An Explicit Presentation of the Grothendieck Ring of Finitely Generated $\mathbb{F}_q[SL_2(\mathbb{F}_q)]$-Modules

Davide A. Reduzzi
University of California at Los Angeles
davredu83@math.ucla.edu
November 1, 2011

Abstract

Let $p$ be a prime and $q = p^g$. We show that the Grothendieck ring of finitely generated $\mathbb{F}_q[SL_2(\mathbb{F}_q)]$-modules is naturally isomorphic to the quotient of the polynomial algebra $\mathbb{Z}[x]$ by the ideal generated by $f(x) = \sum_{j=0}^{\lfloor p/2 \rfloor} (-1)^j p^j (p-j) x^{p-2j}$, and the superscript $[g]$ denotes $g$-fold composition of polynomials. We conjecture that a similar result holds for simply connected semisimple algebraic groups defined and split over a finite field.

1 Introduction

In [5], J-P. Serre discovered a puzzling identity involving characteristic $p$ symmetric powers representations of the group $GL_2(\mathbb{F}_q)$, viewed as elements of the Grothendieck ring $K_0(GL_2(\mathbb{F}_q))$ of finitely generated $\mathbb{F}_q[GL_2(\mathbb{F}_q)]$-modules.

More precisely, fix a rational prime $p$, a positive integer $g$, and set $q = p^g$. Denote by $\mathbb{F}_q$ a field with $q$ elements and by $G$ the group $SL_2(\mathbb{F}_q) \subset GL_2(\mathbb{F}_q)$. For any non-negative integer $k$, denote by $M_k$ the $(k+1)$-dimensional representation $\text{Sym}^k \mathbb{F}_q^2$ of $G$. Motivated by the computation of the Euler-Poincaré characteristic of the twisted sheaf $\mathcal{O}(k)$ on $\mathbb{P}_q^1$, in [3] Serre extended the definition of the modules $M_k$'s for negative values of $k$, and showed that for any integer $k$ the following relation holds in the ring $K_0(G)$:

$$M_k - M_{k-(q+1)} = M_{k-(q-1)} - M_{k-2q}. \quad (\Sigma)$$

The dimensional shiftings by $q+1$ and $q-1$ occurring in Serre’s relation can be obtained by applying opportune intertwining operators $\Theta_q$ and $D$ to the symmetric powers modules. This has been exploited in [3] for the study of cohomological weight shiftings for elliptic modular forms modulo $p$.

Motivated by generalizations of the above considerations to Hilbert modular forms, families of generalized $\Theta_q$ and $D$ operators are defined in [4], and the following identity in $K_0(G)$ is proved for any integers $k, h$ and $i$:

$$M_k^{[i]} M_h^{[i+1]} - M_k^{[i]} M_{h-1}^{[i+1]} = M_k^{[i]} M_h^{[i+1]} - M_k^{[i]} M_{h-1}^{[i+1]} \quad (\Phi)$$

1
Here the superscript \([i]\) denote the \(i\)th Frobenius twisting on the corresponding virtual representation.

Using Glover’s product identity, one sees that \((\Phi)\) is equivalent to \((\Sigma)\) in case \(g = 1\), but it is stronger for \(g > 1\).

In this paper we apply formula \((\Phi)\) to determine an explicit presentation of the Grothendieck ring \(K_0(\mathcal{G})\). We treat the case of \(\mathcal{G} = SL_2(F_q)\) instead of \(GL_2(F_q)\), so we will not need to consider determinant twists that would make the set of relations more complicated; following the same methods we describe below, one could easily work with \(GL_2(F_q)\) instead.

Our main result is the following (cf. Theorem 3.6):

**Theorem 1.1** Denote by \(X\) the standard representation of \(\mathcal{G}\) on \(F_2^{q}\) and let \(x\) be an indeterminate over \(\mathbb{Z}\). The assignment \(X \mapsto x\) induces an isomorphism of rings:

\[
K_0(\mathcal{G}) \simeq \mathbb{Z}[x]/(f^g(x) - x) \mathbb{Z}[x],
\]

where \(f^g(x) = (f \circ \cdots \circ f)(x)\) is the polynomial of \(\mathbb{Z}[x]\) having degree \(p^g\) obtained by \(g\)-fold composition of the monic degree \(p\) polynomial:

\[
f(x) = \sum_{j=0}^{|p/2|} (-1)^j \frac{p}{p - j} \binom{p}{j} x^{p - 2j}.
\]

Proposition 3.9 gives an explicit closed formula for \(f^g(x)\). Notice that, since \(f(x) \equiv x^p (mod p\mathbb{Z}[x])\), the structure of the generic and special fibers of the ring \(K_0(\mathcal{G}) \otimes \mathbb{Z} p\) are easily determined (Corollary 3.7). On the other side, the arithmetic properties of the polynomial \(f(x)\) over \(\mathbb{Q}\) seem to be more complicated.

