We want to establish that in the twisted tensor product of two \( \mathbb{Z}_d \)-graded \( K \)-algebras, \( C \otimes_K C' \), one has that if \( u \in C \) and \( v \in C' \) are forms of degree 1, then

\[
(u \otimes 1 + 1 \otimes v)^d = u^d \otimes 1 + 1 \otimes v^d,
\]
a property reminiscent of the behavior of the Frobenius endomorphism in the commutative case. In order to prove this, we need to develop a “twisted” binomial theorem.

To this end, let \( \tilde{q}, \tilde{U}, \) and \( \tilde{V} \) be non-commuting indeterminates over \( \mathbb{Z} \) and form the free algebra they generate modulo the relations

\begin{align*}
(1) & \quad \tilde{q} \tilde{U} = \tilde{U} \tilde{q} \\
(2) & \quad \tilde{q} \tilde{V} = \tilde{V} \tilde{q} \\
(3) & \quad \tilde{V} \tilde{U} = \tilde{q} \tilde{U} \tilde{V}
\end{align*}

We denote the images of \( \tilde{q}, \tilde{U}, \) and \( \tilde{V} \) by \( q, U, \) and \( V, \) respectively. Thus, \( q \) is in the center of quotient ring \( A \). While \( U \) and \( V \) do not commute, it is clear that every monomial in \( U \) and \( V \) may be rewritten in the form \( q^i U^j V^k \), with \( i, j, k \in \mathbb{N} \), in this ring. In fact, \( A \) is the free \( \mathbb{Z} \)-module spanned by these monomials, with the multiplication

\[
(q^i U^j V^k)(q'^i' U'^j' V'^k') = q^{i+i'} U^{j+j'} V^{k+k'}.
\]

This is forced by iterated use of the relations (1), (2), and (3), and one can check easily that this gives an associative multiplication on the free \( \mathbb{Z} \)-module on the monomials \( q^i U^j V^k \).

In this algebra, one may calculate \( (U + V)^d \) and write it as a linear combination of monomials \( U^i V^j \) each of whose coefficients is a polynomial in \( \mathbb{Z}[q] \). When \( q \) is specialized to 1, the coefficients simply become ordinary binomial coefficients. We want to investigate these coefficients, which are called Gaussian polynomials, Gaussian coefficients, or \( q \)-binomial coefficients. We shall denote the coefficient of \( U^k V^{d-k} \), \( 0 \leq i \leq d \), as \( \left[ \begin{array}{c} d \\ k \end{array} \right]_q \).

For example,

\[
(U + V)^2 = V^2 + UV + VU + U^2 = V^2 + (q + 1)UV + V^2,
\]

and so \( \left[ \begin{array}{c} 2 \\ 0 \end{array} \right]_q = \left[ \begin{array}{c} 2 \\ 2 \end{array} \right]_q = 1 \) while \( \left[ \begin{array}{c} 2 \\ 1 \end{array} \right]_q = q + 1 \).

**Theorem (twisted binomial theorem).** Let notation be as above.

(a) The coefficient polynomials \( \left[ \begin{array}{c} d \\ k \end{array} \right]_q \) are determined recursively by the rules
\[
\begin{align*}
(1) \quad & \binom{d}{0}_q = \binom{d}{d}_q = 1 \text{ and} \\
(2) \quad & \binom{d+1}{k+1}_q = \binom{d}{k}_q + q^{k+1} \binom{d}{k+1}_q.
\end{align*}
\]

(b) For all \(d\) and \(k\), \(\binom{d}{k}_q = \prod_{i=0}^{k-1} \frac{1 - q^{d-i}}{1 - q^{i+1}}\).

