Simple Groups Made Relatively Simple

(or at least as simple as I could possibly make them)

William Paulsen

This is my attempt to make the Chevalley groups, which is the largest class of finite simple groups, understandable to those who are not experts in the field. A basic understanding of linear algebra is needed, plus enough group theory to understand what a simple group is, as well as an automorphism group. If anyone spots an error in this explanation, please let me know.

The classification theorem of finite simple groups says that all finite simple groups are of one of the following categories: Note that q will always be a power of a prime, so $q = p^m$ for some prime p and $m \geq 1$.

1) The cyclic groups Z_p, where p is a prime number.
2) The alternating groups A_n, for $n \geq 5$,
3) The Chevalley groups:
   - 3a) The projective special linear groups $L_n(q)$, with $n \geq 2$, except for $L_2(2)$ and $L_2(3)$.
   - 3b) The special orthogonal groups $B_n(q)$, with $n \geq 2$, except for $B_2(2)$.
   - 3c) The projective sympletic groups $C_n(q)$, with $n \geq 2$, except for $C_2(2)$.
   - 3d) $D_n(q)$, with $n \geq 3$.
4) The exceptional Chevalley groups:
   - 4a) $E_6(q)$, with $q \geq 2$.
   - 4b) $E_7(q)$, with $q \geq 2$.
   - 4c) $E_8(q)$, with $q \geq 2$.
   - 4d) $F_4(q)$, with $q \geq 2$.
   - 4e) $G_2(q)$, with $q \geq 3$.
5) The twisted Chevalley groups:
   - 5a) The projective special unitary groups $U_n(q)$, where $n \geq 3$ and q is a perfect square.
   - 5b) ${}^2D_n(q)$, with $n \geq 2$.
6) The exceptional twisted Chevalley groups:
   - 6a) ${}^3D_4(q)$, with $q \geq 2$.
   - 6b) ${}^2F_4(2^{2n+1})$, where $n \geq 1$.
   - 6c) The Tits group ${}^2F_4(2)'$.
   - 6d) ${}^2G_2(3^{2n+1})$, where $n \geq 1$.
   - 6e) ${}^2B_2(2^{2n+1})$, where $n \geq 1$.
   - 6f) ${}^2E_6(q)$, where $q \geq 2$.
7) One of the 26 sporadic groups, ranging in size from M_{11}, with 7920 elements, to the monster group M with 808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000 elements.

Finite fields

All of the Chevalley groups are based on finite fields, so some knowledge of finite fields are needed. A finite field F is a finite set with two operations, ($+$ and $\cdot$), such that the set is an abelian group with respect to $+$, with additive identity 0, and that $F - \{0\}$ is an abelian group with respect to $\cdot$. Also, the distributive law $x \cdot (y + z) = x \cdot y + x \cdot z$ must hold. The simplest finite fields are Z_p with p prime, where both addition and multiplication is done modulo p.

It turns out that a finite field must have an order that is a power of a prime. Furthermore, if $q = p^m$ for p prime and $m \geq 1$, then there will be (up to isomorphism) exactly one field of order q. In fact, it can be constructed from Z_p fairly easily. We begin by finding *any* irreducible polynomial over Z_p of degree m: $x^m + a_{m-1}x^{m-1} + \cdots + a_2x^2 + a_1x + a_0$. We then let a new variable, say y, denote a "complex" root to this equation. We consider the set of all expressions of the form

$$c_{m-1}y^{m-1} + \cdots + c_2y^2 + c_1y + c_0$$

where $c_0, c_1, \ldots, c_{n-1}$ are in Z_p. Addition of such expressions is done in the natural way, and so is multiplication, except that y^m will be able to be simplified via $y^m = -a_{m-1}y^{m-1} - \cdots - a_2y^2 - a_1y - a_0$.

Ironically, it makes no difference which irreducible polynomial of degree m you choose, they will all give the same field isomorphically. The new field of order $q = p^m$, denoted F_q, will have an additive group

isomorphic to $Z_p \times Z_p \times \cdots \times Z_p$, ($m$ factors), and the multiplicative group of $F - \{0\}$ is cyclic, meaning that there is some element g such that all non-zero elements can be expressed as g^k for some k.

For example, to find the field of order 3, we can choose the irreducible polynomial $x^2 + 1$. This is irreducible in Z_3, since neither 0, 1, or 2 are roots. We can let i be the new element which will be a root to the polynomial. The new field has order 9, and can be called the "complex numbers Mod 3." Here are the addition and multiplication tables of this field.

Addition table for "Complex numbers Mod 3"

$+$	0	1	2	i	$2i$	$1+i$	$2+i$	$1+2i$	$2+2i$
0	0	1	2	i	$2i$	$1+i$	$2+i$	$1+2i$	$2+2i$
1	1	2	0	$1+i$	$1+2i$	$2+i$	i	$2+2i$	$2i$
2	2	0	1	$2+i$	$2+2i$	i	$1+i$	$2i$	$1+2i$
i	i	$1+i$	$2+i$	$2i$	0	$1+2i$	$2+2i$	1	2
$2i$	$2i$	$1+2i$	$2+2i$	0	i	1	2	$1+i$	$2+i$
$1+i$	$1+i$	$2+i$	i	$1+2i$	1	$2+2i$	$2i$	2	0
$2+i$	$2+i$	i	$1+i$	$2+2i$	2	$2i$	$1+2i$	0	1
$1+2i$	$1+2i$	$2+2i$	$2i$	1	$1+i$	2	0	$2+i$	i
$2+2i$	$2+2i$	$2i$	$1+2i$	2	$2+i$	0	1	i	$1+i$

Multiplication table for "complex numbers Mod 3"

$\cdot$	0	1	2	i	$2i$	$1+i$	$2+i$	$1+2i$	$2+2i$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	i	$2i$	$1+i$	$2+i$	$1+2i$	$2+2i$
2	0	2	1	$2i$	i	$2+2i$	$1+2i$	$2+i$	$1+i$
i	0	i	$2i$	2	1	$2+i$	$2+2i$	$1+i$	$1+2i$
$2i$	0	$2i$	i	1	2	$1+2i$	$1+i$	$2+2i$	$2+i$
$1+i$	0	$1+i$	$2+2i$	$2+i$	$1+2i$	$2i$	1	2	i
$2+i$	0	$2+i$	$1+2i$	$2+2i$	$1+i$	1	i	$2i$	2
$1+2i$	0	$1+2i$	$2+i$	$1+i$	$2+2i$	2	$2i$	i	1
$2+2i$	0	$2+2i$	$1+i$	$1+2i$	$2+i$	i	2	1	$2i$

The only other piece of information needed about finite fields is that the mapping $x \to x^p$ will always be an automorphism on the field, called the Frobenius automorphism. This automorphism will have order m. In fact, all field automorphisms are generated from this one, so the automorphism group for a field of order p^m is isomorphic to Z_m. If m is even, we can form the automorphism $\phi(x) = x^{p^{m/2}}$, which will have order 2. This automorphism can be thought of as the "conjugate" automorphism, since $\phi(\phi(x)) = x$ for all x.

We are now ready to understand the Chevalley groups, starting with the easiest.

$\mathbf{L}_n(\mathbf{q})$

The first group to consider is the n by n matrices with determinant 1 over a field of size $q = p^m$, where p is prime. When $m = 1$, we are merely working with matrices over Z_p. For example, if $n = 2$, and $q = 7$, we have some of the matrices to be

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 6 & 0 \end{pmatrix}, \begin{pmatrix} 5 & 5 \\ 2 & 5 \end{pmatrix}, \ldots.$$

Notice that the determinant of all of these is 1 (mod 7), so there is no problem with inverses. However, this is not a simple group, since there is (usually) a non-trivial center!

$$\begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix} A = A \begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}.$$

In fact, aI will be in the center whenever $a^n = 1$ in the field. The solution is to consider the quotient group over the center. That is,

$$L_n(q) = \{n \times n \text{ matrices over } F_q \text{ with determinant } 1\}/\{\text{its center}\}.$$

This is a Chevalley group, since it is basically the continuous group

$$L_n(\mathbb{R}) = \{n \times n \text{ matrices over } \mathbb{R} \text{ with determinant } 1\}/\{\pm I\}.$$

with real numbers replaced with a finite field.

We can introduce the following notation: by $\pm A$, we mean the coset of all matrices aA for which the scalar a satisfies $a^n = 1$. So for $q = 7$,

$$\pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 6 & 6 \\ 0 & 6 \end{pmatrix} \right\}.$$

Usually, $\pm A$ will consist of A and possibly its additive inverse, but there are occasions where $\pm A$ might mean something more. For example, if $n = 3$ and $q = 7$, then there are 3 solutions to $a^3 = 1$. So

$$\pm \begin{pmatrix} 1 & 5 & 0 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & 5 & 0 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 3 & 0 \\ 0 & 2 & 6 \\ 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 6 & 0 \\ 0 & 4 & 5 \\ 0 & 0 & 4 \end{pmatrix} \right\}.$$

In general, the number of solutions to $a^n = 1$ in the finite field of order q is given by $\mathrm{GCD}(n, q-1)$. With this, we can find the size of this group as

$$|L_n(q)| = \frac{q^{n(n-1)/2}}{\mathrm{GCD}(n, q-1)} \prod_{i=2}^{n} (q^i - 1).$$

Here, the $\prod$ symbol is like the $\sum$ symbol, only the terms are multiplied instead of added. Thus,

$$\prod_{i=2}^{n} (q^i - 1) = (q^2 - 1)(q^3 - 1)(q^4 - 1) \cdots (q^n - 1).$$

From this formula, we find that

$$L_2(7) = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ 6 & 0 \end{pmatrix}, \pm \begin{pmatrix} 5 & 5 \\ 2 & 5 \end{pmatrix}, \ldots \right\}$$

and

$$L_3(2) = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ldots \right\}$$

both have 168 elements. In fact, these two simple groups are isomorphic. (We don't need the $\pm$ sign for the elements in $L_3(2)$, since there is only one solution to $a^3 = 1 \bmod 2$.) $L_n(q)$ will be a simple group if $n = 2$ and $q \geq 4$, or if $n \geq 3$. However, $L_2(4) \approx L_2(5) \approx A_5$, $L_2(9) \approx A_6$, and $L_4(2) \approx A_8$.

Alternative names: $L_n(q)$ is also called $\mathrm{PSL}_n(q)$, $\mathrm{PSL}(n, q)$ the *projective special linear group*, and $A_{n-1}(q)$.

$\mathbf{B_n(q)}$

Other simple groups can be formed from subgroups of $L_n(q)$ whose elements possess certain qualities.

If we let J be an $m \times m$ fixed non-singular matrix with elements from F_q, we can consider all $m \times m$ matrices A with elements in F_q such that

$$A^T J A = J, \qquad \text{and} \quad |A| = 1.$$

The set of all such matrices A forms a group, since if $B^T J B = J$ as well,

$$\begin{aligned}(AB^{-1})^T J (AB^{-1}) &= (B^{-1})^T (A^T J A) B^{-1} \\ &= (B^{-1})^T J B^{-1} \\ &= (B^{-1})^T (B^T J B) B^{-1} \\ &= ((B^{-1})^T B^T) J (B B^{-1}) = J.\end{aligned}$$

We can call this subgroup G_J, and as with $L_q(n)$, may contain a non-trivial center. So we can consider the quotient group $G_J/\{\pm I\}$. (If q is even, then the center will be trivial, since $-1 = 1$ in the field.)

However, $G_J/\{\pm I\}$ is (usually) still not a simple group, but like S_n contains a simple group of index 2, so we can assign a *signiture* to the elements of $G_J/\{\pm I\}$. The easiest way to do this (without getting technical) is to say that an element of $G_J/\{\pm I\}$ is even if it can be expressed as a product of squares, and odd if it cannot be expressed as such a product.

If the size of the matrix is odd, say of size $m = 2n+1$, then G_J will yield isomorphically the same group for all non-singular symmetric matrices J. Since it doesn't matter which matrix we pick for J, we might as well pick $J = I$. Furthermore, since m is odd the determinant of $-I$ will be -1, so $-I$ will not be in G_J. In fact, if aI was in the set, then $a^m = 1$ and also $a^2 = 1$, since $(aI)^T(aI)$ must be I. This forces $a = 1$, so in this case, we do not need to take the quotient group of the center. We define (for q odd)

$$B_n(q) = \{\text{Even } (2n+1) \times (2n+1) \text{ matrices over } F_q \text{ such that } A^T A = I, \text{ and } |A| = 1\}.$$

If q is a power of 2, then $-1 = 1$ in the field, so $|A|$ will always be 1 if $A^T A = I$. Also, in this case we do not have to pick out the "even" elements, for we will have the whole group. Again, the center would just be I, so we do not have to take the quotient group of the center. Thus,

$$B_n(2^r) = \{(2n+1) \times (2n+1) \text{ matrices over } F_{2^r} \text{ such that } A^T A = I\}.$$

The size of this group (for both even and odd q) is given by

$$|B_n(q)| = \frac{q^{n^2}}{\mathrm{GCD}(2, q-1)} \prod_{i=1}^{n} (q^{2i} - 1).$$

For example, if $n = 1$ and $q = 3$, we see that this formula produces 12 elements. How can we find these elements? Each row (and each column) of an orthogonal matrix (one that $A^T A = I$) must be a unit vector. Working modulo 3, we find that the only unit vectors (solutions to $a^2 + b^2 + c^2 \equiv 1 \bmod 3$) are $(1,0,0)$, $(2,0,0)$, $(0,1,0)$, $(0,2,0)$, $(0,0,1)$, and $(0,0,2)$. Thus, a 3×3 orthogonal matrix mod 3 must have only 3 non-zero elements. It is not hard to see that this would produce 48 matrices, and if we throw out those with determinant 2 instead of 1, we would have 24 matrices. So which 12 matrices are in $B_1(3)$? Since

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

are squares of each other, these must both be in $B_1(3)$. Also,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 2 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix},$$

so this gives another matrix in $B_1(3)$. The 12 elements generated from these 3 matrices are

$$B_1(3) = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \right.$$
$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 2 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 2 \\ 2 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$
$$\left. \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 2 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \\ 1 & 0 & 0 \end{pmatrix} \right\}.$$

Obviously this is not a simple group, and is in fact isomorphic to A_4. In fact, $B_1(q) \approx L_2(q)$, so we do not get any new simple groups unless $n \geq 2$. However, $B_n(q)$ is a new simple group for all $n \geq 2$ with one exception—$B_2(2)$. This would be 5×5 orthogonal matrices mod 2:

$$B_2(2) = \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}, \dots \right\}$$

In fact, all elements of $B_2(2)$ can be obtained by exchanging rows and/or columns of the few matrices listed here. A simple counting argument shows that there are 720 elements of $B_2(2)$ (recall that when q is even, we do not have to throw out the "odd" elements.) In fact, $B_2(2) \approx S_6$, which is not simple. The smallest new simple group we get this way is $B_2(3)$, which has size 25920.

Alternative names: $B_n(q)$ is also called $O_{2n+1}(q)$, $P\Omega^+_{2n+1}(q)$, $\Omega_{2n+1}(q)$,and $\mathrm{PSO}_{2n+1}(q)$, the *special orthogonal group*.

$\mathbf{U}_n(\mathbf{q})$

Note that there is a natural automorphism on the group $L_n(q)$, given by $\tau(A) = (A^T)^{-1}$, since

$$\tau(AB) = ((AB)^T)^{-1} = (B^T A^T)^{-1} = (A^T)^{-1}(B^T)^{-1} = \tau(A)\tau(B).$$

This automorphism is clearly of order 2, since $\tau(\tau(A)) = A$. But if q is a perfect square, such as the case of "complex numbers mod 3",

$$\{0, 1, 2, i, 2i, 1+i, 2+i, 1+2i, 2+2i\},$$

then there is another automorphism of order 2 arising from the field—namely the "complex conjugate." If q is a perfect square, then $\phi(x) = x^{\sqrt{q}}$ will be a field automorphism, and $\phi(\phi(x)) = x^q = x$ for all elements in the field. ($x^{q-1} = 1$ for all non-zero x, since the multiplicative group is of order $q-1$.) We can extend this field automorphism ϕ to matrices, where we simply take the "complex conjugate" of all of the entries. We will write $\phi(A)$ as $\overline{A}$, the complex conjugate of A.

