EXPLICIT REALIZATION OF THE DICKSON GROUPS
\( G_2(q) \) AS GALOIS GROUPS

Gunter Malle
For any prime power \( q \) we determine a polynomial \( f_q(X) \in F_q(t, u)[X] \) whose Galois group over \( F_q(t, u) \) is the Dickson group \( G_2(q) \). The construction uses a criterion and a method due to Matzat.

1. Introduction.

In this paper we are concerned with the construction of polynomials whose Galois groups are the exceptional simple Chevalley groups \( G_2(q) \), \( q \) a prime power, first discovered by Dickson; see Theorems 4.1 and 4.3.

It was shown by Nori [7] that all semisimple simply-connected linear algebraic groups over \( F_q \) do occur as Galois groups of regular extension of regular function fields over \( F_q \), but his proof does not give an explicit equation or even a constructive method for obtaining such extensions. On the other hand, in a long series of papers Abhyankar has given families of polynomials for groups of classical types (see [1] and the references cited there). His ad hoc approach hasn’t yet led to families with groups of exceptional type (but see [2] for a different construction of polynomials with Galois group the simple groups of Suzuki). Thus it seems natural to try to fill this gap. In his recent paper Matzat [6] describes an algorithmic approach which reduces the construction of generating polynomials for such extensions to certain group theoretic calculations.

More precisely, let \( F := F_q(t) \), with \( t = (t_1, \ldots, t_s) \) a set of indeterminates. We denote by \( \phi_q : F \to F, x \mapsto x^q \), the Frobenius endomorphism. Let \( G \) be a reduced connected linear algebraic group defined over \( F_q \), with a faithful linear representation \( \Gamma : G(F) \hookrightarrow \text{GL}_n(F) \) in its defining characteristic, also defined over \( F_q \). We identify \( G(F) \) with its image in \( \text{GL}_n(F) \). Fix an element \( g \in G(F) \) and assume that \( g \in \text{GL}_n(R) \), where \( R := F_q[t] \). Any specialization homomorphism \( \psi : R \to F_q, t_j \mapsto \psi(t_j) \), can be naturally extended to \( \text{GL}_n(R) \). We define

\[
g_\psi := \psi(g) \cdot \psi(\phi_q(g)) \cdots \psi(\phi_q^{a-1}(g)) \in \text{GL}_n(F_q).
\]

With these notations Matzat [6, Thm. 4.3 and 4.5] shows the following:

**Theorem 1.1** (Matzat). Let \( G(F) \leq \text{GL}_n(F) \) be a reduced connected linear algebraic group defined over \( F_q \). Let \( g \in \text{GL}_n(R) \) such that:
(i) $g \in G(F)$,
(ii) there exist specializations $\psi_i : R \to \mathbb{F}_{q^n}$, $1 \leq i \leq k$, such that no proper subgroup of $G(\mathbb{F}_q) \leq \text{GL}_n(\mathbb{F}_q)$ contains conjugates of all the $g_{\psi_i}$, $1 \leq i \leq k$.

Then $G(\mathbb{F}_q)$ occurs as regular Galois group over $F$, and a generating polynomial $f(t, X) \in F[X]$ for such a $G(\mathbb{F}_q)$-extension can be computed explicitly from the matrix $g$.

Thus the strategy for the computation of a $G_2(q)$-polynomial will be the following: First construct a small faithful matrix representation of $G_2(F)$ in its defining characteristic. For this we use the well-known facts that $G_2(F)$ is a subgroup of an 8-dimensional orthogonal group over $F$, and that this 8-dimensional representation has a faithful irreducible constituent of dimension 6 for $G_2(F)$, if $\text{char}(F) = 2$, respectively of dimension 7 if $\text{char}(F) > 2$. Secondly, we need to find an element $g \in G_2(F)$ with the properties required in the theorem. For this, we make use of the known lists of maximal subgroups of $G_2(q)$ by Cooperstein and Kleidman. (These results require the classification of finite simple groups, but only in a very weak form.) Finally, the corresponding polynomial has to be computed using a version of the Buchberger algorithm.

