Let $\mathbb{F}$ be a field and let $X = \{x_1, \ldots, x_n\}$ be a set of variables. The polynomial ring $\mathbb{F}[X]$ is graded by degree

$$\mathbb{F}[X] = H_0 \oplus H_1 \oplus H_2 \oplus \cdots .$$

The elements of H_k will be called "forms" (over $\mathbb{F}$).

Let $Q(x_1, \ldots, x_n)$ be a quadratic form over $\mathbb{F}$. Let

$$I = \mathbb{F} \cdot Q(X) \oplus H_3 \oplus H_4 \oplus \cdots$$

be the ideal generated by $Q(X)$ and the forms of degree at least 3. The quotient $S_{\mathbb{F},Q} := \mathbb{F}[X]/I$ may be viewed as a graded ring:

$$S_{\mathbb{F},Q} = H_0 \oplus H_1 \oplus H_2/(Q) \oplus 0 \oplus 0 \cdots .$$

In what follows, there will be instances where we have an element $p \in S_{\mathbb{F},Q} = H_0 \oplus H_1 \oplus H_2/(Q)$ whose H_0 component (=constant term) is 0, and we will want to know its H_1 component (=linear term). We write $[p]$ to denote the linear term of p when p has no constant term.

Two quadratic forms Q_1 and Q_2 are equivalent if they differ by an invertible linear change of variables.

Theorem 1. *Let $\mathbb{F}$ be a finite field of odd characteristic p. Let $Q_1(x_1, \ldots, x_n)$ and $Q_2(x_1, \ldots, x_n)$ be nonzero quadratic forms over $\mathbb{F}$.*

1. *$S_{\mathbb{F},Q_1}$ and $S_{\mathbb{F},Q_2}$ have isomorphic $\mathbb{F}$-space structures.*
2. *If $n > 4$ and Q_1 and Q_2 are nondegenerate, then $S_{\mathbb{F},Q_1}$ and $S_{\mathbb{F},Q_2}$ have isomorphic multiplicative monoids.*
3. *$S_{\mathbb{F},Q_1} \ncong S_{\mathbb{F},Q_2}$ as $\mathbb{F}$-algebras, unless Q_1 is equivalent to a nonzero scalar multiple of Q_2.*

Proof. [Item (1)] If $Q \neq 0$, then the $\mathbb{F}$-space structure of $S_{\mathbb{F},Q} = H_0 \oplus H_1 \oplus H_2/(Q)$ is that of a quotient of the space $H_0 \oplus H_1 \oplus H_2$ by a 1-dimensional subspace. This structure is independent of the choice of Q.

[Item (2)] Let's examine the multiplicative structure of $S_{\mathbb{F},Q} = H_0 \oplus H_1 \oplus H_2/(Q)$ where Q is any nondegenerate quadratic form over $\mathbb{F}$ in more than four variables. We partition the elements of $S_{\mathbb{F},Q}$ into five cells:

1. C_0 consists of those elements whose H_0-component is not zero.
2. C_1 consists of those elements whose H_0 component is zero, but whose H_1-component is not zero.
3. C_2 consists of those elements whose H_0- and H_1-components are zero, and which are products of elements from H_1.
4. C_3 are the nonzero elements that remain.
5. $C_4 = \{0\}$.

Notice first that the cardinalities of $H_0, H_1, H_2, H_2/(Q), C_0, C_1$, and $C_2 \cup C_3$ depend only on $n, |\mathbb{F}|$ and the fact that $Q \neq 0$, but do not otherwise depend on Q.

C_0 is the set of units of the ring, which I will also denote G. The structure of the (finite, abelian) group G is easy to determine: it has a subgroup of homogeneous units

$\mathbb{F}^\times \cdot 1 \subseteq G$ and a complementary subgroup of inhomogeneous units $1 + \mathbf{rad}(S_{\mathbb{F},Q})$. The homogeneous units form a cyclic group of size $|\mathbb{F}^\times|$ while the complementary subgroup is an elementary abelian p-group of size $|\mathbf{rad}(S_{\mathbb{F},Q})|$ (since the p-th power of $1 + m \in 1 + \mathbf{rad}(S_{\mathbb{F},Q})$ is $(1+m)^p = 1 + m^p = 1$). Hence

$$G \cong \mathbb{F}^\times \times (1 + \mathbf{rad}(S_{\mathbb{F},Q})) \cong \mathbb{Z}_{|\mathbb{F}^\times|} \times \mathbb{Z}_p^{\dim(\mathbf{rad}(S_{\mathbb{F},Q}))}.$$

The point here is that the structure of this group does not depend on the choice of the quadratic form Q, only on the fact that $Q \neq 0$.