Now the set of elements fixed by $\tau(A)$, that is, the matrices for which $\tau(A) = A$, will simply be the orthogonal matrices of $L_n(q)$. Also, the set of elements for which $\overline{A} = A$ will produce $L_n(\sqrt{q})$. But if we first combine the two automorphisms, $\phi(\tau(A)) = \tau(\phi(A))$, and consider the elements fixed by this combination, we get a new group. If $\phi(\tau(A)) = A$, then $\tau(A) = \phi(A)$, given us $A^T\overline{A} = I$. These are called *unitary matrices.*

We can now define, for q a perfect square,

$$U_n(q) = \{n \times n \text{ matrices over } F_q \text{ with } |A| = 1 \text{ and } A^T\overline{A} = I\}/\{\pm I\}.$$

Then time, we define $\pm I$ to mean the set containing aI for all a such that both $a^n = 1$ and $a\overline{a} = 1$ in the field.

The size of this group is

$$|U_n(q)| = \frac{q^{n(n-1)/4}}{\mathrm{GCD}(n, \sqrt{q}+1)} \prod_{i=2}^{n} (q^{i/2} - (-1)^i).$$

For example, $U_3(9)$ would have 6048 elements. How would we find this matrices? First we would find all 3 dimensional vectors in "complex numbers mod 3" such that $\overline{v}v^T = 1$. Then we would look for sets of these vectors that are mutually "conjugate orthogonal", meaning that $\overline{v}w^T = 0$. There turns out to be 252 vectors for which $\overline{v}v^T = 1$, but all of them look similar to one of the vectors

$$\langle 1, 0, 0\rangle, \langle 1+i, 1+i, 0\rangle, \text{ or } \langle 1+i, 1, 1\rangle,$$

except that the coordinates can be rearranged, and each coordinate can independently be multiplied by either 1, 2, i, or $2i$. Next, we find sets of three such vectors that are mutually conjugate orthogonal. Some examples are

$$\begin{pmatrix} i & 0 & 0 \\ 0 & 2i & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1+i & 1+i \\ 0 & 1+i & 2+2i \end{pmatrix}, \begin{pmatrix} 0 & 1+i & 2+i \\ 2+i & 1 & 2i \\ 1+2i & 1 & 2i \end{pmatrix}, \begin{pmatrix} 2+2i & i & 1 \\ 2i & 2+2i & i \\ 1 & 2i & 2+2i \end{pmatrix}, \ldots.$$

In fact, all matrices for which $A^T\overline{A} = I$ can be obtained from one of these 4 by switching rows and/or columns, and multiplying rows and/or columns by 1, 2, i, or $2i$.

Finally, we have to consider only those matrices that have determinant 1, which gets rid of 3/4 of the matrices. But is there a center of the group that we have to worry about? Since $a^3 = 1$ in this field only when $a = 1$, the answer is no. Thus, $U_3(9) =$

$$\left\{ \begin{pmatrix} i & 0 & 0 \\ 0 & 2i & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 & 0 \\ 0 & 1+i & 1+i \\ 0 & 1+i & 2+2i \end{pmatrix}, \begin{pmatrix} 0 & 1+2i & 1+i \\ 2+i & 1 & 2i \\ 1+2i & 1 & 2i \end{pmatrix}, \begin{pmatrix} 1+2i & 2 & i \\ 1 & 1+2i & 2 \\ i & 1 & 1+2i \end{pmatrix}, \ldots \right\},$$

which gives us 6048 elements. This is the smallest new simple group of this type.

Another example would be to find $U_3(4)$. Since $x^2 = -1$ has a solution in F_2, we need another quadratic equation which does not have a solution in F_2 (any one will do.) So we will let ω be a solution to the equation $x^2 + x = 1$, and so we get the field $F_4 = \{0, 1, \omega, 1+\omega\}$. The "complex conjugate" would fix 0 and 1, but exchange the other two elements. Now all three non-zero elements satisfy $a^3 = 1$ and $a\overline{a} = 1$, so the coset $\pm I$ now contains three matrices. By finding the 36 vectors for which $vv^T = 1$, and then determining which set of three vectors are mutually conjugate orthogonal, we find that $U_3(4)$ has 72 elements:

$$\left\{ \pm \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & 1+\omega \end{pmatrix}, \pm \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & 1+\omega \\ 1 & 1+\omega & \omega \end{pmatrix},$$

$$\pm \begin{pmatrix} 1 & \omega & \omega \\ 1+\omega & \omega & 1+\omega \\ 1+\omega & 1+\omega & \omega \end{pmatrix}, \pm \begin{pmatrix} 1 & 1+\omega & 1+\omega \\ \omega & \omega & 1+\omega \\ \omega & 1+\omega & \omega \end{pmatrix}, \ldots \right\},$$

where the remaining entries are formed by exchanging rows and/or columns on one of these 5 matrices. Since there are no simple groups of order 72, we see that $U_3(4)$ is not simple. Also, $U_4(4) \approx B_2(3)$, but we get new simple groups if $n \geq 3$ and $q \geq 9$, or if $n \geq 5$.

Alternative names: $U_n(q)$ is also called ${}^2A_{n-1}(\sqrt{q})$, ${}^2A_{n-1}(q)$ and $\mathrm{PSU}_n(q)$, the *Projective Special Unitary group*.

$\mathbf{C}_n(\mathbf{q})$

If the size of the matrix is even, then there are other matrices J that produce interesting groups. The first of these is $J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$. We define a $2n \times 2n$ matrix A is *symplectic* if

$$A^T \cdot \left(\begin{array}{c|c} \mathbf{0} & I \\ \hline -I & \mathbf{0} \end{array}\right) \cdot A = \left(\begin{array}{c|c} \mathbf{0} & I \\ \hline -I & \mathbf{0} \end{array}\right)$$

Here, the $2n \times 2n$ matrix J is partitioned into four $n \times n$ pieces. For example, if $n = 1$, then $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and the 2×2 matrix A is symplectic if

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & ad-bc \\ bc-ad & 0 \end{pmatrix}$$

produces J, which of course happens if and only if $|A| = 1$. In fact, all symplectic matrices will have determinant 1. If we factor out the center as we have been doing, we get the group

$$C_n(q) = \{2n \times 2n \text{ symplectic matrices over } F_q\}/\{\pm I\}.$$

Again, if q is a power of 2, then $-I = I$, so the center will be trivial. We saw above that $C_1(q) = L_2(q)$, so nothing new happens unless $n \geq 2$. For example,

$$C_2(2) = \left\{ \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ *&0&1&0 \\ 0&*&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&0 \\ 0&0&0&1 \\ *&0&1&0 \\ 0&1&0&* \end{pmatrix}, \begin{pmatrix} 0&1&0&0 \\ 1&0&0&0 \\ 0&*&0&1 \\ *&0&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0 \\ 1&0&0&0 \\ 1&*&0&1 \\ *&1&1&0 \end{pmatrix}, \ldots \right\}.$$

Here, each $*$ can represent either a 0 or 1. There are 720 elements of $C_2(2)$, which in this case is not simple, since $C_2(2) \approx S_6$.

In general, the size of this group is given by

$$|C_n(q)| = \frac{q^{n^2}}{\text{GCD}(2, q-1)} \prod_{i=1}^{n} (q^{2i} - 1),$$

which you may notice is the same size as $B_n(q)$. In fact, $C_2(q) \approx B_2(q)$, so in order to get new groups, we must have $n \geq 3$. Also, if q is a power of 2, we find that J is a symmetric matrix (since $-1 = 1$), which causes $C_n(2^r) \approx B_n(2^r)$. However, if $n \geq 3$ and q is odd, we get a new simple group $C_n(q)$ that is the same size as $B_n(q)$, yet not isomorphic. If we define "twin simple groups" as two groups that are both simple, have the same size, yet are not isomorphic, then we find that $\{B_n(q), C_n(q)\}$ with q odd and $n \geq 3$ give an infinite number of "twin simple groups". The only other case of a "twin simple group" that is not in this list is $\{A_8, L_3(4)\}$. (Both A_8 and $L_3(4)$ have 20160 elements, yet they are not isomorphic.) The smallest new simple group we get in this way is $C_3(3)$ with 4585351680 elements.

Alternative names: $C_n(q)$ is also called $S_{2n}(q)$, and $\text{PSp}_{2n}(q)$, the *Projective Symplectic group*.

$\mathbf{D}_n(\mathbf{q})$ and ${}^2\mathbf{D}_n(\mathbf{q})$

When the size of the matrix is $2n$, then there are two other simple groups that can be formed by considering the group

$$G_J = \{2n \times 2n \text{ matrices over } F_q \text{ such that } A^T J A = J, \qquad \text{and} \quad |A| = 1\}.$$

for a fixed matrix J. We will begin by first discussing the case where the size of the field q is odd. Unlike the case $B_n(q)$, it will make a difference which symmetric matrix J we pick. For some symmetric matrices J,

the group G_J will be isomorphic to G_I, the group of standard orthogonal matrices for which $A^TA = I$. But for other J, we will get a group isomorphic to G_K, where K is a diagonal matrix with all but one diagonal element equal to 1,

$$K = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & a \end{pmatrix}$$

where a is some element of the field which is not a perfect square. (That is, $x^2 = a$ has no solution in the field. Since q is odd, there will always be such an element.) In fact, for all symmetric matrices J, G_J will either be isomorphic to G_I or G_K, so we only have to consider these two cases. In both cases there will be a non-trivial center, since $|-I| = 1$. As in $B_n(q)$, we will also have to weed out the "odd" elements for the case G_I, but not for G_K. Thus, we have 2 candidates for simple groups when q is odd:

$$O_1(n,q) = \{\text{Even } 2n \times 2n \text{ matrices over } F_q \text{ such that } A^TA = I, \text{ and } |A| = 1\}/\pm I,$$

and

$$O_2(n,q) = \{2n \times 2n \text{ matrices over } F_q \text{ such that } A^TKA = K, \text{ and } |A| = 1\}/\pm I.$$

Both of these are usually simple groups, and it would seem like it would be natural to define $D_n(q)$ to be one of these groups, and ${}^2D_n(q)$ the other. But alas, it is not quite that simple. Instead, we define

$$D_n(q) = \begin{cases} O_1(n,q) & \text{if } q^n \equiv 1 \text{ (Mod 4)} \\ O_2(n,q) & \text{if } q^n \equiv 3 \text{ (Mod 4)} \end{cases},$$

$${}^2D_n(q) = \begin{cases} O_1(n,q) & \text{if } q^n \equiv 3 \text{ (Mod 4)} \\ O_2(n,q) & \text{if } q^n \equiv 1 \text{ (Mod 4)} \end{cases}.$$

For example, if we find all 6×6 orthogonal matrices modulo 3, we find that there are 26127360 of them, and half of these have determinant 1 (Mod 3). A few of which are

$$\left\{ \begin{pmatrix} 2&2&2&2&0&0 \\ 0&0&0&0&1&0 \\ 1&1&1&0&0&1 \\ 1&1&0&1&0&1 \\ 1&0&1&1&0&1 \\ 0&1&1&1&0&1 \end{pmatrix}, \begin{pmatrix} 2&1&2&2&0&0 \\ 1&2&2&2&0&0 \\ 1&1&0&0&1&1 \\ 2&2&0&0&1&1 \\ 0&0&2&1&2&1 \\ 0&0&1&2&2&1 \end{pmatrix}, \begin{pmatrix} 1&2&1&2&0&0 \\ 1&1&2&2&0&0 \\ 0&1&1&0&1&1 \\ 0&2&2&0&1&1 \\ 1&0&0&1&2&1 \\ 1&0&0&2&1&2 \end{pmatrix}, \ldots \right\}$$

We can square this matrices to produce "even" elements of the group, and also divide by the center by inserting a $\pm$ sign. We get

$$\left\{ \pm \begin{pmatrix} 2&2&0&0&2&1 \\ 1&0&1&1&0&1 \\ 0&1&1&0&1&2 \\ 0&1&0&1&1&2 \\ 1&2&1&1&0&0 \\ 2&0&2&2&1&0 \end{pmatrix}, \pm \begin{pmatrix} 2&1&0&0&1&1 \\ 1&2&0&0&1&1 \\ 0&0&1&1&1&2 \\ 0&0&2&2&1&2 \\ 1&1&2&1&0&0 \\ 2&2&2&1&0&0 \end{pmatrix}, \pm \begin{pmatrix} 0&0&1&0&0&0 \\ 2&0&0&1&1&1 \\ 0&2&0&1&1&1 \\ 1&1&0&0&2&2 \\ 1&1&0&2&0&2 \\ 1&1&0&2&2&0 \end{pmatrix}, \ldots \right\},$$

which generates a group of order 3265920. However, this is not the group $D_3(3)$, but rather ${}^2D_3(3)$ from the definition. To get $D_3(3)$, we would begin with the 24261120 matrices for which $A^TKA = K$, (using $a = 2$). Half of these will have determinant 1, but this time we do not have to weed out the odd elements, so when we divide by the center, we get 6065280 elements of $D_3(3)$.

So why this switcheroo? One explanation comes from the fact that it is easier to define the size of these two groups:

$$|D_n(q)| = \frac{q^{n(n-1)}(q^n-1)}{\mathrm{GCD}(q^n-1,4)}\prod_{i=1}^{n-1}(q^{2i}-1),$$

$$|^2D_n(q)| = \frac{q^{n(n-1)}(q^n+1)}{\mathrm{GCD}(q^n+1,4)}\prod_{i=1}^{n-1}(q^{2i}-1).$$

Yet some further explanation is warranted. We say that the $2n \times 2n$ matrix J is *plus type* if there is an n-dimensional subspace V such that $vJv^T = 0$ for all vectors v in V. If there is no such n-dimensional subspace, then J is of *minus type*. It is not too hard to see that if $q^n \equiv 1$ (Mod 4), then I is plus type, and K is minus type. Yet if $q^n \equiv 3$ (Mod 4), then I is minus type, and K is plus type. Consider the case $n = 1$ for $q = 3$ and $q = 5$:

If $q = 3$, then letting $v = \langle x, y\rangle$, we have $vIv^T = x^2 + y^2$, and the only solution for $x^2 + y^2 \equiv 0$ (Mod 3) would be if both x and y are 0. So there is no 1-dimensional subspace V, hence I is of the minus type. On the other hand (picking $a = 2$), $vKv^T = x^2 + 2y^2$, and $x^2 + 2y^2 \equiv 0$ (Mod 3) does have a non-zero solution, $x = y = 1$. By letting V be the 1-dimensional subspace spanned by this solution, we see that K is of plus type.

When $q = 5$, though, the situation is reversed. There is a solution for $x^2 + y^2 \equiv 0$ (Mod 5), yet by trial and error one can see that there is no non-trivial solution for $x^2 + 2y^2 \equiv 0$ (Mod 5). (We can still pick $a = 2$, since it is still not a square.) Thus, when $q = 5$, I is plus type, and K is minus type.

This result can easily be extended to larger n. For example, if $n = 3$ and $q = 3$, we can obtain a plus type matrix J by repeating the 2×2 plus type matrix along the diagonal.

$$J = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

This is plus type, since we have a 3-dimensional subspace V spanned by $\langle 1,1,0,0,0,0\rangle$, $\langle 0,0,1,1,0,0\rangle$, and $\langle 0,0,0,0,1,1\rangle$. Now, for a diagonal matrix, whether it is plus or minus type only depends on whether there is an even or odd number of non-squares along the diagonal. Since both this matrix and K have an odd number of non-square elements, we see that K is of plus type for $n = 3$ and $q = 3$.

If q is a power of 2, we have to step back to the "true" definition of orthogonal transformations. The group G_J is really the set of transformations on $x_1, x_2, \ldots x_{2n}$ that preserve a particular quadratic equation in the variables $x_1, x_2, \ldots x_{2n}$, with every term of degree 2. If q is odd, then there will always be a symmetric matrix J such that the quadratic equation can be written as vJv^T for $v = \langle x_1, x_2, \ldots x_{2n}\rangle$. In which case, the transformation A will preserve this quadratic equation if and only if

$$vA^TJAv^T = vJv^T,$$

and since both sides are symmetric, this can be shown to imply that $A^TJA = J$. But when Q is even, we are sometimes forced to use a non-symmetric J to describe the quadratic equation. For example, the equation $x_1^2 + x_1x_2 + x_2^2$ can be written as

$$\begin{pmatrix} x_1 & x_2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

It it tempting to make a symmetric matrix out of J by writing this as

$$\begin{pmatrix} x_1 & x_2 \end{pmatrix}\begin{pmatrix} 1 & 1/2 \\ 1/2 & 1 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix},$$

but alas, $2 \equiv 0$ in our field, and so is not invertable.