2. Identifying $G_2(F)$ inside the 8-dimensional orthogonal group.

We first introduce some notation. Let $V$ be an 8-dimensional vector space over a field $F$ of characteristic $p \geq 0$, with basis $e_1, \ldots, e_8$ and $Q$ the quadratic form on $V$ defined by

$$Q : V \to F, \quad Q\left(\sum_{i=1}^{8} x_i e_i\right) = \sum_{i=1}^{4} x_i x_{9-i}.$$

We denote by $\text{GO}_8(F)$ the group of isometries of $Q$, the full orthogonal group, and by $\text{SO}_8(F)$ the connected component of the identity in $\text{GO}_8(F)$, of index 2. Thus $\text{SO}_8(F)$ is a simple split algebraic group over $F$ of type $D_4$. The subgroup of upper triangular matrices of $\text{GL}_8(F)$ contains a Borel subgroup $B$ of $\text{SO}_8(F)$. More precisely, the unipotent radical of $B$ is generated by the root subgroups

$$X_i := \{x_i(t) \mid t \in F\}, \quad i = 1, \ldots, 12,$$

where the $x_i(t)$ are defined as in Table 1. Here $E_{i,j}(t)$ denotes the matrix having 1’s on the diagonal and one further nonzero entry $t$ in position $(i, j)$.

A maximal torus $T$ in $B$ is given by the set of diagonal matrices

$$T := \{t = \text{diag}(t_1, t_2, t_3, t_4, t_4^{-1}, t_3^{-1}, t_2^{-1}, t_1^{-1}) \mid t_i \in F^\times\}.$$

The simple roots with respect to $T$ are now $\alpha_i$, $i = 1, \ldots, 4$, with $\alpha_i(t) = t_i/t_{i+1}$ for $i = 1, 2, 3$ and $\alpha_4(t) = t_3 t_4$. In Table 1 we have also recorded the
The group $\text{PSO}_8(F)$ with $G := \text{SO}_8(F)/Z(\text{SO}_8(F))$ possesses an outer automorphism $\gamma$ of order 3 induced by the graph automorphism of the Dynkin diagram $D_4$ which cyclically permutes the nodes 1, 3 and 4 and fixes the middle node 2. The group $\text{PSO}_8(F)^\gamma$ of fixed points in $\text{PSO}_8(F)$ under $\gamma$ is again a simple connected algebraic group over $F$, of type $G_2$. Note that $\gamma$ does not stabilize the natural representation of $\text{SO}_8(F)$. Nevertheless we can construct $G_2(F)$ as a preimage $G$ of $\text{PSO}_8(F)^\gamma$ in $\text{SO}_8(F)$.

The Borel subgroup $B$ of $\text{SO}_8(F)$ contains a Borel subgroup of $G$. Its unipotent radical is the product of the subgroups

$$X_{i,j,k} := \{x_i(t)x_j(t)x_k(t) \mid t \in F\}$$

where $(i,j,k) \in \{(1,3,4),(5,6,7),(8,9,10)\}$, together with the root subgroups $X_i = \{x_i(t) \mid t \in F\}$ for $i \in \{2,11,12\}$ (see for example Carter [3, Prop. 13.6.3]). A maximal torus of $G$ inside $T$ consists of the elements

$$\{t = \text{diag}(t_1,t_2,t_1t_2^{-1},1,1,t_1^{-1}t_2,t_2^{-1},t_1^{-1}) \mid t_i \in F^\times\}.$$ 

From this description we find that the simple roots for $G_2(F)$ are now $\alpha, \beta$, with $\alpha(t) := t_1^{-1}t_2$ and $\beta(t) := t_2^2/t_1$, and with corresponding root subgroups $X_\alpha := X_{1,3,4}, X_\beta := X_2$ respectively.

An easy calculation with the generators of root subgroups given above now shows that $G$ leaves invariant the hyperplane $V_1$ of $V$ consisting of vectors with equal fourth and fifth coordinate, as well as the 1-dimensional subspace $V_2$ of $V$ spanned by $e_4 - e_5$. Thus we obtain an induced action of $G$ on $V_1$, respectively on $V_1/V_2$ when $\text{char}(F) = 2$. This yields a faithful matrix representation $\Gamma : G_2(F) \hookrightarrow \text{GL}_n(F)$ of $G_2(F)$, of dimension $n = 7$ when $\text{char}(F) \neq 2$, respectively of dimension $n = 6$ when $\text{char}(F) = 2$. It is well-known that the smallest possible degree of a faithful representation of $G_2(F)$ is 7, respectively 6 if $\text{char}(F) = 2$, so our representation $\Gamma$ is irreducible.