The group G acts by multiplication on $S_{\mathbb{F},Q}$, and each cell C_i is a union of G-orbits. Moreover, for a fixed i, the G-orbits in C_i are isomorphic to one another as G-sets. To see this it is enough to show that two elements of the same cell have the same stabilizer. Now, $u \in G$ may be written as $\alpha + \beta$ with $\alpha \in H_0$ and $\beta \in H_1 \oplus H_2/(Q)$. For $\alpha + \beta$ to stabilize x we must have $x = \alpha x + \beta x$, which can only happen if $\alpha = 1$ and $\beta \in \mathrm{Ann}(x)$. Thus two elements have the same stabilizer in G iff they have the same annihilator in $S_{\mathbb{F},Q}$. It is easy to see that the annihilator of any element of C_0 is 0, so C_0 is partitioned in (one) G-orbit. The annihilator of any element of $C_2 \cup C_3$ is $\mathfrak{m} = \mathbf{rad}(S_{\mathbb{F},Q}) = H_1 \oplus H_2/(Q) = C_1 \cup C_2 \cup C_3$, so C_2 and C_3 are each partitioned into isomorphic orbits. These orbits consist of a nonzero element and its nonzero scalar multiples. It remains to explain why the annihilator of any element of C_1 is $\mathfrak{m}^2 = H_2/(Q) = C_2 \cup C_3$. If this were not the case, then there would be $p_1, p_2 \in C_1$ such that $p_1 p_2 = 0$. The same would be true is we replaced p_i by its homogeneous linear component, $[p_i] = \ell_i$, so assume $\ell_1, \ell_2 \in H_1$ and $\ell_1\ell_2 = 0$ in $H_2/(Q)$. Considering $\ell_1, \ell_2 \in H_1$ as linear forms in $\mathbb{F}[X]$, we see that $\ell_1\ell_2$ is nonzero in H_2, but it is zero in $H_2/(Q)$. Thus the quadratic form $\ell_1\ell_2$ must be a nonzero scalar multiple of Q. Scaling ℓ_1 if necessary we may assume that $Q = \ell_1\ell_2$. But this is impossible: a nondegenerate quadratic form in more than four variables cannot equal the product of two linear forms. This contradiction shows that all elements of C_1 have the same annihilator, namely $\mathfrak{m}^2$.

Next, I want to choose unique representatives for the G-orbits of the ring. The notation used will be: if r is in the ring, then r_0 will denote the representative of the orbit Gr. If u is a unit, then I choose the representative of its orbit to be the identity element, so $u_0 = 1$. I choose representative elements from the orbits in C_1 arbitrarily.

For the orbits in C_2 I do the following: if $p, q \in C_1$ and $pq \in C_2$, then $(pq)_0 := p_0 q_0$. It is not immediately clear that this way of choosing representatives is well defined, so let's argue that it is. Suppose some orbit in C_2 contains pq and rs where $p, q, r, s \in C_1$. We must argue that $p_0 q_0 = r_0 s_0$. Note that $pq = [p][q]$ if $p, q \in C_1$, where (recall) $[p]$ denotes the linear part of p. Thus, if $pq, rs \in C_2$ lie in the same orbit, say $pq = \alpha rs$ for some $\alpha \in \mathbb{F}^\times$, then the homogeneous quadratic form $[p][q] - \alpha[r][s]$ represents the zero element in $S_{\mathbb{F},Q}$. This can only happen if the form $[p][q] - \alpha[r][s]$ is a scalar multiple of Q. This means that, either $[p][q] - \alpha[r][s]$ is zero as a form, or else Q is a scalar multiple of $[p][q] - \alpha[r][s]$. But this latter possibility cannot happen.

For, if Q is a scalar multiple of $[p][q] - \alpha[r][s]$ and the linear forms $[p], [q], [r], [s]$ are linearly independent, then Q is equivalent to the quadratic form $x_1x_2 - \alpha x_3x_4$. (If the linear forms involved were not linearly independent, then Q would be equivalent to something with even fewer variables.) But in this theorem we only consider forms Q which are nondegenerate forms in $n > 4$ variables. Under such a hypothesis, Q cannot be a scalar multiple of $[p][q]-\alpha[r][s]$. Hence $[p][q]-\alpha[r][s]$ is the zero form. By unique factorization in $\mathbb{F}[X]$ we get that $\{[p], [q]\} = \{\beta\alpha[r], \beta^{-1}[s]\} = \{[\beta\alpha r], [\beta^{-1}s]\}$ for some $\beta \in \mathbb{F}^\times$. If, say $[p] = [\beta\alpha r]$, then $[p_0] = [r_0]$, and similarly $[q_0] = [s_0]$. Thus $p_0q_0 = [p_0][q_0] = [r_0][s_0] = r_0q_0$.

