ON A QUESTION OF RICKARD ON TENSOR PRODUCT OF STABLY EQUIVALENT ALGEBRAS

SERGE BOUC AND ALEXANDER ZIMMERMANN

Abstract. Let r be a positive integer, let p be a prime and $\overline{\mathbb{F}}_p$ denote an algebraic closure of the prime field $\mathbb{F}_p$. After observing that the principal block B of $\overline{\mathbb{F}}_p PSU(3,p^r)$ is stably equivalent of Morita type to its Brauer correspondent b, we compute the radical series of the center $Z(b)$, and, using GAP, the radical series of $Z(B)$ in the cases $p^r \in \{3,4,5,8\}$. In these cases, the dimensions of the last non zero power of the radical of $Z(b)$ and $Z(B)$ are different, and it follows that the algebra $B \otimes_{\overline{\mathbb{F}}_p} \overline{\mathbb{F}}_p[X]/X^p$ is not stably equivalent of Morita type to $b \otimes_{\overline{\mathbb{F}}_p} \overline{\mathbb{F}}_p[X]/X^p$. This yields a negative answer to a question of Rickard.

Introduction

Let K be a field, and let A, B, C and D be finite dimensional K-algebras. Rickard showed in [12] that if A and B are derived equivalent, and if C and D are derived equivalent, then also $A \otimes_K C$ and $B \otimes_K D$ are derived equivalent. Rickard asks in [13, Question 3.8] if this still holds when replacing derived equivalence by stable equivalence of Morita type. It is clear that we have to suppose that all algebras involved have no semisimple direct factor. A result due to Liu [8] shows that then we may suppose that all algebras are indecomposable. In [10] Liu, Zhou and the second author showed that the question has a negative solution in case A, B, C and D are not necessarily selfinjective. However, a derived equivalence between selfinjective algebras A and B induces a stable equivalence of Morita type between A and B. If A and B are not selfinjective, then this implication is not valid. Hence, the natural playground for Rickard's question are selfinjective algebras.

The purpose of this paper is to give a counterexample to Rickard's question. For an algebraically closed base field K of characteristic p we construct symmetric K-algebras A and B which are stably equivalent of Morita type, but $A \otimes_K K[X]/X^p$ and $B \otimes_K K[X]/X^p$ are not stably equivalent of Morita type.

Note that this answers the general case. Indeed, if $A \otimes_K C$ is stably equivalent of Morita type to $B \otimes_K C$ and $B \otimes_K C$ is stably equivalent of Morita type to $B \otimes_K D$ then $A \otimes_K C$ is stably equivalent of Morita type to $B \otimes_K D$. Hence, we may suppose $C = D$.

In recent years many attempts were proposed to lift a stable equivalence of Morita type between selfinjective algebras to a derived equivalence. It is known that this is not possible in general, as is seen by the mod 2 group ring of a dihedral group of order 8 and the stable equivalence induced by a uniserial endotrivial module of Loewy length 3. This was used in [10] for example. In this paper we give a new incidence of this fact. Moreover, we provide two symmetric algebras, which are stably equivalent of Morita type, and have non isomorphic centres.

Our example is the principal p-block of the group $PSU(3,p^r)$ and its Brauer correspondent for $p^r \in \{3,4,5,8\}$.

We recall in the first section some basic facts and results which we need for our construction. In Section 2 we give our main result and its proof, and in Section 3 we display the GAP program needed for the proof. In Section 4 we determine the algebraic structure of

Date: May 2, 2015.

2010 *Mathematics Subject Classification.* Primary 16E35; 18E30; 20C05.

Both authors were supported by a grant STIC Asie 'Escap' from the Ministère des Affaires Étrangères de la France.

the centre of $KN_G(S)$ for $G = PSU(3, p^r)$ and S one of its Sylow p-subgroups for all primes p and integers r.

Acknowledgement: The idea of this paper was born during a visit of both authors in Beijing Normal University. We are very grateful to Yuming Liu for his great hospitality. Moreover, we thank Yuming Liu for suggesting a question to us leading to the present paper, and also for pointing out that it is not sufficient to show an abstract non isomorphism of the centres of the blocks. This led us to complete our proof by adding Lemma 9.

1. Background

Recall the following

Definition 1. [2], (cf also [14, Chapter 5]) Let A and B be two finite dimensional algebras over a field K. Then A and B are stably equivalent of Morita type if there is an $A \otimes_K B^{op}$-module M and a $B \otimes_K A^{op}$-module N such that

- M is projective as A-module, and as B^{op}-module
- N is projective as A^{op}-module and as B-module
- there is a projective $A \otimes_K A^{op}$-module P and a projective $B \otimes_K B^{op}$-module Q such that $M \otimes_B N \simeq B \oplus Q$ as $B \otimes_K B^{op}$-modules and $N \otimes_A M \simeq A \oplus P$ as $A \otimes_K A^{op}$-modules.

Independently Rickard [11] as well as Keller and Vossieck [6], show that if A and B are derived equivalent selfinjective algebras, then A and B are stably equivalent of Morita type.

Broué defined $Z^{st}(A) := \underline{\mathrm{End}}_{A\otimes_K A^{op}}(A)$ and

$$Z^{pr}(A) := \ker(\mathrm{End}_{A\otimes_K A^{op}}(A) \to \underline{\mathrm{End}}_{A\otimes_K A^{op}}(A))$$

where we denote by $\underline{\mathrm{End}}$ the endomorphisms taken in the stable module category.

The centre of an algebra is an invariant of a derived equivalence, as was shown by Rickard. The stable centre $Z^{st}(A)$ is an important invariant under stable equivalences of Morita type, as was shown by Broué.

Proposition 2. *(Broué* [2]*; see also* [14, Chapter 5]*) If A and B are stably equivalent of Morita type, then $Z^{st}(A) \simeq Z^{st}(B)$ as algebras.*

Now, Liu, Zhou and the second author give a criterion to determine the dimension of $Z^{st}(A)$.

Theorem 3. [9, Proposition 2.3 and Corollary 2.7] *Let A be a finite dimensional symmetric algebra over an algebraically closed field K of characteristic $p > 0$. Then* $\dim_K(Z^{pr}(A)) = \mathrm{rank}_p(C_A)$ *where C_A is the Cartan matrix of A and where* $\mathrm{rank}_p(C_A)$ *denotes its rank as matrix over K.*

Moreover, we recall a conjecture of Auslander-Reiten. In [1] Auslander and Reiten conjecture that if A and B are stably equivalent finite dimensional algebras, then the number of simple non-projective A-modules and the number of non-projective simple B-modules coincide. Again in [9] we show

Theorem 4. [9, Theorem 1.1] *Let K be an algebraically closed field and let A and B be two finite dimensional K-algebras, which are stably equivalent of Morita type and which do not have any semisimple direct factor. Then the number of isomorphism classes of non-projective simple A-modules is equal to the number of non-projective simple B-modules if and only if* $\dim_K(HH_0(A)) = \dim_K(HH_0(B))$*, where HH_0 denotes the degree* 0 *Hochschild homology.*

In particular, if A and B are symmetric, then Hochschild homology and cohomology coincide, and the number of non-projective simple A-modules is equal to the number of non-projective simple B-modules if and only if the centres of A and of B have the same dimension.

The following lemma is well-known to the experts, but for the convenience of the reader, and since it is crucial to our arguments, we include the short proof. For an algebra A denote by $J(A)$ its Jacobson radical.

Lemma 5. *Let K be a perfect field and let A and B be finite dimensional K-algebras. Then $J(A\otimes_K B) = J(A)\otimes_K B + A\otimes_K J(B)$.*

Proof. It is clear that $J(A)\otimes_K B + A\otimes_K J(B)$ is a nilpotent ideal of $A\otimes_K B$, and therefore we get

$$J(A)\otimes_K B + A\otimes_K J(B) \subseteq J(A\otimes_K B).$$

Now, $(A\otimes_K B)/(J(A)\otimes_K B + A\otimes_K J(B)) = A/J(A)\otimes_K B/J(B)$ and both K-algebras $A/J(A)$ and $B/J(B)$ are semisimple. Since K is perfect, every finite extension L of K is a separable field extension. By [3, Corollary 7.6] a finite dimensional semisimple K-algebra C is separable if and only if the centres of each of the Wedderburn components is a separable field extension of K. Hence $A/J(A)$ and $B/J(B)$ are both separable K-algebras. By [3, Corollary 7.8] the algebra $A/J(A)\otimes_K B/J(B)$ is semisimple. Therefore

$$J(A)\otimes_K B + A\otimes_K J(B) \supseteq J(A\otimes_K B).$$

This shows the statement. □

Remark 6. (cf e.g. [14, Example 1.7.17]) Lemma 5 is wrong if we drop the assumption that K is perfect: e.g. let p be a prime, and $K = \mathbb{F}_p(U)$ be the field of rational fractions over the finite field $\mathbb{F}_p$. Let $A = K[X]/(X^p - U)$. Then A is a purely inseparable extension of K, of dimension p. In particular it is a reduced (commutative) algebra, i.e. $J(A) = 0$. But $A\otimes_K A \cong K[X,Y]/(X^p - U, Y^p - U)$ contains the non zero element $X - Y$, such that $(X-Y)^p = U - U = 0$. Hence $J(A\otimes_K A) \neq 0$.

Lemma 7. *Let K be an algebraically closed field, let Λ and Δ be finite dimensional K-algebras, and suppose that Δ is local. Then the projective indecomposable $\Lambda\otimes_K\Delta$-modules are precisely the modules $P\otimes_K\Delta$ for projective indecomposable Λ-modules P, and if C_Λ is the Cartan matrix of Λ, then the Cartan matrix of $\Lambda\otimes\Delta$ is $C_{\Lambda\otimes_K\Delta} = \dim_K(\Delta)\cdot C_\Lambda$.*

Proof. Let P and Q be a indecomposable projective Λ-modules. Then $P\otimes_K\Delta$ is a projective indecomposable $\Lambda\otimes_K\Delta$-module. Indeed, $\mathrm{End}_{\Lambda\otimes_K\Delta}(P\otimes_K\Delta)\simeq \mathrm{End}_\Lambda(P)\otimes_K\Delta^{op}$. Moreover, since $\Gamma := \mathrm{End}_\Lambda(P)^{op}$ and Δ are local K-algebras their radical quotient are finite-dimensional skew-fields, and therefore $\Gamma/J(\Gamma)\simeq K\simeq\Delta/J(\Delta)$ since K is algebraically closed. Moreover, by Lemma 5 we get $J(\Gamma\otimes_K\Delta) = J(\Gamma)\otimes\Delta + \Gamma\otimes_K J(\Delta)$. On the other hand,

$$(\Gamma\otimes_K\Delta)/\left(J(\Gamma)\otimes_K\Delta + \Gamma\otimes_K J(\Delta)\right) = K\otimes_K K = K$$

and hence we get $\Gamma\otimes_K\Delta$ is local, and therefore $P\otimes_K\Delta$ is indecomposable. Now,

$$\mathrm{Hom}_{\Lambda\otimes_K\Delta}(P\otimes_K\Delta, Q\otimes_K\Delta) = \mathrm{Hom}_\Lambda(P,Q)\otimes_K\Delta^{op}.$$

Taking K-dimensions proves the lemma. □

Remark 8. As a special case of Lemma 7 we get $C_{A\otimes_K K[X]/X^p} = p\cdot C_A$ for algebraically closed fields K of characteristic p. Hence we get by Theorem 3 that $Z^{pr}(A\otimes_K K[X]/X^p) = 0$ for algebraically closed fields K of characteristic p and symmetric K-algebras A.