By considering J to be non-symmetric means that we have to consider more elements in G_J then just those in which $A^TJA = J$. For example, if $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, then $A^TJA = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \neq J$, yet clearly the transformation that A represents will preserve the quadratic equation $x_1^2 + x_1x_2 + x_2^2$. So we will modify our definition of G_J to be

$$G_J = \{2n \times 2n \text{ matrices over } F_{2^r} \text{ such that } vA^TJAv^T = vJv^T \text{ for all vectors } v \in \mathbb{R}^{2n}\}.$$

There are again isomorphically two types of groups that G_J can become. For a matrix of plus type, consider the matrix corresponding to the quadratic $x_1x_2 + x_3x_4 + x_5x_6 + \cdots x_{2n-1}x_{2n}$, whose matrix is given by

$$K^+ = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

For a matrix of minus type, we add $x_{2n-1}^2 + ax_{2n}^2$ to the quadratic, where a is some element in the field for which $x^2 + x = a$ has no solutions in the field. This gives us

$$K^- = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & a \end{pmatrix}$$

Then we can define

$$D_n(2^r) = \{\text{Even } 2n \times 2n \text{ matrices over } F_{2^r} \text{ such that } |A| = 1 \text{ and } vA^TK^+Av^T = vK^+v^T \text{ for all } v \in \mathbb{R}^{2n}\},$$

and

$${}^2D_n(2^r) = \{\text{Even } 2n \times 2n \text{ matrices over } F_{2^r} \text{ such that } |A| = 1 \text{ and } vA^TK^-Av^T = vK^-v^T \text{ for all } v \in \mathbb{R}^{2n}\}.$$

In these two cases, the center will be trivial, so we don't have to worry about dividing by the center. The number of elements is still given by the above formulas.

For example, to find $D_3(2)$, we look for 6×6 non-singular matrices A in F_2 such that

$$vA^T \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} Av^T = v \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} v^T$$

For all 6 dimension vectors V. There are 40320 such matrices, a random sample of which is

$$\left\{ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}, \ldots \right\}$$

But these may not be "even" elements. But if we take the square of these, we will get elements of $D_3(2)$:

$$\left\{\begin{pmatrix}1&0&0&0&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\end{pmatrix},\begin{pmatrix}1&0&1&0&1&0\\0&0&0&1&1&0\\1&0&0&0&1&0\\0&1&0&1&1&0\\0&0&0&0&1&0\\0&1&1&0&0&1\end{pmatrix},\begin{pmatrix}0&1&0&1&0&1\\1&1&1&0&1&1\\1&1&1&1&0&1\\0&1&1&0&1&0\\1&0&1&0&0&1\\0&1&1&1&1&1\end{pmatrix},\begin{pmatrix}0&1&0&1&0&0\\1&1&0&0&1&1\\1&1&1&1&0&0\\0&0&0&1&0&0\\0&1&0&1&0&1\\0&1&0&1&1&0\end{pmatrix},\ldots\right\}$$

By considering the group generated by these squares, we obtain a group with 20160 elements, and this group happens to be isomorphic to A_8.

But to calculate ${}^2D_3(2)$, we first find an element in the field which cannot be x^2+x. Simple trial and error shows that 1 is the only such element of the two. So we seek for 6×6 non-singular matrices A in F_2 such that

$$vA^T\begin{pmatrix}0&1&0&0&0&0\\0&0&0&0&0&0\\0&0&0&1&0&0\\0&0&0&0&0&0\\0&0&0&0&1&1\\0&0&0&0&0&1\end{pmatrix}Av^T=v\begin{pmatrix}0&1&0&0&0&0\\0&0&0&0&0&0\\0&0&0&1&0&0\\0&0&0&0&0&0\\0&0&0&0&1&1\\0&0&0&0&0&1\end{pmatrix}v^T$$

for all vectors v. This time we find that there are 51840 such elements, a few of which are

$$\left\{\begin{pmatrix}1&0&0&1&0&0\\0&1&0&1&0&0\\0&0&0&1&0&0\\1&1&1&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\end{pmatrix},\begin{pmatrix}1&0&0&1&0&0\\0&0&1&1&1&0\\1&0&0&0&0&0\\1&1&1&1&0&0\\0&0&0&0&1&0\\1&0&0&1&0&1\end{pmatrix},\begin{pmatrix}0&0&1&1&1&0\\1&1&0&0&0&1\\1&1&1&1&0&0\\1&0&1&1&1&0\\0&0&1&1&0&0\\1&0&1&0&1&1\end{pmatrix},\begin{pmatrix}0&0&1&1&0&1\\1&1&0&1&0&1\\1&1&1&0&1&0\\1&1&0&0&0&1\\1&1&0&0&0&0\\1&0&0&1&1&0\end{pmatrix},\ldots\right\}.$$

But again, we must throw out the "odd" elements, so we first find the squares of these elements

$$\left\{\begin{pmatrix}0&1&1&0&0&0\\1&0&1&0&0&0\\1&1&1&1&0&0\\0&0&1&0&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\end{pmatrix},\begin{pmatrix}0&1&1&0&0&0\\0&1&1&1&1&0\\1&0&0&1&0&0\\1&1&0&1&1&0\\0&0&0&0&1&0\\1&1&1&1&0&1\end{pmatrix},\begin{pmatrix}0&1&1&1&1&0\\0&1&0&1&0&0\\1&0&1&1&0&1\\0&1&0&0&0&0\\0&1&0&0&1&0\\0&1&0&1&0&1\end{pmatrix},\begin{pmatrix}1&0&1&1&0&1\\1&0&1&1&1&1\\1&1&0&0&1&0\\0&1&1&1&1&0\\1&1&1&0&0&0\\0&0&1&1&0&0\end{pmatrix},\ldots\right\},$$

and then find the group generated by these elements, obtaining the 25920 elements of ${}^2D_3(2)$.

For one last example, consider ${}^2D_2(4)$. The field with 4 elements can be written as $\{0,1,\omega,1+\omega\}$, where $\omega^2=1+\omega$. This time, we cannot use $a=1$, since $x^2+x=1$ has a solution in the field, namely ω. But $x^2+x=\omega$ has no solution in the field, so we search for all matrices such that

$$vA^T\begin{pmatrix}0&1&0&0\\0&0&0&0\\0&0&1&1\\0&0&0&\omega\end{pmatrix}Av^T=v\begin{pmatrix}0&1&0&0\\0&0&0&0\\0&0&1&1\\0&0&0&\omega\end{pmatrix}v^T$$

for all vectors v. We find 8160 of these, a few of which are

$$\left\{\begin{pmatrix}1&1&1&0\\1&0&0&0\\0&0&1&0\\1&0&0&1\end{pmatrix},\begin{pmatrix}1+\omega&\omega&1&0\\1+\omega&0&0&0\\0&0&1&0\\1+\omega&0&0&1\end{pmatrix},\begin{pmatrix}1&\omega&0&1\\1+\omega&0&0&0\\1+\omega&0&1&0\\0&0&0&1\end{pmatrix},\begin{pmatrix}\omega&\omega&1+\omega&1+\omega\\1+\omega&0&0&0\\\omega&0&1&0\\\omega&0&0&1\end{pmatrix},\ldots\right\}.$$

Once again, we have to take the group generated by the squares of this matrices

$$\left\{\begin{pmatrix}0&1&0&0\\1&1&1&0\\0&0&1&0\\0&1&1&1\end{pmatrix},\begin{pmatrix}1+\omega&1&\omega&0\\\omega&1&1+\omega&0\\0&0&1&0\\1&1&1+\omega&1\end{pmatrix},\begin{pmatrix}0&\omega&0&0\\1+\omega&1&0&1+\omega\\0&1&1&1+\omega\\0&0&0&1\end{pmatrix},\begin{pmatrix}\omega&1+\omega&\omega&\omega\\1&1&\omega&\omega\\1&1+\omega&0&1\\1&1+\omega&1&0\end{pmatrix},\ldots\right\},$$

to obtain a group of size 4080.

The groups $D_1(q)$ and ${}^2D_1(q)$ will always be solvable, and $D_2(q) \approx L_2(q) \times L_2(q)$, so this is not simple either. Also, ${}^2D_2(q) \approx L_2(q^2)$, $D_3(q) \approx L_4(q)$, and ${}^2D_3(q) \approx U_4(q^2)$, so we only get new simple groups if $n \geq 4$, in which case we will always get new simple groups. The smallest examples then are $D_4(2)$ which has 174182400 elements, and ${}^2D_4(2)$ which is slightly larger: 197406720 elements.

Alternative names: $D_n(q)$ is also called $O^+_{2n}(q)$, and $\mathrm{P}\Omega^+_{2n}(q)$. ${}^2D_n(q)$ is also called $O^-_{2n}(q)$, and $\mathrm{P}\Omega^-_{2n}(q)$. Occasionally ${}^2D_n(q)$ is written as ${}^2D_n(q^2)$ because of an alternative way to define it, but this adds confusion. Also, the two sets of groups can be written as $O^\epsilon_{2n}(q)$ or $\mathrm{P}\Omega^\epsilon_{2n}(q)$, where the ϵ can represent either $+$ or $-$.

$\mathbf{G_2(q)}$

In the six sequences $L_n(q)$, $U_n(q)$, $B_n(q)$, $C_n(q)$, $D_n(q)$, and ${}^2D_n(q)$, the size of the matrices involved becomes one of the variables in the definition. However, there are other sequences of simple groups defined by matrices for which the size of the matrix is constant, only the size q of the finite field is allowed to change. These other sequences are called the *exceptional* Chevalley groups (not to be confused with the sporadic simple groups).

The easiest of these exceptional groups to understand is $G_2(q)$. This is rather simple to describe when q is odd, using only 7×7 matrices over the field F_q. Then we will find a slightly more complicated definition using 8×8 matrices which will work for all q.

A 7 dimensional vector can be written as

$$u_1\mathbf{e_1} + u_2\mathbf{e_2} + u_3\mathbf{e_3} + u_4\mathbf{e_4} + u_5\mathbf{e_5} + u_6\mathbf{e_6} + u_7\mathbf{e_7}$$

where $\mathbf{e_1}, \mathbf{e_2}, \ldots \mathbf{e_7}$ are the 7 mutually perpendicular unit vectors pointing in the direction of the 7 axes. We can define the cross product on two 7 dimensional vectors by describing the cross product on these 7 base vectors:

$$\mathbf{e_i} \times \mathbf{e_i} = 0, \qquad \mathbf{e_i} \times \mathbf{e_{i+1}} = -\mathbf{e_{i+1}} \times \mathbf{e_i} = \mathbf{e_{i+3}},$$

$$\mathbf{e_{i+1}} \times \mathbf{e_{i+3}} = -\mathbf{e_{i+3}} \times \mathbf{e_{i+1}} = \mathbf{e_i}, \qquad \mathbf{e_{i+3}} \times \mathbf{e_i} = -\mathbf{e_i} \times \mathbf{e_{i+3}} = \mathbf{e_{i+1}}.$$

If the subscript goes beyond 7, subtract 7 from the subscript. Thus, $\mathbf{e_6} \times \mathbf{e_7} = \mathbf{e_2}$. We also can define the 7 dimensional dot product

$$\vec{u} \cdot \vec{v} = u_1v_1 + u_2v_2 + u_3v_3 + u_4v_4 + u_5v_5 + u_6v_6 + u_7v_7.$$

The 7 dimensional cross product and dot product share many of the same properties that the familiar 3-dimensional versions have.

We can now describe $G_2(q)$ for odd q. The 7-dimensional cross product will work for 7 dimensional vectors whose elements are in F_q. We want to find all 7×7 matrices A such that:

1) Each row is a unit vector, that is, $\vec{u} \cdot \vec{u} = 1$.

2) The first row cross the second row is the fourth row, the second row cross the third row is the fifth row, the third row cross the fourth row is the sixth row, etc., until we get to the last row cross the first row is the third row.

In turns out that all such vectors will be orthogonal, $A^TA = 1$, and A will have determinant 1. If we define such a matrix a "cross product preserving" matrix, then for odd q,

$$G_2(q) = \{7 \times 7 \text{ cross product preserving matrices over } F_q\}.$$

Note that we do not have to divide by the center, nor take only the "even" elements of the group. For example, if $q = 3$, we find that there are 702 possible unit 7 dimensional vectors. By picking two which are orthogonal, and then picking a third which is orthogonal to the other two and their cross product, we can use these vectors for the first 3 rows of a matrix, and then use the cross product preserving property to complete the matrix. Some examples given here:

$$G_2(3) = \left\{ \begin{pmatrix} 0&1&0&0&0&0&0\\ 1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ 0&0&0&2&0&0&0\\ 0&0&0&0&0&0&1\\ 0&0&0&0&0&2&0\\ 0&0&0&0&1&0&0 \end{pmatrix}, \begin{pmatrix} 1&1&1&2&2&2&1\\ 0&1&2&2&1&0&0\\ 2&2&1&0&2&0&0\\ 2&1&0&1&0&0&1\\ 2&1&0&1&0&2&0\\ 0&1&0&0&2&1&2\\ 0&1&1&0&0&1&2 \end{pmatrix}, \begin{pmatrix} 2&1&2&2&0&0&0\\ 2&1&1&1&0&0&0\\ 0&0&0&0&0&1&0\\ 2&2&0&0&2&0&1\\ 0&0&1&2&1&0&1\\ 1&1&0&0&2&0&1\\ 0&0&2&1&1&0&1 \end{pmatrix}, \dots \right\}.$$

There turns out to be 4245696 such matrices.

In general, the size of $G_2(q)$ is given by

$$|G_2(q)| = q^6(q^6-1)(q^2-1).$$

This formula works for both even and odd q. But to define $G_2(q)$ for even q we must first introduce *octonions*, denoted by $\mathbb{O}$. This is an extension of the quaternions, which is a skew field. (A skew field is like a field, only multiplication is not commutative.)

Each 8 dimensional vector can be written as

$$\mathbf{u} = u_0 + u_1\mathbf{e_1} + u_2\mathbf{e_2} + u_3\mathbf{e_3} + u_4\mathbf{e_4} + u_5\mathbf{e_5} + u_6\mathbf{e_6} + u_7\mathbf{e_7}.$$

where the cross product multiplication is slightly altered so that $\mathbf{e_i}^2 = -1$, but the product of two different base vectors is as the 7 dimensional cross product.

If we define the complex conjugate of u by

$$\overline{\mathbf{u}} = u_0 - u_1\mathbf{e_1} - u_2\mathbf{e_2} - u_3\mathbf{e_3} - u_4\mathbf{e_4} - u_5\mathbf{e_5} - u_6\mathbf{e_6} - u_7\mathbf{e_7},$$

then $\overline{\mathbf{uv}} = \overline{\mathbf{v}}\,\overline{\mathbf{u}}$. Also, we find that

$$\overline{\mathbf{u}}\mathbf{u} = \mathbf{u}\overline{\mathbf{u}} = u_0^2 + u_1^2 + u_2^2 + u_3^2 + u_4^2 + u_5^2 + u_6^2 + u_7^2,$$

which will always be positive for non-zero $\mathbf{u}$. Thus, every non-zero octonion $\mathbf{u}$ has an inverse $\mathbf{u}^{-1} = \overline{\mathbf{u}}/(\mathbf{u}\overline{\mathbf{u}})$. Yet the octonions do not form a skew field, because multiplication is not associative. That is, $(ab)c$ is not always $a(bc)$. However, there is a sort of "selective associativity" to the octonions that still allow algebraic manipulation. For example, the sub-algebra generated by any two elements is associative. Thus, $(ab)a = a(ba)$ and $a^{-1}(ab) = (a^{-1}a)b = b$. In these cases, we can omit the parenthesis, and write aba to indicate either $(ab)a$ or $a(ba)$. There are also occasions where we have "accidental associativity":

$$x(yz)x = (xy)(zx),$$

$$x(y(xz)) = ((xy)x)z,$$

$$y(x(zx)) = ((yx)z)x,$$

$$(xy)(y^{-1}zy^{-1}) = (xz)y^{-1}.$$

These can be verified with *Mathematica*. The first 3 of these is called the *Moufang identities*. Ironically, a small change in these formulas will cause them to be no longer valid. For example, $(xy)(y^{-1}zy) \neq (xz)y$, $(yxy^{-1})(yzy^{-1}) \neq y(xz)y^{-1}$.

We can use the complex conjugates to define the inner product of two octonions. Note that

$$\mathrm{Re}(\mathbf{u}\overline{\mathbf{v}}) = \frac{\mathbf{u}\overline{\mathbf{v}} + \mathbf{v}\overline{\mathbf{u}}}{2} = u_0v_0 + u_1v_1 + u_2v_2 + u_3v_3 + u_4v_4 + u_5v_5 + u_6v_6 + u_7v_7.$$

Thus, we can say that two octonions are *orthogonal* if $\mathbf{u}\overline{\mathbf{v}} + \mathbf{v}\overline{\mathbf{u}} = 0$.