In the last paragraph of the paper we prove the following fact (Proposition 4.1): assume \(\mathcal{G}\) is a simply connected, semisimple algebraic group defined and split over \(F_q\). If \(\mathcal{M}\) is an \(F_q[\mathcal{G}]\)-rational module of finite \(F_q\)-dimension, then the multiplicity of an irreducible \(F_q[\mathcal{G}]\)-rational module \(V\) as a Jordan-Hölder constituent of \(\mathcal{M}[i]\) is congruent modulo \(p\) to the multiplicity of \(V\) as a Jordan-Hölder constituent of \(\mathcal{M} \otimes p^i\), for any positive integer \(i\).

Motivated by this result, we are led to conjecture that the Grothendieck ring of a Chevalley group arising from a rank \(\ell\) algebraic group \(G\) as above is isomorphic to the algebra

\[
\frac{\mathbb{Z}[x_1, \ldots, x_\ell]}{\left( \tilde{f}_1^g(x_1) - x_1, \ldots, \tilde{f}_\ell^g(x_\ell) - x_\ell \right) \mathbb{Z}[x_1, \ldots, x_\ell]},
\]

where for any \(i\), \(\tilde{f}_i^g(x_i)\) is the \(g\)-fold composition of the degree \(p\) monic polynomial \(f_i(x_i) \in \mathbb{Z}[x_i]\).

We conjecture that \(\tilde{f}_i(x_i) \equiv f_i^g(\mod p\mathbb{Z}[x_i])\) for any value of \(i\). Some of the evidence for this conjecture is presented at the end of paragraph 4.

**Conventions** All the group representations in this paper are left representations on a module of finite length over a fixed ring. If \(R\) is an algebra over a ring \(A\), and \(S\) is a subset of \(R\), the symbol \(A[S]\) denotes the \(A\)-subalgebra of \(R\) generated by \(S\).
2 Weight shiftings identities in $K_0(\mathfrak{S})$

Fix a rational prime $p$, a positive integer $g$, and set $q = p^g$. Denote by $\mathbb{F}_q$ a finite field with $q$ elements and fix an algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$; let $\sigma \in \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_p)$ be the arithmetic absolute Frobenius element. Denote by $\mathfrak{S}$ the group $SL_2(\mathbb{F}_q)$.

For any $i \in \mathbb{Z}$, the Frobenius power $\sigma^i$ induces a function $\mathfrak{S} \rightarrow \mathfrak{S}$ obtained by applying $\sigma^i$ to each entry of the matrices in $\mathfrak{S}$: composing this map with the action of $\mathfrak{S}$ on a given $\mathbb{F}_q[\mathfrak{S}]$-module $\mathcal{M}$ gives to the latter a new structure of $\mathfrak{S}$-module, that is denoted $\mathcal{M}^{[i]}$ and called the $i$th Frobenius twist of $\mathcal{M}$.

If $f : \mathcal{M} \longrightarrow \mathcal{N}$ is a homomorphism of $\mathbb{F}_q[\mathfrak{S}]$-modules and $i \in \mathbb{Z}$, we denote by $f^{[i]} : \mathcal{M}^{[i]} \longrightarrow \mathcal{N}^{[i]}$ the $\mathfrak{S}$-homomorphism defined by $f^{[i]}(x) = f(x)$ for all $x \in \mathcal{M}^{[i]}$.

Let $\mathfrak{X}$ denote the standard representation of $\mathfrak{S}$ on $\mathbb{F}_q^2$ and, for any positive integer $k$, define

$$\mathcal{M}_k = \text{Sym}^k \mathfrak{X}$$

to be the $k$th symmetric power of $\mathfrak{X}$, so that in particular $\mathfrak{X} = \mathcal{M}_1$. Let $\mathcal{M}_0$ be the trivial representation of $\mathfrak{S}$ on $\mathbb{F}_q$.

Observe that we can identify $\mathcal{M}_k$ with the $\mathbb{F}_q$-vector space of homogeneous degree $k$ polynomials over $\mathbb{F}_q$ in two variables $X$ and $Y$, endowed with the action of $\mathfrak{S}$ induced by:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot X = aX + cY, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot Y = bX + dY.$$

As a consequence of Steinberg’s restriction and tensor product theorems ([6]) we have:

**Proposition 2.1** All and only the irreducible representations of $\mathfrak{S}$ over $\mathbb{F}_q$ are of the form:

$$\bigotimes_{i=0}^{g-1} \mathcal{M}_i^{[k_i]}$$

where $k_0, \ldots, k_{g-1}$ are integers such that $0 \leq k_i \leq p - 1$ for $i = 0, \ldots, g - 1$, and the tensor products are over $\mathbb{F}_q$. Furthermore, the above representations are pairwise non-isomorphic.

Denote by $K_0(\mathfrak{S})$ the Grothendieck group of finitely generated $\mathbb{F}_q[\mathfrak{S}]$-modules. $K_0(\mathfrak{S})$ is isomorphic to the free abelian group generated by the isomorphism classes of irreducible representations of $\mathfrak{S}$ over $\mathbb{F}_q$, so that it has rank $q$ over $\mathbb{Z}$. If $\mathcal{M}$ is an $\mathbb{F}_q[\mathfrak{S}]$-module, we will denote by the same symbol $\mathcal{M}$ its class in $K_0(\mathfrak{S})$, if no confusion arises.

