J. reine angew. Math. **392** (1988), 70—109

Journal für die reine und
angewandte Mathematik
© Walter de Gruyter
Berlin · New York 1988

Exceptional groups of Lie type as Galois groups

By *Gunter Malle**) at Berlin

Introduction

The inverse problem of Galois theory is concerned with the question whether every finite group occurs as a Galois group over the rationals $\mathbb{Q}$ or, more generally, over at most abelian extension fields of $\mathbb{Q}$. An important step towards the solution seems to be the realization of all *simple* groups as Galois groups over such fields. The inverse problem for arbitrary finite groups then reduces to solving embedding problems for Galois extensions. The main source of Galois realizations for finite groups (with trivial center) as Galois groups over the maximal abelian extension field $\mathbb{Q}^{ab}$ of $\mathbb{Q}$ is the sufficient rationality criterion proved in different generalizations by Belyi [3], Matzat [33], and Thompson [43]: *Let G be a finite group with trivial center having a class structure $\mathfrak{C}=(C_1, C_2, C_3)$ which contains just one generating system of elements modulo conjugation. Then G occurs as a Galois group over a suitable abelian number field.* (For notation, see the first paragraph.)

This criterion reduces the inverse problem for simple groups to purely group theoretical calculations. It could be shown to hold for the alternating groups A_n [33], the classical simple groups of Lie type [3], [4], and the sporadic simple groups (see [21] and [37] for references). According to the classification of finite simple groups, which was completed in 1980, only the exceptional groups of Lie type remain to be considered, that is, the ten families G_2, F_4, E_6, E_7, E_8, ${}^2B_2$, ${}^2G_2$, ${}^3D_4$, ${}^2F_4$ and ${}^2E_6$. The only known results for these groups were obtained by Thompson. He showed that $G_2(p)$ occurs as a Galois group over the rationals for all primes p [44] (see also [19]). Here we prove:

Main Theorem. *The following exceptional simple groups of Lie type occur as Galois groups over $\mathbb{Q}^{ab}$:*

(1) *the Ree groups ${}^2G_2(q)$, $q=3^{2n+1}$,*

(2) *the groups $G_2(q)$ for all q,*

(3) *the Steinberg triality groups ${}^3D_4(q)$ for all q,*

(4) *the groups $F_4(q)$ in odd characteristic $p>2$,*

(5) *the groups $E_6(q)$ for $q=p^n\equiv -1 \pmod 3$ and $p\geqq 5$,*

*) The author was supported by the Deutsche Forschungsgemeinschaft.

(6) *the groups* ${}^2E_6(q)$ *for* $q = p^n \equiv 1 \pmod 3$ *and large enough* p *and* q,

(7) *the groups* $E_7(q)$ *in characteristic* $p \geqq 5$,

(8) *the groups* $E_8(q)$ *in characteristic* $p \geqq 7$.

Moreover, the groups $F_4(p)$ *for primes* $p \equiv 2, 6, 7, 11 \pmod{13}$, $p \geqq 19$, *and the groups* $E_8(p)$ *for primes* $p \equiv 3, 7, 9, 10, 11, 12, 13, 14, 17, 18, 19, 20, 21, 22, 24, 28 \pmod{31}$, $p > 127$, *occur as Galois groups over the rationals* $\mathbb{Q}$.

The proof will be given in §§ 2—10. There also Galois realizations for the three groups $Sz(8)$, ${}^2F_4(2)'$ and $F_4(2)$ are determined.

By the definition in [34] of GAR-realization, a Galois realization of a simple group with trivial outer automorphism group is a GAR-realization over the same field of definition. Thus the Main Theorem implies:

Corollary. *The following exceptional simple groups of Lie type possess* GAR-*realizations* (*in the terminology of* [34]) *over* $\mathbb{Q}^{ab}$:

(1) *the groups* $G_2(p)$ *for all primes* $p \geqq 5$,

(2) *the groups* $F_4(p)$ *for all primes* $p \geqq 3$,

(3) *the groups* $E_8(p)$ *for all primes* $p \geqq 7$.

Moreover, the groups $F_4(p)$ *for primes* $p \equiv 2, 6, 7, 11 \pmod{13}$, $p \geqq 19$, *and the groups* $E_8(p)$ *for primes* $p \equiv 3, 7, 9, 10, 11, 12, 13, 14, 17, 18, 19, 20, 21, 22, 24, 28 \pmod{31}$, $p > 127$, *possess* GAR-*realizations over the rationals* $\mathbb{Q}$.

The verification of the rationality criterion for the classical groups was accomplished by Belyi with the help of a lemma using the standard matrix representation of these groups. An application to the exceptional groups of Lie type fails, as they do not have elements of the form required in the lemma of Belyi. On the other hand, a calculation with generators and relations, as it can be carried through for the alternating groups A_n, is only feasable for untwisted groups of small rank, namely for the family G_2. For these groups, the method was successfully applied in [44] and [31]. For "larger" groups the necessary calculations become too long and complicated.

As a third possibility of verifying the criterion, the class number of $\mathfrak{C}$ may be obtained as a multiplication constant from the character table of G. This method was used to handle the sporadic simple groups. The generation of G by a triple of elements from $\mathfrak{C}$ remains to be proved independently, though.

For the families G_2, ${}^2G_2$ and ${}^3D_4$ the character table is known, making the first step trivial after a suitable choice of the class structure. For the other families, one of the classes C is chosen so that its elements generate t.i.-Hall subgroups of G. The irreducible characters of G not vanishing on this class are then described by Feit's theory of exceptional characters; the values on the other classes can often be deduced from the (deep) theory of unipotent characters of groups of Lie type by Deligne and Lusztig [13], [29], [30]. For most of the families we can choose a class structure such that its normalized structure constant $n(\mathfrak{C})$ is equal to one.

The proof of generation again uses the special form of the class C. Only "few" subgroups of G can contain t.i.-Hall subgroups. In fact, apart from local subgroups, only almost simple groups can arise as possible subgroups generated by a triple of elements from $\mathfrak{C}$. With the classification of finite simple groups, which enters at this point, and the knowledge of the minimal degrees of projective modular representations of the groups of Lie type [26], in our case only the simple groups defined in the same characteristic as G remain. This last case, and so the proof of generation, is now completed with the help of divisibility criteria for the group orders. In some instances, more precise reasoning is necessary (for example for the inclusions ${}^2A_2(q^2)$, ${}^3D_4(q) < F_4(q)$ in Paragraph 5).

For groups $F_4(p)$ and $E_8(p)$ and for certain congruences of the prime p, a choice of a rational class structure is possible. This leads to Galois realizations of those groups over the rationals $\mathbb{Q}$.

The families of exceptional groups of Lie type will be treated case by case from Paragraph 2 on. The necessary lemmas are collected in the first paragraph.

I would like to thank Professor B. H. Matzat for the supervision of my thesis [31], which this work is part of. Further I thank Professor J. G. Thompson for helpful comments and for making possible a one year stay at the Department of Pure Mathematics in Cambridge, England. I had helpful and interesting conversations about the groups of Lie type with Professor R. W. Carter, Dr. J. Saxl and Dr. P. Kleidman. The computer calculations were done on the IBM 3081 of the Computing Service of the University of Cambridge.

§ 1. Auxiliary results

In each of the following paragraphs a family of finite simple exceptional groups of Lie type will be investigated for possible Galois realizations over abelian number fields. In spite of the individual properties of the families, a reasonably unified approach is possible, requiring a standard set of auxiliary lemmas. These are collected in the present paragraph for better reference.

1.1. The rationality criterion. The starting point for all the calculations in this work is the rationality criterion already mentioned in the introduction. It gives a sufficient group theoretic condition for a finite (simple) group G to occur as a Galois group over an abelian number field, the latter depending on the group G. The efforts of the other paragraphs aim at showing that the criterion is satisfied for some of the exceptional groups of Lie type.

Central in constructive Galois theory is the notion of a *class structure* $\mathfrak{C} = (C_1, C_2, C_3)$, i.e. of a triple of conjugacy classes C_j of the finite group G. The corresponding *ramification structure* is defined by $\mathfrak{C}^* = \bigcup_{(\nu, |G|) = 1} (C_1^\nu, C_2^\nu, C_3^\nu)$. Further let $\bar{\Sigma}(\mathfrak{C}) = \{(\underline{\sigma}) \in \mathfrak{C} \mid \sigma_1 \sigma_2 \sigma_3 = \imath\}$. The set $\Sigma(\mathfrak{C}) = \{(\underline{\sigma}) \in \bar{\Sigma}(\mathfrak{C}) \mid \langle \sigma_1, \sigma_2, \sigma_3 \rangle = G\}$ contains the generating systems of G in $\mathfrak{C}$. The number of such generating systems modulo conjugation in G, that is, the number $|\Sigma(\mathfrak{C})|/|\mathrm{Inn}(G)|$, will be denoted by $l^i(\mathfrak{C})$. Finally, to formulate the criterion, we need the irreducible (complex) characters χ_i, $i = 1, \ldots, h$ of G.

Rationality Criterion (Belyi, Matzat, Thompson). *Let G be a finite group with trivial center and $\mathfrak{C} = (C_1, C_2, C_3)$ a class structure of G with $l^i(\mathfrak{C}) = 1$. Then G occurs as a Galois group over $K = \mathbb{Q}(\bigcup_{i=1}^{h} \chi_i(C_j))$.*

Different generalizations of this theorem are proved in [3], [33] and [43]. As the character values of finite groups are sums of roots of unity, the field K is always an abelian number field. In particular if all three classes C_j are rational, that is to say, if all characters take rational values on each C_j, or still equivalently, if elements of C_j are conjugate to all of their primitive powers, then G is a Galois group over the rational numbers $\mathbb{Q}$.