If we consider replacing $u_0, u_1, u_2, \ldots, u_7$ with elements of a finite field F_q, then we lose the property that all non-zero elements will be invertible, since $\mathbf{u}\overline{\mathbf{u}} = u_0^2 + u_1^2 + u_2^2 + u_3^2 + u_4^2 + u_5^2 + u_6^2 + u_7^2$ will sometimes be 0. In fact, because multiplication is not associative, we will not even get a ring. We get what is called an *algebra,* which has all the properties of a ring except associative multiplication. If q is odd, we will call this algebra $\mathbb{O}(F_q)$, the *octonion algebra over* F_q. We can now define $G_2(q)$ another way:

$$G_2(q) = \text{ the automorphism group of } \mathbb{O}(F_q).$$

To see the relationship between the two definitions, note that any automorphism ϕ of $\mathbb{O}(F_q)$ must send the identity element to the identity element, and hence all "real" elements map to themselves. The purely imaginary vectors are the vectors which are orthogonal to the unit vector, so any purely imaginary unit vector must map to a purely imaginary unit vector, so in particular $\mathbf{e_1}, \mathbf{e_2}, \ldots \mathbf{e_7}$ would all map to unit 7-vectors. Indeed, the automorphism would be completely determined by where it sends the base unit vectors. By forming a 7×7 matrix from $\phi(\mathbf{e_1}), \phi(\mathbf{e_2}), \ldots \phi(\mathbf{e_7})$, it is clear that this matrix would be cross product preserving, and that a cross product preserving matrix would produce an automorphism. Thus the two definitions are the same.

To define $\mathbb{O}(F_q)$ when q is a power of 2, we need some extra work, since $-1 = 1$ in this field. We begin by finding a new basis for $\mathbb{O}(F_q)$ when q is odd. There will always be two elements a and b in F_q such that $a^2 + b^2 + 1 = 0$, and $b \neq 0$. Then we define

$$x_1 = (\mathbf{e_6} + a\mathbf{e_4} + b\mathbf{e_7})/2, \qquad x_2 = (\mathbf{e_5} + a\mathbf{e_2} + b\mathbf{e_3})/2, \qquad x_3 = (-\mathbf{e_1} + a\mathbf{e_7} - b\mathbf{e_4})/2, \qquad x_4 = (1 - a\mathbf{e_3} + b\mathbf{e_2})/2,$$

$$x_5 = (1 + a\mathbf{e_3} - b\mathbf{e_2})/2, \qquad x_6 = (-\mathbf{e_1} - a\mathbf{e_7} + b\mathbf{e_4})/2, \qquad x_7 = (\mathbf{e_5} - a\mathbf{e_2} - b\mathbf{e_3})/2, \qquad x_8 = (\mathbf{e_6} - a\mathbf{e_4} - b\mathbf{e_7})/2.$$

We get the following multiplication table for these 8 elements:

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
x_1	0	0	0	0	x_1	$-x_2$	x_3	$-x_4$
x_2	0	0	x_1	x_2	0	0	$-x_5$	$-x_6$
x_3	0	$-x_1$	0	x_3	0	$-x_5$	0	x_7
x_4	x_1	0	0	x_4	0	x_6	x_7	0
x_5	0	x_2	x_3	0	x_5	0	0	x_8
x_6	x_2	0	$-x_4$	0	x_6	0	$-x_8$	0
x_7	$-x_3$	$-x_4$	0	0	x_7	x_8	0	0
x_8	$-x_5$	x_6	$-x_7$	x_8	0	0	0	0

Any element of $\mathbb{O}(F_q)$ (for odd q) can be expressed uniquely as

$$u = v_1x_1 + v_2x_2 + v_3x_3 + v_4x_4 + v_5x_5 + v_6x_6 + v_7x_7 + v_8x_8$$

where $v_1, v_2, \ldots v_8$ are in F_q. The above multiplication table will then allow us to multiply any two elements in $\mathbb{O}(F_q)$. This is called the *split form* of $\mathbb{O}(F_q)$. However, we can now use the split form to define $\mathbb{O}(F_q)$ for even q.

To find the "complex conjugate" of an element in $\mathbb{O}(F_q)$, we map $\mathbf{e_i} \mapsto -\mathbf{e_i}$, which when translated to the split form, gives us

$$\overline{u} = -v_1x_1 - v_2x_2 - v_3x_3 + v_5x_4 + v_4x_5 - v_6x_6 - v_7x_7 - v_8x_8.$$

Note that if q is even, then the only difference between u and $\overline{u}$ is that the x_4 and x_5 coordinates are switched. For any q, we find that $u\overline{u}$ is a multiple of the identity $x_4 + x_5$, which can be considered a member of F_q. Thus, u will have a multiplicative inverse if and only if $u\overline{u} \neq 0$.

We are now ready to define

$$G_2(q) = \text{ the automorphism group of } \mathbb{O}(F_q) \text{ in split form}$$

which will work for all q. Every automorphism ϕ can be represented as an 8×8 matrix over F_q, where the first row is the coefficients of $\phi(x_1)$, the second row is the coefficients of $\phi(x_2)$, etc.

How do we find the automorphisms? First of all, the identity element of $\mathbb{O}(F_q)$ is $x_4 + x_5$, so $\phi(0) = 0$ and $\phi(x_4 + x_5) = x_4 + x_5$. Now, $\phi(x_4)^2$ must be $\phi(x_4)$, so we first find all elements in $\mathbb{O}(F_q)$, besides 0 and the identity, which are their own square. ϕ must map x_4 to one of these elements. For each such possible value of $\phi(x_4)$, we find the elements y such that $y\phi(x_4) = 0$ and $\phi(x_4)y = y$. From the table, we see that $\phi(x_1)$, $\phi(x_6)$, and $\phi(x_7)$ must have this property, so we finally choose 3 different elements of this set so that

$$\phi(x_1)(\phi(x_6)\phi(x_7)) = \phi(x_4), \qquad \phi(x_6)(\phi(x_7)\phi(x_1)) = \phi(x_4), \qquad \phi(x_7)(\phi(x_1)\phi(x_6)) = \phi(x_4),$$

$$\phi(x_1)\phi(x_6) = -\phi(x_6)\phi(x_1), \qquad \phi(x_1)\phi(x_7) = -\phi(x_7)\phi(x_1), \qquad \phi(x_6)\phi(x_7) = -\phi(x_7)\phi(x_6),$$

$$(\phi(x_1)\phi(x_6))\phi(x_7) = 1 - \phi(x_4), \qquad (\phi(x_6)\phi(x_7))\phi(x_1) = 1 - \phi(x_4), \qquad (\phi(x_7)\phi(x_1))\phi(x_6) = 1 - \phi(x_4).$$

Once we have found $\phi(x_4)$, $\phi(x_1)$, $\phi(x_6)$, and $\phi(x_7)$, we can set $\phi(x_5) = 1 - \phi(x_4)$, $\phi(x_2) = \phi(x_6)\phi(x_1)$, $\phi(x_3) = \phi(x_1)\phi(x_7)$, and $\phi(x_8) = \phi(x_7)\phi(x_6)$. Then using the Moufang identities we see that ϕ extends to an automorphism on $\mathbb{O}(f_q)$, which can be expressed as an 8×8 matrix.

For example, when $q = 2$, we find 12096 automorphisms of $\mathbb{O}(F_2)$, which can be represented by 8×8 matrices, so $G_2(2) =$

$$\left\{ \begin{pmatrix} 0&0&0&0&0&1&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&1&0&0&0&0&0 \end{pmatrix}, \begin{pmatrix} 1&1&0&1&1&0&1&0\\ 1&0&0&1&1&1&1&1\\ 1&1&1&0&0&1&0&1\\ 0&1&1&0&1&1&1&1\\ 0&1&1&1&0&1&1&1\\ 1&0&1&1&1&1&0&0\\ 0&1&1&0&0&0&0&1\\ 1&1&1&0&0&0&1&1 \end{pmatrix}, \begin{pmatrix} 0&1&0&1&1&0&1&0\\ 1&0&1&0&0&0&0&0\\ 1&1&1&1&1&1&1&1\\ 1&0&1&0&1&0&1&0\\ 1&0&1&1&0&0&1&0\\ 0&0&1&0&0&0&0&0\\ 1&0&0&1&1&0&0&1\\ 0&0&1&0&0&0&1&0 \end{pmatrix}, \dots \right\}.$$

This, however, does not form a simple group. Half of the elements of $G_2(2)$ form a normal subgroup which is isomorphic to $U_3(9)$, which we recall has 6048 elements. However, when $q \geq 3$ then $G_2(q)$ will be a new simple group, the smallest of which is $G_2(3)$ which has 4245696 elements.

${}^3\mathbf{D}_4\mathbf{(q)}$

There is an unusual automorphism of the set of rotations in 8 dimensions:

$$D_4(q) = (8 \times 8 \text{ matrices with determinant 1 such that } AA^T = I)/(\pm I).$$

This comes from a rather outstanding property of octonion algebra $\mathbb{O}(F_q)$: If $u_k(\dots u_3(u_2(u_1 z))\dots) = z$ for all z, then $(\dots((zu_1)u_2)u_3\dots)u_k = \pm z$. This is rather surprising, since this statement is not true for quaternions. But because we don't have associativity, we are given much more than $u_k(\dots u_3(u_2u_1)\dots) = 1$. Here is the proof:

For all x and y, we can use one of the "accidental associativity" Moufang properties repeatedly:

$$\begin{aligned} u_k(\dots u_3(u_2(u_1(xy)u_1)u_2)u_3\dots)u_k &= u_k(\dots u_3(u_2((u_1x)(yu_1))u_2)u_3\dots)u_k \\ &= u_k(\dots u_3((u_2(u_1x))((yu_1)u_2))u_3\dots)u_k = \dots \\ &= (u_k(\dots u_3(u_2(u_1x))\dots))((\dots((yu_1)u_2)u_3\dots)u_k) \\ &= x((\dots((yu_1)u_2)u_3\dots)u_k). \end{aligned}$$

Setting $y = 1$ shows that $u_k(\dots u_3(u_2(u_1xu_1)u_2)u_3\dots)u_k = xr$ for some $r = (\dots(u_1u_2)u_3\dots)u_k$. But if we instead plug in $x = 1$, we find that $u_k(\dots u_3(u_2(u_1yu_1)u_2)u_3\dots)u_k = yr = (\dots((yu_1)u_2)u_3\dots)u_k$. Thus,

$(xy)r = x(yr)$ for all x and y in $\mathbb{O}$. Because of the non-associativity of $\mathbb{O}(F_q)$, this can only happen if $r = \pm 1$, which in turn tells us that $(\dots((zu_1)u_2)u_3\dots)u_k = \pm z$ for all z.

Now, for a fixed unit octonion u, (That is, one in which $u\overline{u} = 1$), we can define $L_u(x) = ux$, and $R_u(x) = xu$. In terms of vectors, we see that both of these do a rotation in 8 dimensions. In fact, we can express these as a matrices

$$L_u = \begin{pmatrix} u_0 & -u_1 & -u_2 & -u_3 & -u_4 & -u_5 & -u_6 & -u_7 \\ u_1 & u_0 & -u_4 & -u_7 & u_2 & -u_6 & u_5 & u_3 \\ u_2 & u_4 & u_0 & -u_5 & -u_1 & u_3 & -u_7 & u_6 \\ u_3 & u_7 & u_5 & u_0 & -u_6 & -u_2 & u_4 & -u_1 \\ u_4 & -u_2 & u_1 & u_6 & u_0 & -u_7 & -u_3 & u_5 \\ u_5 & u_6 & -u_3 & u_2 & u_7 & u_0 & -u_1 & -u_4 \\ u_6 & -u_5 & u_7 & -u_4 & u_3 & u_1 & u_0 & -u_2 \\ u_7 & -u_3 & -u_6 & u_1 & -u_5 & u_4 & u_2 & u_0 \end{pmatrix},$$

$$R_u = \begin{pmatrix} u_0 & -u_1 & -u_2 & -u_3 & -u_4 & -u_5 & -u_6 & -u_7 \\ u_1 & u_0 & u_4 & u_7 & -u_2 & u_6 & -u_5 & -u_3 \\ u_2 & -u_4 & u_0 & u_5 & u_1 & -u_3 & u_7 & -u_6 \\ u_3 & -u_7 & -u_5 & u_0 & u_6 & u_2 & -u_4 & u_1 \\ u_4 & u_2 & -u_1 & -u_6 & u_0 & u_7 & u_3 & -u_5 \\ u_5 & -u_6 & u_3 & -u_2 & -u_7 & u_0 & u_1 & u_4 \\ u_6 & u_5 & -u_7 & u_4 & -u_3 & -u_1 & u_0 & u_2 \\ u_7 & u_3 & u_6 & -u_1 & u_5 & -u_4 & -u_2 & u_0 \end{pmatrix}.$$

Here, we are using the standard basis for $\mathbb{O}(F_q)$, which assumes that q is odd, but a similar argument can be used for even q. Note that $L_uR_u = R_uL_u$, but in general, $L_uR_v \neq R_vL_u$. We are now ready to define the automorphism τ on the group $D_4(q)$. First off, we will state without proof that $D_4(q)$ is generated by the elements L_u for all unit octonions u. That is, each element of $D_4(q)$ can be expressed by $\pm L_{u_1}L_{u_2}L_{u_3}\dots L_{u_k}$ for some k. Then

$$\tau(\pm L_{u_1}L_{u_2}L_{u_3}\dots L_{u_k}) = \pm R_{u_1}R_{u_2}R_{u_3}\dots R_{u_k}.$$

This is in fact well defined, for if $L_{u_1}L_{u_2}L_{u_3}\dots L_{u_k} = L_{v_1}L_{v_2}L_{v_3}\dots L_{v_m}$, then for all z,

$$u_k(\dots u_3(u_2(u_1z))\dots) = v_m(\dots v_3(v_2(v_1z))\dots),$$

$$v_m^{-1}(u_k(\dots u_3(u_2(u_1z))\dots)) = v_m^{-1}(v_m(\dots v_3(v_2(v_1z))\dots)) = v_{m-1}(\dots v_3(v_2(v_1z))\dots),$$

so

$$v_1^{-1}(v_2^{-1}\dots(v_m^{-1}(u_k(\dots u_2(u_1z)\dots)))\dots) = z$$

for all z. The outstanding property of octonions above then says that

$$(\dots(((\dots(zu_1)u_2\dots)u_k)v_m^{-1})\dots v_2^{-1})v_1^{-1} = \pm z$$

which can be unraveled to produce

$$(\dots((zu_1)u_2)u_3\dots)u_k = \pm(\dots((zv_1)v_2)v_3\dots)v_m,$$

so that

$$R_{u_1}R_{u_2}R_{u_3}\dots R_{u_k} = \pm R_{v_1}R_{v_2}R_{v_3}\dots R_{v_m},$$

and hence τ is well defined, assuming that every element of $D_4(q)$ can be expressed as a product of L_u matrices. Given this, it is clear that $\tau(AB) = \tau(A)\tau(B)$ for all A and B in $D_4(q)$.

What is not so clear is what $\tau(\pm R_u)$ will be. Finding R_u as a product of L matrices is like solving a 8 dimensional Rubic's puzzle. Luckily, one can mimic the above outstanding property to determine $\tau(\pm R_u)$ without solving this puzzle.

Suppose that $R_v = L_{u_1}L_{u_2}L_{u_3}\dots L_{u_k}$, so that $u_k(\dots u_3(u_2(u_1 z))\dots) = zv$ for all z. Then

$$\begin{aligned} u_k(\dots u_3(u_2(u_1(xy)u_1)u_2)u_3\dots)u_k =& (u_k(\dots u_3(u_2(u_1 x))\dots))((\dots((yu_1)u_2)u_3\dots)u_k) \\ =& (xv)((\dots((yu_1)u_2)u_3\dots)u_k). \end{aligned}$$

Plugging in $y = 1$ shows that $u_k(\dots u_3(u_2(u_1(xy)u_1)u_2)u_3\dots)u_k = (xv)r$ for some $r = ((\dots(u_1u_2)u_3\dots)u_k)$. But substituting $x = 1$ produces $u_k(\dots u_3(u_2(u_1(y)u_1)u_2)u_3\dots)u_k = (yv)r = v((\dots((yu_1)u_2)u_3\dots)u_k)$, so $((\dots((yu_1)u_2)u_3\dots)u_k) = v^{-1}((yv)r)$, and so $u_k(\dots u_3(u_2(u_1(xy)u_1)u_2)u_3\dots)u_k$ is both $((xy)v)r)$ and $(xv)(v^{-1}((yv)r))$ for all x and y. If $r = \pm v^{-2}$, this in fact works because of one of the "accidental associativity" properties. It is not hard to prove via Mathematica that there are no other solutions. Hence, $((\dots((yu_1)u_2)u_3\dots)u_k) = \pm v^{-1}((yv)v^{-2}) = v^{-1}yv^{-1}$, so $R_{u_1}R_{u_2}R_{u_3}\dots R_{u_k} = \pm L_{v^{-1}}R_{v^{-1}}$. Therefore, $\tau(\pm R_u) = \pm L_{u^{-1}}R_{u^{-1}}$ for all v.

