Our main reference for all this is [1], which has aged beautifully.

Context: V is an n-dimensional vector space with basis $\{b_0, \ldots, b_{n-1}\}$ over field $\mathbb{K}$ of characteristic $p \neq 2$. (We allow $p = 0$ but forbid $p = 2$ here for simplicity.) V is equipped with a symmetric bilinear form $x \cdot y$. Usually V will be non-singular, meaning $\mathrm{rad}(V) = \{o\}$, equivalently $\mathrm{disc}(V) = \det([b_i \cdot b_j]) \neq 0$. Changing the basis will multiply $\mathrm{disc}(V)$ by a square $t^2 \in \mathbb{K}^* := \mathbb{K} \setminus \{0\}$. Thus the discriminant is really an invariant modulo $(\mathbb{K}^*)^2$.
Notation: For $u, v \in \mathbb{K}^*$ write $u \sim v$ if $u = t^2 v$ where $t \in \mathbb{K}^*$.

It is quite possible that such a V have non-zero isotropic vectors x (i.e. $x \cdot x = 0$). This is indeed always the case over finite fields $GF(q), q = p^m$, when $n \geqslant 3$, and also when $n = 2$ in one of the two possible spaces.

For any subspace $U \leqslant V$, let

$$U^{\perp} := \{x \in V : x \cdot y = 0, \forall y \in U\} .$$

General Properties. Assume V non-singular, with various subspaces U, W, etc.

1. $\dim(U) + \dim(U^{\perp}) = n$; $(U^{\perp})^{\perp} = U$; $V^{\perp} = \{0\}$.
2. $\mathrm{rad}(U) = \mathrm{rad}(U^{\perp}) = U \cap U^{\perp}$. (A subspace, eg. the line spanned by an isotropic vector, can be singular even if V is not.)
3. V is a direct sum of mutually orthogonal lines, written $V = \langle c_0 \rangle \perp \ldots \perp \langle c_{n-1} \rangle$. (This holds in general orthogonal spaces; then V is non-singular if-f all c_j are non-isotropic.)
4. U is non-singular if-f $U^{\perp}$ is non-singular. In this case, $V = U \perp U^{\perp}$. Conversely, $V = U \perp W$ implies U, W non-singular with $U^{\perp} = W$.
5. Suppose $\dim V = 2$, V is non-singular, and V has an isotropic vector $p \neq o$. Then V is a sadly named 'hyperbolic plane', meaning that it has a basis $\{p, q\}$ such that
   $p^2 = q^2 = 0, \;\; pq = 1$.

Extending Isometries

1. **Theorem**. Let U be any subspace of a non-singular space V. Suppose $U = \mathrm{rad}(U) \perp W$ and $\{p_1, \ldots, p_r\}$ is a basis for $\mathrm{rad}(U)$. Then
   (a) there exists $\{q_1, \ldots, q_r\}$ in V such that each (p_j, q_j) is a hyperbolic pair, and so that the hyperbolic planes $P_j = \langle p_j, q_j \rangle$ are mutually orthogonal (and all orthogonal to W). Thus $U \subseteq \overline{U} = P_1 \perp \ldots \perp P_r \perp W$, which is also a non-singular subspace of V.
   (b) Suppose V and V' are isometric spaces. Then any isometry σ mapping U **into** V' can be extended to $\overline{\sigma} : \overline{U} \to V'$.

2. **Theorem** (Witt) Let V, V' be isometric non-singular spaces. Let σ be an isometry of a subspace U of V into V'. Then σ can be extended to an isometry $\overline{\sigma} : V \to V'$. Furthermore, it is possible to prescribe the determinant (namely, ± 1) for $\overline{\sigma}$ if–f $\dim U + \dim \operatorname{rad} U < n$.

3. **Some consequences**. Let V be non-singular of dimension n.

   (a) All maximal isotropic subspaces have the same dimension r (the **Witt index**).

   (b) If U_1 and U_2 are isometric subspaces, then $U_1^\perp$ and $U_2^\perp$ are isometric.

   (c) Each maximal hyperbolic subspace (= sum of 'hyperbolic planes') has dimension $2r$, so $r \leqslant \lfloor \frac{n}{2} \rfloor$.

   (d) A hyperbolic subspace H_{2s} is maximal if-f $W = H_{2s}^\perp$ is **anisotropic** (contains no non-trivial isotropic vector): $V = H_{2r} \perp W$. Also, the geometry of W is independent of the choice of the subspace H_{2r}.

4. **Theorem** (fixed hyperplanes) Suppose $\sigma \in O(V)$ fixes a hyperplane H pointwise. Then if H is singular, $\sigma = e$ (identity). But if H is non-singular, then $\sigma = e$ or σ is the reflection in H. Thus isometries are determined in a corresponding way by their effect on any hyperplane.

5. **Theorem** (Cartan-Dieudonné) Say $\dim V = n$. Then every $\sigma \in O(V)$ is a product of at most n reflections (in non-singular hyperplanes).

   Compare what you know in Euclidean space: note here that we consider linear isometries, which do all fix o.

Computing the order and structure of $O(V)$. For deeper structure one really needs to study the Clifford algebra of V. But we can get some sense of more elementary properties of V by employing the above results to systematically count things like isotropic vectors and hyperbolic planes in V.

Orthogonal groups over finite fields.