In general, it is highly nontrivial to calculate $l^i(\mathfrak{C})$ for an arbitrary class structure $\mathfrak{C}$ of some finite group. But an estimate giving an upper limit for $l^i(\mathfrak{C})$ can be obtained from the character table of G. By fundamental character theory, the multiplication constant of $\mathfrak{C}$, that is, the number $|\{(\sigma_1, \sigma_2) \in (C_1, C_2) \mid \sigma_1 \sigma_2 = \sigma_3^{-1}\}|$ for a fixed $\sigma_3 \in C_3$ is equal to

$$m(\mathfrak{C}) = \frac{|G|}{|\mathscr{C}_G(\sigma_1)| \cdot |\mathscr{C}_G(\sigma_2)|} \cdot \sum_{i=1}^{h} \frac{\chi_i(\sigma_1)\,\chi_i(\sigma_2)\,\chi_i(\sigma_3)}{\chi_i(\iota)}.$$

But $\Sigma(\mathfrak{C})$ only contains the triples generating all of G, so $|\Sigma(\mathfrak{C})| \leqq |C_3| \cdot m(\mathfrak{C})$ and consequently $l^i(\mathfrak{C}) \leqq m(\mathfrak{C})/|\mathscr{C}_G(\sigma_3)| =: n(\mathfrak{C})$. With this, the rationality criterion can be reformulated in the form which will be useful to us later on:

Lemma 1. 1. *Let $\mathfrak{C}$ be a class structure of the group G with trivial center. If we have*

$$n(\mathfrak{C}) = \frac{|G|}{|\mathscr{C}_G(\sigma_1)| \cdot |\mathscr{C}_G(\sigma_2)| \cdot |\mathscr{C}_G(\sigma_3)|} \cdot \sum_{i=1}^{h} \frac{\chi_i(\sigma_1)\,\chi_i(\sigma_2)\,\chi_i(\sigma_3)}{\chi_i(\iota)} = 1, \qquad \sigma_j \in C_j,$$

and no triple $(\underline{\sigma}) \in \bar{\Sigma}(\mathfrak{C})$ can generate a proper subgroup of G, then G occurs as a Galois group for the ramification structure $\mathfrak{C}^*$ over $\mathbb{Q}(\bigcup_{i=1}^{h} \chi_i(\sigma_j))$.

Proof (see also [32] or [43]). By the above considerations we already have $l^i(\mathfrak{C}) \leqq n(\mathfrak{C}) = 1$. Because $n(\mathfrak{C}) \neq 0$ there are triples $(\underline{\sigma})$ in $\mathfrak{C}$ which generate all of G. This shows $l^i(\mathfrak{C}) \geqq 1$ and the lemma now follows from the rationality criterion. ∎

1. 2. Groups with cyclic t.i.-Hall subgroups. To be able to calculate the normalized structure constant introduced in the previous section for a class structure of one of the groups of Lie type, it will be important to find a class C of G such that only "few" characters do not vanish on that class. All exceptional groups of Lie type contain large cyclic t.i.-Hall subgroups (trivial intersection), and it turns out that classes of elements from these subgroups have the desired property. Namely the characters not vanishing on such elements are rather easily described by results of Feit. But moreover only few maximal subgroups of G can contain these large cyclic t.i.-groups, so that the question of generation is considerably simplified. In what follows, the two assertions are made precise.

Let $T \leqq G$ be a cyclic Hall subgroup of the group G with the additional property

$$(*) \qquad \mathscr{C}_G(T) = \mathscr{C}_G(t) \quad \text{for all} \quad t \in T^{\#}.$$

This last property is not so hard to verify in the cases of interest to us because T will always be contained in a *maximal torus*, so all its elements will be *semisimple* (see Section 1.4). For these, the centralizer orders in G are known, which will make possible the proof of $(*)$.

Under the assumptions made, T has already the t.i.-property. Namely, for $x \in G$ with $T \cap T^x = R > \{\imath\}$ we have $T^x \leqq \mathscr{C}_G(R) = \mathscr{C}_G(T)$, and $\langle T, T^x \rangle$ is an abelian π-Hall subgroup for the same π as T, so necessarily must be equal to T, which proves $T = T^x$ as required.

The t.i.-property greatly restricts the possible types of subgroups of G containing T:

Lemma 1.2. *Let T be a cyclic Hall subgroup of G with $(*)$. Then any subgroup $H < G$ with $T \leqq H$ has one of the following structures*:

(1) $H \leqq \mathscr{N}_G(T)$, *or*

(2) $H \leqq \mathscr{N}_G(Z_r^\nu)$, $(r, |T|) = 1$ *and there exists* $\mu \leqq \nu$ *with* $|T| \mid (r^\mu - 1)$ *and* $Z_r^{\nu-\mu} \leqq \mathscr{C}_G(T)$, *or*

(3) $R \leqq H \leqq \mathscr{N}_G(R)$, *$R$ a nonabelian simple subgroup of G, or*

(4) *there exists a nonabelian simple* $R \leqq \mathscr{C}_G(T)$, *or*

(5) *there exist two primes* $p \mid |G|$ *with* $p\text{-rank}(G) \geqq |T|$, *or*

(6) *there is a nonabelian simple* $R \leqq G$ *with* $|T| \mid |\mathrm{Out}(R)|$.

Proof. A minimal normal subgroup M of H must form a direct product $R_1 \times \cdots \times R_s$ of isomorphic simple groups $R_i \cong R$. If $M \cap T \neq \{\imath\}$ then we must have $s = 1$ because $T \leqq H$ is a cyclic Hall subgroup. In the case of abelian $R = M = Z_r$, the prime r divides the order of T, and consequently $M \leqq T$. For $x \in \mathscr{N}_G(M)$ we have $T \cap T^x \geqq M > \{\imath\}$, and because of the t.i.-property proved above, we get $x \in \mathscr{N}_G(T)$. This forces $H \leqq \mathscr{N}_G(M) \leqq \mathscr{N}_G(T)$, leading to (1).

In the case of $M = R$ nonabelian, we arrive directly at (3).

So we can now assume $M \cap T = \{\imath\}$. First consider the case of elementary abelian M. Under the operation of T, this splits into $M = \mathscr{C}_M(T) \times S$, with T acting fixed point freely on S. This follows from the property $(*)$, because if $x \notin \mathscr{C}_M(T)$ then we already have $\mathscr{C}_G(x) \cap T = \{\imath\}$. The fixed point free operation on S forces $|T| \mid (|S| - 1)$, and this gives (2).

Finally let $M = R_1 \times \cdots \times R_s$, $R_i \cong R$ nonabelian simple and $T \cap M = \{\imath\}$. In the semidirect product $N := M \rtimes T$, the cyclic group T now acts on the set $\{R_1, \ldots, R_s\}$. Denote by S the normalizer $\mathscr{N}_N(R_1) = \mathrm{Fix}_N(R_1)$ of R_1 in N. If $S \cap T = \{\imath\}$, then T acts faithfully as a $|T|$-cycle on $\{R_1^t \mid t \in T\}$, and we have $s \geqq |T|$. Nonabelian simple groups are not p-groups, so at least two different primes divide the order of R, and case (5) results. If on the other hand $S \cap T > \{\imath\}$, then by Thompson's nilpotency criterion [42] there must exist a $t \in S \cap T^\#$ with $C := \mathscr{C}_S(t) \cap R_1 > \{\imath\}$. With $(*)$ we conclude $T \leqq \mathscr{C}_N(C)$ and so $T \leqq S$. The fourth case occurs for $C = R_1$, while otherwise $T \cap \mathscr{C}_G(R_1) = \{\imath\}$, yielding (6). ■

It is indeed easy to give examples for all six cases of the lemma. In particular, the assumptions are satisfied for any group G having a Sylow subgroup T of prime order. So without further conditions, no stronger result can be expected. But in most of the applications, $\mathscr{C}_G(T)$ is a cyclic t.i.-Hall subgroup itself, restricting the structure of H still further:

Lemma 1. 3. *Let T be abelian, $\mathscr{C}_G(T)$ a cyclic Hall subgroup of G with* $(*)$. *Then a subgroup H of G containing T has the structure*

(1) $H \leqq \mathscr{N}_G(T)$, *or*

(2) $H \leqq \mathscr{N}_G(Z_r^\nu)$ *with* $|T| \mid (r^\nu - 1)$, *i.e. T acts fixed point freely on Z_r^ν, or*

(3) $R \leqq H \leqq \mathrm{Aut}(R)$, *$R$ a nonabelian simple subgroup of G.*

Proof. Observe that T is not supposed to be a Hall subgroup itself. So Lemma 1. 2 can not be applied immediately. But the arguments are quite similar to the preceding proof. Let $M = R_1 \times \cdots \times R_s$ be a minimal normal subgroup of H. If M is abelian, then either $\mathscr{C}_G(T) \cap M > \{1\}$, which means $|R| = r \mid |\mathscr{C}_G(T)|$, whence $s = 1$ ($\mathscr{C}_G(T)$ is a cyclic Hall subgroup). This is case (1) of Lemma 1. 2 (for $\mathscr{C}_G(T)$), yielding (1).

On the other hand if $\mathscr{C}_G(T) \cap M = \{1\}$, T acts fixed point freely on M, as in (2) of the lemma.

Now suppose R is nonabelian simple. If $\mathscr{C}_G(T) \cap M > \{1\}$, then again $s = 1$ (i.e. $M = R$), and $T \leqq \mathscr{N}_G(R)$. But $\mathscr{C}_G(R)$ centralizes the intersection of R and $\mathscr{C}_G(T)$. Because of $(*)$ for $\mathscr{C}_G(T)$ this forces $\mathscr{C}_G(R) \leqq \mathscr{C}_G(T)$. But no nonidentity element of $\mathscr{C}_G(T)$ can centralize R, again due to $(*)$. Thus $\mathscr{C}_G(R) = \{1\}$, and $\mathscr{N}_G(R) \leqq \mathrm{Aut}(R)$ as in (3).