Lemma 9. *Let K be a perfect field and let n, m be positive integers. Let A and B be finite dimensional commutative K-algebras. If $J^{n+1}(A) = 0 \neq J^n(A)$ and $J^{m+1}(B) = 0 \neq J^m(B)$, then*

$$J^{n+m+1}(A\otimes_K B) = 0 \neq J^{n+m}(A\otimes_K B) = J^n(A)\otimes_K J^m(B).$$

Proof. By Lemma 5, we have $J(A\otimes_K B) = J(A)\otimes_K B + A\otimes_K J(B)$. Therefore

$$J^{n+m+1}(A\otimes_K B) = \sum_{k=0}^{n+m+1} J^k(A)\otimes_K J^{n+m+1-k}(B) = 0 \quad .$$

Similarly

$$J^{n+m}(A\otimes_K B)=\sum_{k=0}^{n+m} J^k(A)\otimes_K J^{n+m-k}(B)=J^n(A)\otimes_K J^m(B)\neq 0\quad ,$$

which completes the proof. □

Remark 10. Let K be any field, and A be a K-algebra. We give an elementary argument to determine the centre of $A\otimes_K K[X]/X^p$. It is clear that $A\otimes_K K[X]/X^p\cong A[X]/X^p$. Now, let $a:=a_0+a_1X+\dots a_{p-1}X^{p-1}\in A[X]$. Then for $b:=b_0\in A\cdot 1$ we get

$$ab-ba=(a_0b-ba_0)+\cdots+(a_{p-1}b-ba_{p-1})X^{p-1}$$

and so $a\in Z(A)$ implies that a commutes with any $b\in A$, and hence $a_0,\dots,a_{p-1}$ are all in $Z(A)$. Conversely, it is clear that $Z(A)[X]/X^p\subseteq Z(A[X]/X^p)$ since aX^n commutes with all elements of $A[X]/X^p$ whenever $a\in A$ and since sums of elements in the centre are still central.

Lemma 11. *If K is a perfect field and A is a finite dimensional K-algebra, and if moreover $J^n(Z(A))\neq 0=J^{n+1}(Z(A))$, then*

$$0\neq J^{n+p-1}\big(Z(A\otimes_K K[X]/X^p)\big)=J^n\big(Z(A)\big)\otimes_K X^{p-1}K[X]/X^p$$

and

$$J^{n+p}\big(Z(A\otimes_K K[X]/X^p)\big)=0.$$

Proof. This is an immediate consequence of Lemma 9. □

Corollary 12. *Let K be an algebraically closed field of characteristic $p>0$ and let A and B be two finite dimensional K-algebras and let $n,m\in\mathbb{N}$ such that $J^n(Z(A))\neq 0=J^{n+1}(Z(A))$ and $J^m(Z(B))\neq 0=J^{m+1}(Z(B))$. If $\dim_K(J^n(Z(A)))\neq\dim_K(J^m(Z(B))$, then $A\otimes_K K[X]/X^p$ and $B\otimes_K K[X]/X^p$ are not stably equivalent of Morita type.*

Proof. If $n\neq m$, then $Z(A\otimes_K K[X]/X^p)\not\simeq Z(B\otimes_K K[X]/X^p)$ by Lemma 11 since the Loewy lengths of the centres are different. If $n=m$, then Lemma 11 shows that the centres of $A\otimes_K K[X]/X^p$ and of $B\otimes_K K[X]/X^p$ are not isomorphic since the dimension of the lowest Loewy layers of the centres are not of the same dimension. Remark 8 shows that $Z(A\otimes_K K[X]/X^p)=Z^{st}(A\otimes_K K[X]/X^p)$ and $Z(B\otimes_K K[X]/X^p)=Z^{st}(B\otimes_K K[X]/X^p)$. Since the stable centre is invariant under stable equivalence of Morita type, we get the statement. □

Remark 13. For a field K and a K-algebra A let n_A be the number of isomorphism classes of simple nonprojective A-modules. Auslander-Reiten conjecture [1, page 409, Conjecture (5)] that if A and B are stably equivalent finite dimensional K-algebras, then $n_A=n_B$. Now [9, Theorem 1.1] shows that if K is algebraically closed and if A and B are indecomposable finite dimensional K-algebras which are stably equivalent of Morita type, then $n_A=n_B$ is equivalent to $\dim_K(HH_0(A))=\dim_K(HH_0(B))$. If A is symmetric, then there is a vector space isomorphism $HH_0(A)\simeq HH^0(A)=Z(A)$, we see that the Auslander-Reiten conjecture implies that $\dim_K\big(Z(A)\big)=\dim_K\big(Z(B)\big)$. More precisely by [9, Corollary 1.2], for two indecomposable symmetric algebras A and B over an algebraically closed field K we have $n_A=n_B\Leftrightarrow\dim_K\big(Z^{pr}(A)\big)=\dim_K\big(Z^{pr}(B)\big)$, where by definition $Z^{st}(A)=Z(A)/Z^{pr}(A)$. The link to our proof is now given by the fact that for every algebra the Higman ideal $H(A)$ of A is equal to $Z^{pr}(A)$, and for symmetric algebras A over an algebraically closed field K we have that $\dim_K(H(A))$ is equal to the p-rank of C_A.

2. The Example

Let $\overline{\mathbb{F}}_p$ be the algebraic closure of the prime field $\mathbb{F}_p$ of characteristic p. Let $q = p^r$ for some positive integer r.

We recall some results on the geometry of $PSU(3, q)$ (cf e.g. [5, II Satz 10.12, page 242]). The group $G := PSU(3, q)$ acts doubly transitively on the unitary quadric Q of cardinal $q^3 + 1$. Note that we use the GAP notation, not the notation used in [5, II Satz 10.12, page 242], namely, $PSU(3, q)$ is defined over a field with q^2 elements, and is a natural quotient of a subgroup of $SL_2(q^2)$ (and not of $SL_2(q)$!). The stabiliser of a point X of Q is the normaliser in G of a Sylow p-subgroup P of G. Therefore two different conjugate Sylow p-subgroups P and ${}^gP$ of G fix two different points X and gX of Q. Hence ${}^gP \cap P = 1$ if $g \notin N_G(P)$, or in other words, G has a trivial intersection Sylow p-subgroup structure. This implies that Green correspondence gives a stable equivalence of Morita type between the principal block B of $\overline{\mathbb{F}}_pG$ and its Brauer correspondent b (cf e.g. [14, Chapter 2, Theorem 2.1.21, Proposition 2.1.23 and Proposition 5.3.17]).

The GAP [4] program in Section 3 computes the Loewy series of the ring $Z(\mathbb{F}_2PSU(3, 4))$ and of $Z(\mathbb{F}_2N_{PSU(3,4)}(S))$ for some Sylow 2-subgroup of $PSU(3, 4)$. Observe moreover that $\overline{\mathbb{F}}_2PSU(3, 4)$ has two blocks, the principal one and another block of defect 0 (corresponding to the Steinberg character). Moreover, the dimensions of the Loewy series obtained over $\mathbb{F}_2$ also hold by extending the scalars to $\overline{\mathbb{F}}_2$, using Lemma 5.

We obtain that

$$\begin{aligned}
\dim_{\overline{\mathbb{F}}_2}(Z(B)) &= 21 = \dim_{\overline{\mathbb{F}}_2}(Z(b))\\
\dim_{\overline{\mathbb{F}}_2}(J(Z(B))) &= 20 = \dim_{\overline{\mathbb{F}}_2}(J(Z(b)))\\
\dim_{\overline{\mathbb{F}}_2}(J^2(Z(B))) &= 5 \neq 4 = \dim_{\overline{\mathbb{F}}_2}(J^2(Z(b)))\\
\dim_{\overline{\mathbb{F}}_2}(J^3(Z(B))) &= 0 = \dim_{\overline{\mathbb{F}}_2}(J^3(Z(b))).
\end{aligned}$$

Similarly we get for the centre of the principal block B of $\overline{\mathbb{F}}_2PSU(3, 8)$ and the centre of its Brauer correspondent b

$$\begin{aligned}
\dim_{\overline{\mathbb{F}}_2}(Z(B)) &= 27 = \dim_{\overline{\mathbb{F}}_2}(Z(b))\\
\dim_{\overline{\mathbb{F}}_2}(J(Z(B))) &= 26 = \dim_{\overline{\mathbb{F}}_2}(J(Z(b)))\\
\dim_{\overline{\mathbb{F}}_2}(J^2(Z(B))) &= 3 \neq 2 = \dim_{\overline{\mathbb{F}}_2}(J^2(Z(b)))\\
\dim_{\overline{\mathbb{F}}_2}(J^3(Z(B))) &= 0 = \dim_{\overline{\mathbb{F}}_2}(J^3(Z(b))).
\end{aligned}$$

An immediate variant of the program shows that this is a quite general phenomenon in odd characteristic. The group $PSU(3, 3)$ gives an example in characteristic 3 since, denoting by B the principal block of $\overline{\mathbb{F}}_3PSU(3, 3)$ and by b its Brauer correspondent,

$$\begin{aligned}
\dim_{\overline{\mathbb{F}}_3}(Z(B)) &= 13 = \dim_{\overline{\mathbb{F}}_3}(Z(b))\\
\dim_{\overline{\mathbb{F}}_3}(J(Z(B))) &= 12 = \dim_{\overline{\mathbb{F}}_3}(J(Z(b)))\\
\dim_{\overline{\mathbb{F}}_3}(J^2(Z(B))) &= 4 \neq 3 = \dim_{\overline{\mathbb{F}}_3}(J^2(Z(b)))\\
\dim_{\overline{\mathbb{F}}_3}(J^3(Z(B))) &= 0 = \dim_{\overline{\mathbb{F}}_3}(J^3(Z(b))).
\end{aligned}$$

The group $PSU(3, 5)$ gives an example in characteristic 5 since, denoting by B the principal block of $\overline{\mathbb{F}}_5PSU(3, 5)$ and by b its Brauer correspondent,

$$\begin{aligned}
\dim_{\overline{\mathbb{F}}_5}(Z(B)) &= 13 = \dim_{\overline{\mathbb{F}}_5}(Z(b))\\
\dim_{\overline{\mathbb{F}}_5}(J(Z(B))) &= 12 = \dim_{\overline{\mathbb{F}}_5}(J(Z(b)))\\
\dim_{\overline{\mathbb{F}}_5}(J^2(Z(B))) &= 2 \neq 1 = \dim_{\overline{\mathbb{F}}_5}(J^2(Z(b)))\\
\dim_{\overline{\mathbb{F}}_5}(J^3(Z(B))) &= 0 = \dim_{\overline{\mathbb{F}}_5}(J^3(Z(b))).
\end{aligned}$$

Theorem 14. *Let K be an algebraic closure of $\mathbb{F}_p$ and let B be the principal block of $KPSU(3,p^r)$. Let b be the Brauer correspondent of B in the group ring of the normaliser of a 2-Sylow subgroup of $PSU(3,p^r)$. Then B and b are stably equivalent of Morita type. If moreover $p^r \in \{3,4,5,8\}$, then the square of the Jacobson radical of $Z(B)$ is of different dimension than the square of the Jacobson radical of $Z(b)$, whereas $Z(B)$ and $Z(b)$ both have Loewy length 3. In particular $B \otimes_K K[X]/X^p$ is not stably equivalent of Morita type to $b \otimes_K K[X]/X^p$.*

Proof. As seen at the beginning of this section, B and b are stably equivalent of Morita type by Green correspondence.

