Descendants of algebra 5.1 of order p^7

Michael Vaughan-Lee

July 2013

The following occurs in computing the immediate descendants of order p^7 of algebra 5.1. There are 6 commutator structures possible with L^2 having order p^2, and this problem arises in Case 6, with $pL = L^2$. Here $pa = pd = 0$, and we write

$$\begin{pmatrix} pb \\ pc \\ pe \end{pmatrix} = A \begin{pmatrix} ba \\ ca \end{pmatrix}$$

for a 3×2 matrix A. We consider the orbits of matrices

$$A = \begin{pmatrix} u & v \\ t & x \\ y & z \end{pmatrix}$$

where $(tz - xy)^2 - (ux - vt)(uz - vy)$ is not a square under the action of non-singular matrices $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ given by

$$\begin{pmatrix} u & v \\ t & x \\ y & z \end{pmatrix} \to (ad-bc)^{-2} \begin{pmatrix} (ad+bc) & 2bd & -2ac \\ cd & d^2 & -c^2 \\ -ab & -b^2 & a^2 \end{pmatrix} \begin{pmatrix} u & v \\ t & x \\ y & z \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Each such orbit contains a matrix with $u = 0$ and $v = 1$, and we pick one matrix of this form out of each orbit, giving k algebras

$$\langle a, b, c, d, e \mid da, ea, cb, db-ca, eb, dc, ec, ed-ba, pa, pb-ca, pc-tba-xca, pd, pe-yba-zca, \text{ class } 2\rangle,$$

where $k = 4$ when $p = 3$, $k = (p^2 - 1)/2$ when $p = 1 \bmod 3$, and $k = (p^2 + 1)/2$ when $p = 2 \bmod 3$.

First we consider the action of four particular matrices $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$: $\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$, $\begin{pmatrix} 0 & c \\ b & 0 \end{pmatrix}$. These four matrices transform $\begin{pmatrix} u & v \\ t & x \\ y & z \end{pmatrix}$ into

$$\begin{pmatrix} u + 2tb & v + 2xb - b\,(u + 2tb) \\ t & x - tb \\ -tb^2 - ub + y & z - vb - xb^2 + b\,(tb^2 + ub - y) \end{pmatrix}, \tag{1}$$

$$\begin{pmatrix} u-2yc-c\,(v-2zc) & v-2zc \\ t+uc-c\,(-zc^2+vc+x)-yc^2 & -zc^2+vc+x \\ y-zc & z \end{pmatrix}, \tag{2}$$

$$\begin{pmatrix} \frac{u}{a} & \frac{v}{d} \\ \frac{t}{a^2}d & \frac{x}{a} \\ \frac{y}{d} & z\frac{a}{d^2} \end{pmatrix}, \tag{3}$$

$$\begin{pmatrix} -\frac{v}{b} & -\frac{u}{c} \\ \frac{z}{b^2}c & \frac{y}{b} \\ \frac{x}{c} & t\frac{b}{c^2} \end{pmatrix}. \tag{4}$$

From (1) we see that we can take $u=0$ provided $t \neq 0$, and from (2) and (4) we see that we can take $v=0$ provided $z \neq 0$, and then swap u and v to get $u=0$. In the case when $t=z=0$ and both u and v are non-zero we can use (4) to take $x=y=1$. (None of the rows of $\begin{pmatrix} u & v \\ t & x \\ y & z \end{pmatrix}$ can equal zero.)

Now consider the action of $\begin{pmatrix} a & c \\ -a & c \end{pmatrix}$ on $\begin{pmatrix} u & v \\ 0 & 1 \\ 1 & 0 \end{pmatrix}$. We obtain

$$\frac{1}{4a^2c^2}\begin{pmatrix} 0 & -4a^2c \\ -c\,(c^2-uc^2)-c\,(c^2+vc^2) & a\,(c^2+vc^2)-a\,(c^2-uc^2) \\ c\,(a^2+ua^2)+c\,(a^2-va^2) & a\,(a^2+ua^2)-a\,(a^2-va^2) \end{pmatrix}.$$

This proves that every orbit contains a matrix with first row $(0,1)$.