If finally $\mathscr{C}_G(T) \cap M = \{1\}$, then T would act fixed point freely on M, which is impossible. ■

Corresponding to the simple structure of overgroups of T in G is a simple behaviour of the irreducible characters of G on T. Feit proved in 1960 that apart from a family of so called exceptional characters Λ_j all other irreducible characters are constant on $T^\#$. Moreover, Dade showed that the non exceptional characters take only values $-1, 0$ or 1 on $T^\#$, a result which we will not need here, because it will follow from other facts. The exact formulation of Feit's result is

Lemma 1. 4 (Feit). *Let T be an abelian* t.i.*-subgroup of G, with the normalizer $N := \mathscr{N}_G(T)$ a Frobenius group with kernel T. Further, assume $s := (|T| - 1)/(N : T) \geqq 2$. Then there exist s distinct irreducible characters $\Lambda_1, \ldots, \Lambda_s$ of G, a sign δ and an integer a such that*

(1) *the generalized character*

$$\delta \Lambda_i + a \cdot \sum_{j=1}^{s} \Lambda_j + \sum_{\chi \neq \Lambda_j} \chi(T^\#) \chi$$

vanishes outside $\bigcup_{g \in G} (T^\#)^g$ *for all* $i = 1, \ldots, s$.

(2) *$\Lambda_1, \ldots, \Lambda_s$ are all irreducible characters of G not constant on $T^\#$.*

(3) $(\delta + a)^2 + (s-1) \cdot a^2 + \sum_{\chi \neq \Lambda_j} |\chi(T^\#)|^2 = (N : T) + 1.$

See [22], XI, Theorem 4. 6, for a proof.

1. 3. Divisibility criteria. To realize a group G as Galois group with Lemma 1. 1, the subgroup generated by a triple $(\underline{\sigma}) \in \bar{\Sigma}(\mathfrak{C})$ must be shown to be equal to G. Apart from Lemma 1. 2, which gives restrictions on the possible structure of the generated group, information is needed as to which simple groups can be contained in G. Many inclusions can be ruled out with the theorem of Lagrange, that is to say with divisibility criteria for group orders. Now the orders of the finite groups of Lie type in characteristic p are products of factors of the form $p^{\mu} \pm 1$ with a power p^{λ} (except for the case ${}^3D_4$, which can be treated similarly). Factors of that type tend to have "large" prime divisors. The main result regarding this was shown already in 1892 by Zsigmondy [46]: For all positive integers $\nu \geqq 3$ and all primes p there exists a *primitive* prime divisor r of $p^{\nu}-1$, dividing none of the $p^{\mu}-1$, $\mu<\nu$, except for the case $\nu=6$, $p=2$. If we denote by $\Phi_n(X)$ the n-th cyclotomic polynomial, we can conclude:

Lemma 1. 5. *If $\Phi_n(p^{\nu})$ with $n\nu \geqq 3$ divides the product $\prod_{i=1}^{s} (p^{\mu_i}-1)$, then there exists an index i with $n\nu | \mu_i$ or we have $p=2$, $n\nu=6$.*

Proof. Let r be the primitive divisor of $p^{n\nu}-1$ according to the result of Zsigmondy. Because of $(p^{n\nu}-1) \mid \Phi_n(p^{\nu}) \cdot \prod_{\mu=1}^{n\nu-1} (p^{\mu}-1)$, r must divide already $\Phi_n(p^{\nu})$. By Zsigmondy there exists an i with $n\nu \leqq \mu_i$. But $\gcd(p^{n\nu}-1, p^{\mu}-1) = p^{\gcd(n\nu,\mu)}-1$, so r can only divide $p^{\mu}-1$ if μ is a multiple of $n\nu$. The exception mentioned can occur only for $p=2$, $n\nu=6$. ■

Another criterion to identify the group generated by three elements $\sigma_1, \sigma_2, \sigma_3$ with $\sigma_1\sigma_2\sigma_3 = \iota$ makes use of the orders $o(\sigma_i)$ of the three elements:

Lemma 1. 6. *Let $H := \langle \sigma_1, \sigma_2 \rangle$ with $\sigma_1\sigma_2\sigma_3 = \iota$ and $\gcd(o(\sigma_i), o(\sigma_j)) = 1$ for $i \neq j$. Then H is a perfect group, that is, $H = H'$.*

A proof for this well known result can be found in [43].

1. 4. Local subgroups of simple groups of Lie type. Apart from almost simple groups, local subgroups are mentioned as possible overgroups of t.i.-Hall subgroups in Lemma 1. 3. It therefore seems necessary to shed some light on the structure of local subgroups and Sylow subgroups of simple groups of Lie type. In particular those elementary abelian subgroups admitting a fixed point free operation by a "large" cyclic group (see Lemma 1. 3(2)) must be studied. The main reference for the results cited in this section is the article of Springer and Steinberg in [6], part E.

Let G be a connected reductive algebraic group over the algebraic closure of the finite field $\mathbb{F}_q$ with a Frobenius map $F: G \to G$. The fixed points in G under F then form a finite group G^F, and all finite simple groups of Lie type occur as the nonabelian composition factors of such G^F.

Elements of p-power order in G^F are called *unipotent*, while p-regular elements are called *semisimple*. A maximal abelian subgroup T of G containing only semisimple elements is called a *maximal torus*. The maximal tori T of G fixed by F can be classified ([6], part G). Namely these classes of maximal tori are in bijective correspondence with the F-conjugacy classes of the Weyl group W of G; for trivial action of F on W, that is, for untwisted G^F, these are just the usual conjugacy classes of W. Similarly the maximal tori T^F of G^F are the groups of fixed points under F of the F-stable tori T of G. If T_w^F belongs to the F-class $[w]$, then $\mathcal{N}_G(T_w)^F/T_w^F \cong \mathcal{C}_W(w)$ ([8], Propositions 3.3.3—3.3.6).

For the different types of groups, sets of *torsion primes* can be defined; these are for the type G_2: 2, for the types F_4, E_6, E_7: 2 and 3, and for the type E_8: 2, 3 and 5. With these, the following statements about the structure of local subgroups of the groups G^F hold true:

Lemma 1.7. (1) *The normalizer of a unipotent subgroup $U \leqq G^F$ is contained in a maximal parabolic subgroup of G^F.*

(2) *A direct product $E := Y_1 \times \cdots \times Y_m$ of cyclic semisimple subgroups Y_i of G^F can be embedded into a maximal torus T^F of G^F, if the number of $|Y_i|$ not prime to all torsion primes of G is at most two. In particular, we then have $\mathcal{N}_G(E)/\mathcal{C}_G(E) \leqq W(G)$.*

(3) *A Sylow r-subgroup for r prime to the characteristic and the order of the Weyl group can be embedded into a maximal torus T^F of G^F; in particular, it is abelian.*

Proof. Part (1) is the well known theorem of Borel and Tits [7], Prop. 3.12. Theorem 5.8(c) in [6], E2, shows the first half of part (2). The second assertion follows from the uniqueness of the Bruhat decomposition of elements of G, as is shown in the proof of Proposition 3.7.1 in [8] for example. Part (3) finally is Corollary 5.19(b) in [6], E2. ■

The parabolic subgroups of the finite groups of Lie type are explicitly known, their orders can be calculated easily ([8], p. 43 and p. 63).

1.5. Characters of simple groups of Lie type. Even when using Feits theory of exceptional characters, not all character values necessary for the calculation of a structure constant can be determined. Additional information about the values of the unipotent characters of the groups of Lie type on semisimple or unipotent classes are needed. The theory of unipotent characters was established by Deligne and Lusztig in [13], [28], [29], [30] and gives explicit algorithms to calculate the values of any irreducible character at any semisimple class of exceptional groups of Lie type. Moreover in good characteristic, the values of unipotent characters on some unipotent classes can be effectively computed, with the help of tables of the values of Green functions compiled by Shoji [39] and Beynon and Spaltenstein [5]. The main reference for the first part of the theory is the excellent book of Carter [8]. Some of the newer results are not contained in it; they can be found in the original papers or the book [29] of Lusztig.

The main tool in the character theory of the groups G^F are the characters $R_{T,\theta}$ which were constructed in the fundamental paper [13] of Deligne and Lusztig. For every maximal torus T fixed under F and every irreducible (i.e. linear) character θ of T^F a generalized character $R_{T,\theta}$ of G^F can be defined. On these characters, the equivalence relation of *geometric conjugacy* is introduced, with the property that two characters $R_{T,\theta}$, $R_{T',\theta'}$ have an irreducible component in common only if (T, θ) and (T', θ') are geometric conjugate ([8], Theorem 7.3.8). The irreducible constituents of $R_{T,1}$ (with 1 the trivial character of the torus T^F) are called *unipotent characters.* In Lusztig's classification of the irreducible characters of the groups G^F they play a role similar to the one of the unipotent classes in the classification of all conjugacy classes of G^F (Jordan decomposition). The generalized characters $R_{T,\theta}$, restricted on a maximal unipotent subgroup U^F of G^F (i.e. a p-Sylow subgroup), are the *Green functions* of G^F. The decomposition of the $R_{T,1}$ into their unipotent components was determined by Lusztig [28].