The GAP [4] program in Section 3 shows that the Loewy series of the centres of B and of b are of the same length but the dimensions of the Loewy layers are not equal. In particular the lowest Loewy layers of the algebras $Z(B)$ and $Z(b)$ have different dimension.

Corollary 12 implies that $B \otimes_K K[X]/X^p$ is not stably equivalent of Morita type to $b \otimes_K K[X]/X^p$. □

Remark 15. The above examples suggest that in general, with the notation of Theorem 14, the dimension of $J^2\big(Z(B)\big)$ could always be equal to $1 + \dim_K J^2(Z(b))$. By Theorem 41, this is equal to $\dfrac{p^r+1}{\gamma}$, where γ is the greatest common divisor of p^r+1 and 3.

3. The GAP program

We display here the GAP program we used.

```
# the characteristic p
prem:=2;
#
# The group G
g:=PSU(3,prem^2);
#
# the ground field k
corps:=GF(prem);
#
s:=SylowSubgroup(g,prem);
# the normalizer NS of a Sylow p-subgroup
ns:=Normalizer(g,s);
#
# getting a permutation representation of G of smaller degree
f:=FactorCosetAction(g,ns);
g:=Image(f);
ns:=Image(f,ns);
#
# uncomment next line to replace G by NS
#g:=ns;
#
# computing the structure constants of ZkG
c:=ConjugacyClasses(g);
rc:=List(c,Representative);
lc:=Length(c);
ci:=List([1..lc],x->First([1..lc],y->rc[x]^(-1) in c[y]));
l:=List([1..lc],x->NullMat(lc,lc,corps));
for iu in [1..lc] do
    u:=c[iu];
    if rc[iu]=One(g) then
        for iv in [iu..lc] do
            Print("\r",iu,":",iv,"/",lc,"   ");
            v:=List([1..lc],x->Zero(corps));
            v[iv]:=One(corps);
            l[iu][iv]:=v;
            l[iv][iu]:=v;
```

```
        od;
    else
        for iv in [iu..lc] do
            Print("\r",iu,":",iv,"/",lc,"   ");
            w:=c[ci[iv]];
            v:=List(List(rc),x->One(corps)*Size(Intersection(u,List(w,y->x*y))));
            l[iu][iv]:=v;
            l[iv][iu]:=v;
        od;
    fi;
od;
Print("\n");
za:=Algebra(corps,l);
Print("Dimension of ZkG \t= ",Dimension(za),"\n");
radza:=RadicalOfAlgebra(za);
Print("Dimension of JZkG \t= ",Dimension(radza),"\n");
bradza:=Basis(radza);
vbradza:=BasisVectors(bradza);
vbr:=vbradza;
#
# Computing the powers of the radical of the center
i:=1;
repeat
    i:=i+1;
    l:=Set(List(Cartesian(vbradza,vbr),x->x[1]*x[2]));
    r:=Ideal(za,l);
    br:=Basis(r);
    vbr:=BasisVectors(br);
    d:=Dimension(r);
    Print("Dimension of (JZkG)^",i,"\t= ",d,"\n");
until  d=0;
```

4. The centre of the mod p group ring of the normaliser of the Sylow subgroup of $PSU(3,p^r)$

Recall that we denote by S a Sylow p-subgroup of the projective special unitary group $G = PSU(3,q)$ over the field with q^2 elements, where $q = p^r$, and by N the normaliser of S in G. In this section, we determine the ring structure of the center ZkN of the group algebra kN, where k is any commutative ring.

Notation 16. If $x \in N$, we denote by $x^+ \in ZkN$ the sum of the conjugates of x in N.

Then the elements x^+, for x in a set of representatives of conjugacy classes of N, form a k-basis of ZkN.

Let V be a three dimensional vector space over the field $\mathbb{F}_{q^2}$, with basis B. We endow V with a non degenerate hermitian product, and without loss of generality, we assume that the matrix of this product in B is equal to

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} .$$

Notation 17. For $x \in \mathbb{F}_{q^2}$, we set $\overline{x} = x^q$. Then the map $x \mapsto \overline{x}$ is the automorphism of order 2 of the extension $\mathbb{F}_{q^2}/\mathbb{F}_q$. We also set

$$\Psi = \{x \in \mathbb{F}_{q^2}^\times \mid x\overline{x} = 1\}$$

Let ω be a non zero element of $\mathbb{F}_{q^2}$ such that $\omega + \overline{\omega} = 0$, and τ be an element of $\mathbb{F}_{q^2}$ such that $\tau + \overline{\tau} = -1$.

It follows from [5, II Satz 10.12, page 242] that we can suppose that the group N is equal to the image in G of the group of matrices of the form

$$M(a,b,c)=\begin{pmatrix} a & b & c\\ 0 & \overline{a}/a & -\overline{b}/a\\ 0 & 0 & 1/\overline{a}\end{pmatrix}\quad ,$$

where (a,b,c) belongs to the set

$$\mathcal{Q}=\{(a,b,c)\in\mathbb{F}_{q^2}^{\times}\times(\mathbb{F}_{q^2})^2\mid b\overline{b}+a\overline{c}+c\overline{a}=0\}\quad .$$

Lemma 18. *For $(a,b,c)\in\mathcal{Q}$, let $\hat{M}(a,b,c)$ denote the image of $M(a,b,c)$ in N. Then if $(a',b',c')\in\mathcal{Q}$, we have that $\hat{M}(a,b,c)=\hat{M}(a',b',c')$ if and only if there is $\lambda\in\mathbb{F}_{q^2}$ with $\lambda^{q-2}=1$ and $(a',b',c')=\lambda\cdot(a,b,c)$.*

Proof. $\hat{M}(a,b,c)=\hat{M}(a',b',c')$ if and only if there exists a scalar $\lambda\in\mathbb{F}_{q^2}$ such that

$$\begin{pmatrix} a' & b' & c'\\ 0 & \overline{a'}/a' & -\overline{b'}/a'\\ 0 & 0 & 1/\overline{a'}\end{pmatrix}=\lambda\begin{pmatrix} a & b & c\\ 0 & \overline{a}/a & -\overline{b}/a\\ 0 & 0 & 1/\overline{a}\end{pmatrix}\quad .$$

Equivalently $(a',b',c')=\lambda(a,b,c)$ and $\overline{\lambda}/\lambda=\lambda$, i.e. $\lambda^{q-2}=1$. □

For two non zero integers s,t denote by (s,t) their greatest common divisor. Observe that $(q-2,q^2-1)=(3,q+1)$, to motivate the following:

Notation 19. We set $\gamma=(3,q+1)$, and put

$$\Gamma=\{\lambda\in\mathbb{F}_{q^2}\mid\lambda^{\gamma}=1\}\leq\Psi \text{ as well as } \mathrm{L}=\{a^{\gamma}\mid a\in\mathbb{F}_{q^2}^{\times}\}\quad .$$

With this notation, the group N has order $q^3(q^2-1)/\gamma$. It is equal to the semidirect product of the group S, consisting of the elements $\hat{M}(1,b,c)=\begin{pmatrix} 1 & b & c\\ 0 & 1 & -\overline{b}\\ 0 & 0 & 1\end{pmatrix}$, where b and c are elements of $\mathbb{F}_{q^2}$ such that $b\overline{b}+c+\overline{c}=0$, by the cyclic group C of order $(q^2-1)/\gamma$ consisting of the elements $\hat{M}(a,0,0)=\begin{pmatrix} a & 0 & 0\\ 0 & \overline{a}/a & 0\\ 0 & 0 & 1/\overline{a}\end{pmatrix}$, for $a\in\mathbb{F}_{q^2}^{\times}/\Gamma$.

Lemma 20. (1) *Let (a,b,c) and (x,y,z) be elements of $\mathcal{Q}$. Then*

$$M(a,b,c)M(x,y,z)=M\Big(ax,ay+\frac{b\overline{x}}{x},az-\frac{b\overline{y}}{x}+\frac{c}{\overline{x}}\Big)\quad .$$

(2) *Let $(a,b,c)\in\mathcal{Q}$. Then $M(a,b,c)^{-1}=M\Big(\frac{1}{a},-\frac{b}{\overline{a}},\overline{c}\Big)$.*

(3) *Let (a,b,c) and (x,y,z) be elements of $\mathcal{Q}$. Then*

$$M(a,b,c)M(x,y,z)M(a,b,c)^{-1}=M\left(x,\frac{ab}{\overline{a}}\Big(\frac{\overline{x}}{x}-x\Big)+\frac{a^2}{\overline{a}}y,t\right)\quad ,$$

where $t=a\overline{c}x+\dfrac{\overline{a}c}{\overline{x}}+ay\overline{b}-\dfrac{\overline{a}b\overline{y}}{x}+\dfrac{b\overline{b}\overline{x}}{x}+a\overline{a}z.$

Proof. All the assertions follow from straightforward computations. □

Proposition 21. (1) *Let (x,y,z) and (x',y',z') be elements of $\mathcal{Q}$. If $\hat{M}(x,y,z)$ and $\hat{M}(x',y',z')$ are conjugate in N, then $x^{-1}x'\in\Gamma$.*

(2) *The elements $\hat{M}(x,0,0)$, for $x\in\mathbb{F}_{q^2}/\Gamma$, lie in distinct conjugacy classes of N.*

(3) *Let $(x,y,z)\in\mathcal{Q}$. Then if $x\notin\Gamma$, the element $\hat{M}(x,y,z)$ of N is conjugate to an element of the form $\hat{M}(x,0,xu\omega)$, for some $u\in\mathbb{F}_q$.*

(4) *Let $x \in \mathbb{F}_{q^2}^\times$ and $u \in \mathbb{F}_q$. Then if $x\overline{x} \neq 1$, the element $\hat{M}(x, 0, xu\omega)$ of N is conjugate to $\hat{M}(x, 0, 0)$. If $x\overline{x} = 1$, and if $u \neq 0$, then the element $\hat{M}(x, 0, xu\omega)$ is conjugate to $\hat{M}(x, 0, x\omega)$, and not conjugate to $\hat{M}(x, 0, 0)$.*

(5) *If $(1, y, z) \in \mathcal{Q}$, then either $y \neq 0$ and there exists $u \in \mathbb{F}_q$ such that $z = y\overline{y}(\tau + u\omega)$, or $y = 0$ and there exists $u \in \mathbb{F}_q$ such that $z = u\omega$. Moreover, if $(1, y', z') \in \mathcal{Q}$ and if $\hat{M}(1, y', z')$ and $\hat{M}(1, y, z)$ are conjugate in N, then y and y' are both non zero, or both equal to 0.*

(6) *If $(1, y, z)$ and $(1, y', z')$ are in $\mathcal{Q}$, and if y and y' are both non zero, then $\hat{M}(1, y', z')$ and $\hat{M}(1, y, z)$ are conjugate in N if and only if $y'^{(q^2-1)/\gamma} = y^{(q^2-1)/\gamma}$ in $\mathbb{F}_{q^2}^\times$, i.e. if $y'/y \in \mathrm{L}$. In particular $M(1, y, z)$ is conjugate to $M(1, y, y\overline{y}\tau)$.*

Proof. Assertion (1) follows from Assertion (3) of Lemma 20: if

$$\hat{M}(x', y', z') = \hat{M}\left(x, \frac{ab}{\overline{a}}\Big(\frac{\overline{x}}{x} - x\Big) + \frac{a^2}{\overline{a}}y, t\right) \quad ,$$

then there exists $\lambda \in \Gamma$ such that $x' = \lambda x$ by Lemma 18.

