Let k be a field and let $\mathrm{OS}_n(k) = \left\{ A = A^T \text{ and } AA^T = I_n \right\}$ denote the set of orthogonal symmetric $n \times n$ matrices over k.
Does this set have an interesting structure with regards to the regular matrix operations?
The following simple lemma will be used throughout the following discussion.

Lemma 1
Let k be a field and $\lambda \in k$. Then $\lambda^2 = 1$ implies $\lambda = \pm 1$.

Proof. Factoring the polynomial to get $0 = \lambda^2 - 1 = (\lambda - 1)(\lambda + 1)$. As k is field it has no zero divisors and so either $\lambda - 1 = 0$ or $\lambda + 1 = 0$. □

Notation: I_n denotes the identity matrix of size n and C_m the cyclic group of order m i.e. $C_m = \mathbb{Z}/m\mathbb{Z}$

Addition

The zero matrix is not an element of $\mathrm{OS}_n(k)$ since all elements of $\mathrm{OS}_n(k)$ are invertible (all elements have order 2).
Let A be in $\mathrm{OS}_n(k)$. Then $-A = (-A)^T$ by definition and

$$(-A)(-A)^T = (-A)(-A) = I$$

implies that $-A \in \mathrm{OS}_n(k)$. So $\mathrm{OS}_n(k)$ is not closed under regular matrix addition.

Multiplication

The identity matrix is fortunately included in $\mathrm{OS}_n(k)$.

Case $n \geq 3$

Consider the matrix product:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \notin \mathrm{OS}_n(k)$$

The resulting matrix is not symmetric and by that $\mathrm{OS}_n(k)$ is not closed under multiplication for $n \geq 3$.

Case $n = 1$

All elements trivially fulfill $A = A^T$. This reduces the set to $\mathrm{OS}_1(k) = \left\{ A^2 = 1 \right\}$ or in other words all square roots of unity. Using the above lemma you can conclude $A = \pm 1$. This implies $\mathrm{OS}_1(k) = \begin{cases} C_1 & \text{if } \operatorname{char}(k) = 1 \\ C_2 & \text{if } \operatorname{char}(k) \neq 2 \end{cases}$.

Case $n = 2$

Case $\mathrm{char}(k) \neq 2$

Since $\mathrm{char}(k) \neq 2$ the elements 1 and -1 are not equal and the matrix product

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \notin \mathrm{OS}_2(k)$$

is not contained in $\mathrm{OS}_2(k)$.
Further can $\mathrm{OS}_2(k)$ be embedded into larger $\mathrm{OS}_n(k)$ via:

$$\begin{bmatrix} \mathrm{OS}_2(k) & 0 \\ 0 & I_{n-2} \end{bmatrix} \subseteq \mathrm{OS}_n(k)$$

This mapping preserves multiplication and restates the case for $n \geq 3$.

Case $\mathrm{char}(k) = 2$

All elements have order 2 so you get

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ b & c \end{bmatrix}^2 = \begin{bmatrix} a^2 + b^2 & ab + bc \\ ba + cb & b^2 + c^2 \end{bmatrix} = \begin{bmatrix} a^2 + b^2 & b(a + c) \\ b(a + c) & b^2 + c^2 \end{bmatrix}$$

If $b = 0$ then $a^2 = 1 = c^2$ which implies $a = 1 = c$.
Otherwise $a = c$ as $0 = b(a + c)$ implies $a + c = 0$ since k has no zero divisors. Focusing on the first entry you get

$$1 = a^2 + b^2 = (a + b)^2$$

which using the lemma implies $a + b = 1$ or in other words $b = a + 1$. Putting these all together you get:

$$\mathrm{OS}_2(k) = \left\{ \begin{bmatrix} \lambda & \lambda + 1 \\ \lambda + 1 & \lambda \end{bmatrix} \mid \text{for } \lambda \in k \right\}$$

Furthermore the map

$$k \to \mathrm{OS}_2(k) \,:\, \lambda \mapsto \begin{bmatrix} \lambda & \lambda + 1 \\ \lambda + 1 & \lambda \end{bmatrix}$$

is a bijection between k and $\mathrm{OS}_2(k)$. Whats left to show is that $\mathrm{OS}_2(k)$ is closed under multiplication:

$$\begin{bmatrix} \lambda & \lambda + 1 \\ \lambda + 1 & \lambda \end{bmatrix} \begin{bmatrix} \rho + 1 & \rho \\ \rho & \rho + 1 \end{bmatrix} = \begin{bmatrix} \lambda(\rho + 1) + (\lambda + 1)\rho & \lambda\rho + (\lambda + 1)(\rho + 1) \\ \lambda\rho + (\lambda + 1)(\rho + 1) & (\lambda + 1)\rho + \lambda(\rho + 1) \end{bmatrix} = \begin{bmatrix} \lambda + \rho & \lambda + \rho + 1 \\ \lambda + \rho + 1 & \lambda + \rho \end{bmatrix}$$

So $\mathrm{OS}_2(k)$ has a group structure with regards to the regular matrix multiplication. This calculation also shows that the group is abelian as addition is commutative in k.