Tensor product over $\mathbb{F}_q$ induces on $K_0(\mathfrak{S})$ a structure of commutative ring with identity; we denote the product in $K_0(\mathfrak{S})$ by $\cdot$ or by simple juxtaposition. All the tensor products we will consider in the sequel are over $\mathbb{F}_q$, unless otherwise specified.

We can extend the definition of the virtual representation $\mathcal{M}_k$ for $k < 0$ in a way that is coherent with Brauer character computations. In [5], the determination the Euler-Poincaré characteristic of the twisted sheaf $\mathcal{O}(k)$ on $\mathbb{P}^1_{\mathbb{F}_q}$ suggests the following:

**Definition 2.2** Let $k$ be a negative integer. Define the element $\mathcal{M}_k$ of the Grothendieck group $K_0(\mathfrak{S})$ of $\mathfrak{S}$ over $\mathbb{F}_q$ by:

$$\mathcal{M}_k = \begin{cases} 0 & \text{if } k = -1 \\ \mathcal{M}_{-k-2} & \text{if } k \leq -2. \end{cases}$$

3
The following result summarizes some non-trivial identities that hold in the ring $K_0(G)$:

**Theorem 2.3** Let $k$ and $h$ be any integers. The following identities hold in $K_0(G)$:

\[ M_k = -M_{-k-2} \quad (\Delta_g) \]

\[ M_k - M_{k-(q+1)} = M_{k-(q-1)} - M_{k-2q} \quad (\Sigma_g) \]

\[ M_k M_h = M_{k+h} + M_{k-1} M_{h-1} \quad (\Pi_g) \]

\[ M_k = M_{k-p} M^{[1]} - M_{k-2p}. \quad (\Phi_g) \]

**Proof** Formulae $(\Delta_g)$ and $(\Sigma_g)$ are proved in [5] via a Brauer characters computation. Formula $(\Pi_g)$ comes from an exact sequence of $G$-modules constructed in [1]. Formula $(\Phi_g)$ is proved in section 3 of [4].

We remark that formula $(\Phi_g)$ appeared in [4] also in the form:

\[ M^{[i]} M^{[i+1]} - M^{[i]} M^{[i+1]} = M^{[i]} M^{[i+1]} - M^{[i]} M^{[i+1]}, \]

where $k, h$ and $i$ are any integers.

The product formula $(\Pi_1)$ implies that $(\Phi_1)$ and $(\Sigma_1)$ are equivalent. If $g > 1$, $(\Phi_g)$ cannot be deduced from $(\Sigma_g)$ and $(\Pi_g)$; the proof of this fact, contained in [4], is indirect and throughout the paper the knowledge of Serre’s relation $(\Sigma_g)$ will allow sometimes to bypass long computations involving Frobenius twists, when $g > 1$.

In [4] it is also proved that for $g \geq 1$, we can use the relations $(\Delta_g), (\Phi_g), (\Pi_g)$ to explicitly compute the Jordan-Hölder factors of any virtual representations of the form $\prod_{i=0}^{g-1} M^{[i]}$, where $k_0, \ldots, k_{g-1} \in \mathbb{Z}$.

## 3 Presentation of $K_0(G)$

We keep the notation introduced in the previous paragraph.

**Lemma 3.1** The ring $K_0(G)$ is generated by $X$ as a $\mathbb{Z}$-algebra.

**Proof** By Proposition 2.1, $K_0(G)$ is freely generated as a $\mathbb{Z}$-module by the $q$ elements $\prod_{i=0}^{g-1} M^{[i]}_k$, where $0 \leq k_i \leq p - 1$ for any $i$. It is therefore enough to show that for all integers $i, k$ such that $0 \leq i \leq g - 1$ and $0 \leq k \leq p - 1$ we have $M^{[i]}_k \in \mathbb{Z}[X]$.

Applying $(\Pi_g)$ we obtain the recursive relations:

\[ M_2 = X^2 - 1, \ M_n = X \cdot M_{n-1} - M_{n-2} \quad (n > 2), \]

so that $M_k \in \mathbb{Z}[X]$ for all $k \geq 0$. Twisting $(\Pi)$ by powers of Frobenius, we obtain:

\[ M^{[i]}_2 = (X^{[i]})^2 - 1, \ M^{[i]}_n = X^{[i]} \cdot M^{[i]}_{n-1} - M^{[i]}_{n-2} \quad (n > 2), \]
for all $0 \leq i \leq g - 1$, so that $M_k^{[i]} \in \mathbb{Z}[x, x^{[1]}, \ldots, x^{[g-1]}]$ for all $k \geq 0$ and:

$$K_0(\mathfrak{g}) = \mathbb{Z}[x, x^{[1]}, \ldots, x^{[g-1]}].$$

By $(\Phi_x)$, we have $M_p = M_p^{[1]} - M_{-p}$, and applying $(\Delta_x)$ we obtain $x^{[1]} = M_p - M_{p-2}$, so that $x^{[1]} \in \mathbb{Z}[x]$, as $M_k \in \mathbb{Z}[x]$ for all $k \geq 0$. We also obtain that, for any $0 \leq i \leq g - 1$, we have:

$$x^{[i+1]} = M_p^{[i]} - M_{p-2}^{[i]}, \quad (2)$$

and we conclude $x^{[1]}, \ldots, x^{[g-1]} \in \mathbb{Z}[x]$, implying $K_0(\mathfrak{g}) = \mathbb{Z}[x]$. ■