But we get another bonus: $\tau(\pm L_{u^{-1}}R_{u^{-1}}) = \pm R_{u^{-1}}(L_uR_u) = \pm R_{u^{-1}}R_uL_u = L_u$. Thus, $\tau(\tau(\tau(A))) = A$ for all A in $D_4(q)$. This proves that τ is in fact one-to-one and onto, and so is an automorphism of $D_4(q)$ of order 3. τ is called the *triality automorphism*, (try-AL-eh-tee) not because it is a trial to understand, but because it forms a three-way version of duality. For no other size rotations does such a three-fold automorphism exist.

Now, if we pick a field whose size is a perfect cube, F_{q^3}, then there is another three-way automorphism coming from the field. In F_{q^3}, the mapping $\phi(x) = x^q$ will be a field automorphism, with $\phi(\phi(\phi(x))) = x$, using the same argument as complex conjugate. For a matrix A, define $\widehat{A}$ to be the matrix with ϕ applied to all of the elements of A. Then $\widehat{AB} = \widehat{A}\widehat{B}$, and also $\tau(\widehat{A}) = \widehat{\tau(A)}$.

Then we can define

$${}^3D_4(q) = \{\text{Elements of } D_4(q^3) \text{ for which } \tau(\widehat{A}) = A.\}$$

Unfortunately, the definition of τ makes it hard to use this definition, so we will provide another way of calculating ${}^3D_4(q)$.

We first introduce a "twist" to the algebra $\mathbb{O}(q^3)$ by replacing the ordinary product with a new product $*$ for which $(\alpha x_i) * (\beta x_j) = \widehat{\alpha}\widehat{\beta}(x_ix_j)$ when α and β are in the field F_{q^3}. (We could also use the basis $\{1, \mathbf{e_1}, \mathbf{e_2}, \dots, \mathbf{e_7}\}$, but this definition works for both odd and even q.) We can call this twisted algebra $\widehat{\mathbb{O}}(q^3)$. (Note that this twisted algebra no longer has an identity element.) We now define

$${}^3D_4(q) = \{\text{The automorphisms of } \widehat{\mathbb{O}}(q^3).\}$$

Note that any automorphism of $\mathbb{O}(q)$ extends to become an automorphism of $\widehat{\mathbb{O}}(q^3)$. Thus, it is clear that $G_2(q)$ is a subgroup of ${}^3D_4(q)$. Also, given any $a \in F_{q^3}$ and $b \in F_q$, we have the mapping $x_1 \mapsto ax_1$, $x_2 \mapsto ba^{-1}x_2$, $x_3 \mapsto b^{-1}\widehat{a}\widehat{a}x_3$, $x_4 \mapsto \widehat{a}^{-1}\widehat{a}x_4$, $x_5 \mapsto \widehat{a}^{-1}\widehat{a}$, $x_6 \mapsto b(\widehat{a}\widehat{a})^{-1}$, $x_7 \mapsto b^{-1}a$, $x_8 \mapsto a^{-1}$ will also produce an automorphism of $\widehat{\mathbb{O}}(q^3)$.

The order of ${}^3D_4(q)$ is given by

$$|{}^3D_4(q)| = q^{12}(q^8 + q^4 + 1)(q^6 - 1)(q^2 - 1)$$

For example, when $q = 2$, we first define F_8 by letting ω be a solution to $x^3 + x + 1 = 0$. Then $\widehat{x}$ sends ω to ω^2, ω^2 to $\omega + \omega^2$, and sends $\omega + \omega^2$ back to ω. Since $G_2(2)$ is a subgroup, we can use this to get us started.

$${}^3D_4(2) = \left\{ \begin{pmatrix} \omega & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1+\omega^2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1+\omega^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1+\omega+\omega^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1+\omega^2 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \right.$$

$$\left\{ \begin{pmatrix} 1&1&0&1&1&0&1&0\\ 1&0&0&1&1&1&1&1\\ 1&1&1&0&0&1&0&1\\ 0&1&1&0&1&1&1&1\\ 0&1&1&1&0&1&1&1\\ 1&0&1&1&1&1&0&0\\ 0&1&1&0&0&0&0&1\\ 1&1&1&0&0&0&1&1 \end{pmatrix}, \begin{pmatrix} 0&1&0&1&1&0&1&0\\ 1&0&1&0&0&0&0&0\\ 1&1&1&1&1&1&1&1\\ 1&0&1&0&1&0&1&0\\ 1&0&1&1&0&0&1&0\\ 0&0&1&0&0&0&0&0\\ 1&0&0&1&1&0&0&1\\ 0&0&1&0&0&0&1&0 \end{pmatrix}, \begin{pmatrix} 1&0&1&1&1&1&0&0\\ 1&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&1&1\\ 1&0&0&0&1&1&0&0\\ 1&0&0&1&0&1&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&1\\ 1&0&0&0&0&1&0&0 \end{pmatrix}, \dots \right\}.$$

These elements generate all of ${}^3D_4(2)$, which has 211341312 elements. ${}^3D_4(q)$ will be a new simple group for all q.

Alternative names:

Sometimes ${}^3D_4(q)$ is written as ${}^3D_4(q^3)$, since there are two fields involved, one of order q, and one of order q^3.

${}^2\mathbf{B}_2(\mathbf{2}^{2n+1})$

When q is an odd power of 2, we can form a twisted group on $B_2(q)$. Actually, we will do the twist on $C_2(q)$, for recall that when q is a power of 2, $B_2(q) \approx C_2(q)$. Also recall that, since we are working in characteristic 2, $C_2(q)$ is the set of 4×4 matrices A over F_q for which

$$A^T \begin{pmatrix} 0&0&1&0\\ 0&0&0&1\\ 1&0&0&0\\ 0&1&0&0 \end{pmatrix} A = \begin{pmatrix} 0&0&1&0\\ 0&0&0&1\\ 1&0&0&0\\ 0&1&0&0 \end{pmatrix}.$$

We can define an automorphism on the group $C_2(q)$ by

$$\rho \begin{pmatrix} a_{11}&a_{12}&a_{13}&a_{14}\\ a_{21}&a_{22}&a_{23}&a_{24}\\ a_{31}&a_{32}&a_{33}&a_{34}\\ a_{41}&a_{42}&a_{43}&a_{44} \end{pmatrix} = \begin{pmatrix} \begin{vmatrix} a_{11}&a_{12}\\ a_{21}&a_{22} \end{vmatrix} & \begin{vmatrix} a_{11}&a_{14}\\ a_{21}&a_{24} \end{vmatrix} & \begin{vmatrix} a_{13}&a_{14}\\ a_{23}&a_{24} \end{vmatrix} & \begin{vmatrix} a_{12}&a_{13}\\ a_{22}&a_{23} \end{vmatrix}\\ \begin{vmatrix} a_{11}&a_{12}\\ a_{41}&a_{42} \end{vmatrix} & \begin{vmatrix} a_{11}&a_{14}\\ a_{41}&a_{44} \end{vmatrix} & \begin{vmatrix} a_{13}&a_{14}\\ a_{43}&a_{44} \end{vmatrix} & \begin{vmatrix} a_{12}&a_{13}\\ a_{42}&a_{43} \end{vmatrix}\\ \begin{vmatrix} a_{31}&a_{32}\\ a_{41}&a_{42} \end{vmatrix} & \begin{vmatrix} a_{31}&a_{34}\\ a_{41}&a_{44} \end{vmatrix} & \begin{vmatrix} a_{33}&a_{34}\\ a_{43}&a_{44} \end{vmatrix} & \begin{vmatrix} a_{32}&a_{33}\\ a_{42}&a_{43} \end{vmatrix}\\ \begin{vmatrix} a_{21}&a_{22}\\ a_{31}&a_{32} \end{vmatrix} & \begin{vmatrix} a_{21}&a_{24}\\ a_{31}&a_{34} \end{vmatrix} & \begin{vmatrix} a_{23}&a_{24}\\ a_{33}&a_{34} \end{vmatrix} & \begin{vmatrix} a_{22}&a_{23}\\ a_{32}&a_{33} \end{vmatrix} \end{pmatrix}.$$

If may be far from obvious that this is an automorphism on $C_2(q)$, but furthermore, it is not an *inner* automorphism. (An inner automorphism can be written as $\phi(x) = g^{-1}xg$ for some g in the group.) Its existence has some remarkable consequences. For example, since $C_2(2) \approx S_6$, this show that S_6 has an automorphism besides its inner automorphisms. This is very remarkable, since it is true for no other symmetric group S_n.

There is another automorphism of $C_2(2^{2n+1})$ when $n > 0$, and that is the Frobenius automorphism from the field $\sigma(x) = x^2$. That is, we let $\sigma(A)$ be the matrix with each element of A squared. This automorphism is of order $2n + 1$, because $q = 2^{2n+1}$.

When $q = 2$, and $A \in C_2(2)$, then $\rho\rho(A) = A$. That is, ρ is an automorphism of order 2. But when $q > 2$, then we get a surprise: if $A \in C_2(q)$, then $\rho(\rho(A)) = \sigma(A)$. This means that, in a sense, ρ is the "square root" of the Frobenius automorphism. This automatically means that the two automorphisms commute: $\rho(\sigma(A)) = \sigma(\rho(A))$. But it also means that we can get an automorphism on $C_2(2^{2n+1})$ by applying σ " n and a half" times, giving $\rho(\sigma^n(A))$. We can now define

$$2B_2(2^{2n+1}) = \{A \in C_2(2^{2n+1}) \text{ for which } \rho(\sigma^n(A)) = A\}.$$

For example, when $n = 0$, we get ${}^2B_2(2)$ to be the elements of $C_2(2)$ for which $\rho(A) = A$. This gives us 20 elements:

$$
{}^2B_2(2) = \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix},
$$

$$
\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix},
$$

$$
\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix},
$$

$$
\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \right\}
$$

This of course not a simple group. However, we do get a new simple group for $n \geq 1$. But how do we find the elements for $n \geq 1$?

Clearly, ${}^2B_2(2)$ is a subgroup of ${}^2B_2(2^{2n+1})$, since these 20 elements are also fixed by the Frobenius automorphism σ. But we can always find a diagonal element of ${}^2B_2(2^{2n+1})$, given by

$$
D = \begin{pmatrix} g & 0 & 0 & 0 \\ 0 & g^{(2^{n+1}-1)} & 0 & 0 \\ 0 & 0 & g^{-1} & 0 \\ 0 & 0 & 0 & g^{(1-2^{n+1})} \end{pmatrix},
$$

where g is a generator of the multiplicative group $F^*_{2^{2n+1}}$. This gives us one more element of $2B_2(q)$, but there is good news: $2B_2(q)$ is generated from the 20 elements of $2B_2(2)$ and D.

For example, when $n = 1$, we must work in the field F_8. We can let g be a root to the equation $x^3 + x + 1 = 0$. Then g will indeed be a multiplicative generator of $F_8 - \{0\}$. We get ${}^2B_2(8) =$

$$
\left\{ \begin{pmatrix} g & 0 & 0 & 0 \\ 0 & g^3 & 0 & 0 \\ 0 & 0 & g^6 & 0 \\ 0 & 0 & 0 & g^4 \end{pmatrix}, \begin{pmatrix} g^2 & g^5 & g^4 & g^2 \\ g^5 & g^5 & g^6 & 1 \\ g^4 & g^2 & g^5 & g^4 \\ g^5 & g^2 & g^4 & 1 \end{pmatrix}, \begin{pmatrix} g^2 & g^3 & 1 & g^3 \\ 0 & g^6 & g^5 & g^3 \\ 0 & 0 & g^5 & 0 \\ 0 & 0 & g^2 & g \end{pmatrix}, \begin{pmatrix} g^2 & g^4 & g^3 & g^3 \\ 0 & g^6 & g^6 & 1 \\ g^6 & g^3 & g^5 & g^3 \\ g^3 & g^5 & g^6 & g^2 \end{pmatrix}, \dots \right\}.
$$

We find that 29120 elements are generated by D and ${}^2G_2(2)$. In general, the size of this new simple group is

$$
|{}^2B_2(2^{2n+1})| = 2^{4n+2}(2^{4n+2} + 1)(2^{2n+1} - 1).
$$

Alternative names: ${}^2B_2(2^{2n+1})$ is also called $\mathrm{Suz}(2^{2n+1})$, and $\mathrm{Sz}(2^{2n+1})$, the *Suzuki groups*. This is not to be confused with the sporadic Suzuki group.

${}^2\mathbf{G}_2(\mathbf{3}^{2n+1})$

If q is an odd power of 3, then we can do a similar twist on the group $G_2(q)$. Since q is odd, we can use the 7×7 matrix representation of $G_2(q)$, namely, the matrices over F_q which are cross product preserving. Now, we can define an automorphism on $G_2(q)$, when q is a power of 3, to be $\rho(A) = B$, where

$$
b_{i,j} = \begin{vmatrix} a_{i+2,j+1} & a_{i+2,j+3} \\ a_{i+6,j+1} & a_{i+6,j+3} \end{vmatrix} + \begin{vmatrix} a_{i+1,j+2} & a_{i+1,j+6} \\ a_{i+3,j+2} & a_{i+3,j+6} \end{vmatrix} - \begin{vmatrix} a_{i+1,j+1} & a_{i+1,j+3} \\ a_{i+3,j+1} & a_{i+3,j+3} \end{vmatrix} - \begin{vmatrix} a_{i+2,j+2} & a_{i+2,j+6} \\ a_{i+6,j+2} & a_{i+6,j+6} \end{vmatrix}.
$$

Here, if a subscript goes above 7, we subtract 7 from the subscript. So for example,

$$b_{3,6} = \begin{vmatrix} a_{5,7} & a_{5,2} \\ a_{2,7} & a_{2,2} \end{vmatrix} + \begin{vmatrix} a_{4,1} & a_{4,5} \\ a_{6,1} & a_{6,5} \end{vmatrix} - \begin{vmatrix} a_{4,7} & a_{4,2} \\ a_{6,7} & a_{6,2} \end{vmatrix} - \begin{vmatrix} a_{5,1} & a_{5,5} \\ a_{2,1} & a_{2,5} \end{vmatrix}.$$

It is not clear that the matrix $b = \rho(A)$ is also in $G_2(q)$, let alone that ρ is an automorphism, but indeed it is. Because the root prime is now 3 instead of 2, the Frobenous automorphism on the field is $\sigma(x) = x^3$, which extends to the group $G_2(3^{2n+1})$ by cubing all elements in the matrix. As in the case of ${}^2B_2(2^{2n+1})$, $\rho(\rho(A)) = \sigma(A)$, so we have in essence a square root of the Frobenous automorphism. Hence, we can define, as we did for ${}^2B_2(2^{2n+1})$,

$${}^2G_2(3^{2n+1}) = \{A \in G_2(2^{2n+1}) \text{ for which } \rho(\sigma^n(A)) = A\}.$$

For example, when $n = 0$, we find ${}^2G_2(3)$ to be the set of elements in $G_2(3)$ for which $\rho(A) = A$. This gives us 1512 elements, generated by the four matrices

$$\begin{pmatrix} 2 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 2 \\ 1 & 0 & 1 & 0 & 0 & 2 & 1 \\ 0 & 1 & 0 & 0 & 2 & 1 & 1 \\ 1 & 0 & 0 & 2 & 1 & 1 & 0 \\ 0 & 0 & 2 & 1 & 1 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

which, unfortunately, is not a simple group. It contains a normal subgroup of order 504 which is isomorphic to $L_2(8)$: this subgroup is generated by the first 3 of the four matrices.