(c) Let \(\lambda, u, v\) be elements of any associative ring \(R\) with identity such that \(\lambda\) commutes with \(u\) and \(v\) and \(vu = \lambda uv\). Let \(\binom{d}{k}(\lambda)_q\) denote the element of \(R\) that is the image of \(\binom{k}{d}_q\) under the map \(\mathbb{Z}[q] \to R\) that sends \(q \mapsto \lambda\). Then

\[
(u + v)^d = \sum_{k=0}^{d} \binom{d}{k}(\lambda)_q u^k v^{d-k}.
\]

**Proof.** For part (a), first note that it is evident that the coefficients of \(V^d\) and \(U^d\) in the expansion of \((U + V)^d\) are both 1. Now \((U + V)^{d+1} = (U + V)(U + V)^d\), and it is clear that there are two terms in the expansion that contribute to the coefficient of \(U^{k+1}V^{d-k}\): one is the product of \(U\) with the \(U^{k+1}V^{d-k}\) term in \((U + V)^d\), which gives \(\binom{d}{k} U^{k+1}V^{d-k}\), and the other is the product of \(V\) with the \(U^{k+1}V^{d-k-1}\) term, which gives \(\binom{d}{k+1} V U^{k+1}V^{d-k-1}\). Since \(VU^{k+1} = q^{k+1}U^{k+1}V\), the result follows.

For part (b), it will suffice to show that the proposed expressions for the \(\binom{d}{k}_q\) satisfy the recursion in part (a), that is:

\[
\prod_{i=0}^{k} \frac{1 - q^{d+1-i}}{1 - q^{i+1}} = \prod_{i=0}^{k-1} \frac{1 - q^{d-i}}{1 - q^{i+1}} + q^{k+1} \prod_{i=0}^{k} \frac{1 - q^{d-i}}{1 - q^{i+1}}.
\]

We can clear denominators by multiplying by the denominator of the left hand term to get the equivalent statement:

\[
(*) \quad \prod_{i=0}^{k} (1 - q^{d+1-i}) = (1 - q^{k+1}) \prod_{i=0}^{k-1} (1 - q^{d-i}) + q^{k+1} \prod_{i=0}^{k} (1 - q^{d-i}).
\]

The left hand term may be rewritten as

\[
\prod_{j=-1}^{k-1} (1 - q^{d-j}) = (1 - q^{d+1}) \prod_{i=0}^{k-1} (1 - q^{d-i}).
\]
We may divide both sides of \((\ast)\) by 
\[
\prod_{i=0}^{k-1} (1 - q^{d-i})
\]
to see that \((\ast)\) is equivalent to
\[
1 - q^{d+1} = 1 - q^{k+1} + q^{k+1}(1 - q^{d-k}),
\]
which is true.

Part (c) follows at once, for there is a homomorphism of 
\[ A = \mathbb{Z}[q, U, V] \rightarrow \mathbb{R} \]
such that \(q \mapsto \lambda, U \mapsto u\) and \(V \mapsto v\). □

Recall that the \(d\)th cyclotomic polynomial \(\Psi_d(t)\), \(d \geq 1\), is the minimal polynomial of a primitive \(d\)th root of unity over \(\mathbb{Q}\). It is a monic polynomial with coefficients in \(\mathbb{Z}\) and irreducible over \(\mathbb{Z}\) and \(\mathbb{Q}\). The degree of \(\Psi_d(t)\) is the Euler function \(\Phi(d)\), whose value is the number of units in \(\mathbb{Z}_d\). If \(d = p_1^{k_1} \cdots p_h^{k_h}\) is the prime factorization of \(d\), where the \(p_i\) are mutually distinct, then
\[
\Phi(d) = \prod_{j=1}^{h} (p_j^{k_j} - p_j^{k_j-1}).
\]
The polynomials \(\Psi_d(t)\) may be found recursively, using the fact that
\[
t^d - 1 = \prod_{a|d} \Psi_a(t),
\]
where \(a\) runs through the positive integer divisors of \(d\). We next observe:

**Corollary.** For every \(d\) and \(1 \leq k \leq d - 1\), \(\Psi_d(q)\) divides \(\left[\begin{array}{c}d \\ k\end{array}\right]_q\) in \(\mathbb{Z}[q]\).

**Proof.** Let \(\xi\) be a primitive \(d\)th root of unity in \(\mathbb{C}\). It suffices to show that \(\left[\begin{array}{c}d \\ k\end{array}\right]_q(\xi) = 0\).