Let $x$ be an indeterminate over $\mathbb{Z}$ and define the following two families of polynomials of $\mathbb{Z}[x]$:

$$m_0(x) = 1, \quad m_1(x) = x, \quad m_2(x) = x^2 - 1, \quad m_n(x) = x \cdot m_{n-1}(x) - m_{n-2}(x) \quad (n > 2);$$

$$i^{[0]}(x) = x, \quad i^{[1]}(x) = m_p(x) - m_{p-2}(x), \quad i^{[i]}(x) = i^{[i]}(x) - m_{p-2}(i^{[i-1]}(x)) \quad (i > 1).$$

Observe that for any non-negative integer $n$, $m_n(x)$ is a monic polynomial of degree $n$, so that for any non-negative integer $i$, $i^{[i]}(x)$ is a monic polynomial of degree $p^i$.

**Lemma 3.2** For any non-negative integer $i$, we have $i^{[i]}(x) = x^{[i]}$ in $K_0(\mathfrak{g})$.

**Proof** Notice first that, by definition of $m_n(x)$ and by formula (3), one has:

$$m_n(x) = M_n \quad (3)$$

in $K_0(\mathfrak{g}) \quad (n \geq 0)$. To prove the lemma, we use induction on $i$. If $i = 0$, the statement is clear; if $i = 1$ it follows from formulae (3) and (2). Assume $i \geq 1$ fixed and suppose $i^{[i]}(x) = x^{[i]}$.

We have:

$$i^{[i+1]}(x) = m_p(i^{[i]}(x)) - m_{p-2}(i^{[i]}(x)) = m_p(x^{[i]}) - m_{p-2}(x^{[i]}).$$

Observe that Frobenius twists do not act on the coefficients of virtual representations in $K_0(\mathfrak{g})$, so that the last term above is equal to $m_p(x^{[i]}) - m_{p-2}(x^{[i]})$. By formula (3), the latter is $M_p^{[i]} - M_{p-2}^{[i]}$. By formula (2), this is $M_p^{[i]} - M_{p-2}^{[i]} = x^{[i+1]}$. ■

**Proposition 3.3** There is an isomorphism of rings:

$$\frac{\mathbb{Z}[x]}{(i^{[i]}(x) - x) \mathbb{Z}[x]} \simeq K_0(\mathfrak{g}),$$

induced by mapping the indeterminate $x$ of the polynomial ring $\mathbb{Z}[x]$ into the class of the representation $x$ of $\mathfrak{g}$. 5
Lemma 3.4  \( \ker m \) (Where, for any integer \( X \))

**Proof** By Proposition \ref{prop:3.4} the ring homomorphism \( \mathbb{Z}[x] \rightarrow K_0(\mathcal{G}) \) induced by \( x \mapsto x \) is surjective. Since \( X^{[g]} = x \) in \( K_0(\mathcal{G}) \), and since by the above lemma we have \( f^{[g]}(x) = x^{[g]} \), the above assignment induces an epimorphism

\[
\pi : \frac{\mathbb{Z}[x]}{(f^{[g]}(x) - x) \mathbb{Z}[x]} \rightarrow K_0(\mathcal{G}).
\]

Since \( f^{[g]}(x) - x \) is a polynomial of degree \( p^g \) and since \( K_0(\mathcal{G}) \) is \( \mathbb{Z} \)-free of rank \( p^g \), after tensoring with \( \mathbb{Q} \) the map \( \pi \) defines an isomorphism of \( \mathbb{Q} \)-vector spaces. This implies that \( \ker \pi \) is a finitely generated torsion \( \mathbb{Z} \)-submodule of \( \frac{\mathbb{Z}[x]}{(f^{[g]}(x) - x) \mathbb{Z}[x]} \), and hence it is trivial since \( f^{[g]}(x) - x \) is monic. We conclude that \( \pi \) is an isomorphism of rings. \( \blacksquare \)

We are now left with determining an explicit formula for the polynomial \( f^{[g]}(x) \in \mathbb{Z}[x] \).

**Lemma 3.4** For any non-negative integer \( n \) we have:

\[
m_n(x) = \sum_{j=0}^{[n/2]} (-1)^j \binom{n-j}{j} x^{n-2j}.
\]

(Where, for any integer \( h \), \( [h] \) denotes the largest integer not greater than \( h \)).