To find ${}^2G_3(3^{2n+1})$ for $n \geq 1$, we need to find some elements in this group which, together with ${}^2G_3(3)$, generate the whole group. The strategy we used in ${}^2B_2(2^{2n+1})$ was to consider diagonal matrices. However, all diagonal matrices in $G_2(3^{2n+1})$ are in $G_2(3)$, so this does not help us. However, we can use the basis $\{x_1, x_2, \ldots x_8\}$ instead, and look at the 8×8 diagonal matrices in $G_2(3^{2n+1})$ using this basis. It is easy to see that $x_1 \mapsto \alpha\beta x_1$, $x_2 \mapsto \alpha x_2$, $x_3 \mapsto \beta x_3$, $x_4 \mapsto x_4$, $x_5 \mapsto x_5$, $x_6 \mapsto \beta^{-1} x_6$, $x_7 \mapsto \alpha^{-1} x_7$, $x_8 \mapsto (\alpha\beta)^{-1} x_8$ forms an automorphism of $\mathbb{O}(F_q)$ for all non-zero $\alpha, \beta \in F_q$. Converting this back to the original (Using $a = b = 1$ for our choice which makes $a^2 + b^2 + 1 = 0$) we get the matrix $D(\alpha, \beta) =$

$$\begin{pmatrix} -\beta - \beta^{-1} & 0 & 0 & \beta^{-1} - \beta & 0 & 0 & \beta - \beta^{-1} \\ 0 & \alpha + \alpha^{-1} - 1 & \alpha + \alpha^{-1} + 1 & 0 & \alpha - \alpha^{-1} & 0 & 0 \\ 0 & \alpha + \alpha^{-1} + 1 & \alpha + \alpha^{-1} - 1 & 0 & \alpha - \alpha^{-1} & 0 & 0 \\ \beta - \beta^{-1} & 0 & 0 & \gamma^{-1} + \gamma + \beta + \beta^{-1} & 0 & \gamma - \gamma^{-1} & \gamma^{-1} + \gamma - \beta - \beta^{-1} \\ 0 & \alpha^{-1} - \alpha & \alpha^{-1} - \alpha & 0 & -\alpha - \alpha^{-1} & 0 & 0 \\ 0 & 0 & 0 & \gamma^{-1} - \gamma & 0 & -\gamma - \gamma^{-1} & \gamma^{-1} - \gamma \\ \beta^{-1} - \beta & 0 & 0 & \gamma^{-1} + \gamma - \beta - \beta^{-1} & 0 & \gamma - \gamma^{-1} & \gamma^{-1} + \gamma + \beta + \beta^{-1} \end{pmatrix}$$

where we replaced $\alpha\beta$ with γ to save space. One can check that D really is an orthogonal matrix modulo 3, and in fact is an element of $G_2(3^{2n+1})$. What happens if we apply the automorphism ρ to this matrix? It turns out that $\rho(D(\alpha, \beta)) = D(\alpha\beta^2, \alpha\beta^{-1})$. That is, ρ applied to the above matrix is the same thing as replacing every α with $\alpha\beta^2$, every β with $\alpha\beta^-1$, and every γ with $\alpha^2\beta$. From this, we can see that $\rho(\rho(D(\alpha, \beta))) = D(\alpha^3, \beta^3) = \sigma(D(\alpha, \beta))$.

To get this to be a member of ${}^2G_2(3^{2n+1})$, we need $\rho(\sigma^n(D(\alpha, \beta))) = D(\alpha, \beta)$. This will happen if both $\alpha^{3^n}\beta^{2 \cdot 3^n} = \alpha$, and $\alpha^{3^n}\beta^{-3^n} = \beta$. Both of these equations can be solved by letting $\alpha = \beta^{(3^{n+1}+1)}$, since $\beta^{(3^{2n+1}-1)} = 1$. Thus, if we let β be a generator of the multiplicative group F_q^*, and let $\alpha = \beta^{(3^{n+1}+1)}$ and $\gamma = \beta^{(3^{n+1}+2)}$, then the $D(\alpha, \beta)$ listed above will be in ${}^2G_2(3^{2n+1})$. In fact, this matrix, along with the 4 other matrices in ${}^2G_2(3)$ mentioned above, will generate ${}^2G_2(3^{2n+1})$.

This will produce a new simple group for $n \geq 1$. The size of the group is given by

$$|{}^2G_2(3^{2n+1})| = 3^{6n+3}(3^{6n+3} + 1)(3^{2n+1} - 1).$$

For example, when $n = 1$, we get ${}^2G_2(27)$ with 10073444472 elements.

Alternative names: ${}^2G_2(3^{2n+1})$ is also called Ree(3^{2n+1}), or R(3^{2n+1}), the *Small Ree groups*.

$\mathbf{F}_4(\mathbf{q})$

To define the next Chevalley group, we will introduce the Albert algebras. Normal multiplication of $n \times n$ matrices is associate, but not commutative. However, if we define a new multiplication

$$A \circ B = (AB + BA)/2$$

we get a commutative multiplication, with the identity element still being I. Of course, we lose associativity, but this new product satisfies the Jordan identity

$$((A \circ A) \circ B) \circ A = (A \circ A) \circ (B \circ A).$$

A Jordan algebra is an algebra (that is, a ring without associative multiplication) for which the Jordan identity holds. We can construct a special Jordan algebra with the help of the octonions.

Consider the set of all 3×3 matrices with elements in $\mathbb{O}(F_q)$ for which $A^T = \overline{A}$, where $\overline{A}$ is the matrix formed by taking the complex conjugate of all of the entries of A. This forces the diagonal elements to be in F_q, and in fact, we can express all such matrices as

$$A = \begin{pmatrix} a & w & \overline{v} \\ \overline{w} & b & u \\ v & \overline{u} & c \end{pmatrix},$$

where a, b, and c are in F_q, and u, v, and w are in $\mathbb{O}(F_q)$. We can abbreviate this matrix by the 6-tuple $(a, b, c|u, v, w)$. We define the product of two such matrices by $A \circ B = (AB + BA)/2$, and in spite of the non-commutativity of the octonions, we find that the Jordan identity holds. Even with the abbreviated 6-tuple, the product can be quite cumbersome. We get $(a_1, b_1, c_1|u_1, v_1, w_1) \circ (a_2, b_2, c_2|u_2, v_2, w_2) =$

$$\left(a_1a_2 + \frac{w_1\overline{w}_2 + \overline{v}_1v_2 + w_2\overline{w}_1 + \overline{v}_2v_1}{2}, b_1b_2 + \frac{\overline{w}_1w_2 + u_1\overline{u}_2 + \overline{w}_2w_1 + u_2\overline{u}_1}{2},\right.$$

$$c_1c_2 + \frac{v_1\overline{v}_2 + \overline{u}_1u_2 + v_2\overline{v}_1 + \overline{u}_2u_1}{2} \Bigg| \frac{\overline{w}_1\overline{v}_2 + \overline{w}_2\overline{v}_1 + b_1u_2 + c_2u_1 + b_2u_1 + c_1u_2}{2},$$

$$\left.\frac{\overline{u}_1\overline{w}_2 + \overline{u}_2\overline{w}_1 + a_1v_2 + c_2v_1 + a_2v_1 + c_1v_2}{2}, \frac{\overline{v}_1\overline{u}_2 + \overline{v}_2\overline{u}_1 + a_1w_2 + b_2w_1 + a_2w_1 + b_1w_2}{2}\right).$$

Of course this formula will not work if q is even, since we then cannot divide by 2. So as with $\mathbb{O}(q)$, we can change the basis to a split form so that $\circ$ can be defined without any division.

If q is odd, we can let

$$y_0 = (-1, 1, 1|0, 0, 0), \qquad y_0' = (1, -1, 1|0, 0, 0), \qquad y_0'' = (1, 1, -1|0, 0, 0),$$

and for $1 \le i \le 8$,

$$y_i = (0, 0, 0|2x_i, 0, 0), \qquad y_i' = (0, 0, 0|0, 2x_i, 0), \qquad y_i'' = (0, 0, 0|0, 0, 2x_i).$$

Then we have the following products, for $i, j > 0$:

$$y_0 \circ y_0 = y_0' \circ y_0' = y_0'' \circ y_0'' = y_0 + y_0' + y_0'' = 1,$$

$$y_0 \circ y_0' = -y_0'', \qquad y_0' \circ y_0'' = -y_0, \qquad y_0'' \circ y_0 = -y_0',$$

$$y_0 \circ y_i = y_i, \qquad y_0' \circ y_i' = y_i', \qquad y_0'' \circ y_i'' = y_i''$$

$$y_0 \circ y_i' = y_0 \circ y_i'' = y_0' \circ y_i = y_0' \circ y_i'' = y_0'' \circ y_i = y_0'' \circ y_i' = 0,$$
$$y_i \circ y_{9-i} = y_0 + 1, \qquad y_i' \circ y_{9-i}' = y_0' + 1, \quad y_i'' \circ y_{9-i}'' = y_0'' + 1.$$
$$y_i \circ y_j = y_i' \circ y_j' = y_i'' \circ y_j'' = 0 \text{ if } j \neq 9 - i,$$
$$y_i \circ y_j' = \epsilon y_k'', \qquad y_i' \circ y_j'' = \epsilon y_k, \qquad y_i'' \circ y_j = \epsilon y_k', \text{ where } \epsilon \text{ is choosen so that} x_i x_j = \epsilon \overline{x_k}.$$

Because all of the products for this basis do not involve any division, we can *define* $\mathbb{J}(F_q)$, the Albert algebra over the field F_q by these products. We can then define

$$F_4(q) = \text{ the automorphism group of } \mathbb{J}(F_q) \text{ in split form.}$$

That is, we first can express an element of $\mathbb{J}(F_4)$ as

$$i_0y_0+i_1y_1+i_2y_2+i_3y_3+i_4y_4+i_5y_5+i_6i_6+i_7y_7+i_8y_8+j_0y_0'+j_1y_1'+j_2y_2'+j_3y_3'+j_4y_4'+j_5y_5'+j_6y_6'+j_7y_7'+j_8y_8'$$
$$+k_0y_0'' + k_1y_1'' + k_2y_2'' + k_3y_3'' + k_4y_4'' + k_5y_5'' + k_6i_6'' + k_7y_7'' + k_8y_8''.$$

Then each element of $F_4(q)$ can then be represented by a 27×27 matrix. Actually, we could get by with a 26×26 matrices, since the identity element must map to itself, but this would destroy the 3-fold symmetry.

So what are the automorphisms of $\mathbb{J}(F_q)$? One can easily check that because of the 3-way symmetry,

$$(a, b, c|u, v, w) \mapsto (b, c, a|v, w, u)$$

is an automorphism, along with the mappings

$$(a, b, c|u, v, w) \mapsto (a, c, b|\overline{u}, \overline{w}, \overline{v}), \quad \text{and} \quad (a, b, c|u, v, w) \mapsto (a, b, c|u, -v, -w).$$

However, we need another way to express these automorphisms, since using 27 by 27 matrices would be prohibitive. One way to express many of the automorphisms is via cycles. For example, we can express the first of these two by the product of 3-cycles

$$(y_0, y_0', y_0'')(y_1, y_1', y_1'')(y_2, y_2', y_2'')(y_3, y_3', y_3'')(y_4, y_4', y_4'')(y_5, y_5', y_5'')(y_6, y_6', y_6'')(y_7, y_7', y_7'')(y_8, y_8', y_8'')$$

This means that for every element of $\mathbb{J}(F_q)$, we replace y_0 with y_0', replace y_0' with y_0'', replace y_0'' with y_0, replace y_1 with y_1', etc, to produce a new element of $\mathbb{J}(F_q)$. The second automorphism can be expressed via 2 cycles

$$(y_0', y_0'')(y_1, -y_1)(y_2, -y_2)(y_3, -y_3)(y_4, y_5)(y_6, -y_6)(y_7, -y_7)(y_8, -y_8)$$
$$\cdot(y_1', -y_1'')(y_2', -y_2'')(y_3', -y_3'')(y_4', y_5'')(y_5', y_4'')(y_6', -y_6'')(y_7', -y_7'')(y_8', y_8'').$$

This means that y_1 is replaced with $-y_1$, y_1' is replaced with $-y_1''$, and since $-y_1''$ is replaced by y_1' we have y_1'' replaced by $-y_1'$. With this new notation, we can now express some other automorphisms of $\mathbb{J}(F_q)$:

$$r = (y_2, -y_2)(y_7, -y_7), (y_4, -y_5)(y_3, y_6)(y_1', y_2')(y_3', y_4')(y_5', y_6')(y_7', y_8')(y_1'', -y_2'')(y_3'', y_5'')(y_4'', y_6'')(y_7'', -y_8''),$$

$$s = (y_0, y_0'')(y_1, y_1')(y_3, y_3')(y_6, y_6')(y_8, y_8')(y_2, y_4', -y_2, -y_4')(y_5, y_2', -y_5, -y_2')(y_4, y_7', -y_4, -y_7')$$
$$\cdot \quad (y_7, y_5', -y_7, -y_5')(y_1'', y_3'', -y_1'', -y_3'')(y_4'', y_5'')(y_6'', -y_8'', -y_6'', y_8'')(y_2'', -y_2'')(y_7'', -y_7''),$$

It is also a rather straightforward calculation to show that

$$(a, b, c|u, v, w) \mapsto (a, b, c|zu, vz, \overline{z}w\overline{z})$$

is an automorphism whenever z is a unit octonion.

Another way we can represent more complicated elements of $F_4(q)$ is by indicating where the base vectors are mapped to, which do not map to themselves. For example, the mapping

$$y_7 \mapsto y_7 + ay_1, \quad y_7' \mapsto y_7' + ay_1', \quad y_7'' \mapsto y_7'' + ay_1'', \quad y_8 \mapsto y_8 - ay_2, \quad y_8' \mapsto y_8' - ay_2', \quad y_8' \mapsto y_8' - ay_2'$$

is an automorphism of $\mathbb{J}(F_q)$ for every $a \in F_q$. Every base vector not mentioned here is mapped to itself. Here is another example:

$$y_0 \mapsto y_0 + ay_5'', \quad y_0' \mapsto y_0' - ay_5'', \quad y_1' \mapsto y_1' + ay_1, \quad y_8 \mapsto y_8 - ay_8' \quad y_2 \mapsto y_2 - ay_2', \quad y_7' \mapsto y_7' + ay_7,$$

$$y_3 \mapsto y_3 - ay_3', \quad y_6' \mapsto y_6' + ay_6, \quad y_5 \mapsto y_5 + ay_4', \quad y_5' \mapsto y_5' - ay_4, \quad y_4'' \mapsto y_4'' - ay_0 + ay_0' - a^2y_5''.$$

We can define the *trace* of a matrix to be the sum of the diagonal elements. So the trace of the matrix corresponding to $(a, b, c|u, v, w)$ is element of F_q given by $a+b+c$. It can be shown that any automorphism of $\mathbb{J}$ preserves the trace, that is, if ϕ is any automorphism, then $\mathrm{Tr}(\phi(A)) = \mathrm{Tr}(A)$. We can then define an inner product on $\mathbb{J}$, by saying that $A \cdot B = \mathrm{Tr}(A \circ B)$. Then two matrices are *orthogonal* if $\mathrm{Tr}(A \circ B) = 0$. So any automorphism will send orthogonal matrices to orthogonal matrices. (Care must be taken in characteristic 3, since the identity matrix would have trace 0.) We can also define the *triple product* of three matrices by $\mathrm{Tr}((A \circ B) \circ C)$, which is reminiscent of the triple product of vectors $\vec{u} \cdot (\vec{v} \times \vec{w})$. It is clear that $\mathrm{Tr}((A \circ B) \circ C) = \mathrm{Tr}((B \circ A) \circ C)$, but what is surprising it that $\mathrm{Tr}((A \circ B) \circ C) = \mathrm{Tr}((A \circ C) \circ B)$ as well, so that the order of the three matrices do not affect the triple product. The trace is of great assistance in finding the automorphisms of $\mathbb{J}$.

The group $F_4(q)$ will always give us a new simple group, whose size is

$$|F_4(q)| = q^{24}(q^{12} - 1)(q^8 - 1)(q^6 - 1)(q^2 - 1).$$

However, it becomes a major challenge to determine what the elements of this group are. However, if we know where an automorphism ϕ sends y_1, y_6, y_7, y_5, and y_5', then we can see where ϕ sends all of the other base vectors. ($\phi(y_1'') = -\phi(w_1) \circ \phi(w_5')$, $\phi(w_3') = -\phi(w_1'') \circ \phi(w_7)$, etc.)