Assertion (2) is a straightforward consequence of Assertion (1).

For Assertion (3), we use Assertion (3) of Lemma 20 again: since $x \notin \Gamma$, we have $\frac{\overline{x}}{x} \neq x$, and we can set $a = 1$, $b = -\frac{y}{\frac{\overline{x}}{x} - x}$, and $c = b\overline{b}\tau$. Then $(a, b, c) \in \mathcal{Q}$ and $M(a, b, c)M(x, y, z)M(a, b, c)^{-1}$ is of the form $M(x, 0, t)$, for some $t \in \mathbb{F}_{q^2}$. In particular $(x, 0, t) \in \mathcal{Q}$, hence $x\overline{t} + t\overline{x} = 0$. In other words $t = vx$ with $v + \overline{v} = 0$. Then $v = u\omega$ and $u = \overline{u}$, that is $u \in \mathbb{F}_q$.

For Assertion (4), we have to decide when two elements of the form $n = \hat{M}(x, 0, xu\omega)$ and $n' = \hat{M}(x', 0, x'u'\omega)$ are conjugate in N, where $x, x' \notin \Gamma$, and $u, u' \in \mathbb{F}_q$. By Assertion (1), we can assume that $x = x'$, and then n and n' are conjugate if and only if there exists $(a, b, c) \in \mathcal{Q}$ such that

$$M(a, b, c)M(x, 0, xu\omega)M(a, b, c)^{-1} = M(x, 0, xu'\omega) \quad .$$

By Assertion (3) of Lemma 20, we have $\frac{ab}{\overline{a}}\Big(\frac{\overline{x}}{x} - x\Big) = 0$, hence $b = 0$. Now $xu'\omega$ is equal to the element t of Lemma 20, in the case $y = b = 0$ and $z = xu\omega$, that is

$$xu'\omega = a\overline{c}x + \frac{\overline{a}c}{\overline{x}} + a\overline{a}xu\omega \quad .$$

Moreover $a\overline{c} + c\overline{a} = 0$, since $(a, 0, c) \in \mathcal{Q}$. So there exists $v \in \mathbb{F}_q$ such that $c = av\omega$. This gives

$$xu'\omega = -a\overline{a}xv\omega + \frac{a\overline{a}xv\omega}{\overline{x}} + a\overline{a}xu\omega \quad ,$$

or equivalently

$$u' = a\overline{a}\Big(u - v(1 - \frac{1}{x\overline{x}})\Big) \quad .$$

Thus n and n' are conjugate in N if and only if there exist $a \in \mathbb{F}_{q^2}^\times$ and $v \in \mathbb{F}_q$ such that $u' = a\overline{a}\Big(u - v(1 - \frac{1}{x\overline{x}})\Big)$. If $x\overline{x} \neq 1$, then we can take $a = 1$ and $v = \frac{u - u'}{1 - \frac{1}{x\overline{x}}}$, so n and n' are conjugate. And if $x\overline{x} = 1$, then n and n' are conjugate if and only if there exists $a \in \mathbb{F}_{q^2}^\times$ such that $u' = a\overline{a}u$, or equivalently, if there exists $\lambda \in \mathbb{F}_q^\times$ such that $u' = \lambda u$. So either $u = u' = 0$, or u and u' are both non zero. This completes the proof of Assertion (4).

For Assertion (5), assume that $(1, y, z) \in \mathcal{Q}$. Then $y\overline{y} + z + \overline{z} = 0$. If $y \neq 0$, set $v = \frac{z}{y\overline{y}} - \tau$. Then $v + \overline{v} = 0$, so there exists $u \in \mathbb{F}_q$ such that $v = u\omega$, thus $u = y\overline{y}(\tau + u\omega)$. And if $y = 0$, then $z + \overline{z} = 0$, so $z = u\omega$ for some $u \in \mathbb{F}_q$.

Now by Assertion (3) of Lemma 20, for $(1,y,z)$ and $(1,y',z')$ in $\mathcal{Q}$, the elements $n = \hat{M}(1,y,z)$ and $n' = \hat{M}(1,y',z')$ are conjugate in N if and only if there exists $(a,b,c) \in \mathcal{Q}$ such that

$$y' = \frac{a^2}{\overline{a}}y \ \text{ and } \ z' = a\overline{c} + \overline{a}c + ay\overline{b} - \overline{a}b\overline{y} + b\overline{b} + a\overline{a}z \quad ,$$

that is

$$y' = \frac{a^2}{\overline{a}}y \ \text{ and } \ z' = ay\overline{b} - \overline{a}b\overline{y} + a\overline{a}z \quad ,$$

In particular y is non zero if and only if y' is non zero. Assertion (5) follows.

Assume now that both y and y' are non zero. If n and n' are conjugate, then there exists $a \in \mathbb{F}_{q^2}^\times$ such that $y' = \frac{a^2}{\overline{a}}y = a^{2-q}y$. It follows that y'/y belongs to the subgroup of $\mathbb{F}_{q^2}^\times$ consisting of $(q-2)$-th powers, i.e. the subgroup of γ-th powers, i.e. the unique subgroup of order $(q^2-1)/\gamma$ of $\mathbb{F}_{q^2}^\times$. Equivalently $(y'/y)^{(q^2-1)/\gamma} = 1$. Conversely, suppose that there exists $a \in \mathbb{F}_{q^2}^\times$ such that $y' = \frac{a^2}{\overline{a}}y$. There are elements u and u' of $\mathbb{F}_q$ such that $z = y\overline{y}(\tau + u\omega)$ and $z' = y'\overline{y'}(\tau + u'\omega)$. If we can find b and c such that $(a,b,c) \in \mathcal{Q}$ and $z' = a\overline{b}y - \overline{a}b\overline{y} + a\overline{a}z$, then n and n' are conjugate in N. This can also be written

$$a\overline{a}y\overline{y}(\tau + u'\omega) = a\overline{b}y - \overline{a}b\overline{y} + a\overline{a}y\overline{y}(\tau + u\omega) \quad ,$$

or equivalently

$$(*) \qquad \frac{1}{\omega}\Big(\frac{\overline{b}}{\overline{a}\overline{y}} - \frac{b}{ay}\Big) = u' - u \quad .$$

Now the map $b \mapsto \frac{1}{\omega}\Big(\frac{\overline{b}}{\overline{a}\overline{y}} - \frac{b}{ay}\Big)$ is a non zero $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^2}$ to F_q. Hence it is surjective, and there exists $b \in \mathbb{F}_{q^2}$ such that (*) holds. Now we set $c = \frac{b\overline{b}}{\overline{a}}\tau$, and then $(a,b,c) \in \mathcal{Q}$, and the elements n and n' are conjugate in N. This proves Assertion (6), and completes the proof of Proposition 21. □

Corollary 22. *The set*

$$E = \big\{\hat{M}(x,0,0) \mid x \in \mathbb{F}_{q^2}^\times/\Gamma\big\} \bigsqcup \big\{\hat{M}(x,0,x\omega) \mid x \in \Psi/\Gamma\big\} \bigsqcup \big\{\hat{M}(1,y,y\overline{y}\tau) \mid y \in \mathbb{F}_{q^2}^\times/\mathrm{L}\big\}$$

is a set of representatives of conjugacy classes of N. In particular, there are $\frac{q^2+q}{\gamma} + \gamma$ conjugacy classes in N.

Proof. Indeed, by Proposition 21, the set E is a set of representatives of conjugacy classes of N. Its cardinality is

$$|E| = \frac{q^2-1}{\gamma} + \frac{q+1}{\gamma} + \gamma = \frac{q^2+q}{\gamma} + \gamma \quad .$$

□

Notation 23.

- For $x \in \mathbb{F}_{q^2}^\times$, we set $d_x = \hat{M}(x,0,0)$ and $D_x = d_x^+ \in ZkN$.
- For $x \in \Psi$, we set $t_x = \hat{M}(x,0,x\omega)$ and $T_x = t_x^+$.
- For $y \in \mathbb{F}_{q^2}^\times$, we set $u_y = \hat{M}(1,y,y\overline{y}\tau)$ and $U_y = u_y^+$.

Proposition 24.

(1) *For $x \in \mathbb{F}_{q^2}^\times - \Psi$,*

$$d_x^N = \big\{\hat{M}(x,y,z) \mid y,z \in \mathbb{F}_{q^2},\ y\overline{y} + x\overline{z} + z\overline{x} = 0\big\} \quad .$$

In particular $|d_x^N| = q^3$.

(2) *For* $x \in \Psi - \Gamma$,
$$d_x^N = \{\hat{M}(x, y(\overline{x}^2 - x), y\overline{y}(\overline{x}^2 - x)) \mid y \in \mathbb{F}_{q^2}\} \quad .$$
In particular $|d_x^N| = q^2$.

(3) *For* $x \in \Gamma$, *the element* d_x *is the identity element of* N, *and* $|d_x^N| = 1$.

(4) *For* $x \in \Psi$, *the conjugacy class of* t_x *in* N *has cardinality* $q^2(q-1)$ *if* $x \notin \Gamma$, *and* $q-1$ *otherwise. The conjugacy class of* T_1 *consists of the elements* $\hat{M}(1, 0, \lambda\omega)$, *for* $\lambda \in \mathbb{F}_q^\times$.

(5) *For* $x \in \mathbb{F}_{q^2}^\times$,
$$u_x^N = \{\hat{M}(1, v, v\overline{v}\tau + \lambda\omega) \mid v \in x\mathrm{L},\ \lambda \in \mathbb{F}_q\} \quad .$$
In particular $|u_x^N| = \dfrac{q(q^2-1)}{\gamma}$.

Proof. It follows from Proposition 21 that if $(x, y, z) \in \mathcal{Q}$ and $x\overline{x} \neq 1$, then $\hat{M}(x, y, z)$ is conjugate to d_x, and that conversely, any conjugate of d_x in N is of the form $\hat{M}(x, y, z)$, for some elements $y, z \in \mathbb{F}_{q^2}$ such that $(x, y, z) \in \mathcal{Q}$. This proves Assertion (1).