**Proof** We use induction on \( n \geq 0 \); denote by \( m'_n(x) \) the right hand side of the above formula. We have \( m'_0(x) = 1 = m_0(x) \), \( m'_1(x) = x = m_1(x) \) and \( m'_2(x) = x^2 - 1 = m_2(x) \). If \( n > 2 \) we have by induction:

\[
m_n(x) = \sum_{j=0}^{[n/2]-1} (-1)^j \binom{n-j}{j} x^{n-2j} + \sum_{j=1}^{[n/2]} (-1)^j \binom{n-j-1}{j-1} x^{n-2j} + \sum_{j=0}^{[n/2]} (-1)^j \binom{n-j}{j} x^{n-2j}.
\]

If \( n > 2 \) is even, \( [n-1)/2] = [(n-2)/2] = (n/2) - 1 \) and:

\[
m_n(x) = \sum_{j=0}^{(n/2)-1} (-1)^j \binom{n-j}{j} x^{n-2j} + \sum_{j=1}^{(n/2)} (-1)^j \binom{n-j-1}{j-1} x^{n-2j} + \sum_{j=0}^{[n/2]} (-1)^j \binom{n-j}{j} x^{n-2j}.
\]

If \( n > 2 \) is odd, \( [(n-1)/2] = (n-1)/2, [(n-2)/2] = (n-3)/2 \) and:

\[
m_n(x) = \sum_{j=0}^{(n-1)/2} (-1)^j \binom{n-j}{j} x^{n-2j} + \sum_{j=1}^{(n-1)/2} (-1)^j \binom{n-j-1}{j-1} x^{n-2j} + \sum_{j=0}^{(n-1)/2} (-1)^j \binom{n-j}{j} x^{n-2j}.
\]

\( \blacksquare \)
Corollary 3.5 Let $n \geq 2$ be an integer. Then:

$$m_n(x) - m_{n-2}(x) = \sum_{j=0}^{\lfloor n/2 \rfloor} (-1)^j \frac{n}{n-j} \binom{n-j}{j} x^{n-2j}.$$ 

Proof This is a computation using the previous lemma. We distinguish two cases: if $n \geq 2$ is even we have:

$$m_n(x) - m_{n-2}(x) = \sum_{j=0}^{n/2} (-1)^j \binom{n-j}{j} x^{n-2j} - \sum_{j=0}^{(n/2)-1} (-1)^j \binom{n-2-j}{j} x^{n-2(j+1)}$$

$$= \sum_{j=0}^{n/2} (-1)^j \binom{n-j}{j} x^{n-2j} + \sum_{j=1}^{n/2} (-1)^j \binom{n-1-j}{j-1} x^{n-2j}$$

$$= x^n + \sum_{j=1}^{n/2} (-1)^j \left( \binom{n-j}{j} + \binom{n-1-j}{j-1} \right) x^{n-2j}$$

$$= x^n + \sum_{j=1}^{n/2} (-1)^j \frac{n}{n-j} \binom{n-j}{j} x^{n-2j}. \quad \blacksquare$$

If $n \geq 3$ is odd we have:

$$m_n(x) - m_{n-2}(x) = \sum_{j=0}^{(n-1)/2} (-1)^j \binom{n-j}{j} x^{n-2j} - \sum_{j=0}^{(n-3)/2} (-1)^j \binom{n-2-j}{j} x^{n-2(j+1)}$$

$$= \sum_{j=0}^{(n-1)/2} (-1)^j \binom{n-j}{j} x^{n-2j} + \sum_{j=1}^{(n-1)/2} (-1)^j \binom{n-1-j}{j-1} x^{n-2j}$$

$$= x^n + \sum_{j=1}^{(n-1)/2} (-1)^j \left( \binom{n-j}{j} + \binom{n-1-j}{j-1} \right) x^{n-2j}$$

$$= x^n + \sum_{j=1}^{(n-1)/2} (-1)^j \frac{n}{n-j} \binom{n-j}{j} x^{n-2j}. \quad \blacksquare$$

We have proved:

Theorem 3.6 Let $g$ be a positive integer, $p$ a prime, $q = p^g$ and set $\mathfrak{g} = SL_2(\mathbb{F}_q)$. Denote by $\mathfrak{X}$ the standard representation of $\mathfrak{g}$ on $\mathbb{F}_q^2$ and let $x$ be an indeterminate over $\mathbb{Z}$. The assignment $\mathfrak{X} \mapsto x$ induces an isomorphism of rings:

$$K_0(\mathfrak{g}) \simeq \frac{\mathbb{Z}[x]}{(f^g(x) - x) \mathbb{Z}[x]},$$

where $f^g(x) = (\circ \circ \circ \circ \circ f)(x)$ is the monic polynomial of $\mathbb{Z}[x]$ having degree $p^g$ that is obtained by composing $g$-times with itself the monic degree $p$ polynomial:

$$f(x) := \sum_{j=0}^{|p/2|} (-1)^j \frac{p}{p-j} \binom{p-j}{j} x^{p-2j}.$$

At the time of writing of this paper, we do not know much about the properties of the polynomial $f^g(x) - x$ when viewed over $\mathbb{Z}$. Notice that if $p > 2$, $f^g(x) - x$ is an odd polynomial; using the easy to check facts that for any integer $n \geq 0$ we have $m_n(2) = n + 1$, and that:

$$m_n(1) = \begin{cases} 
-1, & \text{if } n \equiv 3, 4 \pmod{6} \\
0, & \text{if } n \equiv 2, 5 \pmod{6} \\
1, & \text{if } n \equiv 0, 1 \pmod{6}, 
\end{cases}$$

7
Proposition 3.9

We have

when

the following proposition uses Serre’s relation \( \sum g \).