This is immediate from the formula in part (b) of the Theorem, since one of the factors in the numerator, corresponding to \(i = 0\), is \(q^d - 1\), which vanishes when \(q = \xi\), while the exponents on \(q\) in the factors in the denominator vary between 1 and \(k < d\), and so the denominator does not vanish when we substitute \(q = \xi\). □

**Corollary.** In the twisted tensor product \(C \otimes C'\) of two \(\mathbb{Z}_d\)-graded \(K\)-algebras, if \(u\) is any form of degree 1 in \(C\) and \(v\) is any form of degree 1 in \(C'\), then \((u \otimes 1 + 1 \otimes v)^d = u^d \otimes 1 + 1 \otimes_d v^d\).

**Proof.** By the preceding Corollary, all the \(q\)-binomial coefficients of the terms involving both \(u \otimes 1\) and \(1 \otimes v\) vanish. □
Theorem. Let \( f \) and \( g \) be forms of degree \( d \) over a field \( K \) in disjoint sets of variables, say \( X_1, \ldots, X_n \) and \( Y_1, \ldots, Y_m \). Then there is a surjective \( \mathbb{Z}_d \)-graded \( K \)-algebra homomorphism \( C(f + g) \to C(f) \otimes_K C(g) \). Hence, if \( M \) is a Clifford module over \( C(f) \) and \( N \) is a Clifford module over \( C(g) \), then the twisted tensor product \( M \otimes_K N \) is a Clifford module over \( C(f + g) \).

Proof. Let \( V \) be the dual of the \( K \)-span of \( X_1, \ldots, X_n \), with dual \( K \)-basis \( e_1, \ldots, e_n \), and let \( V' \) the dual of the \( K \)-span of \( Y_1, \ldots, Y_m \), with dual basis \( e'_1, \ldots, e'_m \). Then \( C(f + g) \) is the quotient of \( T(V \oplus V') \) by the two-sided ideal generated by all relations of the the form

\[
(c_1 e_1 + \cdots + c_n e_n + c'_1 e'_1 + \cdots + c'_m e'_m)^d - f(c_1, \ldots, c_n) - g(c'_1, \ldots, c'_m),
\]

where \( c = c_1, \ldots, c_n \in K \) and \( c' = c'_1, \ldots, c'_m \in K \). The maps \( T(V) \to C(f) \) and \( T(V') \to C(g) \) will induce a map \( C(f + g) \to C(f) \otimes_K C(g) \) provided that each of the relations \((*)\) maps to 0 in \( C(f) \otimes_K C(g) \). With

\[
u = c_1 e_1 + \cdots + c_n e_n
\]

and

\[
v = c'_1 e'_1 + \cdots + c'_m e'_m,
\]

we have that

\[
(v \otimes 1)(u \otimes 1) = \xi (u \otimes 1)(1 \otimes v)
\]

in the twisted tensor product, and so \((u + v)^d\) maps to \( u^d \otimes 1 + 1 \otimes v^d \). Thus, the element displayed in \((*)\) maps to

\[
u^d \otimes 1 + 1 \otimes v^d - f(c)(1 \otimes 1) - g(c')(1 \otimes 1) = (u^d - f(c)) \otimes 1 + 1 \otimes (v^d - g(c')) = 0 + 0 = 0,
\]

as required. \( \square \)

We now use these ideas to get a matrix factorization for a generic form. In a sense, we carry this out over the field \( \mathbb{Q}[\xi] \), but we observe that the entries of the matrices are actually in \( \mathbb{Z}[\xi] \). We then embed \( \mathbb{Z}[\xi] \) in a ring of matrices over \( \mathbb{Z} \) to get a solution over \( \mathbb{Z} \). This result gives the a version of the theorem over any ring, by applying a suitable homomorphism.

We first introduce two notations. If \( \alpha_1, \ldots, \alpha_d \) are square matrices, then \( \text{diag}(a_1, \ldots, a_d) \) denotes the square matrix whose size is the sum of the sizes of the \( \alpha_1, \ldots, \alpha_d \), and whose block form is

\[
\begin{pmatrix}
\alpha_1 & 0 & 0 & \cdots & 0 \\
0 & \alpha_2 & 0 & \cdots & 0 \\
0 & 0 & \alpha_3 & \cdots & 0 \\
& & & \ddots & \\
0 & 0 & 0 & \cdots & \alpha_d
\end{pmatrix}
\]
This matrix corresponds to the direct sum of the maps represented by the \( \alpha_1, \ldots, \alpha_d \).