The main result about the values of the characters of G^F at semisimple classes was proved in 1976 in [13], Corollary 7. 6. It makes use of the representability of the characteristic function of a semisimple class $[s]$ as a linear combination of $R_{T,\theta}$'s with known coefficients. From this, the values of arbitrary characters on $s \in G^F$ can be determined. For a finite group H, let $\hat{H}$ denote the character group. For a subgroup D of G, the connected component of the identity is D^o. Further let ε_T be the sign defined in [8], p. 197, for a maximal torus T of G. Then $\varepsilon_s := \varepsilon_{\mathscr{C}_G^o(s)}$ is defined to be ε_T for a maximally split torus T of $\mathscr{C}_G^o(s)$ ([8], p. 199). Following [28] the formulae take a simpler form if we replace the $R_{T,1}$ by generalized characters R_χ indexed by the irreducible characters χ of the Weyl group W of G:

$$R_\chi := |W|^{-1} \sum_{w \in W} \chi(w) \cdot R_{T_w,1}.$$

Lemma 1. 8 (Deligne, Lusztig). *The value of the unipotent character ϱ of the group G^F on the semisimple element $s \in G^F$ is given by*

$$\varrho(s) = \varepsilon_s \cdot |\mathscr{C}_G^o(s)^F|_p^{-1} \cdot \sum_{\chi \in \hat{W}} (\varrho, R_\chi) \cdot \sum_{T_w : s \in T_w} \varepsilon_{T_w} \chi(w).$$

Here χ runs over all irreducible characters of W and T over all tori T_w^F of G^F containing s.

The multiplicities (ϱ, R_χ) are described in [28], Theorem 1. 5, and tables of these numbers can be found in [8], 13. 6.

To effectively calculate $\sum\limits_T \varepsilon_{T_w} \chi(w)$, which runs over all tori T^F of G^F containing s, the fact is used that all these T^F lie in $\mathscr{C}_G^o(s)^F$ ([8], Prop. 3. 5. 2). By [8], Theorem 3. 5. 4, $\mathscr{C}_G^o(s)$ is a reductive algebraic group itself. So the maximal tori $T^F \ni s$ of G^F are exactly the maximal tori T^F of $\mathscr{C}_G^o(s)^F$. The structure of $\mathscr{C}_G^o(s)^F$ is known for all semisimple $s \in G^F$ of exceptional simple groups G^F of Lie type [35], [14], [15]. The maximal tori of untwisted reductive groups were given by Carter in [6], part G. Let $C := \mathscr{C}_G^o(s)^F$, then the C-class $[T_w^F]$ contains exactly $|C|/|\mathscr{N}_C(T_w^F)|$ different maximal tori conjugate to T^F. If we denote the Weyl group of C by W_0, then we therefore have

$$|\mathscr{N}_C(T_w^F)| = |T^F| \cdot (\mathscr{N}_C(T^F) : T^F) = |T^F| \cdot |\mathscr{C}_{W_0}(w)|$$

and the formula of Lemma 1. 8 becomes

$$\varrho(s) = \varepsilon_s \cdot |\mathscr{C}_G^o(s)^F|_{p'} \cdot \sum_{\chi \in \hat{W}} (\varrho, R_\chi) \cdot \sum_{[w] \subseteqq W_0} \varepsilon_{T_w} \frac{\chi(w)}{|T^F| \cdot |\mathscr{C}_{W_0}(w)|}.$$

Now only the fusion of W_0 into W has to be known to effectively compute the sum in Lemma 1. 8 for all unipotent characters ϱ of G^F.

The theory of the values of irreducible characters on unipotent classes is not yet complete. In principal, one has to know the values of the Green functions on the unipotent classes and the decomposition of the $R_{T,\theta}$ into irreducible characters of G^F. In addition, some so called *uniform functions* on the unipotent classes have to be found. At the moment the Green functions of exceptional groups of Lie type are known only for good primes p ([30], [23], [39], [5]). With these the values of unipotent characters on some unipotent classes $[u]$ of G^F can be calculated. The main result here is Theorem 1. 5 in [28] (see also Corollary 4. 25 in [29]).

§ 2. The groups ${}^2G_2(q)$ as Galois groups over $\mathbb{Q}^{ab}$

The simple Ree groups ${}^2G_2(3^{2n+1})$ are an easy test case for the criteria presented in the first paragraph. A large part of their character table was determined by Ward [45], as well as the local subgroups of these groups. Recently, Kleidman obtained a complete list of maximal subgroups [25]. Using this, the proof of rigidity is rather easy. It should however be noted that even without the knowledge of the maximal subgroups the desired result can be shown [31].

To define a class structure of $G := {}^2G_2(3^{2n+1})$ let C_2 be the unique class of involutions, C_3 the class of 3-elements which are central in a Sylow 3-subgroup (this class is denoted by $[X]$ in [45]), and let $C_{q\pm r+1}$ be classes of elements of orders $q \pm r + 1$, with $r := 3^{n+1}$.

Theorem 2. 1. *The groups ${}^2G_2(q)$, $q = 3^{2n+1}$, $n \geqq 1$, occur as Galois groups over $\mathbb{Q}^{ab}$ for the ramification structures $\mathfrak{C}_1^* = (C_2, C_3, C_{q+r+1})^*$ and $\mathfrak{C}_2^* = (C_2, C_3, C_{q-r+1})^*$. A proper field of definition $K^{\pm}(q)$ has index six in the field $\mathbb{Q}(\zeta_{q\pm r+1})$ of $(q \pm r + 1)$-th roots of unity.*

Proof. From the character table in [45], the normalized structure constants are calculated by Lemma 1. 1 as

$$n(\mathfrak{C}_1) = \frac{(q^3+1)\,q^3(q-1)}{q(q^2-1)\,q^3(q+r+1)} \cdot \left(1 + 2\frac{(q-1)(3q-r)2}{4(q-1)\,r(q-r+1)}\right) = 1$$

and

$$n(\mathfrak{C}_2) = \frac{(q^3+1)\,q^3(q-1)}{q(q^2-1)\,q^3(q-r+1)} \cdot \left(1 - 2\frac{(q-1)(3q+r)2}{4(q-1)\,r(q+r+1)}\right) = 1.$$

Now by the criterion in Lemma 1. 1 we have to show that any triple in $\bar{\Sigma}(\mathfrak{C}_j)$ generates G. Then the assertion about the exact field of definition can be read off from the character table in [45] (i.e. from the fact that C_2 and C_3 are rational classes, while elements in $C_{q\pm r+1}$ are conjugate to six of their primitive powers). So let $H := \langle \sigma_1, \sigma_2 \rangle$ for $(\underline{\sigma}) \in \bar{\Sigma}(\mathfrak{C}_j)$. By comparing with the list of maximal subgroups in [25] we find that either H is contained in the normalizer of the cyclic group generated by σ_3 or we have $H=G$. But the orders of σ_1, σ_2 and σ_3 are pairwise prime, so H is nonsolvable by Lemma 1.6. This excludes the first possibility and therefore $H=G$. ■

By a suitable change of the non rational class, a smaller field of definition may be obtained in some cases:

Proposition 2.1. *Let s be a primitive prime divisor of q^2-q+1 in the notation of Lemma 1.5. Then ${}^2G_2(q)$ is a Galois group for the ramification structure $\mathfrak{C}^*=(C_2, C_3, C_s)^*$ over a field of index six in $\mathbb{Q}(\zeta_s)$.*

Proof. Because of $q^2-q+1=(q+r+1)\cdot(q-r+1)$ exactly one of the two factors is divisible by s. The character table in [45] shows $n(\mathfrak{C}^*)=1$ in this case as well. The group generated by a triple $(\underline{\sigma})\in\bar{\Sigma}(\mathfrak{C})$ is nonsolvable, and due to the choice of s, only $H=G$ remains from the list in [25]. The proposition now follows by Lemma 1.1 and the remark above about the structure of the normalizer of an element of order s. ■

The group $\Gamma L_2(8)={}^2G_2(3)$ was already shown in [33] to occur as Galois group over $\mathbb{Q}$, so all groups ${}^2G_2(q)$ are Galois groups over cyclotomic fields.

§ 3. The groups $G_2(q)$ as Galois groups over $\mathbb{Q}^{ab}$

Being the smallest untwisted exceptional groups of Lie type, the groups $G_2(q)$ are well suited for an application of the criteria for Galois realization mentioned in the introduction. Due to the transparent structure of these groups, much is known about them. The conjugacy classes were determined by Chang [9] and Enomoto [17], and in odd characteristic, the character table is known by work of Chang and Ree [10] and Enomoto [18]. In even characteristic, the Deligne-Lusztig theory will be invoked to get enough information about the irreducible characters. It is even possible to do explicit calculations with generators and relations to prove rigidity for a given class structure of G. This was first demonstrated by Thompson in [44] for the groups $G_2(p)$, $p\geqq 5$, which were shown to be rationally rigid. The results of Thompson were subsequently reproved by Feit and Fong with the help of character theory and the classification of the finite simple groups [19]. The author generalized Thompson's method to arbitrary prime powers $q=p^n$, $p\geqq 5$, in [31], to get these groups as Galois groups over $\mathbb{Q}^{ab}$.

3.1. The case p odd. The cases of odd p can be treated in a more or less uniform way, while in even characteristic a different approach will be needed because the character table of $G_2(2^n)$ is not known. So in this section, let $G:=G_2(p^n)$, $p\neq 2$. A complete list of maximal subgroups of $G_2(q)$ was recently obtained by Kleidman [25]. It will be used here to shorten the proof. But our results can be obtained independently of [25] (see [31]).

Now define class structures of G. First let $p\geqq 5$. Then the first class will contain semisimple elements of order three, namely $C_3:=[k_3]$ in the notation of [10]. Let the second class be $C_{2p}:=[k_{2,1}]$. The third class will contain elements generating a t.i.-Hall subgroup, namely $C^+:=[h_6]$, $C^-:=[h_3]$. (Two different cases have to be distinguished according to $q\equiv 1$ or $q\equiv -1 \pmod 3$.)