**Table 1. Root subgroups of $\text{SO}_8(F)$.**

<table>
<thead>
<tr>
<th>$x_1(t)$</th>
<th>$x_2(t)$</th>
<th>$x_3(t)$</th>
<th>$x_4(t)$</th>
<th>$x_5(t)$</th>
<th>$x_6(t)$</th>
<th>$x_7(t)$</th>
<th>$x_8(t)$</th>
<th>$x_9(t)$</th>
<th>$x_{10}(t)$</th>
<th>$x_{11}(t)$</th>
<th>$x_{12}(t)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E_{1,2}(t) - E_{7,8}(t)$</td>
<td>$E_{2,3}(t) - E_{6,7}(t)$</td>
<td>$E_{3,4}(t) - E_{5,6}(t)$</td>
<td>$E_{3,5}(t) - E_{4,6}(t)$</td>
<td>$E_{1,3}(t) - E_{6,8}(t)$</td>
<td>$E_{2,4}(t) - E_{5,7}(t)$</td>
<td>$E_{2,5}(t) - E_{4,7}(t)$</td>
<td>$E_{1,4}(t) - E_{5,8}(t)$</td>
<td>$E_{2,6}(t) - E_{3,7}(t)$</td>
<td>$E_{1,5}(t) - E_{4,8}(t)$</td>
<td>$E_{1,6}(t) - E_{3,8}(t)$</td>
<td>$E_{1,7}(t) - E_{2,8}(t)$</td>
</tr>
</tbody>
</table>
Remark 2.1. The matrices given in [4, p. 34] do not define a representation of $G_2(2^f)$. Indeed, the matrix for $h_a(t)$ does not have determinant 1, as it should have (since $G_2(2^f)$ is simple for $f > 1$). Its second diagonal entry should be $t^{-1}$. Conjugating $X_a(t)$ by $h_a(t')$ one sees that the middle off-diagonal entry of $X_a(t)$ should be $t^2$ instead of $t$. The commutator relations (see Carter [3, 12.4]; [4, (2.1)] contains misprints) then show that similarly in the matrices for $X_{a+b}(t)$ and $X_{2a+b}(t)$ the second nonzero off-diagonal entry $t$ should be replaced by $t^2$. In this way one recovers the representation constructed above.

3. Finding a suitable element.

Let first $q = 2^f$ be even. Then an easy calculation shows that in our 6-dimensional representation $\Gamma : G_2(F) \rightarrow \text{GL}_6(F)$ constructed above, we have

$$x_\alpha(t) = \begin{pmatrix} 1 & t & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & t^2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & t \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad x_\beta(t) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & t & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

and the longest element of the Weyl group of $G_2(F)$ is represented by

$$w_0 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

We choose $g := x_\alpha(t)x_\beta(u)w_0 \in G_2(F)$ and let

$$D := \Gamma(g) = \begin{pmatrix} 0 & 0 & 0 & tu & t & 1 \\ 0 & 0 & 0 & u & 1 & 0 \\ 0 & t^2u & t^2 & 1 & 0 & 0 \\ 0 & u & 1 & 0 & 0 & 0 \\ t & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Proposition 3.1. Let $q$ be even and $D$ be defined as above. Then no proper subgroup of $G_2(q)$ contains conjugates of all specializations of $D$.

Proof. We use the fact that all maximal subgroups of the finite groups $G_2(q)$ are known by Cooperstein [4]. For $q = 2$ specializations into $\mathbb{F}_8$ yield elements of orders 7 and 12, and no maximal subgroup of $G_2(2)$ contains elements of both orders. For $q = 4$ specializations into $\mathbb{F}_4$ yield elements of
orders 13, 15 and 21. The only maximal subgroup of order divisible by 7 · 13 is PSL$_2(13)$, but its order is not divisible by 5, so we are done again.