For example, to find the "diagonal" matrices of $F_4(q)$, we can assume that $\phi(y_1) = \alpha y_1$, $\phi(y_6) = \beta y_6$, $\phi(y_7) = \gamma y_7$, $\phi(y_5') = \delta y_5'$, and $\phi(y_5) = \epsilon(y_5)$, where $\alpha, \beta, \gamma, \delta$, and ϵ are elements of $F(q)$. After some computation, we find that $\phi(1 + w_0) = \alpha\beta\gamma\delta^2\epsilon(1 + w_0)$ But since $\phi(w_0) \circ \phi(w_0) = \phi(1) = 1$, this forces $\alpha\beta\gamma\delta^2\epsilon = 1$. If we let $\epsilon = (\alpha\beta\gamma\delta^2)^{-1}$, we get the following automorphism of $\mathbb{J}(F_q)$:

$$y_1 \mapsto \alpha y_1, \quad y_1' \mapsto (\beta\gamma\delta)^{-1}y_1', \quad y_1'' \mapsto -\alpha\delta y_1'',$$

$$y_2 \mapsto \gamma^{-1}y_2, \quad y_2' \mapsto \alpha\beta\delta y_2', \quad y_2'' \mapsto -(\gamma\delta)^{-1}y_2''$$

$$y_3 \mapsto \beta^{-1}y_3, \quad y_3' \mapsto \alpha\gamma\delta y_3', \quad y_3'' \mapsto -(\beta\delta)^{-1}y_3'',$$

$$y_4 \mapsto \alpha\beta\gamma\delta^2 y_4, \quad y_4' \mapsto \delta^{-1}y_4', \quad y_4'' \mapsto -(\alpha\beta\gamma\delta)^{-1}y_4'',$$

$$y_5 \mapsto (\alpha\beta\gamma\delta^2)^{-1}y_5, \quad y_5' \mapsto \delta y_5', \quad y_5'' \mapsto -\alpha\beta\gamma\delta y_5'',$$

$$y_6 \mapsto \beta y_6, \quad y_6' \mapsto (\alpha\gamma\delta)^{-1}y_6', \quad y_6'' \mapsto -\beta\delta y_6'',$$

$$y_7 \mapsto \gamma y_7, \quad y_7' \mapsto (\alpha\beta\delta)^{-1}y_7', \quad y_7'' - \gamma\delta y_7'',$$

$$y_8 \mapsto \alpha^{-1}y_8, \quad y_8' \mapsto \beta\gamma\delta y_8', y_8'' \mapsto -(\alpha\delta)^{-1}y_8''.$$

We will call this $\mathrm{diag}(\alpha, \beta, \gamma, \delta)$, which are the *diagonal* elements of $F_4(q)$. We now have given enough elements of $F_4(q)$ to generate the entire group.

${}^2\mathbf{F}_4(\mathbf{2}^{2n+1})$

When q is an odd power of 2, we can define a similar twist as we did with G_2 and B_2. The plan is exactly the same: we define an automorphism ρ that sends elements of $F_4(q)$ to $F_4(q)$ such that $\rho(\rho(A)) = \sigma(A)$, where $\sigma(A)$ is the field automorphism, which in this case squares every element of the matrix A. In this case, though, the matrices are 27×27, and so if we have $B = \rho(A)$, we would have to have 729 formulas to describe the entries of B. (Unlike the situation we had for G_2, there is not a single formula that works for all entries.) It is clear that we need a different strategy for computing $\rho(A)$.

To define how the operator ρ applies to an automorphism ϕ, we will first introduce a new kind of product on the elements of $\mathbb{JJ}(F_q)$. We define the product $\times$ so that the distributive law holds, and we have the following products of base elements:

$\times$	y_1	y_2	y_3	y_4	y_5	y_6	y_7	y_8
y_1	0	y_1	y_2''	y_2'	y_1'	y_1''	y_2	y_0''
y_2	y_1	0	y_4'	y_5''	y_3''	y_3'	y_0'	y_7
y_3	y_2''	y_4'	0	y_6	y_5	y_0	y_6'	y_8''
y_4	y_2'	y_5''	y_6	0	1	y_4	y_6''	y_8'
y_5	y_1'	y_3''	y_5	1	0	y_3	y_4''	y_7'
y_6	y_1''	y_3'	y_0	y_4	y_3	0	y_5'	y_7''
y_7	y_2	y_0'	y_6'	y_6''	y_4''	y_5'	0	y_8
y_8	y_0''	y_7	y_5''	y_8'	y_7'	y_7''	y_8	0

$\times$	y_1'	y_2'	y_3'	y_4'	y_5'	y_6'	y_7'	y_8'
y_1'	0	y_1	y_2''	y_1'	y_4'	y_3''	y_5	y_0''
y_2'	y_1	0	y_2'	y_1''	y_5''	y_3'	y_0'	y_4
y_3'	y_2''	y_2'	0	y_2	y_6	y_0	y_6'	y_6''
y_4'	y_1'	y_1''	y_2	0	1	y_3	y_4''	y_5'
y_5'	y_4'	y_5''	y_6	1	0	y_7	y_8''	y_8'
y_6'	y_3''	y_3'	y_0	y_3	y_7	0	y_7'	y_7''
y_7'	y_5	y_0'	y_6'	y_4''	y_8''	y_7'	0	y_8
y_8'	y_0''	y_4	y_6''	y_5'	y_8'	y_7''	y_8	0

$\times$	y_1''	y_2''	y_3''	y_4''	y_5''	y_6''	y_7''	y_8''
y_1''	0	y_1	y_2''	y_4'	y_2'	y_5''	y_6	y_0''
y_2''	y_1	0	y_1'	y_3''	y_1''	y_3'	y_0'	y_3
y_3''	y_2''	y_1'	0	y_5	y_2	y_0	y_6'	y_4''
y_4''	y_4'	y_3''	y_5	0	1	y_7	y_8''	y_7'
y_5''	y_2'	y_1''	y_2	1	0	y_4	y_6''	y_5'
y_6''	y_5''	y_3'	y_0	y_7	y_4	0	y_8'	y_7''
y_7''	y_6	y_0'	y_6'	y_8''	y_6''	y_8'	0	y_8
y_8''	y_0''	y_3	y_4''	y_7'	y_5'	y_7''	y_8	0

any products not mentioned in this table will be 0, such as $y_0 \times z = 0$ for all z, or $y_i \times y_j' = 0$ for all i and j. Although this multiplication is commutative, it is far from associative, and is only defined to explain how the operator ρ works.

If ϕ is an automorphism on $\mathbb{JJ}(F_q)$, with q a power of 2, then $\rho(\phi)$ will be another automorphism which sends

$$y_1 \mapsto (\phi(y_1) \times \phi(y_2) + \phi(y_1') \times \phi(y_2') + \phi(y_1'') \times \phi(y_2'')),$$

$$y_6 \mapsto (\phi(y_3) \times \phi(y_4) + \phi(y_3') \times \phi(y_5') + \phi(y_1'') \times \phi(y_7'')),$$

$$y_7 \mapsto (\phi(y_2) \times \phi(y_8) + \phi(y_5') \times \phi(y_6') + \phi(y_4'') \times \phi(y_6'')),$$

$$y_5 \mapsto (\phi(y_3) \times \phi(y_5) + \phi(y_1') \times \phi(y_7') + \phi(y_3'') \times \phi(y_4'')),$$

$$y_5' \mapsto (\phi(y_6) \times \phi(y_7) + \phi(y_4') \times \phi(y_8') + \phi(y_5'') \times \phi(y_8'')).$$

The rest of the automorphism is determined by where $\rho(\phi)$ sends these 5 elements. Actually, though, you may notice a pattern here—each base vector is mapped to the sum of three terms, each of which is determined by the three ways a $\times$ product can equal that base vector. That is, since $y_6 = y_3 \times y_4 = y_3' \times y_5' = y_1'' \times y_7''$, we see how the three terms for the formula for y_6 are created. This pattern works for all base vectors *except* y_0, y_0', and y_0''. But for these three base vectors, we can use the property that $y_0 = y_1 \circ y_8 - 1$, $y_0' = y_1' \circ y_8' - 1$, and $y_0'' = y_1'' \circ y_8'' - 1$ to finish the automorphism.

Here is an example to demonstrate how this works. Suppose that we start with ϕ to be the automorphism

$$y_7 \mapsto y_7 + ay_1, \quad y_7' \mapsto y_7' + ay_1', \quad y_7'' \mapsto y_7'' + ay_1'',$$

$$y_8 \mapsto y_8 + ay_2, \quad y_8' \mapsto y_8' + ay_2', \quad y_8'' \mapsto y_8'' + ay_2'',$$

where a is an element of F_q. Then $\rho(\phi)$ will map

$$y_1 \mapsto (y_1) \times (y_2) + (y_1') \times (y_2') + (y_1'') \times (y_2'') = y_1 + y_1 + y_1 = y_1.$$

$$y_6 \mapsto (y_3) \times (y_4) + (y_3') \times (y_5') + (y_1'') \times (y_7'' + ay_1'') = y_6 + y_6 + (y_6 + 0) = y_6.$$

$$y_7 \mapsto (y_2) \times (y_8 + ay_2) + (y_5') \times (y_6') + (y_4'') \times (y_6'') = (y_7 + 0) + y_7 + y_7 = y_7.$$

$$y_5 \mapsto (y_3) \times (y_5) + (y_1') \times (y_7' + ay_1') + (y_3'') \times (y_4'')) = y_5 + (y_5 + 0) + y_5 = y_5.$$

$$y_5' \mapsto (y_6) \times (y_7 + ay_1) + (y_4') \times (y_8' + ay_2') + (y_5'') \times (y_8'' + ay_2'') = (y_5' + ay_1'') + (y_5' + ay_1'') + (y_5' + ay_1'') = y_5' + ay_1''.$$

The rest of the automorphism can be determined from these. The base vectors which do not map to themselves are given here:

$$y_0' \mapsto y_0' + ay_1, \quad y_0'' \mapsto y_0'' + ay_1, \quad y_4'' \mapsto y_4'' + ay_1',$$

$$y_5' \mapsto y_5' + ay_1'', \quad y_6' \mapsto y_6' + ay_2'', \quad y_6'' \mapsto y_6'' + ay_2',$$

$$y_7' \mapsto y_7' + ay_3'', \qquad y_7'' \mapsto y_7'' + ay_3', \qquad y_8 \mapsto y_8 + ay_0' + ay_0'' + a^2y_1,$$

$$y_8' \mapsto y_8' + ay_5'', \qquad y_8'' \mapsto y_8'' + ay_4'.$$

For a more complicated example, let us consider what $\rho(\rho(\phi))$ is, that is, we will do the same procedure to this new automorphism. We see that $\rho(\rho(\phi))$ will send

$$y_1 \mapsto (y_1) \times (y_2) + (y_1') \times (y_2') + (y_1'') \times (y_2'') = y_1 + y_1 + y_1 = y_1.$$

$$y_6 \mapsto (y_3) \times (y_4) + (y_3') \times (y_5' + ay_1'') + (y_1'') \times (y_7'' + ay_3') = y_6 + (y_6 + 0) + (y_6 + 0) = y_6.$$

$$y_7 \mapsto (y_2) \times (y_8 + ay_0' + ay_0'' + a^2y_1) + (y_5' + ay_1'') \times (y_6' + ay_2'') + (y_4'' + ay_1') \times (y_6'' + ay_2') =$$

$$(y_7 + 0 + 0 + a^2y_1) + (y_7 + 0 + 0 + a^2y_1) + (y_7 + 0 + 0 + a^2y_1) = y_7 + a^2y_1.$$

$$y_5 \mapsto (y_3) \times (y_5) + (y_1') \times (y_7' + ay_3'') + (y_3'') \times (y_4'' + ay_1')) = y_5 + (y_5 + 0) + (y_5 + 0) = y_5.$$

$$y_5' \mapsto (y_6) \times (y_7) + (y_4') \times (y_8' + ay_5'') + (y_5'') \times (y_8'' + ay_4') = y_5' + (y_5' + 0) + (y_5' + 0) = y_5'.$$

So far, this is looking just like the original ϕ, only with a replaced with a^2. Since these five determine the automorphism, we see that this pattern must continue—$\rho(\rho(\phi))$ is given by

$$y_7 \mapsto y_7 + a^2y_1, \quad y_7' \mapsto y_7' + a^2y_1', \quad y_7'' \mapsto y_7'' + a^2y_1'',$$

$$y_8 \mapsto y_8 + a^2y_2, \quad y_8' \mapsto y_8' + a^2y_2', \quad y_8'' \mapsto y_8'' + a^2y_2'',$$

and fixes the other base elements. It is obvious in this case that this is just ϕ with all of the coefficients squared. In fact, this will happen for all automorphisms ϕ, and so $\rho(\rho(A)) = \sigma(A)$, where σ is the field automorphism of F_q.

Now we can proceed as with ${}^2B_2$ and ${}^2G_2$. We let

$${}^2F_4(2^{2n+1}) = \{\phi \in F_4(2^{2n+1}) \text{ for which } \rho(\sigma^n(\phi)) = \phi\}.$$

To find the elements of ${}^2F_4(2^{2n+1})$, we will begin by determining which of the diagonal elements of $F_4(2^{2n+1})$ are in ${}^2F_4(2^{2n+1})$. We can see that $\rho(\mathrm{diag}(\alpha, \beta, \gamma, \delta))$ sends

$$y_1 \mapsto \alpha\gamma^{-1}y_1, \quad y_6 \mapsto \alpha\gamma\delta^2 y_6, \quad y_7 \mapsto (\alpha\gamma)^{-1}y_7, \quad y_5 \mapsto (\alpha\beta^2\gamma\delta^2)^{-1}y_5, \quad y_5' \mapsto \beta\gamma y_5'.$$

Thus, $\rho(\mathrm{diag}(\alpha, \beta, \gamma, \delta)) = \mathrm{diag}(\alpha\gamma^{-1}, \alpha\gamma\delta^2, (\alpha\gamma)^{-1}, \beta\gamma)$. In order for this to satisfy $\rho(\sigma^n(\phi)) = \phi$, we need to have

$$\alpha^{(2^n)}\gamma^{(-2^n)} = \alpha, \qquad \alpha^{(2^n)}\gamma^{(2^n)}\delta^{(2^{n+1})} = \beta, \qquad \alpha^{(-2^n)}\gamma^{(-2^n)} = \gamma, \quad \text{and} \quad \beta^{(2^n)}\gamma^{(2^n)} = \delta.$$

Because $x^{(2^{2n+1})} = x$ for all x in the field, we find that all four of these equations is satisfied if $\alpha = \gamma^{(-2^{n+1}-1)}$, and $\delta = \beta^{(2^n)}\gamma^{(2^n)}$. Thus we see that

$$\mathrm{diag}(\gamma^{(-2^{n+1}-1)}, \beta, \gamma, \beta^{(2^n)}\gamma^{(2^n)}) \in {}^2F_4(2^{2n+1}).$$

Here are some other elements of ${}^2F_4(2^{2n+1})$, in fact, these are in ${}^2F_4(2)$:

$$r = (y_4, y_5)(y_3, y_6)(y_1', y_2')(y_3', y_4')(y_5', y_6')(y_7', y_8')(y_1'', y_2'')(y_3'', y_5'')(y_4'', y_6'')(y_7'', y_8'').$$

$$s = (y_0, y_0'')(y_1, y_1')(y_3, y_3')(y_6, y_6')(y_8, y_8')(y_2, y_4')(y_5, y_2')(y_4, y_7').$$

$$z : y_0' \mapsto y_0' + y_1, \quad y_0'' \mapsto y_0'' + y_1, \quad y_4'' \mapsto y_4'' + w_1', \quad y_5' \mapsto y_5' + y_1'', \quad y_6' \mapsto y_6' + y_2'', \quad y_6'' \mapsto y_6'' + y_2',$$

$$y_7 \mapsto y_7 + y_1, \quad y_7' \mapsto y_7' + y_1' + y_3'', \quad y_7'' \mapsto y_7'' + y_1'' + y_3', \quad y_8 \mapsto y_8 + y_0' + y_0'' + y_1 + y_2, \quad y_8' \mapsto y_8' + y_2' + y_5'',$$

$$y_8'' \mapsto y_8'' + y_2'' + y_4'.$$

$$t : y_0 \mapsto y_0 + y_5'', \quad y_0' \mapsto y_0' + y_5'', \quad y_1' \mapsto y_1' + y_1, \quad y_2 \mapsto y_2 + y_2', \quad y_3 \mapsto y_3 + y_3', \quad y_3'' \mapsto y_3'' + y_1'',$$

$$y_4' \mapsto y_4' + y_2', \quad y_4'' \mapsto y_4'' + y_0 + y_0' + y_5'', \quad y_5 \mapsto y_5 + y_2 + y_2' + y_4', \quad y_5' \mapsto y_5' + y_4,$$

$$y_6' \mapsto y_6' + y_6, \quad y_7 \mapsto y_7 + y_4, \quad y_7' \mapsto y_7' + y_4 + y_5' + y_7, \quad y_8 \mapsto y_8 + y_8', \quad y_8'' \mapsto y_8'' + y_6''.$$

$$x : y_0' \mapsto y_0' + y_3, \quad y_0'' \mapsto y_0'' + y_3, \quad y_1'' \mapsto y_1'' + y_1' + y_2'', \quad y_2' \mapsto y_2' + y_1' + y_1'', \quad y_2'' \mapsto y_2'' + y_1', \quad y_3 \mapsto y_3 + y_5$$

$$y_3' \mapsto y_3' + y_3'' + y_4, \quad y_4 \mapsto y_4 + y_0' + y_0'' + y_5 + y_6, \quad y_4' \mapsto y_4' + y_3'', \quad y_5' \mapsto y_5' + y_4'' + y_6, \quad y_5'' \mapsto y_5'' + y_3' + y_3''$$

$$y_6 \mapsto y_6 + y_0' + y_0'' + y_3 + y_5, \quad y_6' \mapsto y_6' + y_4'', \quad y_6'' \mapsto y_6'' + y_4'' + y_5', \quad y_7'' \mapsto y_7'' + y_7' + y_8'', \quad y_8' \mapsto y_8' + y_7' + y_7'', \quad y_8'' \mapsto y_8'' + y_7'.$$

These elements, together with the diagonal elements that we found, will generate all of the group ${}^2F_4(2^{2n+1})$.