Theorem 3. 1. *The groups $G_2(q)$, $q=p^n\equiv\varepsilon\,(\mathrm{mod}\,3)$, $p\geqq 5$, occur as Galois groups over $\mathbb{Q}^{ab}$ for the ramification structure $\mathfrak{C}_\varepsilon^*=(C_3, C_{2p}, C^\varepsilon)^*$ (the corresponding classes containing elements of orders $(3, 2p, q^2-\varepsilon q+1)$). More precisely a proper field of definition $K_\varepsilon(q)$ has index six in the abelian field $\mathbb{Q}(\zeta_{q^2-\varepsilon q+1})$.*

Proof. The formula in Lemma 1. 1 for $n(\mathfrak{C})$ requires the knowledge of those irreducible complex characters of G not vanishing on all three classes of $\mathfrak{C}$. In characteristic $p\geqq 5$, these can be found in [10], p. 409—411:

	$\{\iota\}$	C_3	C_{2p}	C^+
χ_{11}	1	1	1	1
χ_{16}	$\frac{1}{6}q\Phi_2^2\Phi_3$	$\frac{1}{3}\Phi_2\Phi_3$	$\frac{1}{2}\Phi_2$	-1

for $q\equiv 1\,(\mathrm{mod}\,3)$,

	$\{\iota\}$	C_3	C_{2p}	C^-
χ_{11}	1	1	1	1
χ_{18}	$\frac{1}{6}q\Phi_1^2\Phi_6$	$\frac{1}{3}\Phi_1\Phi_6$	$\frac{1}{2}\Phi_1$	1

for $q\equiv -1\,(\mathrm{mod}\,3)$ respectively. With $|G|=q^6(q^2-1)(q^6-1)$, $|\mathscr{C}_G(\varrho)|=q^3(q^2-1)(q^3-\varepsilon)$, $|\mathscr{C}_G(\sigma)|=q^2(q^2-1)$, $|\mathscr{C}_G(\tau_\varepsilon)|=q^2-\varepsilon q+1$ for a triple $(\varrho,\sigma,\tau)\in\bar{\Sigma}(\mathfrak{C}_\varepsilon)$ one gets $n(\mathfrak{C}_\varepsilon)=1$ in both cases.

Now let $H:=\langle\varrho,\sigma\rangle$ for such a triple (ϱ,σ,τ). As the orders of the three generators are pairwise prime, H is nonsolvable and perfect by Lemma 1. 6. Checking the list of maximal subgroups in [25] with the help of the divisibility criterion of Lemma 1. 5, one is left with the possibility $H=L_3(q)$ or $U_3(q)$. In a first case let $o(\tau)=q^2-q+1$, that is, $q\equiv 1\,(\mathrm{mod}\,3)$. Then the order of τ does not divide the order of $L_3(q)$. If $H\neq G$ then by the above $H=U_3(q)$. This group has unique classes of elements or order three, and of unipotent elements with even centralizer order. These would have to fuse to the classes C_3 and $C_p:=(C_{2p})^2$ of G. But the structure constant $n(C_3, C_p, [\tau])_U=1$ by [40], while $n(C_3, C_{2p}^2, [\tau])_{G_2}=0$ from [10]. This proves $H=G_2(q)$ if $q\equiv 1\,(\mathrm{mod}\,3)$. The case $o(\tau)=q^2+q+1$, leading to the possibility $H=L_3(q)$, is treated exactly the same way. The theorem now follows with Lemma 1. 1. ■

In characteristic three, a slightly different class structure will be considered. Namely there are no semisimple elements of order three in this case. So the first class $C_3:=A_2$ in the notation of [18] will contain the unipotent elements central in a Sylow 3-subgroup. Let the second class be $C_6:=B_3$ (still in the notation of [18]). As the third class we can take either $C^+:=E_5$ or $C^-:=E_6$.

Theorem 3. 2. *The groups $G_2(q)$, $q=3^n$, $n \geqq 2$, occur as Galois groups over $\mathbb{Q}^{ab}$ for the two ramification structures $\mathfrak{C}_\varepsilon^* = (C_3, C_6, C^\varepsilon)^*$, $\varepsilon = \pm 1$, the corresponding classes containing elements of orders $(3, 6, q^2 - \varepsilon q + 1)$. More precisely a proper field of definition $K_\varepsilon(q)$ has index six in the abelian field $\mathbb{Q}(\zeta_{q^2-\varepsilon q+1})$.*

Proof. The characters not vanishing on all three classes are read of from [18], p. 240—247:

	$\{\iota\}$	C_3	C_6	C^+	C^-
θ_0	1	1	1	1	1
θ_1	$\frac{1}{6} q \Phi_2^2 \Phi_3$	$\frac{1}{6} q \Phi_2 (2q+1)$	$\frac{1}{2} \Phi_2$	-1	$\cdot$
θ_2	$\frac{1}{2} q \Phi_2^2 \Phi_6$	$\frac{1}{2} q \Phi_2$	$\frac{1}{2} \Phi_2$	$\cdot$	-1
θ_{10}	$\frac{1}{6} q \Phi_1^2 \Phi_6$	$\frac{1}{6} q \Phi_1 (2q-1)$	$\frac{1}{2} \Phi_1$	$\cdot$	1
θ_{11}	$\frac{1}{2} q \Phi_1^2 \Phi_3$	$-\frac{1}{2} q \Phi_1$	$\frac{1}{2} \Phi_1$	1	$\cdot$

As we have $|\mathscr{C}_G(\varrho)| = q^6(q^2-1)$, $|\mathscr{C}_G(\sigma)| = q^2(q^2-1)$, $|\mathscr{C}_G(\tau_\varepsilon)| = q^2 - \varepsilon q + 1$ for a triple $(\varrho, \sigma, \tau) \in \bar{\Sigma}(\mathfrak{C}_\varepsilon)$, $n(\mathfrak{C}_\varepsilon) = 1$ follows in both cases.

Again by the results of Kleidman [25], either H is contained in the normalizer of the cyclic group generated by τ, or it is one of $L_3(q)$, $U_3(q)$ or $G_2(q)$. But the solvable normalizer of $\langle \tau \rangle$ cannot possess two elements of orders three and six with their product being τ. This becomes obvious by looking at the cyclic group of order six obtained by factoring out $\langle \tau \rangle$. Now assume $\varepsilon = 1$. Then H is either $U_3(q)$ or G. The group $U_3(q)$ contains two classes of elements of order three, one of which has even centralizer order. This one has to fuse in $C_3' := C_6^2$ of G. In G, the classes C_3 and C_3' are different, so C_3 has to correspond to the other class of 3-elements of $U_3(q)$. But for this fusion we get $n(C_3, C_3, C^+)_U = q^2 + q - 1$ (see [40]), in contradiction to $n(C_3, C_3, C^+)_G = 0$. This leaves only $H = G$. The case $\varepsilon = -1$ with the possibility $H = L_3(q)$ is treated analogously. The theorem now follows from Lemma 1. 1. ■

The remaining group in odd characteristic, $G = G_2(3)$, behaves a bit exceptional and will be considered in the next section.

3. 2. Construction of exceptional characters. Contrary to the situation in odd characteristic, the character table of $G_2(2^n)$ is not published. So we will have to apply the previously described theory of exceptional characters to deduce a large enough portion of the character table of the groups $G := G_2(2^n)$. Using results of Deligne and Lusztig about character values at semisimple elements, a structure constant can be calculated. For the proof of generation, we can make use of the list of maximal subgroups of G given by Cooperstein [12]. (But obviously, the method applied in the cases where the maximal subgroups are not known would suffice to complete the proof.

The result of Cooperstein is just used to shorten the argument.) As before, a suitable t.i.-subgroup of G is generated by elements of order $q^2-\varepsilon q+1$, $q\equiv\varepsilon\,(\operatorname{mod} 3)$. The conjugacy classes of the class structure are then chosen to be C_3, containing elements ϱ of order three with $|\mathscr{C}_G(\varrho)|=q^3(q^2-1)(q^3-\varepsilon)$, $C_{q+\varepsilon}$, containing elements σ of order $q+\varepsilon$ with $|\mathscr{C}_G(\sigma)|=q(q+\varepsilon)(q^2-1)$ and finally C^ε a class of elements τ generating a cyclic Hall subgroup of order $q^2-\varepsilon q+1$ (see [17], Table 1).

Proposition 3. 1. *For* $\mathfrak{C}_\varepsilon=(C_3, C_{q+\varepsilon}, C^\varepsilon)$ *of* $G_2(q)$, $q=2^n\equiv\varepsilon\,(\operatorname{mod} 3)$, $n\geqq 2$, *we have* $n(\mathfrak{C}_\varepsilon)=1$.