Lemma 2
$\mathrm{OS}_2(k)$ is an abelian group.

Proof. All elements have order 2 by definition. Let A and B be in $\mathrm{OS}_2(k)$

$$AB = AB\ I_2 = AB\ (BA)^2 = AB\ BA\ BA = BA$$

This means that all elements commute with each other. □

Theorem 1
Let k be a finite field with $|k| = 2^m$, then $\mathrm{OS}_2(k) = C_2^m$

Proof. Using the classification of finite abelian groups you get that $\mathrm{OS}_2(k) = C_2^M$ for some $M \in \mathbb{N}$. Using the above bijection you get

$$2^m = |k| = |\,\mathrm{OS}_2(k)| = |C_2^M| = 2^M$$

and you can conclude $m = M$. □

Numerical exploration

The code for this implementation can be found in its git repository:

```
git://git.lemen.xyz/orthosymmetrical.git
```

The above shows that $\mathrm{OS}_n(k)$ carries no relevant structure for $n \geq 3$. Noting that the field $k = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ has exactly 2 elements, which can be easily mapped to binary bits, the following mapping into the integers is immediate:

$$M_{n\times n} \to \mathbb{Z} \ : \ \begin{bmatrix} b_1 & b_2 & \dots & b_n \\ b_{n+1} & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & b_{n\times n} \end{bmatrix} \mapsto \sum_{i=1}^{n^2} b_i 2^{i-1}$$

This mapping sends a matrix to the integer represented by a binary string (in least significant bit order) and gives also rise to an ordering on $M_{n\times n}$ by retracting the ordering on $\mathbb{Z}$ back onto the matrices. In other words: You interpret the matrix as a single binary represented integer. The ordering is used in the following discussion when talking about the *smallest* and *largest* matrices. With this mapping you can easily enumerate all matrices in $M_{n\times n}$ by using its partial inverse map.
Examples $n = 3$

$$1 = 100000000_2 \mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad 311 = 111011001_2 \mapsto \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

The enumeration has been implemented to calculate the sizes of the sets $\mathrm{OS}_n(\mathbb{F}_2)$ for some small n:

n	1	2	3	4	5	6	7	8	9
$\lvert \mathrm{OS}_n(\mathbb{F}_2) \rvert$	1	2	4	20	76	752	5104	104960	?

This sequence is currently not found in the OEIS which indicates that the above discussion probably fruitless. Also the sizes of the matrix rings $M_{n\times n}(\mathbb{F}_2)$ are increasing exponentially, so enumerating them becomes inefficient.

Implementation details

Some speedups can be achieved when considering the inherent structure of $\mathrm{OS}_n(k)$. As we are only considering symmetric matrices it is enough to set half the matrix and reflect it along its diagonal. This reduces the search space from n^2 to $n(n+1)/2$ and cuts it approximately in half. It is also useful to note that this reduction preserves the ordering. In the case for $n = 4$:

$$b_1 \cdots b_{10} \mapsto \begin{bmatrix} b_1 & b_2 & b_3 & b_4 \\ b_2 & b_5 & b_6 & b_7 \\ b_3 & b_6 & b_8 & b_9 \\ b_4 & b_7 & b_9 & b_{10} \end{bmatrix}$$

The smallest index is a matrix with 1 on its anti-diagonal:

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Proof. You can calculate that the proposed starting index is indeed in $\mathrm{OS}_n(k)$.
As each element in $\mathrm{OS}_n(k)$ is invertible, the minimal element can not have a zero row or column. This implies that each row must have at least one 1. Indeed it is the case that there is no smaller invertible matrix with that property:
None of the entries right of the anti-diagonal can be 1 as they would be larger than the proposed starting index. This leaves a matrix in triangle form. As the matrix is invertible it needs to have full rank. If any of the entries on the anti-diagonal would be 0 the rank would not be full. Then if any of the entries left of the anti-diagonal would be 1 it would again be bigger than the proposed matrix. □

The end indices depend on the dimension:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

even dimension odd dimension

Proof. You can check that both type of matrices are contained in their respective $\mathrm{OS}_n(k)$.
Consider the even case first. Every row and column needs to have an odd number 0s or the square will not be equal to I_n. It follows that every row needs to have at least one 0. This implies that the last row is equal to the proposed row as shifting the 0 to any other place would decrease the associated index. The same reasoning can be applied to the next row with the caveat that the 0 can't be further left as this would duplicate a row beneath it.
The argument for the odd case is similar with the difference that every row needs to have an even number of 0s. No row can have only 1s as this would make the square not equal I_n again. □