1. Suppose $\mathbb{K} = GF(q)$, $q = p^m$, p odd. Then the map

$$\begin{array}{rcl} \mathbb{K}^* & \to & \mathbb{K}^* \\ t & \mapsto & t^2 \end{array}$$

   is a homomorphism with kernel ± 1. Thus the squares $(\mathbb{K}^*)^2$ have index 2 in $\mathbb{K}^*$, say with coset representatives 1 and some **fixed non-square** η.
   Example: In $\mathbb{Z}_p$ can take $\eta = -1$, if $p \equiv 3 \pmod 4$.

2. The orthogonal group $O(V) = \{g \in GL(V) : g(x) \cdot g(y) = x \cdot y, \forall x, y, \in V\}$. Notice that $O(V)$ is *unaffected by rescaling the form* (say $x * y := \alpha(x \cdot y)$ for some fixed $\alpha \in \mathbb{K}^*$). If $\mathrm{disc}(V) \neq 0$, then $\det(g) = \pm 1$ for $g \in O(V)$. The subgroup of isometries with determinant 1 is called the *special orthogonal group*, denoted $SO(V)$.

3. $n = 1$, say $V = \langle a \rangle$. One kind of geometry: up to rescaling, $a \cdot a = 1$, with orthogonal group $O(1, q, 0) \simeq \{\pm 1\}$. The parameter $\varepsilon = 0$ in $O(1, q, 0)$ is merely a convenient reminder that the dimension n is odd.

4. $n = 2$: There are two quite distinct geometries, distinguished by the parameter $\varepsilon = +1$ or -1.

   • If $\varepsilon = +1$, V has an isotropic basis and is thus a 'hyperbolic plane' (in the sense used in geometric algebra). For some basis the Gram matrix is $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $\mathrm{disc}(V) \sim -1$. Here $O(2, q, +1)$ is dihedral of order $2(q-1)$; and $x \cdot x$ takes on all values in $\mathbb{K}$. As generators we could take the reflections

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & \alpha \\ 1/\alpha & 0 \end{bmatrix},$$

   where α is a primitive generator for the cyclic group $\mathbb{K}^*$.

   • If $\varepsilon = -1$, V is anisotropic (only o is isotropic). For some basis the Gram matrix is $\begin{bmatrix} 1 & 0 \\ 0 & -\eta \end{bmatrix}$, and $\mathrm{disc}(V) \sim -\eta$. Again $x \cdot x$ takes on all values in $\mathbb{K}$. But $O(2, q, -1)$ has order $2(q+1)$. It is a little more involved to describe generating reflections.

5. $n = 3$: Again, there one kind of geometry, up to rescaling, with group $O(3, q, 0)$. The order of this group is $2q(q^2 - 1)$. For any dimension $n \geqslant 3$, V contains non-zero isotropic vectors.

6. **The general situation**.

If n is odd, then $O(n,q,0)$ has order $2\varphi_n$, where

$$\varphi_n := q^{(n-1)^2/4} \prod_{j=1}^{(n-1)/2} (q^{2j}-1) \, .$$

Each maximal totally isotropic subspace has dimension $(n-1)/2$.

If n is even, then $O(n,q,\varepsilon)$ has order $2\varphi_n$, where now

$$\varphi_n := q^{n(n-2)/4} \, (q^{n/2}-\varepsilon) \prod_{j=1}^{(n-2)/2} (q^{2j}-1) \, .$$

When $\varepsilon = +1$, the maximal totally isotropic subspaces all have dimension $n/2$ and $\mathrm{disc}(V) \sim (-1)^{n/2}$. When $\varepsilon = -1$, the maximal totally isotropic subspaces have dimension $(n/2)-1$; and $\mathrm{disc}(V) \sim (-1)^{n/2}\eta$.

7. **Some significant subgroups**.

It is known that $O(V)$ is generated by reflections (Cartan-Dieudonné). Recall that these must look like

$$r(x) = x - 2\frac{a \cdot x}{a \cdot a} a \, .$$

The root a is non-zero but clearly can be rescaled by any $t \in \mathbb{K}^*$, without affecting r or the quadratic nature of $a \cdot a$. Put otherwise, we can assume either that $a \cdot a = 1$ or that $a \cdot a = \eta$.

One can show that $O(n,q,\varepsilon)$ has precisely two conjugacy classes of reflections, namely those for which $a \cdot a = 1$ versus those with $a \cdot a = \eta$. These generate subgroups which we denote $O_1(n,q,\varepsilon)$, respectively $O_2(n,q,\varepsilon)$.

We need to be a little cautious: these subgroups will be swapped if we rescale our form by a non-square. But keeping that in mind, we find that usually $O_j(n,q,\varepsilon)$ has index 2 in $O(n,q,\varepsilon)$, and hence has order φ_n. (The exceptions are the 'smallish groups' $O(3,3,0)$ and $O(4,3,+1)$; see [2, Prop. 3.1] for details.)

When n is odd, the subgroups $O_1(n,q,\varepsilon)$ and $O_2(n,q,\varepsilon)$ are definitely non-isomorphic; but when n is even, the two subgroups are isomorphic.

References

[1] E. Artin, *Geometric Algebra*, Interscience, New York, 1957.

[2] B. Monson and E.Schulte, *Reflection groups and polytopes over finite fields- I*, Advances in Applied Mathematics, 33 (2004), pp. 290–217.