Now let (a, b, c) and (x, y, z) be elements of $\mathcal{Q}$. By Assertion (1) of Lemma 20, comparing the diagonal elements in the product in the two possible orders, the elements $\hat{M}(a, b, c)$ and $\hat{M}(x, y, z)$ commute if and only if

$$(**) \qquad ay + \frac{b\overline{x}}{x} = xb + \frac{y\overline{a}}{a} \ \text{ and } \ az - \frac{b\overline{y}}{x} + \frac{c}{\overline{x}} = xc - \frac{y\overline{b}}{a} + \frac{z}{\overline{a}}$$

- If $y = z = 0$, this gives $\frac{b\overline{x}}{x} = xb$ and $\frac{c}{\overline{x}} = xc$. If moreover $x\overline{x} = 1$ but $x^2 \neq \overline{x}$, then $b = 0$, but a and c are arbitrary, only subject to $a\overline{x} + c\overline{a} = 0$. In this case the centraliser of d_x in N has cardinality $\dfrac{q(q^2-1)}{\gamma}$, and the conjugacy class of d_x in N has cardinality q^2. Now Assertion (2) follows from the fact that the elements
$$\hat{M}(1, y, y\overline{y}\tau)\hat{M}(x, 0, 0)\hat{M}(1, y, y\overline{y}\tau)^{-1} = \hat{M}(x, y(\overline{x}^2 - x), y\overline{y}(\overline{x}^2 - x)) \quad ,$$
for $y \in \mathbb{F}_{q^2}$, are all distinct.
  Finally if $x^2 = \overline{x}$, then $x \in \Gamma$, so d_x is the identity element of N, and Assertion (3) follows.
- If $x \in \Psi$, $y = 0$ and $z = x\omega$, then the relations (**) give
$$b\overline{x}^2 = xb \ \text{ and } \ ax\omega + cx = xc + \frac{x\omega}{\overline{a}} \quad ,$$
that is $b(x - \overline{x}^2) = 0$ and $a\overline{a} = 1$. If $x \neq \overline{x}^2$, i.e. if $x \notin \Gamma$, this is equivalent to $b = 0$ and $a\overline{a} = 1$. Then c is arbitrary, only subject to $a\overline{x} + c\overline{a} = 0$. In this case the centraliser of t_x in N has cardinality $\dfrac{q(q+1)}{\gamma}$, and the conjugacy class of t_x in N has cardinality $q^2(q-1)$. Now if $x^2 = \overline{x}$, the only condition left is $a\overline{a} = 1$, so the centraliser of t_x in N has cardinality q^3 (it is equal to S), and the conjugacy class of t_x in N has cardinality $q - 1$. Moreover, by Lemma 20, the conjugates of $t_1 = \hat{M}(1, 0, \omega)$ are the elements $\hat{M}(1, 0, a\overline{a}\omega)$, for $a \in \mathbb{F}_{q^2}^\times$. This completes the proof of Assertion (4).
- If $x = 1$, $y \in \mathbb{F}_{q^2}^\times$, and $z = y\overline{y}\omega$, then the relations (**) give
$$ay = \frac{y\overline{a}}{a} \ \text{ and } \ ay\overline{y}\omega - b\overline{y} = -\frac{y\overline{b}}{a} + \frac{y\overline{y}\omega}{\overline{a}} \quad .$$
Since $y \neq 0$, the first relation gives $a^2 = \overline{a}$, i.e. $a \in \Gamma$, so we can assume $a = 1$ by Lemma 18. Now the second relation reads $b\overline{y} = y\overline{b}$, i.e. $b = uy$, for $u \in \mathbb{F}_q$. Since c is subject to $c + \overline{c} + b\overline{b} = 0$, it follows that the centraliser of u_y in N has cardinality q^2, and the conjugacy class of u_y in N has cardinality $\dfrac{q(q^2-1)}{\gamma}$.

Now Assertion (5) follows from the fact that by Proposition 21, the element $\hat{M}(1, v, v\bar{v}\tau + \lambda\omega)$, for $v \in x\mathrm{L}$ and $\lambda \in \mathbb{F}_q$, is conjugate to u_x, and that there are $\dfrac{q(q^2-1)}{\gamma}$ such elements in N.

□

We recall the following well known fact (cf e.g. [3, (9.28)]):

Lemma 25. *Let G be a finite group and k be a commutative ring. For $x \in G$, let $x^+ \in ZkG$ denote the sum of the elements of the conjugacy class x^G of x in G. Then for $x, y \in G$*

$$x^+ \cdot y^+ = \sum_{z \in [G]} m_{x,y}^z z^+ \quad ,$$

where $[G]$ denotes a set of representatives of conjugacy classes of G, and

$$m_{x,y}^z = |\{(x', y') \in x^G \times y^G \mid x'y' = z\}| \quad .$$

Clearly $m_{x,y}^z = m_{y,x}^z$ and $m_{x^{-1},y^{-1}}^{z^{-1}} = m_{x,y}^z$ for any $x, y, z \in G$, but since

$$m_{x,y}^z |z^G| = |\{(x', y', z') \in x^G \times y^G \times z^G \mid x'y' = z'\}| \quad ,$$

we have also $m_{x,y}^z |z^G| = m_{z,y^{-1}}^x |x^G| = m_{z,x^{-1}}^y |y^G|$.

Observe that $Z(kN) = k \otimes_{\mathbb{Z}} Z(\mathbb{Z}N)$ and hence we may and will suppose for the rest of this section that $k = \mathbb{Z}$, unless otherwise stated.

Proposition 26. (1) *Let $x \in F_{q^2}^\times - \Psi$ and $y \in \mathbb{F}_{q^2}^\times$ such that $xy \notin \Psi$. Then*

$$D_x D_y = \begin{cases} q^3 D_{xy} & \text{if } y \notin \Psi \\ q^2 D_{xy} & \text{if } y \in \Psi \end{cases} .$$

(2) *Let $x \in F_{q^2}^\times - \Psi$ and $y \in \Psi$. Then*

$$D_x T_y = \begin{cases} q^2(q-1) D_{xy} & \text{if } y \notin \Gamma \\ (q-1) D_{xy} & \text{if } y \in \Gamma \end{cases} .$$

(3) *Let $x \in F_{q^2}^\times - \Psi$ and $y \in \mathbb{F}_{q^2}^\times$. Then $D_x U_y = \dfrac{q(q^2-1)}{\gamma} D_x$.*

Proof. The three assertions follow from the fact that the product of an element in the conjugacy class of $r = \hat{M}(x_1, y_1, z_1)$ of N and an element in the conjugacy class of $s = \hat{M}(x_2, y_2, z_2)$ of N is an element of the form $\hat{M}(x_1 x_2, \alpha, \beta)$, for some α and β in $\mathbb{F}_{q^2}$. In each assertion, the assumption implies that all these elements are in the conjugacy class of $t = d_{x_1 x_2}$, since $x_1 x_2 \in \mathbb{F}_{q^2} - \Psi$. It follows that there exists an integer m such that $r^+ s^+ = m D_{x_1 x_2}$.

Now the augmentation map $\varepsilon : kN \to k$ restricts to a ring homomorphism $ZkN \to k$, sending x^+ to $|x^G|$. Hence $|r^N||s^N| = m|t^N|$. For the three assertions, we can assume that $r = d_x$ and $x \notin \Psi$, thus $|r^N| = q^3$. Similarly $t = d_{xy}$ for Assertions (1) and (2), and $xy \notin \Psi$, so $|t^N| = q^3$. For Assertion (3), we have $t = d_x$, so $|t^N| = q^3$ again. It follows that the integer m is equal to $|s^N|$, and $s = d_y$ in Assertion (1), $s = t_y$ in Assertion (2), and $s = u_y$ in Assertion (3). Now Proposition 26 follows from the values of the cardinalities $|s^N|$ given by Proposition 24. □

Proposition 27. *Let $x, y \in \mathbb{F}_{q^2} - \Psi$, such that $xy \in \Psi - \Gamma$. Then $D_x D_y = q^3 D_{xy} + q^3 T_{xy}$.*

Proof. Any element in the product $d_x^N \cdot d_y^N$ is of the form $\hat{M}(xy, \alpha, \beta)$, for some $\alpha, \beta \in \mathbb{F}_{q^2}$. It follows that there are integers a and b such that $D_x D_y = a D_{xy} + b T_{xy}$. Setting $z = xy$, the integer a is equal to $m_{d_x, d_y}^{d_z}$. Thus $a|d_z^N| = m_{d_z, d_y^{-1}}^{d_x} |d_x^N|$, by Lemma 25. But by Proposition 26, we have $D_zD_{y^{-1}} = q^2D_x$, so $m^{d_x}_{d_z,d_y^{-1}} = q^2$. It follows that $a|z^N| = aq^2 = q^2q^3$, thus $a = q^3$. Taking augmentation gives

$$\varepsilon(D_xD_y) = q^6 = a\varepsilon(D_z) + b\varepsilon(T_z) = aq^2 + bq^2(q-1) \quad .$$

It follows that $b = \dfrac{q^6 - q^5}{q^2(q-1)} = q^3$. □

Proposition 28. *Let $x \in \Psi$. Then $D_xT_1 = T_x$.*

Proof. If $x \in \Gamma$, there is nothing to prove, because D_x is equal to the identity, in this case. If $x \notin \Gamma$, then D_xT_1 is a sum of elements of the form $\hat{M}(x, \alpha, \beta)$, so there are natural integers a and b such that $D_xT_1 = aD_x + bT_x$. Taking augmentation of this equality gives $q^2(q-1) = aq^2 + bq^2(q-1)$, that is $q - 1 = a + b(q-1)$. Since the product d_xt_1 is equal to t_x, it follows that $b > 0$. Hence $b = 1$ and $a = 0$. □

Proposition 29. *Let $x \in \Psi - \Gamma$, and $y \in \mathbb{F}^\times_{q^2}$. Then $D_xU_y = \dfrac{q^2-1}{\gamma}(D_x + T_x)$.*

Proof. Again D_xU_y is a sum of elements of N of the form $\hat{M}(x, \alpha, \beta)$. Hence there are natural integers a and b such that $D_xU_y = aD_x + bT_x$. The integer a is equal to $m^{d_x}_{d_x,u_y}$, i.e.

$$a = |\{(d', u') \in d_x^N \times u_y^N \mid d'u' = d_x\}| \quad .$$

By Proposition 24, the element $d' \in d_x^N$ is equal to $\hat{M}\big(x, w(\overline{x}^2 - x), w\overline{w}(\overline{x}^2 - x)\big)$, for $w \in \mathbb{F}_{q^2}$, and the element u' is equal to $\hat{M}(1, v, v\overline{v}\tau + \lambda\omega)$, for $v \in x\mathrm{L}$ and $\lambda \in \mathbb{F}_q$. Now

$$d'u' = \hat{M}\big(x, xv + w(\overline{x}^2 - x), x(v\overline{v}\tau + \lambda\omega) - w\overline{v}(\overline{x}^2 - x) + w\overline{w}(\overline{x}^2 - x)\big) \quad .$$

This is equal to d_x if and only if

$$xv + w(\overline{x}^2 - x) = 0 \;\text{ and }\; x(v\overline{v}\tau + \lambda\omega) - w\overline{v}(\overline{x}^2 - x) + w\overline{w}(\overline{x}^2 - x) = 0 \quad .$$

Since $x \notin \Gamma$, the first relation gives $w = \dfrac{v}{1 - \overline{x}^3}$. Multiplying by $\overline{x}$, the second one reads

$$v\overline{v}\tau + \lambda\omega - w\overline{v}(\overline{x}^3 - 1) + w\overline{w}(\overline{x}^3 - 1) = 0 \quad .$$

This gives

$$v\overline{v}\tau + \lambda\omega + v\overline{v} - \frac{v\overline{v}}{1 - x^3} = 0 \quad ,$$

that is

$$\lambda = \frac{1}{\omega}\big(\overline{\tau} + \frac{1}{1 - x^3}\big) \quad .$$

This defines an element λ of $\mathbb{F}_q$, since $\tau + \overline{\tau} = -1$ and

$$\frac{1}{1 - x^3} + \frac{1}{1 - \overline{x}^3} = \frac{2 - x^3 - \overline{x}^3}{(1 - x^3)(1 - \overline{x}^3)} = 1 \quad .$$

In other words w and λ are determined by $v \in x\mathrm{L}$, which may be chosen arbitrarily. It follows that $a = \dfrac{q^2 - 1}{\gamma}$.