Now in a matrix $\begin{pmatrix} 0 & 1 \\ t & x \\ y & z \end{pmatrix}$, the condition "$(tz-xy)^2-(ux-vt)(uz-vy)$ is not a square" reduces to "$(tz-xy)^2-ty$ is not a square", so neither t nor y can be zero. The action of $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ on $\begin{pmatrix} 0 & 1 \\ t & x \\ y & z \end{pmatrix}$ gives $\begin{pmatrix} 0 & 1 \\ \frac{t}{a^2} & \frac{x}{a} \\ y & za \end{pmatrix}$, and so every orbit contains a matrix $\begin{pmatrix} 0 & 1 \\ t & x \\ y & z \end{pmatrix}$ where t is either one or the least non-square modulo p, where $0 \leq x \leq \frac{p-1}{2}$, and where when $x=0$, $0 \leq z \leq \frac{p-1}{2}$. It seems experimentally that every orbit contains a matrix with $u=0$, $v=t=1$, but I have no proof of this.

Next we show that if we have (u,v,t,x,y,z) satisfying these conditions, and if we act on $\begin{pmatrix} u & v \\ t & x \\ y & z \end{pmatrix}$ with a non-identity matrix $\begin{pmatrix} a & 0 \\ b & d \end{pmatrix}$, then we obtain $\begin{pmatrix} u' & v' \\ t' & x' \\ y' & z' \end{pmatrix}$

where (u', v', t', x', y', z') which is lexicographically higher than (u, v, t, x, y, z). The action of $\begin{pmatrix} a & 0 \\ b & d \end{pmatrix}$ on $\begin{pmatrix} 0 & 1 \\ t & x \\ y & z \end{pmatrix}$ gives

$$\begin{pmatrix} 2\frac{t}{a^2}b & a\left(\frac{1}{ad} + 2\frac{x}{a^2}\frac{b}{d}\right) - 2\frac{t}{a^2}\frac{b^2}{d} \\ \frac{t}{a^2}d & \frac{x}{a} - \frac{t}{a^2}b \\ d\left(\frac{y}{d^2} - \frac{t}{a^2}\frac{b^2}{d^2}\right) & -a\left(\frac{1}{a}\frac{b}{d^2} - \frac{z}{d^2} + \frac{x}{a^2}\frac{b^2}{d^2}\right) - b\left(\frac{y}{d^2} - \frac{t}{a^2}\frac{b^2}{d^2}\right) \end{pmatrix},$$

which is lexicographically higher unless $b = 0$ and $d = 1$. But when $b = 0$ and $d = 1$, then the action gives $\begin{pmatrix} 0 & 1 \\ \frac{t}{a^2} & \frac{x}{a} \\ y & za \end{pmatrix}$, which is lexicographically higher unless $a = 1$.

So we only need to consider the action of matrices $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ where $c \neq 0$, and we write such a matrix as $k\begin{pmatrix} a & 1 \\ b & d \end{pmatrix}$. The action of $\begin{pmatrix} a & 1 \\ b & d \end{pmatrix}$ on $\begin{pmatrix} 0 & 1 \\ t & x \\ y & z \end{pmatrix}$ gives

$$\frac{1}{(b-ad)^2}\begin{pmatrix} a(2z-2dy-d)+b(2td^2-1-2xd) & b\left(2ya-2tbd\right)+a\left(b-2za+ad+2xbd\right) \\ z-d-xd^2-d\left(y-td^2\right) & a\left(xd^2+d-z\right)+b\left(y-td^2\right) \\ ab+xb^2-za^2-d\left(tb^2-ya^2\right) & b\left(tb^2-ya^2\right)-a\left(-za^2+ab+xb^2\right) \end{pmatrix}.$$

So we need $a(2z-2dy-d)+b(2td^2-1-2xd) = 0$ and we want to take

$$k = \frac{1}{(b-ad)^2}\left(b\left(2ya-2tbd\right)+a\left(b-2za+ad+2xbd\right)\right).$$

The MAGMA program note2dec5.1.m finds a set of representatives for the orbits. The integer parameters t, x, y, z correspond to $t1, x1, y1, z1$ in $\mathrm{GF}(p)$.