The University of Sydney
School of Mathematics and Statistics

# Solutions to Algebras and Reductive Groups in Magma

MagmaMondays: 23 October 2023 — Semester 2, 2023

Web Page: `https://sites.google.com/view/magma-mondays/`
Lecturer: Don Taylor

**1.** Recall from the lecture that the octonions over a ring $R$ have a basis $e_1$, $e_2$, $\ldots$, $e_8$ such that $e_i^2 = 1$ (for $i \geq 2$) and $e_i e_j = \varepsilon(i, j, k) e_k$ for a choice of signs $\varepsilon(i, j, k) = \pm 1$ where $\{i, j, k\}$ belongs to

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

Let $A = \mathbb{O}(\mathbb{Q})$ denote the algebra of octonions over the rational field $\mathbb{Q}$,

(a) Let $a$ be the matrix corresponding to the permutation $(2, 3, 4, 5, 6, 7, 8)$. Show that $a$ is an automorphism of $A$ that permutes the vectors $\pm e_i$.

**Hint:** PermutationMatrix( . . . )

***Solution:*** First construct the octonions as a structure constant algebra as in the lecture.

```
T := [<f[1^g],f[2^g],f[3^g],Sign(g)> : g in Sym(3), f in fano];
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] ];
octonions := func< R | Algebra< R, 8 | T > >;
A := octonions(Rationals());
```

Convert the permutation to a permutation matrix over the rationals.

```
a := PermutationMatrix(Rationals(),Sym(8) ! (2,3,4,5,6,7,8));
```

Check that $a$ preserves multiplication of basis elements.

```
B := Basis(A);
forall{<u,v> : u,v in B | (u*v)*a eq (u*a)*(v*a) };
```

```
true
```

```
BB := B cat [-v : v in B];
forall{e : e in BB | e*a in BB };
```

(b) Let $b_0$ be the permutation $(2, 7)(3, 4)$. Show that $b_0$ is an automorphism of the 7-point plane defined by *fano*. Then find a diagonal matrix $d = \operatorname{diag}(\pm 1, \pm 1, \ldots, \pm 1)$ such that $db$ is an automorphism of $A$ that permutes the vectors $\pm e_i$, where $b$ is the permutation matrix of $b_0$.

***Solution:*** First change the 'lines' of the 7-point plane to 3-element sets instead of triples.

```
sfano := {@{2 + n, 2 + (n+1) mod 7, 2 + (n+3) mod 7} : n in [0..6]@};
b0 := Sym(8) ! (2,7)(3,4);
```

Check that $b_0$ preserves the lines.

```
forall{ln : ln in sfano | ln^b0 in sfano };
```

```
true
```

To find the diagonal matrix, define a function *isAuto*$(A, g)$ to check whether a matrix $g$ is an automorphism of $A$.

```
isAuto := func< A, g |
    forall{<u,v> : u,v in Basis(A) | (u*v)*g eq (u*g)*(v*g) } >;
```

Convert *b* to a permutation matrix.

```
b := PermutationMatrix(Rationals(), b0);
```

A moments thought shows that we only need to find the signs at positions 2, 3, 4 and 7.

```
for s2, s3, s4, s7 in [1, -1] do
    d0 := DiagonalMatrix(Rationals(), [1, s2, s3, s4, 1, 1, s7, 1]);
    if isAuto(A, d0*b) then s2, s3, s4, s7; d := d0; end if;
end for;
```

```
1 1 -1 -1
-1 -1 1 1
```

(c) Let $G$ be the subgroup of $\mathrm{GL}(8,\mathbb{Q})$ generated by the matrices $a$ and $db$. Show that the order of $G$ is 1 344 and that $G$ has a normal abelian subgroup $E$ of order 8 such that the quotient $G/E$ is isomorphic to $\mathrm{SL}(3,2)$. Furthermore, this extension is *non-split*; that is, there is no subgroup of $G$ isomorphic to $\mathrm{SL}(3,2)$.

***Solution:*** Using the matrix *d* found in the previous part of this exercise we have

```
G := sub<GL(8, Rationals()) | a, d*b >;
#G;
```

```
1344
```

```
E := pCore(G, 2);
#E;
```

```
8
```

```
S := quo< G | E >;
check := IsIsomorphic(S, SL(3,2)); check;
```

```
true
```

Use the second cohomology group to find the type of the extension.

```
S32 := SL(3,2);
V := GModule(S32);
CM := CohomologyModule(S32, V);
H2 := CohomologyGroup(CM, 2);
H2;
```

```
Full Vector space of degree 1 over GF(2)
```

```
extn1 := Extension(CM, H2 ! [0]);
extn2 := Extension(CM, H2 ! [1]);
```

Convert from GrpFP to a permutation group so that we can use IsIsomorphic.

```
perm1 := CosetImage(extn1, sub<extn1|>);
ok := IsIsomorphic(perm1, AGL(3,2)); ok;
```

```
true
```

```
perm2 := CosetImage(extn2, sub<extn2|>);
ok := IsIsomorphic(perm2, G);
```

```
true
```

**2.** Let $\mathcal{M}$ be the set of elements of norm 1 in the integral octonions.

(a) 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.