Now applying the augmentation to the relation $D_xU_y = aD_x + bT_x$ gives

$$q^2\frac{q(q^2 - 1)}{\gamma} = aq^2 + bq^2(q-1) \quad .$$

It follows that

$$\frac{q(q^2 - 1)}{\gamma} = \frac{q^2 - 1}{\gamma} + b(q-1) \quad ,$$

hence $b = \dfrac{q^2 - 1}{\gamma}$. □

Proposition 30.

(1) *Let $x \in \Psi - \Gamma$. Then*
$$D_x D_{x^{-1}} = q^2\mathrm{Id} + q \sum_{y\in\mathbb{F}_{q^2}^\times/\mathrm{L}} U_y \quad .$$

(2) *Let $x \in \mathbb{F}_{q^2}^\times - \Psi$. Then*
$$D_x D_{x^{-1}} = q^3\mathrm{Id} + q^3 T_1 + q^3 \sum_{y\in\mathbb{F}_{q^2}^\times/\mathrm{L}} U_y \quad .$$

Proof. For $x \in \mathbb{F}_{q^2}^\times$, the product $D_x D_{x^{-1}}$ is a sum of elements of the form $\hat{M}(1,\alpha,\beta)$ of N. So there are integers $a, b, c_y \in \mathbb{N}$, for $y \in \mathbb{F}_{q^2}^\times/\mathrm{L}$ such that

$$(***) \qquad D_x D_{x^{-1}} = a\mathrm{Id} + bT_1 + \sum_{y\in\mathbb{F}_{q^2}^\times/\mathrm{L}} c_y U_y \quad .$$

Then $a = m^{\mathrm{Id}}_{d_x, d_{x^{-1}}} = |\{(d', d'') \in d_x^N \times d_{x^{-1}}^N \mid d'd'' = \mathrm{Id}\}| = |d_x^N|$. Thus $a = q^2$ if $x \in \Psi - \Gamma$, and $a = q^3$ if $x \in \mathbb{F}_{q^2}^\times - \Psi$.

On the other hand, by Lemma 25, for $y \in \mathbb{F}_{q^2}^\times$,
$$c_y|u_y^N| = m^{u_y}_{d_x,d_{x^{-1}}}|u_y^N| = m^{d_x}_{u_y,d_x}|d_x^N|$$

- If $x \in \Psi - \Gamma$, then $m^{d_x}_{u_y,d_x} = \dfrac{q^2-1}{\gamma}$, by Proposition 29. It follows that
$$c_y\frac{q(q^2-1)}{\gamma} = \frac{q^2-1}{\gamma}q^2 \quad ,$$
hence $c_y = q$.

  Applying augmentation to equation (***), we get $q^2q^2 = a + b(q-1) + q\cdot\gamma q\dfrac{q^2-1}{\gamma}$. This gives $b(q-1) = q^4 - q^2 - q^2(q^2-1) = 0$, which proves Assertion (1).
- If $x \in \mathbb{F}_{q^2}^\times - \Psi$, then $m^{d_x}_{u_y,d_x} = \dfrac{q(q^2-1)}{\gamma}$ by Proposition 26. Thus $c_y = q^3$ in this case. Applying augmentation to equation (***) gives
$$q^3\cdot q^3 = q^3 + b(q-1) + q^3\gamma\cdot\frac{q(q^2-1)}{\gamma} \quad ,$$
that is $b(q-1) = q^6 - q^3 - q^4(q^2-1) = q^3(q-1)$, hence $b = q^3$, which proves Assertion (2).

□

Proposition 31. *Let $x, y \in \Psi - \Gamma$ such that $xy \notin \Gamma$. Then $D_xD_y = D_{xy} + (q+1)T_{xy}$.*

Proof. The product D_xD_y is a sum of elements of N of the form $\hat{M}(xy,\alpha,\beta)$, so there are integers a and b such that $D_xD_y = aD_{xy} + bT_{xy}$. The integer a is the number of pairs (d', d'') in $d_x^N \times d_y^N$ such that $d'd'' = d_{xy}$.

By Proposition 24, the class d_x^N consists of the elements $\hat{M}\big(x, \alpha(\overline{x}^2 - x), \alpha\overline{\alpha}(\overline{x}^2 - x)\big)$, for $\alpha \in \mathbb{F}_{q^2}$. Equivalently, in a form that will be more convenient for computation, it consists of the elements $d' = \hat{M}(x, u, v)$, for $u \in \mathbb{F}_{q^2}$ and $v = \dfrac{u\overline{u}}{x^2 - \overline{x}}$. Similarly, the class d_y^N consist of the elements $d'' = \hat{M}(y, r, s)$, for $r \in \mathbb{F}_{q^2}$ and $s = \dfrac{r\overline{r}}{y^2 - \overline{y}}$. Since $x\overline{x} = 1 = y\overline{y}$, we have
$$d'd'' = \begin{pmatrix} x & u & v \\ 0 & \overline{x}^2 & -\overline{u}\,\overline{x} \\ 0 & 0 & x \end{pmatrix}\begin{pmatrix} y & r & s \\ 0 & \overline{y}^2 & -\overline{r}\,\overline{y} \\ 0 & 0 & y \end{pmatrix} \quad .$$

The product $d'd''$ is equal to d_{xy} if and only if

$$xr + u\overline{y}^2 = 0 \ \text{ and } \ xs - u\overline{r}\,\overline{y} + vy = 0 \quad .$$

The first equation gives $r = -u\overline{x}\,\overline{y}^2$, thus $r\overline{r} = u\overline{u}$. Now the second equation becomes

$$\frac{xu\overline{u}}{y^2 - \overline{y}} + u\overline{u}xy + \frac{yu\overline{u}}{x^2 - \overline{x}} = 0 \quad .$$

Then either $u = 0$, hence $r = s = v = 0$, or

$$\frac{x}{y^2 - \overline{y}} + xy + \frac{y}{x^2 - \overline{x}} = 0 \quad .$$

Equivalently $(x^3 - 1) + (x^3 - 1)(y^3 - 1) + (y^3 - 1) = 0$, thus $x^3y^3 = 1$, which doesn't hold since $xy \notin \Gamma$, using the remark after Lemma 18.

So the only pair $(d', d'') \in d_x^N \times d_y^N$ such that $d'd'' = d_{xy}$ is the pair (d_x, d_y). It follows that $a = 1$.

Applying augmentation to the equality $D_xD_y = aD_{xy} + bT_{xy}$ now gives $q^4 = q^2 + bq^2(q-1)$, hence $b = q + 1$ □

Proposition 32. *Let $x \in \Psi - \Gamma$ and $y \in \mathbb{F}_{q^2}^\times$ with $xy \notin \Gamma$. Then*

$$D_xT_y = (q^2 - 1)D_{xy} + (q^2 - q - 1)T_{xy} \quad .$$

Proof. The product D_xT_y is a sum of elements of the form $\hat{M}(xy, \alpha, \beta)$, so there are integers a and b such that $D_xT_y = aD_{xy} + bT_{xy}$. By Lemma 25, Proposition 24, and Proposition 31, we have

$$aq^2 = m_{d_x,t_y}^{d_{xy}} |d_{xy}^N| = m_{d_{xy},d_x^{-1}}^{t_y} q^2(q-1) = q^2(q^2 - 1) \quad ,$$

hence $a = q^2 - 1$. Taking augmentation gives

$$\varepsilon(D_xT_y) = q^2q^2(q-1) = a\varepsilon(D_{xy}) + b\varepsilon(T_{xy}) = (q^2 - 1)q^2 + bq^2(q-1) \quad ,$$

hence $b = q^2 - q - 1$. □

Proposition 33. (1) $T_1^2 = (q-1)\mathrm{Id} + (q-2)T_1$.
(2) *If $x \in \Psi - \Gamma$, then $T_xT_1 = (q-1)D_x + (q-2)T_x$.*

Proof. By Proposition 24, the product of any two conjugates of t_1 is either the identity, or again a conjugate of t_1. It follows that there are integers a and b such that $T_1^2 = a\mathrm{Id} + bT_1$. Moreover a is equal to the cardinality of the conjugacy class of t_1, that is $a = q - 1$. Now taking augmentation gives $(q-1)^2 = a + (q-1)b$, hence $b = q - 2$. Now for $x \in \Psi - \Gamma$,

$$T_xT_1 = D_xT_1^2 = (q-1)D_x + (q-2)T_x \quad ,$$

since $D_xT_1 = T_x$ by Proposition 28. □

Proposition 34. *Let $x \in \Psi - \Gamma$. Then $D_xT_{x^{-1}} = q^2T_1 + q(q-1) \sum\limits_{y \in \mathbb{F}_{q^2}^\times/\mathrm{L}} U_y$.*

Proof. Again $D_xT_{x^{-1}}$ is a sum of elements of the form $\hat{M}(1, \alpha, \beta)$, so there are integers a, b, and c_y, for $y \in \mathbb{F}_{q^2}^\times/\mathrm{L}$, such that $D_xT_{x^{-1}} = a\mathrm{Id} + bT_1 + \sum\limits_{y \in \mathbb{F}_{q^2}^\times/\mathrm{L}} c_yU_y$. Since $t_{x^{-1}} = t_x^{-1}$, and since no conjugate of d_x is a conjugate of t_x, we have $a = 0$. Then $b = m_{d_x,t_{x^{-1}}}^{t_1}$, hence $b(q-1) = m_{t_1,d_x}^{t_x} q^2(q-1) = q^2(q-1)$, by Proposition 28. Hence $b = q^2$. Similarly $c_y = m_{d_x,t_{x^{-1}}}^{u_y}$, so $c_y\dfrac{q(q^2-1)}{\gamma} = m_{u_y,d_{x^{-1}}}^{t_{x^{-1}}} q^2(q-1)$, hence $c_y\dfrac{q(q^2-1)}{\gamma} = \dfrac{q^2-1}{\gamma}q^2(q-1)$, thus $c_y = q(q-1)$. □

Proposition 35. *Let $x \in \Psi - \Gamma$ and $y \in \mathbb{F}_{q^2}$. Then $T_xU_y = \dfrac{(q^2-1)(q-1)}{\gamma}(D_x + T_x)$.*

Proof. By Proposition 28 and Proposition 29, we have that

$$\begin{aligned} T_xU_y = D_xT_1U_y &= \frac{(q^2-1)}{\gamma}(D_x+T_x)T_1 \\ &= \frac{(q^2-1)}{\gamma}\big(T_x+(q-1)D_x+(q-2)T_x\big) \\ &= \frac{(q^2-1)(q-1)}{\gamma}(D_x+T_x) \end{aligned}$$

