >`.

Highest weight representations

The *weight lattice* is $\Lambda = \{ x \in \mathbb{Q}\Phi \mid \langle x, \alpha^\star \rangle \in \mathbb{Z} \text{ for all } \alpha \in \Phi \}$. It has a basis $\varpi_1, \dots, \varpi_\ell$ of fundamental weights dual to the simple coroots. A weight $\lambda \in \Lambda$ is *dominant* if $\langle \lambda, \alpha^\star \rangle \geqslant 0$ for all simple roots α; i.e., a non-negative linear combination of the fundamental weights.

Let L be a finite-dimensional rational $\mathbf{G}$-module, where $\mathbf{G}$ is a reductive group. Then $L = \bigoplus_\lambda L_{\lambda \in \Lambda}$, where

$$L_\lambda = \{ v \in L \mid v(y \otimes t) = t^{\langle \lambda, y \rangle} v \;\text{ for all } y \in Y, t \in K^\times \}$$

and λ is a *weight of* L if $L_\lambda \neq 0$. If $\mathbf{G}$ is semisimple and λ is a dominant weight, there is an irreducible $\mathbf{G}$-module whose *highest weight* is λ. The restriction to a finite group of Lie type need not be irreducible.

```
> G := GroupOfLieType(RD,GF(3));
> rho := HighestWeightRepresentation(G,[3,0]); rho;
Mapping from: GrpLie: G to GL(77, GF(3)) given by a rule [no inverse]
> IsIrreducible(Image(rho));
false
```

Symbolic computation

```
> RD := RootDatum("G2" : Isogeny := "SC");
```

If t is a field element, the MAGMA code for $x_{\alpha_i}(t)$, where α_i is the ith root in the group `G` of Lie type is `elt<G | <i,t> >`.

Using the function field (i.e., the ring of fractions of the polynomial ring) of the finite field $\mathbb{F}_5$ we can carry out symbolic calculations.

```
> FF<w,z> := FunctionField(GF(5),2);
> G := GroupOfLieType(RD,FF);
> elt<G| <1,w» * elt<G|<2,z»;
x2(z) x3(w*z) x6(w^3*z^2) x4(w^2*z) x5(w^3*z) x1(w)
> std := StandardRepresentation(G); std(TorusTerm(G,3,z));
[    z     0     0     0     0     0     0]
[    0   z^2     0     0     0     0     0]
[    0     0   1/z     0     0     0     0]
[    0     0     0     1     0     0     0]
[    0     0     0     0     z     0     0]
[    0     0     0     0     0 1/z^2     0]
[    0     0     0     0     0     0   1/z]
```

Application: constructive recognition

Given a matrix group H with generators Y, construct an isomorphism between H and a 'standard copy'. Use this this to write an arbitrary element of H as a *straight-line program* (SLP) in Y.

If we know that H is a homomorphic image of a simply connected finite group of Lie type $G(q)$ we can do the following.

- Identify the Lie type of H.
- Use the Liebeck–O'Brien algorithm to construct a Curtis–Steinberg–Tits (CST) presentation for H.
- Construct a homomorphism $\rho : G(q) \to H$ using the CST generators of $G(q)$.
- Construct $\varphi : H \to G(q)$ such that $\rho(\varphi(h)) = h$. For $h \in H$, $\varphi(h)$ will be a word in the Steinberg generators of $G(q)$.

Recognising $\mathrm{Aut}(\mathbb{O}(q))$

Let C be the algebra of octonions over the finite field $\mathbb{F}_q$ of q elements and suppose that q is odd. We shall construct $A = \mathrm{Aut}(C)$ as a matrix group and then find an explicit isomorphism with a group of Lie type defined by Chevalley–Steinberg generators.

```
> q := 5;
> C := octonions(GF(q));
```

In order to proceed we need some automorphisms.

An *orthogonal pair* is an ordered pair (a, b) of elements of norm 1 in C such that a and b are orthogonal to 1 and to each other. Equivalently, (a, b) is an orthogonal pair if $a^2 = b^2 = -1$ and $ab = -ba$. Thus the linear span of 1, a, b and ab is a 'quaternion algebra'.

Theorem. *The automorphism group of C acts transitively on the set of orthogonal pairs.*

For a proof, see the function on the next slide.

Transitivity on orthogonal pairs

Given orthogonal pairs `p1` and `p2`, the following function returns the matrix of an automorphism of $\mathbb{O}(q)$ transforming `p1` to `p2`.

```
> orthogPairAut := function(p1,p2)
>   a1, b1 := Explode(p1);
>   a2, b2 := Explode(p2);
>   C := Parent(a1);
>   V := VectorSpace(C);
>   B1 := [V| One(C), a1, b1, a1*b1 ];
>   B1perp := OrthogonalComplement(V,sub<V|B1>);
>   assert exists(c1){ c : v in B1perp | norm(c) ne 0 where c is C!v};
>   mu := norm(c1);
>   B1 cat:= [V| c1, c1*a1, c1*b1, c1*(a1*b1) ];
>   B2 := [V| One(C), a2, b2, a2*b2 ];
>   B2perp := OrthogonalComplement(V,sub<V|B2>);
>   assert exists(c2){ d : v in B2perp | norm(d) eq mu where d is C!v};
>   B2 cat:= [V| c2, c2*a2, c2*b2, c2*(a2*b2) ];
>   return Matrix(B1)^-1*Matrix(B2);
> end function;
```

Warning! No error checking.