Now let $q \geq 8$. Let $G$ be a subgroup of $G_2(q)$ containing conjugates of all specializations of $D$. Let $\alpha \in \mathbb{F}_q^{\times}$ of order $q + 1$. Then the minimal polynomial of $\alpha$ over $\mathbb{F}_q$ has the form $X^2 + \text{Tr}(\alpha)X + 1$, where $\text{Tr}(\alpha) = \alpha + \alpha^q \in \mathbb{F}_q$. Thus any element of $\mathbb{F}_q^{\times}$ of order $q + 1$ occurs as a root of a polynomial of the shape

$$X^2 + vX + 1, \quad v \in \mathbb{F}_q.$$  

Clearly, all elements of $\mathbb{F}_q^{\times}$ also occur as zeros of such a polynomial. Now for $v \in \mathbb{F}_q$ consider the specialization  

$$\psi_v : \mathbb{F}_q[t, u] \rightarrow \mathbb{F}_q, \quad t \mapsto 0, \; u \mapsto v.$$  

Then the specialization $\psi_v(D)$ of $D$ has characteristic polynomial

$$X^6 + (v^2 + 1)X^4 + (v^2 + 1)X^2 + 1 = (X + 1)^2(X^2 + vX + 1)^2.$$  

The 1-eigenspace of $\psi_v(D)$ only has dimension 1 for $v \neq 0$, so the order of $\psi_v(D)$ is divisible by 2. By our above considerations, we hence find elements of orders $2(q + 1)$ and $2(q - 1)$ as specializations of $D$. (This can also be seen as follows: If $t = 0$ then $g$ specializes to

$$x_{\beta}(u)w_0 = x_{\beta}(u)(w_{\beta}w_{\alpha})^2 = x_{\beta}(u)w_{\beta} \cdot w'$$

where $w' = w_{\alpha}w_{\beta}w_{\alpha}w_{\beta}w_{\alpha}$ has order 2, centralizes $x_{\beta}(u)w_{\beta}$, and $x_{\beta}(u)w_{\beta}$ represents the element

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

in the subgroup $\langle X_{\beta}, X_{-\beta} \rangle \cong \text{SL}_2(q)$.)

Next, consider the specialization  

$$\psi'_v : \mathbb{F}_q[t, u] \rightarrow \mathbb{F}_q, \quad t \mapsto v, \; u \mapsto 0.$$  

Here, $\psi'_v(D)$ has characteristic polynomial

$$(X^2 + vX + 1)^2(X^2 + v^2X + 1).$$

By the argument above, this again yields elements of orders $2(q - 1)$ and $2(q + 1)$. But note that this time these elements never have an eigenvalue 1, nor have any of their powers of order larger than 2. Thus $G$ contains subgroups of order $(q \pm 1)^2$. Theorem 2.3 in [4] shows that either $G \leq \text{SL}_2(q) \times \text{SL}_2(q)$ or $G = G_2(q)$.

Finally, consider the specialization

$$\psi''_v : \mathbb{F}_q[t, u] \rightarrow \mathbb{F}_q, \quad t \mapsto v, \; u \mapsto 1.$$  

The corresponding specialization of $D$ has characteristic polynomial

$$(X^3 + v^2X + 1)(X^3 + v^2X^2 + 1).$$
If \( X^3 + v^2X + 1 \) is reducible over \( \mathbb{F}_q \), then it has a linear factor \( X + a \), \( a \in \mathbb{F}_q \), and \( X^3 + v^2X + 1 = (X + a)(X^2 + aX + 1/a) \). Clearly, the case \( a = 0 \) is not possible, so for at least one of the \( q \) possibilities for \( v \in \mathbb{F}_q \) the characteristic polynomial has an irreducible factor of degree 3. In this case, the specialization of \( D \) has order dividing \( q^2 + q + 1 \), but not \( q - 1 \). Since \( SL_2(q) \times SL_2(q) \) doesn’t contain such elements, we have \( G = G_2(q) \), as claimed.