Furthermore, from computer elaborations, \( f^{[2]}(\bar{x}) - \bar{x} \) seems to have only real roots.

In general, it is natural to ask what we can say about the irreducible factors over \( \mathbb{Q} \) of \( f^{[g]}(\bar{x}) - \bar{x} \). We do not have an answer for this. Nevertheless, after tensoring \( K_0(\mathfrak{G}) \) with \( \mathbb{Z}_p \), we can prove:

Corollary 3.7

Let \( K_0(\mathfrak{G})_p = K_0(\mathfrak{G}) \otimes \mathbb{Z}_p \).

For any positive divisor \( d \) of \( g \), let \( \psi(d) \) be the number of monic irreducible polynomials of degree \( d \) in \( \mathbb{F}_p[x] \). Then:

(a) The special fiber of \( K_0(\mathfrak{G})_p \) is a split \( \mathbb{F}_p \)-algebra isomorphic to \( \prod_{d|g} \mathbb{F}_p^{\psi(d)} \);

(b) The generic fiber of \( K_0(\mathfrak{G})_p \) is a split \( \mathbb{Q}_p \)-algebra isomorphic to \( \prod_{d|g} \mathbb{Q}_p^{\psi(d)} \).

(Here we denoted by \( \mathbb{Q}_p^d \) the degree \( d \) unramified extension of \( \mathbb{Q}_p \) contained in a fixed algebraic closure of \( \mathbb{Q}_p \)).

Proof

By the explicit formula given above for \( f(\bar{x}) \), we see that \( f(\bar{x}) \equiv x^q \pmod{p\mathbb{Z}[x]} \): this is clear if \( p = 2 \), otherwise notice that \( \frac{p-j}{p-j} = p \cdot \frac{q-j-1}{p-j} \) and the last denominator is prime to \( p \) if \( 1 \leq j \leq \frac{p-1}{2} \), implying that \( \frac{q-j-1}{p-j} \in \mathbb{Z} \). We conclude that

\[ f^{[g]}(\bar{x}) - \bar{x} \equiv x^q - x \pmod{p\mathbb{Z}[x]} \]

and statement (a) follows. Part (b) follows from (a) and Hensel’s lemma. ■

Remark 3.8

We also have isomorphisms of algebras: \( K_0(\mathfrak{G})_p \otimes \mathbb{Z}_p \mathbb{F}_q \simeq (\mathbb{F}_q)^g \) and \( K_0(\mathfrak{G})_p \otimes \mathbb{Z}_p \mathbb{Q}_q \simeq (\mathbb{Q}_q)^g \).

It is interesting to notice that we can give an explicit formula also for \( f^{[g]}(\bar{x}) \). As the following proposition uses Serre’s relation \( (\Sigma_g) \), it seems that an explicit formula for \( f^{[g]}(\bar{x}) \) when \( i \neq 1 \) would probably require more work.

Proposition 3.9

We have \( f^{[g]}(\bar{x}) = m_q(\bar{x}) - m_{q-2}(\bar{x}) \), so that:

\[ f^{[g]}(\bar{x}) = \sum_{j=0}^{\lfloor q/2 \rfloor} (-1)^j \frac{q-j}{q-j} \binom{q-j}{j} x^{q-2j}. \]

Proof

Let \( \bar{x} : \mathbb{Z}[x] \to K_0(\mathfrak{G}) \) be the epimorphism of rings obtained by sending \( x \) to \( \mathfrak{X} \). Relation \( (\Sigma_g) \) implies that \( M_1 = M_q - M_{q-2} \in K_0(\mathfrak{G}) \), that is \( M_q - M_{q-2} = 0 \). This means, by formula (3), that \( \mathfrak{X} \) satisfies the polynomial \( m_q(\bar{x}) - m_{q-2}(\bar{x}) - \bar{x} \in \mathbb{Z}[x] \), so that \( m_q(\bar{x}) - m_{q-2}(\bar{x}) - \bar{x} \in \ker \bar{x} = (f^{[g]}(\bar{x}) - \bar{x}) \mathbb{Z}[x] \). Since \( m_q(\bar{x}) - m_{q-2}(\bar{x}) - \bar{x} = f^{[g]}(\bar{x}) - \bar{x} \) are both monic of degree \( q \), the last relation implies that they have to be equal and \( f^{[g]}(\bar{x}) = m_q(\bar{x}) - m_{q-2}(\bar{x}) \). The proposition now follows from Corollary 3.5. ■
4 A conjecture

The following fact was pointed out to us by G. Savin:

**Proposition 4.1** Let $p$ be a prime and $q = p^i > 1$ be an integral power of $p$. Let $G$ be a simply connected semisimple algebraic group defined and split over $\mathbb{F}_q$, and denote by $K_0(G)$ the Grothendieck ring of $\mathbb{F}_q[G]$-rational modules of finite $\mathbb{F}_q$-dimension. If $\mathcal{M}$ is an element of $K_0(G)$ and $i$ is any non-negative integer, we have:

$$\mathcal{M}^i \equiv \mathcal{M}^{pi} \pmod{pK_0(G)}.$$ 

**Proof** Let $T$ be a maximal torus of $G$ defined and split over $\mathbb{F}_q$, and denote by $X = X(T)$ its character group. For any $\lambda \in X$, denote by $e(\lambda)$ the corresponding basis element of the group ring $\mathbb{Z}[X]$, so that $e(\lambda + \lambda') = e(\lambda)e(\lambda')$ for any characters $\lambda$ and $\lambda'$.