□

Proposition 36. *Let $x \in \Psi - \Gamma$. Then*

$$T_xT_{x^{-1}} = q^2(q-1)\mathrm{Id} + q^2(q-2)T_1 + q(q-1)^2 \sum_{y\in \mathbb{F}_{q^2}^\times/\mathrm{L}} U_y \quad .$$

Proof. Indeed by Proposition 30, Proposition 28, Proposition 33 and Proposition 34

$$\begin{aligned} T_xT_{x^{-1}} &= D_xT_1D_{x^{-1}}T_1 \\ &= D_xD_{x^{-1}}T_1^2 \\ &= D_xD_{x^{-1}}\big((q-1)\mathrm{Id}+(q-2)T_1\big) \\ &= D_x\big((q-1)D_{x^{-1}}+(q-2)T_{x^{-1}}\big) \\ &= (q-1)\Big(q^2\mathrm{Id}+q\sum_{y\in \mathbb{F}_{q^2}^\times/\mathrm{L}} U_y\Big)+(q-2)\Big(q^2T_1+q(q-1)\sum_{y\in \mathbb{F}_{q^2}^\times/\mathrm{L}} U_y\Big) \\ &= q^2(q-1)\mathrm{Id}+q^2(q-2)T_1+q(q-1)^2\sum_{y\in \mathbb{F}_{q^2}^\times/\mathrm{L}} U_y \quad . \end{aligned}$$

□

Proposition 37. *Let $x, y \in \Psi - \Gamma$ such that $xy \notin \Gamma$. Then*

$$T_xT_y = (q-1)(q^2-q-1)D_{xy} + \big(q(q-1)^2+1\big)T_{xy} \quad .$$

Proof. Indeed, by Proposition 31, Proposition 28 and Proposition 33

$$\begin{aligned} T_xT_y &= D_xT_1D_yT_1 \\ &= \big(D_{xy}+(q+1)T_{xy}\big)\big((q-1)\mathrm{Id}+(q-2)T_1\big) \\ &= (q-1)D_{xy}+(q-2)T_{xy}+(q^2-1)T_{xy}+(q-2)(q+1)\big((q-1)D_{xy}+(q-2)T_{xy}\big) \\ &= (q-1)(q^2-q-1)D_{xy}+\big(q(q-1)^2+1\big)T_{xy} \end{aligned}$$

□

Proposition 38. *Let $x \in \mathbb{F}_{q^2}^\times$. Then $T_1U_x = (q-1)U_x$.*

Proof. The product T_1U_x is a linear combination of elements of N of the form $\hat{M}(1, \alpha, \beta)$. Hence there are integers a, b and c_y, for $y \in \mathbb{F}_{q^2}^\times/\mathrm{L}$, such that

$$(\#) \qquad T_1U_x = a\mathrm{Id} + bT_1 + \sum_{y\in \mathbb{F}_{q^2}^\times/\mathrm{L}} c_yU_y \quad .$$

Observe now that t_1 and u_x^{-1} are not conjugate in N, e.g. because the conjugacy class of t_1 has cardinality $q-1$, and the conjugacy class of u_x has cardinality $\dfrac{q(q^2-1)}{\gamma} \neq q-1$. It follows that $a = 0$.

Now by Proposition 24, the conjugacy class of T_1 consists of the elements $\hat{M}(1, 0, \lambda\omega)$, for $\lambda \in \mathbb{F}_q^\times$, and the conjugacy class of u_x consists of the elements $\hat{M}(1, v, v\overline{v}\tau + \mu\omega)$, for $v \in x\mathrm{L}$ and $\mu \in \mathbb{F}_q$. The product $\pi = \hat{M}(1, 0, \lambda\omega)\hat{M}(1, v, v\overline{v}\tau + \mu\omega)$ is equal to $u_y = \hat{M}(1, y, y\overline{y}\tau)$ if and only if $v = y$ and $v\overline{v}\tau + \mu\omega + \lambda\omega = y\overline{y}\tau$. It follows that $c_y = 0$ unless $y \in x\mathrm{L}$, i.e. unless $y\mathrm{L} = x\mathrm{L}$. If $y\mathrm{L} = x\mathrm{L}$, then u_y is conjugate to u_x in N, and we can assume that $y = x$. In this case $\pi = u_x$ if and only if $v = x$ and $\mu = -\lambda$. It follows that $c_x = q - 1$.

Applying augmentation to Equation (#) now gives '

$$(q-1)\cdot\frac{q(q^2-1)}{\gamma} = b(q-1) + (q-1)\cdot\frac{q(q^2-1)}{\gamma} \quad ,$$

hence $b = 0$. □

Proposition 39. (1) *If $3 \nmid q+1$, then $\mathrm{L} = \mathbb{F}_{q^2}^\times$, and*

$$U_1^2 = q(q^2-1)\mathrm{Id} + q(q^2-1)T_1 + q(q^2-2)U_1 \quad .$$

(2) *If $3 \mid q+1$, then $\mathbb{F}_{q^2}/\mathrm{L} = \{\mathrm{L}, t\mathrm{L}, t^2\mathrm{L}\}$, where t is any non cube element of $\mathbb{F}_{q^2}^\times$. Let $l = |\{v \in \mathrm{L} \mid 1 - v \in \mathrm{L}\}|$, $m = |\{v \in \mathrm{L} \mid t - v \in \mathrm{L}\}|$, and $n = |\{v \in \mathrm{L} \mid t - v/t \in \mathrm{L}\}|$. Then for $x \in \mathbb{F}_{q^2}^\times/\mathrm{L}$,*

$$\begin{aligned} U_x^2 &= \frac{q(q^2-1)}{\gamma}(\mathrm{Id} + T_1) + qlU_x + qm(U_{tx} + U_{t^2x}) \\ U_xU_{tx} &= qnU_{t^2x} + qm(U_x + U_{tx}) \quad . \end{aligned}$$

Proof. By Proposition 24, for $x \in \mathbb{F}_{q^2}^\times$, the conjugacy class of u_x in N consists of the elements $\hat{M}(1, v, v\overline{v}\tau + \lambda\omega)$, for $v \in x\mathrm{L}$ and $\lambda \in \mathbb{F}_q$. Since the inverse of $u_x = \hat{M}(1, x, x\overline{x}\tau)$ is $\hat{M}(1, -x, x\overline{x}\tau)$, and since $-x \in x\mathrm{L}$ as $-1 = (-1)^\gamma \in \mathrm{L}$, we have that u_x^{-1} is conjugate to u_x.

For $x, y \in \mathbb{F}_{q^2}^\times$, the product U_xU_y is a sum of elements of the form $\hat{M}(1, \alpha, \beta)$, hence there are integers a, b and $c_{x,y}^z$, for $z \in \mathbb{F}_{q^2}^\times/\mathrm{L}$, such that

$$(\#\#) \qquad U_xU_y = a\mathrm{Id} + bT_1 + \sum_{z\in\mathbb{F}_{q^2}^\times/\mathrm{L}} c_{x,y}^z U_z \quad .$$

Note that for $x, y, z \in \mathbb{F}_{q^2}^\times$, we have

$$c_{x,y}^z|u_z^N| = m_{u_x,u_y}^{u_z}\frac{q(q^2-1)}{\gamma} = m_{u_z,u_x^{-1}}^{u_y}\frac{q(q^2-1)}{\gamma} = c_{z,x}^y\frac{q(q^2-1)}{\gamma} = c_{z,x}^y|u_z^N| \quad ,$$

as u_x^{-1} is conjugate to u_x. So $c_{x,y,z}$ is a symmetric function of x, y, z.

If $x\mathrm{L} \neq y\mathrm{L}$, then no conjugate of u_x^{-1} is conjugate to u_y, so $a = 0$. In this case, we also have

$$(\#\#\#) \qquad b|t_1^N| = m_{u_x,u_y}^{t_1}(q-1) = m_{t_1,u_x^{-1}}^{u_y}|u_y^N| \quad ,$$

and $m_{t_1,u_x^{-1}}^{u_y} = 0$ by Proposition 38. It follows that $b = 0$ in this case.

If $x\mathrm{L} = y\mathrm{L}$, i.e. $U_x = U_y$, then clearly $a = |u_x^N| = \dfrac{q(q^2-1)}{\gamma}$. Moreover Equation (###) gives $b(q-1) = (q-1)|u_y^N|$, hence $b = \dfrac{q(q^2-1)}{\gamma}$.

In the case $3 \nmid q+1$, we have $\gamma = 1$ and $\mathrm{L} = \mathbb{F}_{q^2}^\times$. Then

$$U_1^2 = q(q^2-1)(\mathrm{Id} + T_1) + c_{1,1}^1U_1 \quad .$$

Taking augmentation gives

$$\big(q(q^2-1)\big)^2 = q(q^2-1)(1 + q - 1) + c_{1,1}^1q(q^2-1) \quad ,$$

hence $c_{1,1}^1 = q(q^2-2)$, which completes the proof of Assertion (1).

In the case $3 \mid q+1$, then $\gamma = 3$, and L has index 3 in $\mathbb{F}_{q^2}^\times$, so $\mathbb{F}_{q^2}^\times/\mathrm{L} = \{1, t\mathrm{L}, t^2\mathrm{L}\}$ for any non cube element t of $\mathbb{F}_{q^2}^\times$.

For $x, y, z \in \mathbb{F}_{q^2}^\times$, the product of the element $u' = \hat{M}(1, v, v\overline{v}\tau + \lambda\omega)$ in the conjugacy class of u_x (where $v \in x\mathrm{L}$ and $\lambda \in \mathbb{F}_q$) by the element $u'' = \hat{M}(1, r, r\overline{r}\tau + \mu\omega)$ in the conjugacy class of u_y (where $r \in y\mathrm{L}$ and $\mu \in \mathbb{F}_q$) is equal to u_z if and only if

$$v + r = z \quad \text{and} \quad r\overline{r}\tau + \mu\omega - v\overline{r} + v\overline{v}\tau + \lambda\omega = z\overline{z}\tau \quad .$$

The second equation determines μ once v, r and λ are known, and λ can be chosen arbitrarily in $\mathbb{F}_q$, once v and r satisfy $v + r = z$. Hence in Equation (##), we have

$$c_{x,y}^z = q\,\big|\{v \in x\mathrm{L} \mid z - v \in y\mathrm{L}\}\big| \quad .$$

In particular for any $x \in \mathbb{F}_{q^2}^\times$

$$c_{x,x}^x = q\,\big|\{v \in x\mathrm{L} \mid x - v \in x\mathrm{L}\}\big| = q\,\big|\{w \in \mathrm{L} \mid x - xw \in x\mathrm{L}\}\big| = l \quad .$$

Similarly

$$c_{x,x}^{xt} = q\,\big|\{v \in x\mathrm{L} \mid xt - v \in x\mathrm{L}\}\big| = q\,\big|\{w \in \mathrm{L} \mid xt - xw \in x\mathrm{L}\}\big| = m \quad .$$

Finally

$$c_{x,xt}^{xt^2} = q\,\big|\{v \in x\mathrm{L} \mid xt^2 - v \in xt\mathrm{L}\}\big| = q\,\big|\{w \in \mathrm{L} \mid t^2 - w \in t\mathrm{L}\}\big| = n \quad .$$

This completes the proof, since $c_{x,y}^z$ is symmetric in x, y, z. □

Remark 40. Applying augmentation to the equations of Proposition 39 gives that $n = l+1$ and $n + 2m = \dfrac{q^2-1}{3}$. So it suffices to know l, and then m and n can be computed.