***Solution:*** Recall that the ring of integral octonions is a maximal order in the algebra $A$ of octonions over the rationals.

```
X := { Include( {h^π : h in line}, 2 ) : line in fano }
                    where π is Sym(8) ! (1,2); X;
X join:= {{1..8} diff x : x in X };
```

Change the elements of $X$ to sequences.

```
X := { SetSeq(x) : x in X };
```

Define the Moufang loop $\mathcal{M}$.

```
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};
```

Check the alternative laws:

```
forall{<x,y> :x,y in M | (x*y)*x eq x*(y*x) and x*(x*y) eq x^2*y
     and (x*y)*y eq x*y^2 };
```

```
true
```

Check non-associativity:

```
exists{ <x,y,z> : x,y,z in M | (x*y)*z ne x*(y*z) };
```

```
true
```

(b) Show that every element of $\mathcal{M}$ has an inverse.

***Solution:***

```
conj := func< ξ | 2*ξ[1]*Parent(ξ) ! 1-ξ>;
forall{ x : x in M | x*conj(x) eq 1 };
```

```
true
```

(c) The *reflection* $r_\alpha$ in the hyperplane orthogonal to $\alpha$ is

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

In $\mathbb{O}(\mathbb{Q})$ we have $(u,v) = u\overline{v} + v\overline{u}$ and so for $\alpha \in \mathcal{M}$ we have $vr_\alpha = -\alpha\overline{v}\alpha$.

```
norm := func< ξ | (ξ*conj(ξ))[1] >;
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) >;
```

Use Magma to check that $\mathcal{M}$ is a root system. That is,

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

***Solution:***

```
0 notin M,
forall{<a,b> : a,b in M | ref(a,b) in M },
{ (u*conj(v) + v*conj(u))[1] : u,v in M };
```

```
true true {-2, -1, 0, 1, 2 }
```

**3.** If $w$ has order 3, the map $x \mapsto \overline{w}xw$ is an automorphism of $\mathbb{O}_{\mathbb{Z}}$. The matrix of this automorphism is *automat*($w$), where

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

Let *gens* be the set of all automorphisms of $\mathbb{O}_{\mathbb{Z}}$ constructed from the elements of order 3 in $\mathcal{M}$ and let $G$ be the group they generate.

(a) Show that the elements of *gens* are involutions and that $G$ can be generated by three of them.

***Solution:***

```
trace := func< ξ | 2*ξ[1] >;
M3 := [ x : x in M | trace(x) eq -1 ];
reps := [ Rep(Q) : Q in {{x, x^-1} : x in M3}];
gens := [ automat(w) : w in reps ];
{ Order(g) : g in gens };
```

```
{ 3 }
```

```
G := sub<GL(8, Rationals()) | gens >;
exists{ g : g in gens | G eq sub< G | gens[1], gens[2], g > };
```

```
true
```

(b) Find the orbits of $G$ on $\mathcal{M}$ and their lengths.

***Solution:*** The elements of $G$ act on the underlying vector space of the algebra $A$ of rational quaternions. First check that the elements of order 3 form a single orbit as do the elements of order 6.

```
V := VectorSpace(A);
#M3;
```

```
56
```

```
ω := Rep(M3);
orb3 := { ω * g : g in G };
orb6 := { -g : g in orb3 };
#orb3, #orb6, orb3 eq orb6;
```

```
56 56 false
```

Similarly the elements of order 4 form a single orbit.

```
M4 := [ x : x in M | x^2 eq -1 ];
i := Rep(M4);
orb4 := { i * g : g in G };
#orb4, Set(orb4) eq Set(M4);
```

```
126 true
```

Since $G$ fixes 1 and $-1$ this accounts for all the elements of $\mathcal{M}$.

(c) Show that the set $M_4$ of elements of order 4 in $\mathcal{M}$ is a root system of type $E_7$.