Proof. First let $q\equiv\varepsilon\equiv 1\,(\operatorname{mod} 3)$. The cyclic subgroups T of order q^2-q+1 generated by elements from C^+ are Hall subgroups with the property (∗) of Section 1. 2, as can be seen from the list of centralizer orders in [17], Table 1. In particular, they form t.i.-sets with $(\mathscr{N}_G(T):T)=6$. So the theory of exceptional characters in Lemma 1. 4 applies: There are $s:=(q^2-q)/6$ irreducible characters Λ_i of G not constant on $T^\#$. Furthermore there exist $\delta\in\{\pm 1\}$, $a\in\mathbb{Z}$, such that

$$(\delta+a)^2+(s-1)a^2+\sum_{\chi\neq\Lambda_j}|\chi(T^\#)|^2=(\mathscr{N}_G(T):T)+1,$$

i.e.

$$(\delta+a)^2+\left(\frac{q^2-q}{6}-1\right)a^2+\sum_{\chi\neq\Lambda_j}|\chi(T^\#)|^2=7.$$

As $s=(q^2-q)/6\geqq 40$ for $q\geqq 16$, we conclude $a=0$ if $q\neq 4$. To identify the remaining characters not vanishing on $T^\#$, we introduce the unipotent characters of G (see Section 1. 5). The degrees of these irreducible characters are known by the work of Lusztig [29], p. 372 (or [8], p. 478). There are exactly six of them with degree not divisible by q^2-q+1, these degrees being 1, q^6, $\frac{q}{6}\Phi_2^2\Phi_3$, $\frac{q}{2}\Phi_1^2\Phi_3$ and two times $\frac{q}{3}\Phi_1^2\Phi_2^2$. From the definition of these characters it is clear that they are constant on $T^\#$, so they can not be exceptional characters for T. Consider an element $\tau'\in T^\#$ of prime order. This order then does not divide the degrees of the above six characters, which means that they must take nonzero values on τ'. By the formulas above about the character values, these are the only irreducibles apart from the exceptional characters not vanishing on τ'. The values of the six unipotent characters χ_i on $T^\#$ can now be obtained from $\chi_i(\tau)\equiv\chi_i(\iota)$ $(\operatorname{mod} q^2-q+1)$. Alternatively the formula of Deligne-Lusztig about the values of unipotent characters on semisimple elements could be invoked.

The already mentioned result of Deligne-Lusztig also permits to calculate the values of the unipotent characters on the semisimple classes C_3 and C_{q+1}. Evaluating the formula in Lemma 1. 4 for ι yields

$$-\delta\Lambda_i(\iota)=\sum_{j=1}^{6}\chi_j(T^\#)\,\chi_j(\iota)=\Phi_1^2\Phi_2^2\Phi_3,$$

so $\Lambda_i(\iota)=\Phi_1^2\Phi_2^2\Phi_3$. From vanishing theorems for characters of simple groups we get $\Lambda_i(C_{q+1})=\Lambda_i(C_3)=0$. This leads to the following part of the character table of G:

	$\{\iota\}$	C_3	C_{q+1}	$T^\#$
χ_1	1	1	1	1
χ_2	q^6	q^3	$-q$	1
χ_3	$\frac{1}{6}q\Phi_2^2\Phi_3$	$\frac{1}{3}\Phi_2\Phi_3$	$\cdot$	-1
χ_4	$\frac{1}{2}q\Phi_1^2\Phi_3$	$\cdot$	Φ_1	1
χ_5	$\frac{1}{3}q\Phi_1^2\Phi_2^2$	$-\frac{1}{3}\Phi_1^2\Phi_2$	$\cdot$	1
χ_6	$\frac{1}{3}q\Phi_1^2\Phi_2^2$	$-\frac{1}{3}\Phi_1^2\Phi_2$	$\cdot$	1
Λ_i	$\Phi_1^2\Phi_2^2\Phi_3$	$\cdot$	$\cdot$	??

Only the trivial and the Steinberg character take nonzero values on all three classes. Together with the centralizer orders given above this shows $n(\mathfrak{C}_+)=1$.

The considerations were not valid for $q=4$, but in that case the result is easily deduced from the Atlas character table [11], p. 98. If on the other hand we have $q\equiv\varepsilon\equiv-1 \pmod 3$, then the cyclic subgroups of order q^2+q+1 form t.i.-sets with the desired properties. In this case we arrive at unipotent characters χ_i of degrees $1, q^6, \frac{q}{6}\Phi_1^2\Phi_6, \frac{q}{2}\Phi_2^2\Phi_6$ and twice $\frac{q}{3}\Phi_1^2\Phi_2^2$. The relevant part of the character table then is:

	$\{\iota\}$	C_3	C_{q-1}	$T^\#$
χ_1	1	1	1	1
χ_2	q^6	$-q^3$	q	1
χ_3	$\frac{1}{6}q\Phi_1^2\Phi_6$	$\frac{1}{3}\Phi_1\Phi_6$	$\cdot$	1
χ_4	$\frac{1}{2}q\Phi_2^2\Phi_6$	$\cdot$	Φ_2	-1
χ_5	$\frac{1}{3}q\Phi_1^2\Phi_2^2$	$-\frac{1}{3}\Phi_1\Phi_2^2$	$\cdot$	-1
χ_6	$\frac{1}{3}q\Phi_1^2\Phi_2^2$	$-\frac{1}{3}\Phi_1\Phi_2^2$	$\cdot$	-1
Λ_i	$\Phi_1^2\Phi_2^2\Phi_6$	$\cdot$	$\cdot$	??

This proves $n(\mathfrak{C}_-)=1$. ■

Theorem 3. 3. *The groups $G_2(q)$, $q=2^n\equiv\varepsilon\pmod 3$, $n\geqq 2$, occur as Galois groups over $\mathbb{Q}^{ab}$ for the ramification structure $\mathfrak{C}_\varepsilon^*=(C_3, C_{q+\varepsilon}, C^\varepsilon)^*$ (the corresponding classes containing elements of orders $(3, q+\varepsilon, q^2-\varepsilon q+1)$). More precisely a proper field of definition $K_\varepsilon(q)$ is the compositum of the maximal real subfield of $\mathbb{Q}(\zeta_{q+\varepsilon})$ with a field of index six in $\mathbb{Q}(\zeta_{q^2-\varepsilon q+1})$.*

Proof. It remains to show that a triple $(\varrho, \sigma, \tau)\in\bar{\Sigma}(\mathfrak{C}_\varepsilon)$ generates $G:=G_2(2^n)$. So let $H=\langle\varrho, \sigma\rangle$ and assume first $2^n=q\equiv\varepsilon\equiv 1\pmod 3$. A short look at the list of maximal subgroups in [12] reveals that only groups $U_3(2^n)\cdot 2$, and in case $q=4$ an exceptional $L_2(13)$, have order divisible by q^2-q+1. The latter case can be excluded immediately because the order $q+1=5$ of σ does not divide the order of $L_2(13)$. If $\langle\varrho, \sigma\rangle\leqq U_3(q)\cdot 2$, then by Lemma 1. 6 we even have $H\leqq U_3(q)$. Therefore it suffices to show that no element of C_3 can be contained in such a $U_3(q)$. For this purpose, the normalized structure constant $n(C_3, C_3, C^\varepsilon)$ will be calculated in both groups. In $U_3(q)$ there exists just one class of elements of order three, and from [40] we find $n(C_3, C_3, C^\varepsilon)_U=q^2+q+1$. For G itself we get $n(C_3, C_3, C^\varepsilon)_G=0$ from the part of the character table constructed in the proof of Proposition 3. 1. For $q=4$ this can again be seen from the character table of $G_2(4)$ in [11], p. 98. Consequently the original (ϱ, σ, τ) can not be contained in $U_3(q)$ and the theorem follows in this case.

The same procedure applies if $2^n\equiv\varepsilon\equiv -1\pmod 3$, showing that $\langle\varrho, \sigma\rangle$ could only lie in an $L_3(q)$. But again the comparison of the structure constants of $(C_3, C_3, C^\varepsilon)$ in G and $L_3(q)$ excludes that possibility. ■

The proof of Theorem 3. 3 remains valid if the class $C_{q+\varepsilon}$ is replaced by any class $\tilde{C}$ of powers of elements of $C_{q+\varepsilon}$ which have the same centralizer order. As already for ${}^2G_2(q)$, the class C^ε could be replaced by any class of elements with order a primitive divisor of $q^2-\varepsilon q+1$, without changing the rigidity, to obtain a smaller field of definition for the Galois extensions.

Theorems 3. 1 to 3. 3 give Galois realizations over $\mathbb{Q}^{ab}$ for all groups of type G_2 with the exception of

$$G_2(2)\cong U_3(3)\cdot 2 \text{ and } G_2(3).$$

The last two groups are treated in the next theorem. The notation for the conjugacy classes is taken from the Atlas [11].

Theorem 3. 4. *The group $G_2(2)$ occurs as a Galois group over $\mathbb{Q}$ for the ramification structure $\mathfrak{C}^*=(2B, 4C, 12A)^*$.*

The group $G_2(3)$ occurs as a Galois group over $\mathbb{Q}(\sqrt{13})$ for the ramification structure $\mathfrak{C}^*=(3A, 6B, 13A)^*$.

Proof. The group $G_2(2)$ has a primitive permutation representation of degree 28. The conditions of the rationality criterion can therefore be verified directly by computer calculations with this representation.

In the case of $G_2(3)$ one first determines $n(3A, 6B, 13A)=1$ from the character table in [11], p. 60. Again by [11] the only maximal subgroups of G with order divisible by thirteen are $L_2(13)$ and two classes of $L_3(3)$. But $L_2(13)$ does not intersect the class $3A$ of G. Furthermore the permutation characters of the two $L_3(3)$'s vanish either on $3A$ or on $6B$. Therefore the triples in $\mathfrak{C}^*$ generate all of G, and by Lemma 1. 1 this completes the proof of the second part of the theorem. ■

§ 4. The groups ${}^3D_4(q)$ as Galois groups over $\mathbb{Q}^{ab}$

The character table [16], [41] and the maximal subgroups [24] of the Steinberg triality groups ${}^3D_4(q)$, $q=p^n$, are known. Using this information, the groups $G:={}^3D_4(q)$ can be realized as Galois groups over suitable abelian extension fields of $\mathbb{Q}$. Denote the conjugacy classes C of G by their representative elements σ given in [16] as $C=[\sigma]$.