By definition $l = |\{v \in \mathrm{L} \mid 1 - v \in \mathrm{L}\}|$. Since $3 \mid q + 1 \mid q^2 - 1$, the field $\mathbb{F}_{q^2}$ contains all cubic roots of unity. Now clearly

$$l = |\{(x, y) \in \mathbb{F}_{q^2}^\times \times \mathbb{F}_{q^2}^\times \mid x^3 + y^3 = 1\}|/9 \quad ,$$

since multiplying x or y by any cubic root of unity doesn't change x^3 nor y^3. It follows that $9l$ is almost equal to the number of points of the elliptic curve $x^3 + y^3 = z^3$ over $\mathbb{F}_{q^2}$: the difference consists of three points $(\theta, 0, 1)$ of the projective plane over $\mathbb{F}_{q^2}$, where θ is any cubic root of 1, three points $(0, \theta, 1)$, and three points $(\theta, -1, 0)$. It follows that $9l = N_2 - 9$, where N_2 is the number of points over $\mathbb{F}_{q^2}$ of the Fermat cubic E with equation $x^3+y^3 = z^3$.

Now this is an elliptic curve, and by [7, (2.6)], the zeta function of E can be defined as

$$Z_E(u) = \exp\Big(\sum_{m\geq 1} N_m \frac{u^m}{m}\Big) \quad ,$$

where N_m is the number of points of E over $\mathbb{F}_{q^m}$. By [7, Theorem 2.8], it has the following form

$$Z_E(u) = \frac{1 - au + qu^2}{(1-u)(1-qu)} \quad ,$$

where $a = 1 + q - N_1$. Comparing the terms of degree 2 in u in the expansion of those two expressions of $Z_E(u)$ as series in u gives $N_2 = N_1\big(2(q + 1) - N_1\big)$.

Now since $3 \mid q+1$, it follows that $3 \nmid q-1$, and $x \mapsto x^3$ is a bijection of $\mathbb{F}_q$. Hence E has as many points over $\mathbb{F}_q$ as the projective line with equation $x + y = z$, that is $N_1 = q + 1$. Hence $N_2 = (q + 1)^2$, which gives the following values for l, n and m:

$$l = \Big(\frac{q+1}{3}\Big)^2 - 1, \quad m = \frac{q^2 - q - 2}{9}, \quad n = \Big(\frac{q+1}{3}\Big)^2 \quad .$$

Theorem 41. *Let k be a field of characteristic p. Then:*

(1) *The radical $J(ZkN)$ of the center of the group algebra kN has a k-basis consisting of the elements D_x, for $x \in \mathbb{F}_{q^2}^\times/\Gamma - \{\Gamma\}$, T_x, for $x \in \Psi/\Gamma - \{\Gamma\}$, $T_1 + \mathrm{Id}$, and U_x, for $x \in \mathbb{F}_{q^2}^\times/\mathrm{L}$. In particular, the dimension of $J(ZkN)$ is equal to $\dfrac{q^2+q}{\gamma} + \gamma - 1$.*

(2) *The square* $J^2(ZkN)$ *of* $J(ZkN)$ *has a* k *basis consisting of the elements* $D_x + T_x$, *where* $x \in \Psi/\Gamma - \{\Gamma\}$. *In particular, the dimension of* $J^2(ZkN)$ *is equal to* $\frac{q+1}{\gamma} - 1$.
(3) *The cube* $J^3(ZkN)$ *of* $J(ZkN)$ *is equal to 0.*

Proof. As the group algebra kN is indecomposable when k is a field of characteristic p, the radical $J(ZkN)$ is equal to the kernel of the augmentation $\varepsilon : ZkN \to k$. If X is the sum of the elements of a conjugacy class C of N, then $\varepsilon(X) = |C|$, and by Proposition 24, this is a multiple of p, unless C is the class of the identity element of N, or C is the class of t_1, and $|C| = q-1$ in this case. It follows that the elements listed in Assertion (1) generate $J(ZkN)$. Moreover, they are obviously linearly independent, so they form a basis $\mathcal{B}$ of $J(ZkN)$.

Now by Proposition 28, for $x \in \Psi - \Gamma$, we have that $D_x(\mathrm{Id} + T_1) = D_x + T_x$ in ZkN, so the elements $D_x + T_x$, where $x \in \Psi/\Gamma - \{\Gamma\}$, are indeed in $J^2(ZkN)$, and they are clearly linearly independent. Moreover, reducing mod p the formulas for products stated in Propositions 26 to 39, one checks easily that any product of two elements of the basis $\mathcal{B}$ is equal to a (possibly zero) scalar multiple of an element $D_x + T_x$, for some $x \in \Psi - \Gamma$, and that the product of any three elements of $\mathcal{B}$ vanishes. This completes the proof of Theorem 41. □

If k is a field of characteristic p it is not difficult to give the explicit structure of $Z(kN)$ as a quotient of a polynomial ring in several variables.

Proposition 42. *Let* γ *be the greatest common divisor of* 3 *and* $q+1$, *and let*

$$\Gamma := \{x \in \mathbb{F}_{q^2} \mid x^\gamma = 1\}, \;\; \Psi := \{x \in \mathbb{F}_{q^2} \mid x^{q+1} = 1\}, \;\; \mathrm{L} := \{a^\gamma \mid a \in \mathbb{F}_{q^2}^\times\} \quad .$$

Let $\mathfrak{U} := \mathbb{F}_{q^2}^\times/\Gamma$, *let* $\mathfrak{V} := \Psi/\Gamma$ *and let* $\mathfrak{W} := \mathbb{F}_{q^2}^\times/\mathrm{L}$. *Let* k *be a field of characteristic* $p > 0$ *and let* N *be the normaliser of a Sylow* p*-subgroup of* $PSU(3,q)$, *where* p *divides* q. *Then,*

$$Z(kN) \simeq k[T, X_n, Y_m \mid n \in \mathfrak{W}, m \in \mathfrak{U}]/I$$

where I *is the ideal generated by*

$$T^2,\ TX_{n_1},\ TY_{m_1},\ X_{n_1}X_{n_2},\ X_{n_1}Y_{m_1},\ Y_{m_1}Y_{m_2},$$
$$X_{n_1}Y_{m_2} + \frac{1}{\gamma}X_{n_1}T,\ Y_{m_2}Y_{m_3} - (1 - \delta_{m_2,m_3^{-1}})X_{m_2m_3}T$$

where

$$n_1, n_2 \in \mathfrak{W}, m_1 \in \mathfrak{U} - \mathfrak{V}, m_2, m_3 \in \mathfrak{V}$$

and $\delta_{a,b}$ *is the Kronecker symbol.*

Proof. We have a basis of $Z(kN)$ given in Theorem 41 by the elements D_x, for $x\Gamma \in \mathbb{F}_{q^2}^\times/\Gamma$, T_x, for $x\Gamma \in \Psi/\Gamma - \{\Gamma\}$, $T_1 + \mathrm{Id}$, and U_x, for $x\mathrm{L} \in \mathbb{F}_{q^2}^\times/\mathrm{L}$. Observe that $D_1 = 1$. Moreover, by Proposition 28 we do not need to include T_x as variable of the polynomial ring. This element is already the product of T_1 and U_x.

We obtain the following multiplication table.

	$T_1 + id$	U_y	D_y $(y \notin \Psi)$	D_y $(y \in \Psi - \Gamma)$
$T_1 + id$	0 Prop. 33	0 Prop. 38	0 Prop. 26(2)	$T_y + D_y$ Props. 28
U_x	0 Prop. 38	0 Prop. 39	0 Prop. 26(3)	$-\frac{1}{\gamma}(D_x + T_x)$ Prop. 29
D_x $(x \notin \Psi)$	0 Prop. 26(2)	0 Prop. 26(3)	0 Props. 27,26(1),30	0 Prop. 26(1)
D_x $(x \in \Psi - \Gamma)$	$T_x + D_x$ Prop. 28	$-\frac{1}{\gamma}(D_x + T_x)$ Prop. 29	0 Prop. 26(1)	$(1 - \delta_{xy\Gamma,\Gamma})(T_{xy} + D_{xy})$ Props. 31,30

Now, mapping T to $T_1 + id$, X_n to U_n and Y_m to D_m gives an algebra homomorphism of the corresponding polynomial ring with kernel precisely the ideal I. □

References

[1] Maurice Auslander, Idun Reiten and Sverre Smalø, Representation Theory of Artin Algebras, Cambridge University Press 1995.

[2] Michel Broué, *Equivalences of blocks of group algebras.* In: *Finite dimensional algebras and related topics.* Vlasta Dlab and Leonard L.Scott (eds.), Kluwer, 1994, 1-26.

[3] Charles W. Curtis and Irving Reiner, Methods of Representation Theory Vol. 1, Wiley Interscience, New York 1990.

[4] GAP – Groups, Algorithms, and Programming, Version 4.7.6, The GAP Group, `http://www.gap-system.org`,

[5] Bertram Huppert, Endliche Gruppen I, Springer Verlag Berlin 1983.

[6] Bernhard Keller and Dieter Vossieck, *Sous les catégories dérivées*, Comptes Rendus de l'Académie des Sciences Paris **305** (1987) 225-228.

[7] AA. M. Robert, *Elliptic curves.* Lecture Notes in Mathematics no 326, Springer (1973).

[8] Yuming Liu, *Summands of stable equivalences of Morita type.* Communications of Algebra **36** (2008), no. 10, 3778-3782.

[9] Yuming Liu, Guodong Zhou and Alexander Zimmermann, *Higman ideal, stable Hochschild homology and Auslander-Reiten conjecture*, Mathematische Zeitschrift **270** (2012) 759-781.

[10] Yuming Liu, Guodong Zhou and Alexander Zimmermann, *Two questions on stable equivalences of Morita type*, preprint 2014.

[11] Jeremy Rickard, *Derived categories and stable equivalence*, Journal of Pure and Applied Algebra **61** (1989) 303-317.

[12] Jeremy Rickard, *Derived equivalences as derived functors*, Journal of the London Mathematical Society **43** (1991) 37-48.

[13] Jeremy Rickard, Some recent advances in modular representation theory. Algebras and modules, I (Trondheim, 1996), 157-178, CMS Conference Proceedings **23**, American Mathematical Society, Providence, Rhode Island, 1998.

[14] Alexander Zimmermann, Representation Theory; A homological algebra point of view, Springer Verlag London 2014.

S.B.: Université de Picardie,
LAMFA (UMR 7352 du CNRS),
33 rue St Leu,
F-80039 Amiens Cedex 1,
France

E-mail address: `serge.bouc@u-picardie.fr`

A.Z.: Université de Picardie,
Département de Mathématiques et LAMFA (UMR 7352 du CNRS),
33 rue St Leu,
F-80039 Amiens Cedex 1,
France

E-mail address: `alexander.zimmermann@u-picardie.fr`