Fix a $G$-module $\mathcal{M}$ and write its formal character as:

$$\text{ch} \mathcal{M} = \sum_{\lambda \in X} m_{\lambda} \cdot e(\lambda),$$

where $m_{\lambda}$ is the dimension of the $\lambda$-isotypic submodule of $\mathcal{M}$. For a positive integer $i$, the $p^i$th power automorphism of $\mathbb{F}_q$ induces an action on $\mathbb{Z}[X]$ by sending a basis element $e(\lambda)$ to $e(p^i\lambda)$, so that:

$$\text{ch} (\mathcal{M}^{(i)}) = \sum_{\lambda \in X} m_{\lambda} \cdot e(\lambda)^{p^i} = (\sum_{\lambda \in X} m_{\lambda} \cdot e(\lambda))^{p^i} \pmod{p\mathbb{Z}[X]}.$$ 

The formal character $(\sum_{\lambda \in X} m_{\lambda} \cdot e(\lambda))^{p^i}$ is the element associated to $\mathcal{M}^{pi}$ by the map $\text{ch} : K_0(G) \rightarrow \mathbb{Z}[X]$. We have therefore:

$$\text{ch} (\mathcal{M}^{(i)}) \equiv \text{ch} (\mathcal{M}^{pi}) \pmod{p\mathbb{Z}[X]}.$$ (1)

Let $\mathcal{W}$ denotes the Weyl group of the pair $(G, T)$. By [2] II.5.8, the map $\text{ch}$ induces an isomorphism of commutative rings:

$$\text{ch} : K_0(G) \xrightarrow{\sim} \mathbb{Z}[X]^\mathcal{W}.$$ 

Write $\text{ch} (\mathcal{M}^{(i)}) = \sum_{\lambda \in X} a_{\lambda} \cdot e(\lambda)$ and $\text{ch} (\mathcal{M}^{pi}) = \sum_{\lambda \in X} b_{\lambda} \cdot e(\lambda)$, so that $\text{ch} (\mathcal{M}^{(i)} - \mathcal{M}^{pi}) = \sum_{\lambda \in X} (a_{\lambda} - b_{\lambda}) \cdot e(\lambda)$ is such that:

$$\sum_{\lambda \in X} (a_{\lambda} - b_{\lambda}) \cdot e(\lambda) = \sum_{\lambda \in X} (a_{\lambda} - b_{\lambda}) \cdot e(w_{\lambda})$$ (2)

for all $w \in \mathcal{W}$.

By [1], there are integers $c_{\lambda}$ such that $a_{\lambda} - b_{\lambda} = p c_{\lambda}$ for all $\lambda \in X$. Since $\mathbb{Z}[X]$ is $\mathbb{Z}$-flat, we can view it as a subring of $\mathbb{Q}[X]$, in which we have, for any $w \in \mathcal{W}$:

$$w \cdot \left( \sum_{\lambda \in X} c_{\lambda} \cdot e(\lambda) \right) = \frac{1}{p} \sum_{\lambda \in X} (a_{\lambda} - b_{\lambda}) \cdot e(w_{\lambda})$$

$$= \frac{1}{p} \sum_{\lambda \in X} (a_{\lambda} - b_{\lambda}) \cdot e(\lambda),$$
where the last equality follows from (2). Therefore $w \cdot \left( \sum_{\lambda \in X} c_{\lambda} \cdot e(\lambda) \right) = \sum_{\lambda \in X} c_{\lambda} \cdot e(\lambda)$ in $\mathbb{Z}[X]$ for all $w \in W$ and

$$\text{ch}(\mathcal{M}^i - \mathcal{M}^{\nu}) \in p\mathbb{Z}[X]^W.$$  

This implies that $\mathcal{M}^i$ is congruent to $\mathcal{M}^{\nu}$ modulo the ideal generated by $p$ in $K_0(\mathbb{G})$. 

Motivated by Theorem 3.6, Corollary 3.7 and Proposition 4.1, we are led to the following:

**Conjecture 4.2** Let $p$ be a prime and $q = p^q > 1$ be an integral power of $p$. Let $\mathbb{G}$ be a simply connected semisimple algebraic group defined and split over $\mathbb{F}_q$, whose rank is $\ell > 0$. Denote by $K_0(\mathbb{G}(\mathbb{F}_q))$ the Grothendieck ring of finitely generated $\mathbb{F}_q[\mathbb{G}(\mathbb{F}_q)]$-modules. Then there exist $\ell$ monic polynomials $f_i(x_1) \in \mathbb{Z}[x_1], \ldots, f_i(x_\ell) \in \mathbb{Z}[x_\ell]$ having degree $p$ such that:

$$K_0(\mathbb{G}(\mathbb{F}_q)) \simeq \frac{\mathbb{Z}[x_1, \ldots, x_\ell]}{(f_1^{[p]}(x_1) - x_1, \ldots, f_{\ell}^{[p]}(x_\ell) - x_\ell)} \mathbb{Z}[x_1, \ldots, x_\ell].$$

where for any $i$, $1 \leq i \leq \ell$, $f_i^{[p]}(x_i)$ is the polynomial obtained by composing $f_i(x_i)$ with itself $g$ times.