Theorem 4. 1. *The groups ${}^3D_4(q)$, $q=p^n$, are Galois groups over $\mathbb{Q}^{ab}$ for the ramification structure $\mathfrak{C}^*=([u_1],[u_5],[s_{14}])^*$ (here the corresponding classes contain elements of orders $(p, p^?, q^4-q^2+1)$). A proper field of definition $K(q)$ is a field of index four in the abelian field $\mathbb{Q}(\zeta_{q^4-q^2+1})$.*

Proof. From [41] and [16] the only irreducible characters not vanishing on the class $[s_{14}]$ are the unipotent characters $1, \varrho_1, {}^3D_4[-1], St$ and the family χ_{14} of semisimple characters. The values on the three classes are:

	$\{\iota\}$	$[u_1]$	$[u_5]$	$[s_{14}]$
1	1	1	1	1
ϱ_1	$\frac{1}{2}q^3\Phi_2^2\Phi_6^2$	$\frac{1}{2}q^3\Phi_2\Phi_6$	$\cdot$	-1
${}^3D_4[-1]$	$\frac{1}{2}q^3\Phi_1^2\Phi_3^2$	$-\frac{1}{2}q^3\Phi_1\Phi_3$	$\cdot$	1
St	q^{12}	$\cdot$	$\cdot$	1
χ_{14}	$\Phi_1^2\Phi_2^2\Phi_3^2\Phi_6^2$	$-\Phi_1\Phi_2\Phi_3\Phi_6$	1	$\{-1\}$

Here $\{-1\}$ in the last line signifies that the values on s_{14} of the characters in the family χ_{14} add up to -1. This information is sufficient for the calculation of the structure constant. (The values of the χ_{14} on u_1 and u_5 are obtained from the orthogonality of the corresponding columns to the one for s_{14} or alternatively from [41].)

With the centralizer orders

$$|\mathscr{C}_G(u_1)|=q^{12}(q^6-1),\quad |\mathscr{C}_G(u_5)|=q^6,\quad |\mathscr{C}_G(s_{14})|=q^4-q^2+1$$

and $|G|=q^{12}(q^2-1)(q^6-1)(q^8+q^4+1)$ we now get $n(\mathfrak{C})=1$.

By [24] the only maximal subgroups of G containing elements τ of order dividing $q^4-q^2+1=\Phi_{12}(q)$ are the normalizers $\mathscr{N}_G(\langle\tau\rangle)$ of the cyclic groups generated by them of order $\Phi_{12}(q)\cdot 4$. The elements u_1 and u_5 are unipotent, so they have p-power order, which proves generation in the case of odd q. In the case $p=2$ the element u_1 is an involution while u_5 has order 4. (This can be seen from the Chevalley commutator formula.) But a Frobenius group of type $\Phi_{12}(q)\cdot 4$ can not have a generating triple of elements of orders $(2, 4, \Phi_{12}(q))$. Lemma 1. 1 now yields $l^i(\mathfrak{C})=1$, and the assertion about the field of definition can be read off from the character table [16]. ■

This can be strengthened to

Theorem 4. 2. *Let s be a primitive divisor of q^4-q^2+1 in the notation of Lemma 1. 5. Then ${}^3D_4(q)$ is a Galois group for the ramification structure $\mathfrak{C}^*=([u_1],[u_5],C_s)^*$ over a field of index four in $\mathbb{Q}(\zeta_s)$.*

§ 5. Groups $F_4(q)$ as Galois groups over $\mathbb{Q}^{ab}$

In contrast to the situation for the groups treated until now, the maximal subgroups of $G:=F_4(q)$ are not known. But actually, if we choose one class in the class structure so that its elements generate a t.i.-Hall subgroup, less information is necessary to prove generation. Indeed, in view of Lemma 1. 3, all what is needed is a survey of the possible simple subgroups of G. This task is partly achieved in the following lemma:

Lemma 5. 1. *A nonabelian simple subgroup of $F_4(p^n)$ is either a group of Lie type in characteristic p or it belongs to the following exceptional set:*

(1) *$L_2(r^m)$ with $r^m\in\{7, 8, 13, 16, 17, 19, 25, 27, 37, 49\}$ or*

(2) *$L_3(3)$, $L_3(4)$, $L_4(3)$, $L_5(2)$, $S_4(3)$, $S_4(4)$, $S_6(2)$, $S_6(3)$, $U_3(3)$, $U_3(4)$, $U_4(3)$, $U_5(2)$, $U_6(2)$, $O_8^+(2)$, $G_2(3)$, ${}^3D_4(2)$, ${}^2F_4(2)'$, $Sz(8)$ or*

(3) *A_m with $5\leqq m\leqq 11$ or*

(4) *a sporadic simple group.*

Proof. At this point of the argument, the classification of the finite simple groups is needed. We will first assume that H is a group of Lie type in characteristic $r\neq p$. As $F_4(q)$ has a projective modular representation of degree 26 over $\mathbb{F}_q$, every finite simple subgroup must also have a faithful representation of degree at most 26 in characteristic p. In their paper [26], Landazuri and Seitz compiled a list of minimal degrees of projective representations of groups of Lie type in the "wrong" characteristic. This was achieved by looking at suitable p-subgroups of these groups. With the help of their result, one is left with the cases $H=L_2(r^m)$, $r^m\leqq 53$, the groups under (2) and the four additional groups $L_3(5)$, $S_4(5)$, $S_4(7)$, $U_3(5)$. The Weyl group of G has order $|W|=2^7 3^2$, so by Lemma 1. 7(3), for primes $r\notin\{2,3,p\}$ dividing $|G|$, the Sylow r-groups of $F_4(q)$ are abelian. The only Lie groups in characteristic r with abelian r-Sylows are those of type $L_2(r^m)$. This excludes the four cases $L_3(5)$, $S_4(5)$, $S_4(7)$, $U_3(5)$. The groups $L_2(r^m)$ contain a Frobenius group of order $r^m(r^m-1)/2$. By Lemma 1. 7(2) this can only happen in G if (r^m-1) divides $2|W|$, leading to the cases $r^m\in\{5, 7, 13, 17, 19, 25, 37, 49\}$. Collecting the groups in characteristic 2 and 3 as well, we arrive at (1), (2) and (3) of the lemma.

According to the classification, only the alternating groups remain to be considered. But A_{11} contains an 11-cycle, conjugate to five of its powers. By Lemma 1. 7 this is only possible in $F_4(q)$ in characteristic 11, and because all A_m, $m\geqq 11$, have A_{11} as a subgroup, the lemma is shown if $p\neq 11$. In characteristic 11, look at the centralizer of a 3-cycle in $A_m<F_4(11^n)$. It contains an A_{m-3}. On the other hand by [38], Table 8, the centralizer of an element of order three in $F_4(q)$, $(3,q)=1$, is a group of Lie type B_3, C_3 or $A_2\cdot A_2$. All of these possess projective representations of degree at most seven over $\bar{\mathbb{F}}_q$. The smallest degree of such a representation of A_9 over $\bar{\mathbb{F}}_{11^n}$ has degree eight.

Consequently the centralizer of an element of order three in $F_4(11^n)$ contains at most an A_8, which proves $m \leqq 11$, and thus the lemma. (The idea for the last step was pointed out to me by J. Saxl.) ■

The above results could be strengthened considerably with a bit more work, (excluding, for example, most of the sporadic groups), but the actual formulation is strong enough for our purposes.

5. 1. The general case. In [31], rigidity was shown for $F_4(q)$, q odd, with a class structure consisting of three semisimple classes. But this could not be generalized to characteristic 2 because the class of involutions is not semisimple for $p=2$. Moreover the three cases $q=3, 5, 7$ had to be treated separately. Here we will work with a different class structure which is defined for all q. With the knowledge about the Green functions available at the moment, we will prove rigidity for $F_4(q)$, $p \geqq 5$. The case $p=3$ is handled separately. But this class structure has the advantage that it yields Galois realizations over $\mathbb{Q}$ for some $F_4(p)$, $p \in \mathbb{P}$. This will be shown in the second section.

In odd characteristic, $G=F_4(q)$ possesses two classes of involutions, one with centralizer structure B_4, the other with C_3+A_1 [38]. Both centralizers contain elements of order $q+1$ with abstract centralizer structure A_2+A_1, one of them having h_{10} as a representative in [38], Table 8, the other h_{16}. The element h_{16} has the involution with centralizer B_4 as a power. With this information, we are ready to define the class structure for G in characteristic $p \neq 2$. Let C_p be the unipotent class of elements central in a Sylow p-subgroup (i.e. $C_p=[x_1]$ in the notation of [38]), let $C_{q+1}=[h_{16}]$ (by [38], Table 8, such a class exists whenever $q>3$), and finally choose $C_T := [h_{99}]$ to contain elements of order $\Phi_{12}(q)=q^4-q^2+1$.

Proposition 5. 1. *For $\mathfrak{C}=(C_p, C_{q+1}, C_T)$ of $F_4(q)$, $q=p^n$, $p \geqq 5$, we have $n(\mathfrak{C})=1$.*

Proof. An element $\tau \in C_T$ generates a cyclic Hall subgroup T of G with property (*), as can be seen from Table 9 in [38]. So we can apply Lemma 1. 4 to $T<G$. As $(\mathcal{N}_G(T):T)=12$ there exist $s:=(q^4-q^2)/12$ exceptional characters Λ_i for T and $\delta \in \{\pm 1\}$, $a \in \mathbb{Z}$ (*a priori* depending on q), so that by Lemma 1. 4(3)

$$(\delta+a)^2+\left(\frac{q^4-q^2}{12}-1\right)a^2+\sum_{\chi \neq \Lambda_j}|\chi(T^\#)|^2=13.$$

Now $s=(q^4-q^2)/12 \geqq 50$ for the relevant values of q, so we must have $a=0$. Moreover the unipotent characters of $F_4(q)$ are classified independently of q, and exactly twelve of them have a degree prime to $|T|=q^4-q^2+1$ ([8], p. 479). Those twelve χ_i cannot vanish on an element $\tilde{\tau} \in T$ of prime order, and now the t.i.-property of T shows that they take a constant nonzero value on all of $T^\#$. With congruences for character values (or the theory described in Section 1. 5 of values of unipotent characters at semisimple elements, or the results of Dade mentioned in 1. 2), the $\chi_i(T^\#)$ are determined. Due to the above formula, the unipotent characters are all the non exceptional characters of G not vanishing on $T^\#$. To determine the values of the χ_i on C_{q+1} using Lemma 1. 8, one has to know the maximal tori of the centralizer of an element from C_{q+1}. But this is equivalent to knowing the F-conjugacy classes in the corresponding Weyl group. The centralizer of an element in C_{q+1} has the Weyl group $A_2+\tilde{A}_1 \cong S_3 \times Z_2$, so the maximal tori can be determined. (A list of them is reproduced in [31], Table 5. 2.) With vanishing theorems for characters one deduces that the exceptional Λ_i take value zero on C_{q+1}.