***Solution:*** Since $M_4$ is a subset of $M$, which is a root system of type $E_8$, in order to check that it is a root system it is enough to show that for all $a, b$ in $M_4$ we have $ar_b \in M_4$ where $r_b$ denotes the reflection.

```
forall{ <a,b> : a, b in M4 | ref(a, b) in M4 };
```

```
true
```

Find positive roots and simple roots using the code from the lecture.

```
z := A ! [2^i : i in [1..8]];
P := {@ v : v in M4 | InnerProduct(z, v) gt 0 @};
S := P diff {@ u+v : u, v in P | u+v in P @};
ChangeUniverse(~S, V);
C := Matrix(Integers(), #S, #S, [2*(a, b)/(b, b) : a, b in S]);
DynkinDiagram(C);
```

```
E7    5 - 6 - 3 - 1 - 7 - 4
              |
              2
```

(d) Let $i$ be an element of $M_4$ and let $G_0$ be its stabiliser in $G$. Find the lengths of the orbits of $G_0$ on $M_4$.

***Solution:*** Using the element $i$ in $M_4$ from above:

```
G0 := Stabiliser(G, V ! i);
orbs := [];
while &+[Integers()| #oo : oo in orbs ] lt #M4 do
    j := rep{ v : v in M4 | v notin &join orbs };
    Append(~orbs, { j*g : g in G0 });
end while;
[#oo : oo in orbs ];
```

```
[ 48, 12, 16, 16, 16, 16, 1, 1 ]
```

**4.** 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 $C = AB^\top$.)

***Solution:***

```
C3 := CartanMatrix("A3");
I3 := IdentityMatrix(Integers(), 3);
A3 := Matrix([[1, 0, 0], [0, 1, 0], [1, 0, 2]]);
B3 := Matrix([[2, −1, −1], [−1, 2, 0], [0, −1, 1]]);
C3; A3*Transpose(B3) eq C3;
```

```
[ 2 -1  0]
[-1  2 -1]
[ 0 -1  2]
true
```

```
R1 := RootDatum(I3, C3);
R2 := RootDatum(C3, I3);
R3 := RootDatum(A3, B3);
IsIsomorphic(R1, R2), IsIsomorphic(R2, R3), IsIsomorphic(R1, R3);
```

```
false false false
```

**5.** The MAGMA code

```
P<x> := PolynomialRing(Rationals());
F<τ> := NumberField(x^2 − x −1);
```

creates the field $F$ generated over the rationals by the element $\tau$ such that $\tau^2 = \tau + 1$. Then the code

```
H<i,j,k> := QuaternionAlgebra< F | −1, −1 >;
```

creates the algebra of quaternions over $F$ with basis 1, $i$, $j$, $k$ such that

$$i^2 = j^2 = k^2 = ijk = -1.$$

Let

```
π := (1/2)*(−1 + i + j + k);
σ := (1/2)*(τ^−1 +i +τ*j);
X := {H ! 1, π, σ};
```

and let $I$ be the smallest multiplicatively closed subset of $H$ containing $X$.

(a) Show that $I$ is isomorphic to $\mathrm{SL}(2,5)$.

***Solution:***

```
Π := Matrix(F, 4, 4, [ Eltseq(b*π) : b in Basis(H) ]);
Σ := Matrix(F, 4, 4, [ Eltseq(b*σ) : b in Basis(H) ]);
S, f := sub< GL(4, F) | Π, Σ >;
I := { H ! f(g)[1] : g in S };
X subset I and forall{ <x, y> : x, y in I | x*y in I};
```

```
true
```

```
bool, _ := IsIsomorphic(S, SL(2, 5)); bool;
```

```
true
```

(b) Show that $I$ is a root system (when considered as a subset of $H$). What is its Cartan type?

***Solution:***

```
S := [π, −σ];
Append(~S, rep{ s : s in I | InnerProduct(s, S[1]) eq 0 and
      2*InnerProduct(s, S[2]) eq −1 });
Append(~S, rep{ s : s in I | InnerProduct(s, S[1]) eq 0 and
      InnerProduct(s, S[2]) eq 0 and 2*InnerProduct(s, S[3]) eq −τ });
CartanName( Matrix(F, 4, 4, [2*InnerProduct(s, t) : s, t in S]) );
```

```
H4
```

**6.** Let $p$ be a prime and let $S$ be the simply connected group of Lie type $A$ and rank 1 over the finite field of $p$ elements. For $p = 2, 3, 5$ find the dimensions of the highest weight representations of $S$ (as computed by Magma)?

***Solution:***

```
for p in [2, 3, 5] do
    S := GroupOfLieType("A1", GF(p) : Isogeny := "SC");
    [Dimension(Codomain(HighestWeightRepresentation(S, [n]))) : n in [1..2*p+1]];
end for;
```

```
[ 2, 3, 4, 5, 6 ]
[ 2, 3, 4, 5, 6, 7, 8 ]
[ 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 ]
```