For odd \( q = p^f \) we again choose \( g := x_\alpha(t)x_\beta(u)w_0 \in G_2(F) \). With

\[
x_\alpha(t) = \begin{pmatrix} 1 & t & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & t \cdot -t^2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -t \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},
\]

\[
x_\beta(t) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & t & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -t \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},
\]

and

\[
w_0 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},
\]

this gives

\[
D := \Gamma(g) = \begin{pmatrix} 0 & 0 & 0 & 0 & tu & -t & 1 \\ 0 & 0 & 0 & 0 & u & -1 & 0 \\ 0 & -t^2 & -t^2 & -t & 1 & 0 & 0 \\ 0 & -2tu & -2t & -1 & 0 & 0 & 0 \\ 0 & u & 1 & 0 & 0 & 0 & 0 \\ -t & -1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.
\]
in this case. This matrix has separable characteristic polynomial
\[
X^7 + (t^2 + 1) X^6 - (2t^2 + u^2 + 3) X^5 - (t^4 + 3t^2 + u^2 + 3) X^4
+ (t^4 + 3t^2 + u^2 + 3) X^3 + (2t^2 + u^2 + 3) X^2 - (t^2 + 1) X - 1.
\]

We need the following result:

**Lemma 3.2.** Let \( q > 3 \) be an odd prime power. Then there exists \( v \in \mathbb{F}_q \) such that
\[
X^3 - (v^2 + 2)X - 1
\]
is irreducible over \( \mathbb{F}_q \).

**Proof.** Assume that \( f := X^3 - (v^2 + 2)X - 1 \) is reducible. Then \( f \) has a zero \( a \in \mathbb{F}_q \), and \( X^3 - (v^2 + 2)X - 1 = (X - a)(X^2 + aX + a^{-1}) \). These zeros are just the first coordinates of the \( \mathbb{F}_q \)-points on the elliptic curve \( E \) defined by \( U^3 - (V^2 + 2)U - 1 \). By the Weil bounds, \( E \) has at most \( q + 1 + 2\sqrt{q} \) points \((u, v)\) over \( \mathbb{F}_q \). Clearly, with \((u, v)\) the point \((u, -v)\) also lies on \( E \), hence there are at most \( q/2 + 1 + \sqrt{q} \) distinct values \( a \) which can occur as zeros of \( f \).

Next, we estimate how often \( f \) splits completely into linear factors. This happens if in addition the discriminant \((a^3 - 4)/a\) of \( X^2 + aX + a^{-1} \) is a square in \( \mathbb{F}_q \). Thus we need to count points on the \( \mathbb{F}_q \)-curve \( C \) defined by the two equations
\[
U^3 - (V^2 + 2)U - 1, \quad U^3 - W^2U - 4.
\]
Subtracting these two equations we see that \( U \) lies in the function field \( \mathbb{F}_q(V, W) \). Since both \( V, W \) have degree at most 2 over \( \mathbb{F}_q(U) \), the curve \( C \) has genus at most 4. Moreover, the only singular point of \( C \) is the point with coordinates \((4, 0, 0)\) in characteristic 5. Again by the Weil bounds, this means that \( C \) has at least \( q + 1 - 2 \cdot 4\sqrt{q} - 6 \) points over \( \mathbb{F}_q \). For each such point, changing the sign of the \( V, W \)-coordinates again yields a point, hence there are at least \((q - 5 - 8\sqrt{q})/4\) distinct \( a \in \mathbb{F}_q \) for which \( f \) splits completely. Thus we obtain at most
\[
(q/2 + 1 + \sqrt{q} - (q - 5 - 8\sqrt{q})/4 = (q + 9)/4 + 3\sqrt{q}
\]
factorizations of \( f \) into a linear and a quadratic factor. The discriminant of \( f \) is a polynomial in \( v \) of degree 6, hence \( f \) is inseparable for at most six values of \( v \). Apart from those, each completely splitting \( f \) accounts for three different values of \( a \), so we obtain a total of at most
\[
(q + 9)/4 + 3\sqrt{q} + ((q - 5 - 8\sqrt{q})/4 - 6)/3 + 6 = (2q + 35)/6 + 7/3\sqrt{q}
\]
reducible polynomials when \( v \) runs over \( \mathbb{F}_q \). Hence there remain at least
\[
(q + 1)/2 - ((2q + 35)/6 + 7/3\sqrt{q}) = (q - 32)/6 - 7/3\sqrt{q}
\]
irreducible polynomials. This is positive for \( q \geq 257 \). For the remaining prime powers \( 3 < q < 257 \) a computer check shows that the assertion is
also satisfied. (For \( q = 5, 9 \) there is just one irreducible polynomial of the required shape, for \( q = 3 \) there is none.)