When \( \alpha_1, \ldots, \alpha_d \) are square matrices of the same size, say \( s \), we write \( \text{cyc}(\alpha_1, \ldots, \alpha_d) \) for the matrix whose block form is

\[
\begin{pmatrix}
0 & 0 & 0 & \cdots & 0 & \alpha_1 \\
\alpha_d & 0 & 0 & \cdots & 0 & 0 \\
0 & \alpha_{d-1} & 0 & \cdots & 0 & 0 \\
& & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & 0 & \cdots & \alpha_2 & 0
\end{pmatrix}
\]

Here “cyc” stands for “cyclic.” One may think about this matrix as follows. Suppose that the \( \alpha_i \) are thought of as linear transformations on a vector space \( V \) of dimension \( s \) over \( K \). Let \( V_i = V, 1 \leq i \leq d \), and let \( W = V^{\oplus d} \) thought of as \( V_1 \oplus \cdots \oplus V_d \). Then \( \text{cyc}(\alpha_1, \ldots, \alpha_d) \) corresponds to the linear transformation of \( V \) whose restriction to \( V_i \) is given by \( \alpha_{d+1-i} : V_i \to V_{i+1} \). The subscript \( i \) should be read modulo \( d \), so that the restriction to \( V_d \) is \( \alpha_1 : V_d \to V_1 \). Thus, \( (\text{cyc}(\alpha_1, \ldots, \alpha_d))^d \), when restricted to \( V_i \), is the composite

\[
(V_{i-1} \xrightarrow{\alpha_{d+1-(i-1)}} V_i) \circ \cdots \circ (V_{i+1} \xrightarrow{\alpha_{d-i}} V_{i+2}) \circ (V_i \xrightarrow{\alpha_{d+1-i}} V_{i+1}),
\]

i.e.,

\[
\alpha_{d+2-i} \alpha_{d+3-i} \cdots \alpha_d \alpha_1 \cdots \alpha_{d-i} \alpha_{d+1-i}.
\]

Hence, if \( \alpha_1, \ldots, \alpha_d \) is a matrix factorization of \( f \) of size \( s \), one also has a matrix factorization of \( f \) of size \( ds \) with \( d \) factors all of which are equal to \( \text{cyc}(\alpha_1, \ldots, \alpha_d) \).

**Theorem.** Let \( d \geq 2 \) and \( s \geq 1 \) be integers, and let \( f \) denote the degree \( d \) linear form over \( \mathbb{Z} \) in \( sd \) variables given as

\[
f = X_{1,1}X_{1,2} \cdots X_{1,d} + \cdots + X_{s,1}X_{s,2} \cdots X_{s,d}.
\]

Note that \( f \) is the sum of \( s \) products of \( d \) variables, where all of the variables that occur are distinct. Let \( \xi \) be a primitive \( d \)th root of unity. Then \( f \) has a matrix factorization \( f\text{I}_{d-1} = \alpha_1 \cdots \alpha_d \) over

\[
R = \mathbb{Z}[\xi][X_{ij} : 1 \leq i \leq s, 1 \leq j \leq d]
\]

of size \( s^{d-1} \) such that \( I(\alpha) = (X_{ij} : 1 \leq i \leq s, 1 \leq j \leq d)R \). Moreover, every entry of every matrix is either 0 or of the form \( \xi^k X_{ij} \).

**Proof.** We use induction on \( s \). We construct the factorization over \( \mathbb{Q}[\xi] \), but show as we do so that the entries of the matrices constructed are in \( \mathbb{Z}[\xi] \).

If \( s = 1 \) we have that

\[
(x_{1,1}x_{1,2} \cdots x_{1,d}) = (x_{1,1})(x_{1,2}) \cdots (x_{1,d}).
\]
By part (b) of the Proposition on p. 3 of the Lecture Notes of November 13, we have a corresponding Clifford module.