Another version of `orthogPairAut`

```
> orthogPairAut2 := function(p1,p2)
>   extendBasis := function(p : lambda := 0) // local function
>     a, b := Explode(p);
>     assert a^2 eq -1 and b^2 eq -1 and a*b eq -b*a; // error check
>     C := Parent(a);
>     V := VectorSpace(C);
>     B := [V| One(C), a, b, a*b];
>     Bperp := OrthogonalComplement(V,sub<V|B>);
>     c := (lambda eq 0) select rep{c : v in Bperp | norm(c) ne 0
>           where c is C!v}
>       else rep{c : v in Bperp | norm(c) eq lambda where c is C!v};
>     return B cat [V| c*C!x : x in B], norm(c);
>   end function;
>   B1, lambda := extendBasis(p1);
>   B2, _ := extendBasis(p2 : lambda := lambda);
>   return Matrix(B1)^-1*Matrix(B2);
> end function;
```

$\mathbb{O}(q) = \mathbb{B} \oplus c\mathbb{B}$ where $\mathbb{B}$ is the quaternion algebra.

Automorphisms

The lines of the Fano plane provide a supply of orthogonal pairs.

```
> p1 := <C.2,C.3>;
> auts := [orthogPairAut(p1,<C.i,C.j>) : pp in fano[2..7] |
>           true where i,j is Explode(pp)];
> L := sub< GL(8,q) | auts >; #L;
1344
```

Not quite large enough. Let's find another automorphism.

```
> a := &+[C.i : i in [3..8]];
> b := C![0,0,3,2,3,0,2,0];
> a^2 eq -1, b^2 eq -1, a*b + b*a eq 0;
true true true
> g := orthogPairAut(p1,<a,b>);
> A := sub<GL(8,q) | L, g >;
> LieType(A,5);
true <"G", 2, 5>
```

Exercise. Use MAGMA to find `b` (or equivalent).

The group $G_2(q)$

```
> G := GroupOfLieType("G2",q : Isogeny := "SC");
> flag, _, _, _, _, X, _ :=
>                   ExceptionalConstructiveRecognition(A,"G",2,5);
> rho := Morphism(G,X[1],X[2] : GS);
> rho(elt<G|<1,2»);
[1 0 0 0 0 0 0 0]
[0 4 3 0 3 3 2 2]
[0 1 4 4 3 2 4 3]
[0 4 2 4 3 4 2 4]
[0 2 2 2 1 0 2 2]
[0 3 2 0 0 4 1 4]
[0 4 0 2 3 0 4 1]
[0 3 2 1 3 1 4 1]
> f := Inverse(rho);
> f(A.1);
x2(1) x3(2) x6(3) x5(3) n2 n1 n2 n1 n2 x2(4) x3(3) x5(2)
```

Miscellaneous properties of $\mathrm{Aut}(\mathbb{O}(q))$

```
> FactoredOrder(A);
[ <2, 6>, <3, 3>, <5, 6>, <7, 1>, <31, 1> ]
> M := GModule(A);
> DirectSumDecomposition(M);
[
    GModule of dimension 1 over GF(5),
    GModule of dimension 7 over GF(5)
]
```

Borel subgroup

```
> bgens := [ elt<G| <1,1» ,elt<G|<2,1» ];
> borel := sub<A | [rho(x) : x in bgens] >;
> FactoredOrder(borel);
[ <5, 6> ]
```

Torus

```
> tgens := [TorusTerm(G,i,2) : i in [1,2]];
> torus := sub< A | [rho(x) : x in tgens] >;
> FactoredOrder(torus);
[ <2, 4> ]
```

The stabiliser of a vector

MAGMA cannot compute the stabiliser of `C.2` directly nor can `C.2` be coerced directly into the module `M`. Instead, we do the following.

```
> A1 := Stabiliser(A,Vector(C.2));
> CompositionFactors(A1);
    G
    |  A(2, 5)                          = L(3, 5)
    1
```

The group `A1` $\simeq \mathrm{PSL}(3,5)$ is not maximal. It has index 2 in its normaliser.

```
> N1 := Normaliser(A,A1);
> Index(N1,A1);
2
```

However, `N1` is maximal because the action of `A` on the cosets of `N1` is primitive.

```
> B := CosetImage(A,N1);
> IsPrimitive(B);
true
```

Links

Magma Resources

The Magma Handbook
http://magma.maths.usyd.edu.au/magma/handbook/

Literate Magma programming
https://www.maths.usyd.edu.au/u/don/code/Magma/magmatex.html

Magma package examples
https://www.maths.usyd.edu.au/u/don/software.html

Editing utilities
http://magma.maths.usyd.edu.au/magma/extra/

User-defined types. An example
https://www.maths.usyd.edu.au/u/don/code/Magma/Nearfields.pdf