Note that the counting of singular points and of inseparable \( f \) was very rough and a more detailed analysis would have reduced the bound considerably.

\[ \Box \]

**Proposition 3.3.** Let \( q \) be odd and \( D \) be the matrix defined in (2). Then no proper subgroup of \( G_2(q) \) contains conjugates of all specializations of \( D \).

**Proof.** Again all maximal subgroups of \( G_2(q) \) are known by work of Kleidman [5]. For \( q = 3 \), specializations into \( \mathbb{F}_9 \) yield elements of orders 7, 9, 13, but that has no elements of order 9. For \( q = 5 \), specialization into \( \mathbb{F}_5 \) yields element orders 7, 20 and 31, thus we are done again.

For \( q \geq 7 \) let \( G \) be a subgroup of \( G_2(q) \) containing conjugates of all specializations of \( D \). We again consider the specialization

\[ \psi_v : \mathbb{F}_q[t, u] \rightarrow \mathbb{F}_q, \quad t \mapsto 0, \quad u \mapsto v. \]

Then the square of \( \psi_v(D) \) has characteristic polynomial

\[ (X - 1)^3(X^2 - (v^2 + 2)X + 1)^2. \]

This gives rise to elements of orders \( q \pm 1 \) in \( G \). Similarly, the specialization

\[ \psi'_v : \mathbb{F}_q[t, u] \rightarrow \mathbb{F}_q, \quad t \mapsto v, \quad u \mapsto 0, \]

yields the characteristic polynomial

\[ (X - 1)(X^2 - (v^4 + 4v^2 + 2)X + 1)(X^2 - (v^2 + 2)X + 1)^2 \]

for the image of \( D^2 \). So as in the previous proof we deduce that \( G \) must contain subgroups of orders \((q \pm 1)^2\). Theorem A in [5] shows that either \( G \) is contained in the central product \( \text{SL}_2(q) \circ \text{SL}_2(q) \), or \( G = G_2(q) \). Finally, for the specialization

\[ \psi''_v : \mathbb{F}_q[t, u] \rightarrow \mathbb{F}_q, \quad t \mapsto v, \quad u \mapsto 1, \]

we obtain the characteristic polynomial

\[ (X - 1)(X^3 + (v^2 + 2)X^2 - 1)(X^3 - (v^2 + 2)X - 1) \]

for \( \phi''_v(D) \). Since \( q \geq 7 \) is odd, Lemma 3.2 shows that there exists \( v \in \mathbb{F}_q \) such that the degree 3 factors of this polynomial are irreducible over \( \mathbb{F}_q \). But \( \text{SL}_2(q) \circ \text{SL}_2(q) \) does not contain such elements, hence we have \( G = G_2(q) \). \[ \Box \]
4. The polynomials.

It remains to determine generating polynomials for the $G_2(q)$-extensions whose existence is guaranteed by Theorem 1.1 in conjunction with Propositions 3.1 and 3.3.

**Theorem 4.1.** Let $q = 2^f$ be a power of 2. Then the polynomial
\[ X^{q^6} + u^{e_2} t^{e_4} X^{q^5} + (u^{e_1} t^{e_1} + u^{e_3} t^{e_1} + t^{e_1} + t^{e_3} + 1)X^{q^4} \\
+ u^{e_2} t^{e_4} (t^{q^3} - q + 1)X^{q^3} \\
+ t^{e_1} (u^{e_1} t^{q^2 + q} + u^{e_1} + u^{e_3} + 1)X^{q^2} \\
+ u^{e_2} t^{q^4 + 2q - 2} X^q + u^{e_1} t^{q^4 - 1} X, \]
with $e_1 := q^4 - q^2$, $e_2 := q^4 - q^3$, $e_3 := q^4 + q^3$, $e_4 := q^4 - q^3 + 2q^2$, has Galois group $G_2(q)$ over $\mathbb{F}_q(t,u)$.

**Proof.** In Proposition 3.1 we have shown that the assumptions of Matzat’s Theorem 1.1 are satisfied for the matrix $D$ defined in (1). According to Matzat [6, §1], a generating polynomial for a field extension with group $G_2(q)$ can now be obtained by solving the non-linear system of equations given by
\[ y = Dy^q, \]
where $y = (y_1, \ldots, y_6)^t$, for one of the variables. Solving for $y_6$ yields the equation displayed in the statement. \(\square\)

By the Hilbert irreducibility theorem, there exist 1-parameter specializations of the polynomial in Theorem 4.1 with group $G_2(q)$.