Furthermore, $f_i(x_i) \equiv f_i^p \pmod{p\mathbb{Z}[x_i]}$ for any $i$, $1 \leq i \leq \ell$.

The idea behind the above statement is that if $\pi$ is an isomorphism of $\mathbb{Z}[x_1, \ldots, x_\ell]/(f_1^{[p]}(x_1) - x_1, \ldots, f_{\ell}^{[p]}(x_\ell) - x_\ell)$ onto $K_0(\mathbb{G}(\mathbb{F}_q))$, and if we set $X_i := \pi(x_i)$ for $1 \leq i \leq \ell$, then $f_i(X_i) \in K_0(\mathbb{G}(\mathbb{F}_q))$ should be the Frobenius twist $X_i^{[1]}$. This means that the relations imposed above in the algebra $\mathbb{Z}[x_1, \ldots, x_\ell]$ are the obvious ones that translate into $X_i^{[p]} = X_i$ for all $i$.

Here is some evidence for the conjecture:

(a) As proved in the previous paragraph, the conjecture is true for $G = SL_2$ over $\mathbb{F}_q (\ell = 1)$, in which case we can also give an explicit formula for the polynomial $f(x) = f_1(x_1)$ (Theorem 3.6).

(b) A theorem of Steinberg (10) states that if $\mathbb{G}$ is a simply connected semisimple algebraic group over $\mathbb{F}_q$, the number of semisimple conjugacy classes of $\mathbb{G}(\mathbb{F}_q)$ is equal to $q^{\ell}$, where $\ell$ is the rank of $G$. Therefore $K_0(\mathbb{G}(\mathbb{F}_q)) \simeq \mathbb{Z}^{q^\ell}$ as $\mathbb{Z}$-modules, which follows from the conjecture.

(c) Since $h(x_1, \ldots, x_\ell)^q = h(x_1^q, \ldots, x_\ell^q)$ for any polynomial $h(x_1, \ldots, x_\ell) \in \mathbb{F}_q[x_1, \ldots, x_\ell]$, the conjecture implies that $\frac{\mathbb{M}^i}{\mathbb{M}^{\nu}} = \mathbb{M}^1$ for any $\mathbb{M} \in K_0(\mathbb{G}(\mathbb{F}_q)) \otimes_{\mathbb{Z}} \mathbb{F}_q$. This fact is also a consequence of Proposition 4.1.

(d) Assume we are given a surjective homomorphism of $\mathbb{F}_q$-algebras:

$$\gamma: \mathbb{F}_q[x_1, \ldots, x_\ell] \rightarrow K_0(\mathbb{G}(\mathbb{F}_q)) \otimes_{\mathbb{Z}} \mathbb{F}_q.$$  

Proposition 4.1 implies that $\gamma(x_i)^q = \gamma(x_i)$ for any integer $i$, $1 \leq i \leq \ell$; in particular the kernel of $\gamma$ contains the ideal generated by the polynomials $x_1^q - x_1, \ldots, x_\ell^q - x_\ell$. By dimension reasons we must have an isomorphism of $\mathbb{F}_q$-algebras:

$$\frac{\mathbb{F}_q[x_1, \ldots, x_\ell]}{(x_1^q - x_1, \ldots, x_\ell^q - x_\ell)} \rightarrow K_0(\mathbb{G}(\mathbb{F}_q)) \otimes_{\mathbb{Z}} \mathbb{F}_q.$$  

This is predicted by Conjecture 4.2.
If Conjecture 4.2 is correct, one would like to determine explicit formulae for the polynomials $f_1(x_1), \ldots, f_\ell(x_\ell)$ and to relate factorization properties of these polynomials in $\mathbb{Z}[x_i]$ to algebraic properties of the group $G(\mathbb{F}_q)$.

References

[1] D. J. Glover, *A study of certain modular representations*, J. Algebra 51 (1978), 425–475.

[2] J. C. Jantzen, *Representations of algebraic groups, Second edition*, Mathematical Surveys and Monographs 107, AMS, 2003.

[3] D. A. Reduzzi, *Reduction mod $p$ of cuspidal representations of $GL_2(\mathbb{F}_{p^n})$ and symmetric powers*, J. Algebra 324 (2010), 3507–3531.

[4] ________, *Cohomological weight shiftings for automorphic forms on definite quaternion algebras over totally real fields*. (Preprint), (2011).

[5] J-P. Serre, *Lettre Mme Hamer*, 2 Juillet 2001.

[6] R. Steinberg, *Representations of algebraic groups*, Nagoya Math. J. 22 (1963), 33–56.