The elements of C_3 lie in orbits in which any two elements differ by a nonzero scalar. I choose representatives of these orbits arbitrarily. Of course, the representative for $C_4 = \{0\}$ is 0.

Now that these generalities are out of the way, let Q_1 and Q_2 be nondegenerate quadratic forms in more than four variables. Define a function $\varphi\colon S_{\mathbb{F},Q_1} \to S_{\mathbb{F},Q_2}$ as follows.

(1) Defining φ to be a group isomorphism on the respective unit groups.
(2) Extend φ to an arbitrary bijection between the C_1-orbit representatives.
(3) Further extend φ to a bijection between the C_2-orbit representatives in the following way: If $p, q \in C_1$ (and so $pq \in C_2$) and pq is in the orbit represented by $(pq)_0 = p_0q_0$, then define $\varphi((pq)_0) = \varphi(p_0)\varphi(q_0)$ $(= \varphi(p_0)_0\varphi(q_0)_0)$.
(4) Extend further to a bijection between C_3 orbit representatives, then extend so that $\varphi(0) = 0$.
(5) Finally, extend φ to each orbit so that φ is a G-set isomorphism from $S_{\mathbb{F},Q_1}$ to $S_{\mathbb{F},Q_2}$. (By this I mean that if $p = \alpha p_0$ in $S_{\mathbb{F},Q_1}$, then $\varphi(p) = \varphi(\alpha)\varphi(p_0)$ in $S_{\mathbb{F},Q_2}$.)

We have already said enough to see that it is possible to do this. (I.e., the unit groups are isomorphic, the number and isomorphism types of orbits in each cell are the same.)

To complete the proof of Item (2) of the theorem we must show that φ is a monoid isomorphism. Since it is a G-set isomorphism, what remains to check is that if $pq = r$ with $p, q \in \mathbf{rad}(S_{\mathbb{F},Q_1})$, then $\varphi(p)\varphi(q) = \varphi(r)$. The only nontrivial case to check is when $p, q \in C_1$. Assume that $\alpha, \beta \in G$ are such that $p = \alpha p_0$ and $q = \beta q_0$. Then since φ is a G-set isomorphism and it preserves orbit representatives, $\varphi(p) = \varphi(\alpha)\varphi(p_0) = \varphi(\alpha)\varphi(p_0)_0$, $\varphi(q) = \varphi(\beta)\varphi(q_0) = \varphi(\beta)\varphi(q_0)_0$, and $\varphi(pq) = \varphi(\alpha\beta)\varphi((pq)_0)_0$. Hence

$$\varphi(p)\varphi(q) = \varphi(\alpha)\varphi(p_0)_0\varphi(\beta)\varphi(q_0)_0 = \varphi(\alpha\beta)\varphi((pq)_0)_0 = \varphi(pq).$$

[Item (3)] Suppose $\varphi\colon S_{\mathbb{F},Q_1} \to S_{\mathbb{F},Q_2}\colon x_i \mapsto p_i$ is an $\mathbb{F}$-algebra isomorphism. In the domain $\mathbb{F}$-algebra we have that

(1) $x_i^3 = 0$ for each i,
(2) $Q_1(x_1, \ldots, x_n) = 0$, and

(3) the set $\{x_1, \ldots, x_n\}$ is linearly independent.

The third of these items can be re-expressed as "no nonzero linear combination of the elements $\{x_1, \ldots, x_n\}$ annihilates all of the radical of $S_{\mathbb{F},Q_1}$". In the codomain algebra we must therefore have

(1) $p_i^3 = 0$ for each i,
(2) $Q_1(p_1, \ldots, p_n) = 0$, and
(3) no nonzero linear combination of the elements $\{p_1, \ldots, p_n\}$ annihilates all of the radical of $S_{\mathbb{F},Q_1}$.

Notice that the same three properties will hold if we replace each p_i by its homogeneous linear part, $[p_i] = \ell_i$. But for the homogeneous quadratic polynomial $Q_1(\ell_1, \ldots, \ell_n)$ to agree with 0 in $S_{\mathbb{F},Q_2}$ it is necessary that the form $Q_1(\ell_1, \ldots, \ell_n)$, which is obtained from Q_1 by an invertible linear change of variables, be a scalar multiple of $Q_2(x_1, \ldots, x_n)$. Thus if $S_{\mathbb{F},Q_1} \cong S_{\mathbb{F},Q_2}$ as $\mathbb{F}$-algebras, then Q_1 is equivalent to a nonzero scalar multiple of Q_2. □