The group ${}^2F_4(2)$ is not simple, which is not too surprising since ${}^2B_2(2)$ and ${}^2G_2(3)$ were not simple. What is surprising is that ${}^2F_4(2)$, containing 35942400 elements, contains a simple group which we have not seen before! The Tits group is a subgroup of ${}^2F_4(2)$ containing half of its elements, 17971200. Technically, the Tits group is not a Chevalley group, so it should be classified with the 26 sporatic groups. But historically, the Tits group is considered to be an "honorary" Chevalley group, and is denoted by ${}^2F_4(2)'$, where the prime indicates the derived subgroup, which in this case produces the subgroup with half of the elements of ${}^2F_4(2)$.

If $n \geq 1$, then ${}^2F_4(2^{2n+1})$ is a new simple group, whose order is given by

$$|{}^2F_4(2^{2n+1})| = 2^{24n+12}(2^{12n+6}+1)(2^{8n+4}-1)(2^{6n+3}+1)(2^{2n+1}-1).$$

Alternative names: ${}^2F_4(2^{2n+1})$ is also called $\mathrm{Ree}(2^{2n+1})$, or $\mathrm{R}(2^{2n+1})$, the *Large Ree groups*.

$\mathbf{E}_6(\mathbf{q})$

Normally, one cannot take the determinant of a matrix when the elements are from a non-commutative ring, let alone a non-associate one. However, there is a natural way to define the determinant of an element of $\mathbb{J}(F_q)$.

$$\begin{vmatrix} a & w & \overline{v} \\ \overline{w} & b & u \\ v & \overline{u} & c \end{vmatrix} = abc + 2\mathrm{Re}(uvw) - au\overline{u} - bv\overline{v} - cw\overline{w}.$$

Note that this is well defined, since $\mathrm{Re}((uv)w) = \mathrm{Re}(u(vw))$. This is easy to see because both sides are zero if u, v, w all come from the set $\{1, \mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e_7}\}$ unless u, v, and w lie in a quaternion subalgebra, which is associative. In fact, $\mathrm{Re}(uvw) = \mathrm{Re}(vwu) = \mathrm{Re}(wuv)$. However, $\mathrm{Re}(uvw)$ is not always the same as $\mathrm{Re}(wvu)$. Beware that many of the familiar identities such as $\det(x \circ y) = \det(x)\det(y)$ are no longer true. Note that this will work even in characteristic 2, since we can rewrite $2\,\mathrm{Re}(uvw)$ as $(uv)w + \overline{(uv)}w$. Notice that if x is in $\mathbb{J}(F_q)$, then $\det(x) \in F_q$.

If we say that

$$u = u_1x_1 + u_2x_2 + u_3x_3 + u_4x_4 + u_5x_5 + u_6x_6 + u_7x_7 + u_8x_8,$$

$$v = v_1x_1 + v_2x_2 + v_3x_3 + v_4x_4 + v_5x_5 + v_6x_6 + v_7x_7 + v_8x_8,$$

$$w = w_1x_1 + w_2x_2 + w_3x_3 + w_4x_4 + w_5x_5 + w_6x_6 + w_7x_7 + w_8x_8,$$

then we find that

$$\det(x) = abc - au_1u_8 - au_2u_7 - au_3u_6 - au_4u_5 - bv_1v_8 - bv_2v_7 - bv_3v_6 - bv_4v_5 - cw_1w_8 - cw_2w_7 - cw_3w_6 - cw_4w_5$$
$$- u_8v_4w_1 - u_7v_6w_1 + u_6v_7w_1 - u_5v_8w_1 + u_8v_3w_2 - u_7v_5w_2 - u_4v_7w_2 - u_3v_8w_2 - u_8v_2w_3 - u_6v_5w_3 - u_4v_6w_3$$
$$+ u_2v_8w_3 - u_7v_2w_4 - u_6v_3w_4 + u_4v_4w_4 - u_1v_8w_4 - u_8v_1w_5 + u_5v_5w_5 - u_3v_6w_5 - u_2v_7w_5 + u_7v_1w_6 - u_5v_3w_6$$
$$- u_3v_4w_6 - u_1v_7w_6 - u_6v_1w_7 - u_5v_2w_7 - u_2v_4w_7 + u_1v_6w_7 - u_4v_1w_8 + u_3v_2w_8 - u_2v_3w_8 - u_1v_5w_8.$$

This actually forms a simple pattern: the term $-u_iv_jw_k$ appears if $x_ix_jx_k = -x_4$ or $-x_5$, while $+u_iv_jw_k$ appears if $x_ix_jx_k = x_4$ or x_5.

If we consider x to be a 27 dimensional vector, then we can consider a 27×27 matrix A, and Ax can then be considered in $\mathbb{J}(F_q)$. This allows us to define

$$E_6(q) = \{27 \times 27 \text{ matrices over } F_q \text{ such that } \det(Ax) = \det(x) \text{ for all } x \in \mathbb{J}(F_q)\}/\pm I.$$

As we have seen many times before, we have to factor out the center of the group $\pm I$, where $\pm$ is shorthand for all solutions to the equation $\omega^3 = 1$ in the field F_q. There will be 3 solutions to this equation if $q \equiv 1$ (Mod 3), overwise there $\pm I$ is just I.

In fact, we can express the determinant in terms of the trace and $\circ$ operations, as long as q is coprime to 6,

$$\det(x) = \frac{1}{3}\mathrm{Tr}(x \circ x \circ x) - \frac{1}{2}\mathrm{Tr}(x \circ x)\mathrm{Tr}(x) + \frac{1}{6}\mathrm{Tr}(x)^3.$$

Since $\mathrm{Tr}((x \circ x) \circ x) = \mathrm{Tr}(x \circ (x \circ x))$, this is also well defined. Because the determinant can be defined in terms of the trace, any element of $F_4(q)$ is in $E_6(q)$, or at least is in one of the cosets if $q \equiv 1$ (Mod 3). This immediately shows that $F_4(q)$ is a subgroup of $E_6(q)$. In fact, any element of E_6 which sends the identity element in $\mathbb{J}(F_q)$ to itself must be an automorphism. This gives us a much faster way of determining whether a mapping is in $F_4(q)$.

Notice that we have changed the basis vectors slightly from the previous two sections. There we had

$$y_0 = (-1,1,1|0,0,0), \qquad y_0' = (1,-1,1|0,0,0), \qquad y_0'' = (1,1,-1|0,0,0),$$

and for $1 \le i \le 8$,

$$y_i = (0,0,0|2x_i,0,0), \qquad y_i' = (0,0,0|0,2x_i,0), \qquad y_i'' = (0,0,0|0,0,2x_i).$$

If we introduce $y_9 = y_0' + y_0'' = (2,0,0|0,0,0)$, $y_9' = y_0 + y_0'' = (0,2,0|0,0,0)$, and $y_9'' = y_0 + y_0' = (0,0,2|0,0,0)$, we find that we can then scale all base vectors by a factor of 2, hence scaling the determinant by a factor of 8. Thus, if we let

$$\hat{y}_0 = (1,0,0|0,0,0), \qquad \hat{y}_0' = (0,1,0|0,0,0), \qquad \hat{y}_0'' = (0,0,1|0,0,0),$$

and for $1 \le i \le 8$,

$$\hat{y}_i = (0,0,0|x_i,0,0), \qquad \hat{y}_i' = (0,0,0|0,x_i,0), \qquad \hat{y}_i'' = (0,0,0|0,0,x_i),$$

then any element x of $\mathbb{J}(F_q)$ can be written as

$$x = i_1\hat{y}_1 + i_2\hat{y}_2 + i_3\hat{y}_3 + i_4\hat{y}_4 + i_5\hat{y}_5 + i_6\hat{y}_6 + i_7\hat{y}_7 + i_8\hat{y}_8 + a\hat{y}_9$$
$$+ j_1\hat{y}_1' + j_2\hat{y}_2' + j_3\hat{y}_3' + j_4\hat{y}_4' + j_5\hat{y}_5' + j_6\hat{y}_6' + j_7\hat{y}_7' + j_8\hat{y}_8' + b\hat{y}_9'$$
$$+ k_1\hat{y}_1'' + k_2\hat{y}_2'' + k_3\hat{y}_3'' + k_4\hat{y}_4'' + k_5\hat{y}_5'' + k_6\hat{y}_6'' + k_7\hat{y}_7'' + k_8\hat{y}_8'' + c\hat{y}_9''$$

Then $\det(x)$ would be given by the above formula. Although this new basis would affect the $\circ$ product, we are not using this product in the definition of E_6. In fact, we can still use most of the original basis, since $y_5 \mapsto y_5 + y_6'$ does the same thing as $\hat{y}_5 \mapsto \hat{y}_5 + \hat{y}_6'$.

Let us first consider the diagonal elements of A that are in $E_6(q)$. Of course we would get the diagonal elements that are in $F_4(q)$,

$$y_1 \mapsto \alpha y_1, \quad y_1' \mapsto (\beta\gamma\delta)^{-1} y_1', \quad y_1'' \mapsto -\alpha\delta y_1'',$$

$$y_2 \mapsto \gamma^{-1} y_2, \quad y_2' \mapsto \alpha\beta\delta y_2', \quad y_2'' \mapsto -(\gamma\delta)^{-1} y_2''$$
$$y_3 \mapsto \beta^{-1} y_3, \quad y_3' \mapsto \alpha\gamma\delta y_3', \quad y_3'' \mapsto -(\beta\delta)^{-1} y_3'',$$
$$y_4 \mapsto \alpha\beta\gamma\delta^2 y_4, \quad y_4' \mapsto \delta^{-1} y_4', \quad y_4'' \mapsto -(\alpha\beta\gamma\delta)^{-1} y_4'',$$
$$y_5 \mapsto (\alpha\beta\gamma\delta^2)^{-1} y_5, \quad y_5' \mapsto \delta y_5', \quad y_5'' \mapsto -\alpha\beta\gamma\delta y_5'',$$
$$y_6 \mapsto \beta y_6, \quad y_6' \mapsto (\alpha\gamma\delta)^{-1} y_6', \quad y_6'' \mapsto -\beta\delta y_6'',$$
$$y_7 \mapsto \gamma y_7, \quad y_7' \mapsto (\alpha\beta\delta)^{-1} y_7', \quad y_7'' - \gamma\delta y_7'',$$
$$y_8 \mapsto \alpha^{-1} y_8, \quad y_8' \mapsto \beta\gamma\delta y_8', y_8'' \mapsto -(\alpha\delta)^{-1} y_8''.$$

But we can also consider multiplying this by

$$y_2 \mapsto \epsilon^{-1} y_2, \quad y_2' \mapsto \zeta^{-1} y_2', \quad y_2'' \mapsto \epsilon\zeta y_2'',$$

$$y_3 \mapsto \epsilon^{-1} y_3, \quad y_3' \mapsto \zeta^{-1} y_3', \quad y_3'' \mapsto \epsilon\zeta y_3'',$$
$$y_8 \mapsto \epsilon^{-1} y_8, \quad y_8' \mapsto \zeta^{-1} y_8', \quad y_8'' \mapsto \epsilon\zeta y_8'',$$
$$y_4 \mapsto \epsilon^{-1}\zeta^{-1} y_4, \quad y_4' \mapsto \epsilon y_4', \quad y_4'' \mapsto \zeta y_4'',$$
$$y_5 \mapsto \zeta y_5, \quad y_5' \mapsto \epsilon^{-1}\zeta^{-1} y_5', \quad y_5'' \mapsto \epsilon y_5'',$$
$$y_9 \mapsto \epsilon y_5, \quad y_9' \mapsto \zeta y_9', \quad y_9'' \mapsto \epsilon^{-1}\zeta^{-1} y_9''.$$

where ϵ and ζ are non-zero elements of F_q.

There is another way of finding elements of $E_6(q)$ due to an important property of the determinant. If A is in $E_6(q)$, so that $\det(Ax) = \det(x)$ for all x, then $\det(A^T x) = \det(x)$ as well, so that $A^T \in E_6(q)$. Note that if A happens to be in $F_4(q)$ as well, A^T may not be in $F_4(q)$, since A^T may not fix the identity element. None-the-less, the transpose of all of the elements of $F_4(q)$ will be in $E_6(q)$, and together with the diagonal elements mentioned above, we generate all of $E_6(q)$.

$E_6(q)$ will be a new simple group for all q, whose size is

$$|E_6(q)| = \frac{q^{36}}{\mathrm{GCD}(3, q-1)}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5-1)(q^2-1).$$

${}^2\mathbf{E}_6\mathbf{(q)}$

The fact that A^T will be in E_6 whenever $A \in E_6(q)$ suggests that we can create an automorphism as we did for $L_n(q)$. By defining $\tau(A) = (A^T)^{-1}$, we find that $\tau(AB) = \tau(A)\tau(B)$, and τ will be of order 2. Now if we consider a field of size q^2, there will be a complex conjugate operation of order 2 as well. So just as we did for $U_n(q)$, we can consider the set of elements of $E_6(q^2)$ for which $\tau(A) = \overline{A}$, or equivalently,

$${}^2E_6(q) = \{27 \times 27 \text{ matrices over } F_{q^2} \text{ such that } A^T\overline{A} = I \text{ and } \det(Ax) = \det(x) \text{ for all } x \in \mathbb{J}(F_q)\}/\pm I.$$

This will give a new simple group for all q, whose size is

$$|{}^2E_6(q)| = \frac{q^{36}}{\mathrm{GCD}(3, q+1)}(q^{12}-1)(q^9+1)(q^8-1)(q^6-1)(q^5+1)(q^2-1).$$

Alternative names: ${}^2E_6(q)$ is sometimes written as ${}^2E_6(q^2)$, since the field used is of order q^2.

$\mathbf{E_7(q)}$

To introduce $E_7(q)$, we introduce a sort of conjugate operator on $\mathbb{J}(F_q)$. If $A \in \mathbb{J}(F_q)$, with

$$A = \begin{pmatrix} a & w & \overline{v} \\ \overline{w} & b & u \\ v & \overline{u} & c \end{pmatrix},$$

we define

$$\tilde{A} = \begin{pmatrix} bc - u\overline{u} & \overline{vu} - cw & wu - b\overline{v} \\ uv - c\overline{w} & ac - v\overline{v} & \overline{wv} - au \\ \overline{uw} - bv & vw - a\overline{u} & ab - w\overline{w} \end{pmatrix}.$$

Then $\tilde{A}$ has an amazing property:

$$A \circ \tilde{A} = \det(A) \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

We now consider a 56 dimensional vector $x = \langle p, P, q, Q \rangle$, where $p, q \in F_q$ and $P, Q \in \mathbb{J}(F_q)$. We define the two polynomials on x as follows:

$$C_1(x) = P \circ Q,$$

$$C_2(x) = (pq + \mathrm{Tr}(P \circ Q))^2 + p\mathrm{Tr}(Q \circ \tilde{Q}) + q\mathrm{Tr}(P \circ \tilde{P}) + \mathrm{Tr}(\tilde{P} \circ \tilde{Q}).$$

Then E_7 is the set of automorphisms on these two polynomials. That is,

$$E_7(q) = \{56 \times 56 \text{ matrices } A \text{ over } F_q \text{ such that } C_1(Ax) = C_1(x) \text{ and } C_2(Ax) = C_2(x) \text{ for all } x\}/ \pm I.$$

This produces a new simple group for all q. The size of the group is

$$|E_7(q)| = \frac{q^{63}}{\mathrm{GCD}(2, q-1)}(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^{10}-1)(q^8-1)(q^6-1)(q^2-1),$$

which is starting to get enormous. Even the smallest such group, $E_7(2)$, contains

$$7,997,476,042,075,799,759,100,487,262,680,802,918,400$$

elements.

$\mathbf{E_8(q)}$

The final Chevalley group is extremely complex, and I have not found an easy explanation E_8. Perhaps someone can help me to explain this last group, and finish the project. I can say that $E_8(q)$ will produce new simple groups for all q, and that

$$|E_8(q)| = q^{120}(q^{30}-1)(q^{24}-1)(q^{20}-1)(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^8-1)(q^2-1).$$

These groups are of ridiculously immense size. In fact, the smallest E_8 group, $E_8(2)$, is larger that the Monster group.