Now suppose that we have constructed a matrix factorization $\beta_1, \ldots, \beta_d$ of size $d^{s-1}$ for

$$f_1 = X_{11}X_{12} \cdots X_{1d} + \cdots + X_{s-1,1}X_{s-1,2} \cdots X_{s-1,d}$$

that satisfies the conditions of the theorem. Let $M$ be the corresponding Clifford module. We also have a factorization for $g = x_{s,1} \cdots x_{s,d}$, namely

$$(x_{s,1}x_{s,2} \cdots x_{s,d}) = (x_{s,1})(x_{s,2}) \cdots (x_{s,d}).$$

Since the two sets of variables occurring in $f_1$ and $g$ respectively are disjoint, the twisted tensor product $M \otimes_K N$, where $K = \mathbb{Q}[\xi]$, of the corresponding Clifford modules is a Clifford module $Q$ over $C(f_1 + g) = C(f)$, by the Theorem at the top of p. 4 of today’s Lecture Notes. Note that each $N_j$ has dimension 1, and that

$$(*) \quad Q_i = M_{i-1} \otimes_K N_1 \oplus M_{i-2} \otimes_K N_2 \oplus \cdots \oplus M_i \otimes_K N_d$$

has dimension $s^{d-1}$. Then $Q$ gives a matrix factorization of $f = f_1 + g$ of size $d^{s-1}$ over $\mathbb{Q}[\xi]$.

However, we shall give explicit bases for the $Q_i$, and show that the matrices that occur have entries of the form specified in the statement of the theorem, which shows that one has a matrix factorization over $\mathbb{Z}[\xi]$. We use all the tensors of pairs of basis elements, one from one of the $M_i$ and one from one of the $N_j$ but order the basis for $Q_i$ as indicated in the direct sum displayed in ($*$) above. The result is that the map from $Q_i \rightarrow Q_{i+1}$ that comes from multiplication by $c_{1,1}e_{1,1} + \cdots + c_{s-1,d}e_{s-1,d}$ (the indexing on the scalars $c_{i,j}$ corresponds to the indexing on the variables $X_{i,j}$) has as its matrix the result obtained by substituting the $c_{i,j}$ for the $X_{i,j}$ in $\text{diag}(\beta_{d+1-i-1}, \beta_{d+1-i-2}, \cdots, \beta_{d+1-i})$, for the map is the direct sum of the maps $M_{i-j} \otimes_K N_j \rightarrow M_{i-j+1} \otimes_K N_j$ induced by the maps $M_{i-j} \rightarrow M_{i-j+1}$.

On the other hand, the map from $Q_i \rightarrow Q_{i+1}$ given by multiplication by $c_1' e_1' + \cdots c_d'e_d'$ maps the $j$th term $M_{i-j} \otimes_K N_j$ to the $j + 1$st term $M_{i-j} \otimes_K N_{j+1}$, and corresponds to multiplication by $\xi^{i-j}X_{s,d+1-j}$ evaluated at $(c')$ on the summand $M_{i-j} \otimes_K N_{j}$, which has $K$-vector space dimension $d^{s-2}$. The result $\gamma_{d+1-i}$ is the matrix

$$\text{cyc}(\xi^{-d}X_{s,1}I_{d^s-2}, \xi^{-(d-1)}X_{s,2}I_{d^s-2}, \ldots, \xi^{i-1}X_{s,1}I_{d^s-2}).$$

Therefore, we get a matrix factorization of $f$ with $d$ factors of size $d^{s-1}$ in which

$$\alpha_i = \text{diag}(\beta_{i-1}, \beta_{i-2}, \cdots, \beta_i) + \gamma_i.$$

Since all of the coefficients needed are 0 or powers of $\xi$, this is a factorization over $\mathbb{Z}[\xi]$. All of the variables occur, possibly with coefficient $\xi^k$, but $\xi$ is a unit in $\mathbb{Z}[\xi]$, and so all of the conditions of the theorem are satisfied. $\square$