**Example 4.2.** By arguments similar to those used in the proof of Proposition 3.1 it can be checked that the polynomial
\[ X^{64} + t^{24} X^{32} + (t^{36} + t^{12} + 1) X^{16} + (t^{30} + t^{36} + t^{24}) X^{8} \\
+ (t^{24} + t^{36} + t^{27} + t^{30} + t^{12}) X^4 + t^{30} X^2 + t^{27} X \]
obtained by setting $u = t$ has Galois group $G_2(2)$ over $\mathbb{F}_2(t)$.

**Theorem 4.3.** Let $q = p^f$ be an odd prime power. Then the polynomial
\[ X^{q^7} + u^{e_1} t^{e_4} (t^{e_6} + 1) X^{q^6} - (t^{e_2} u^{e_3} + t^{q^3 + q^2} + t^{e_2}) u^{e_2} + t^{e_3} + t^{e_2} + 1)X^{q^5} \\
- u^{e_1} t^{e_4} (t^{e_5} (u^{q^3} + u^{e_3}) + (t^{e_6} + 1)(t^{q^4 + q^3} + t^{e_5} + 1))X^{q^4} \\
+ t^{e_2} (u^{e_3} + (t^{e_6} + 1)(t^{e_6} + t^{q^2 - q} + 1) u^{e_2} + 1)X^{q^3} \\
+ u^{e_1} t^{q^2} t^{q^3 - 2q} (u^{q^3 + q^2} + t^{q^2 + q} + t^{q^2 + q} + t^{q^2 - 1} + 1) u^{e_5} + t^{e_6} + 1)X^{q^2} \\
- u^{e_2} t^{q^3 - q} (t^{e_6} + 1) X^q - u^{q^2 - q^2} t^{q^3 - q^3 - q^2 - 1} X, \]
where $e_1 := q^5 - q^4$, $e_2 := q^5 - q^3$, $e_3 := q^5 + q^4$, $e_4 := q^5 - q^4 + q^3 - q^2$, \(\square\)
\( e_5 := q^4 - q^2, \ e_6 := q^3 + q^2, \) has Galois group \( G_2(q) \) over \( \mathbb{F}_q(t,u) \).

The proof is as for the preceding theorem, starting this time from the matrix \( D \) given in (2), solving for \( y_7 \), and using Proposition 3.3.

**Remark 4.4.** The sporadic simple Janko groups \( J_1 \) and \( J_2 \) are subgroups of \( G_2(11) \), respectively of \( G_2(4) \). It would be nice to find Galois extensions for these groups in characteristic 11 respectively 2 by the above method, possibly as specializations of the polynomials in Theorems 4.1 and 4.3.

**Remark 4.5.** The next smallest simple exceptional group is the one of type \( F_4 \). Its smallest faithful representation has dimension 26, respectively 25 in characteristic 3. In principle, the methods of this paper should make it possible to produce an \( F_4(q) \)-polynomial.

**Remark 4.6.** The group \( G_2(q), \ q \ odd \), has \( q \) orbits on nonzero vectors in its 7-dimensional representation. Thus, the polynomial \( f_q(t,u,X) \) in Theorem 4.3 has \( q \) factors, of degrees roughly \( q^6 \), and a linear factor. On the other hand, any specialization of \( f_q \) has factors of degree at most \( q^2 + q + 1 \), the maximal element order in \( G_2(q) \). Thus, \( f_q \) seems a good candidate for testing factorization algorithms. Using Maple we have not been able to find the factorization of \( f_q \) for \( q = 3 \).

Similarly, for \( q \ even \ G_2(q) \) has a single orbit on the nonzero vectors of the 6-dimensional module. Hence \( f_q(t,u,X) \) in Theorem 4.1 is irreducible apart from the trivial linear factor. Again Maple was not able to confirm this for \( q = 4 \).

**Acknowledgement.** I’m indebted to N. Elkies for pointing out an overzealous simplification in a previous version.

**References**


Fachbereich Mathematik/Informatik
Universität Kassel
Heinrich-Plett-Str. 40, D–34132 Kassel
Germany
E-mail address: malle@mathematik.uni-kassel.de