Finally for $p \geqq 5$, the values of the twelve unipotent characters χ_i on the class C_p are calculated from the Green functions in [39] and the Fourier transform matrices in [29] or [8]. (In [30] and private communication to the author, Lusztig proved that these values are actually correct for all good primes, that is to say for $p \geqq 5$.) The values are collected in Table 1.

Table 1: Irreducible characters of $F_4(q)$, $q = p^n$, $p \geqq 5$, not vanishing on $T^\#$.

	$\{\imath\}$	C_p	C_{q+1}	C_T
$\phi_{1,0}$	1	1	1	1
$\phi_{1,24}$	q^{24}	$\cdot$	q^4	1
$\phi_{4,1}$	$\frac{1}{2} q \Phi_2^2 \Phi_6^2 \Phi_8$	$\frac{1}{2} q \Phi_2 \Phi_6 (q^4 + q^3 + 1)$	$\cdot$	-1
$B_2, 1$	$\frac{1}{2} q \Phi_1^2 \Phi_3^2 \Phi_8$	$-\frac{1}{2} q \Phi_1 \Phi_3 (q^4 - q^3 + 1)$	$-\Phi_1^2$	1
$\phi_{4,13}$	$\frac{1}{2} q^{13} \Phi_2^2 \Phi_6^2 \Phi_8$	$\frac{1}{2} q^{13} \Phi_2 \Phi_6$	$\cdot$	-1
B_2, ε	$\frac{1}{2} q^{13} \Phi_1^2 \Phi_3^2 \Phi_8$	$-\frac{1}{2} q^{13} \Phi_1 \Phi_3$	$-q^2 \Phi_1^2$	1
$\phi_{6,6''}$	$\frac{1}{12} q^4 \Phi_3^2 \Phi_4^2 \Phi_6^2 \Phi_8$	$\frac{1}{12} q^4 \Phi_3 \Phi_4 \Phi_6 (3q^4 + 2q^2 + 1)$	$-2q\Phi_6$	1
B_2, r	$\frac{1}{4} q^4 \Phi_1^2 \Phi_2^2 \Phi_3^2 \Phi_6^2 \Phi_8$	$-\frac{1}{4} q^4 \Phi_1 \Phi_2 \Phi_3 \Phi_6 \Phi_8$	$\cdot$	-1
$F_4[\theta]$	$\frac{1}{3} q^4 \Phi_1^4 \Phi_2^4 \Phi_4^2 \Phi_8$	$-\frac{1}{3} q^4 \Phi_1^3 \Phi_2^3 \Phi_4$	$\cdot$	1
$F_4[\theta^2]$	$\frac{1}{3} q^4 \Phi_1^4 \Phi_2^4 \Phi_4^2 \Phi_8$	$-\frac{1}{3} q^4 \Phi_1^3 \Phi_2^3 \Phi_4$	$\cdot$	1
$F_4[i]$	$\frac{1}{4} q^4 \Phi_1^4 \Phi_2^4 \Phi_3^2 \Phi_6^2$	$-\frac{1}{4} q^4 \Phi_1^3 \Phi_2^3 \Phi_3 \Phi_6$	$\cdot$	1
$F_4[-i]$	$\frac{1}{4} q^4 \Phi_1^4 \Phi_2^4 \Phi_3^2 \Phi_6^2$	$-\frac{1}{4} q^4 \Phi_1^3 \Phi_2^3 \Phi_3 \Phi_6$	$\cdot$	1
Λ_i	$\Phi_1^4 \Phi_2^4 \Phi_3^2 \Phi_4^2 \Phi_6^2 \Phi_8$	$-\Phi_1^3 \Phi_2^3 \Phi_3^2 \Phi_4 \Phi_6^2$	$\cdot$	$\{-1\}$

The desired result $n(\mathfrak{C}) = 1$ now follows from the centralizer orders

$$|\mathscr{C}_G(\varrho)| = q^{24}(q^2-1)(q^4-1)(q^6-1),$$

$$|\mathscr{C}_G(\sigma)| = q^4(q+1)(q^2-1)^2(q^3+1),$$

$$|\mathscr{C}_G(\tau)| = q^4 - q^2 + 1,$$

for $(\varrho, \sigma, \tau) \in \bar{\Sigma}(\mathfrak{C})$ and

$$|G| = q^{24}(q^2-1)(q^6-1)(q^8-1)(q^{12}-1). \quad \blacksquare$$

Theorem 5. 1. *The groups $F_4(q)$, $q=p^n$, $p\geqq 5$, occur as Galois groups over $\mathbb{Q}^{ab}$ for the ramification structure $\mathfrak{C}^*=(C_p, C_{q+1}, C_T)^*$ (the corresponding classes containing elements of orders $(p, q+1, q^4-q^2+1)$). More precisely a proper field of definition $K(q)$ is the compositum of the maximal real subfield of $\mathbb{Q}(\zeta_{q+1})$ with a field of index 12 in $\mathbb{Q}(\zeta_{q^4-q^2+1})$.*

Remark. The restriction $p\geqq 5$ in the theorem only stems from the insufficient knowledge of the Green functions. By a conjecture of Shoji, the values should be the same in bad characteristic, giving rigidity with this class structure for all $q\geqq 4$. The proof of generation will be formulated so that it is valid for $p=3$ as well.

Proof of the theorem. With Proposition 5. 1, only generation remains to be proved. So let $(\varrho, \sigma, \tau)\in\bar{\Sigma}(\mathfrak{C})$. The torus $T=\langle\tau\rangle$ was already identified in the proof of Proposition 5. 1 as a self centralizing Hall subgroup satisfying (*). Therefore $H:=\langle\varrho, \sigma\rangle$ has one of the structures described in Lemma 1. 3. The first possibility is immediately excluded by order considerations because $|\mathcal{N}_G(T)|=|T|\cdot 12$, while $p(q+1)\mid |H|$. The order of the Weyl group $|W(F_4)|=1152=2^7 3^2$ is prime to $o(\tau)=q^4-q^2+1$, so by Lemma 1. 7(2) T cannot act fixed point freely on an r-local subgroup for a prime $r\notin\{2, 3, p\}$. Next we obtain an estimate for the 2-rank and the 3-rank of $F_4(q)$ for $p\neq 2$, $p\neq 3$ respectively, as follows: If $q\equiv 1\ (\mathrm{mod}\, 4)$, the semisimple subgroup $(q-1)^4\cdot W$ contains a Sylow 2-subgroup of G. (In the terminology of BN-pairs, this is the group N, in the theory of algebraic groups the normalizer of a maximally split torus of $F_4(q)$.) The Weyl group $W(F_4)$ contains $W(B_4)\cong 2^4\cdot S_4$ (with the natural action) as a subgroup of index three, so $W(F_4)$ has the same 2-rank as $2^4\cdot S_4$, which is equal to four. Consequently, a Sylow 2-subgroup S of G can have at most

$$2\text{-rank}\,(S)\leqq 2\text{-rank}\,(q-1)^4+2\text{-rank}\,(W)\leqq 4+4 \ \text{ if } \ p\neq 2.$$

In the case $q\equiv -1\ (\mathrm{mod}\, 4)$, a subgroup of structure $(q+1)^4\cdot W$ yields the same result. Analogously 3-rank$\,(F_4(q))\leqq 6$ in characteristic $p\neq 3$. As $3^6=729$, $2^8=256$ and either $|T|\geqq 7^4-7^2+1=2353$ or $|T|\in\{241, 601\}$, H can not be 2- or 3-local in the sense of Lemma 1. 3(2) either. Finally none of the parabolic subgroups of $F_4(q)$ has order divisible by $\Phi_{12}(q)$. This excludes the local cases.

The orders of ϱ, σ and τ are pairwise prime, so by Lemma 1. 3(3) and Lemma 1. 6 H must be a nonabelian simple subgroup of G, that is, one of the groups in Lemma 5. 1. But none of the "exceptional" groups listed in Lemma 5. 1 has elements of order larger than $241\leqq o(\tau)=q^4-q^2+1$, forcing H to be a group of Lie type in characteristic p. Only those of Lie rank at most four can be contained in G, as is seen by a comparison of parabolic subgroups (see [27], fact 1, for an exact formulation). Applying the divisibility criterion of Lemma 1. 5 to the orders of Lie groups K in characteristic p to $|K(p^\nu)|\mid |F_4(q)|$ and $\Phi_{12}(q)\mid |K(p^\nu)|$, one is left with eleven cases, namely $A_1(q^6)$, $A_2(q^4)$, ${}^2A_2(q^2)$, ${}^2A_3(q^2)$, $B_2(q^3)$, ${}^2B_2(q^3)$, $G_2(q^2)$, ${}^2G_2(q^2)$, ${}^3D_4(q)$, ${}^2F_4(q)$ and $F_4(q)$. Some of these cannot be contained in G: The centralizer of an element of order $|T|=q^4-q^2+1$ has order $(q^6+1)/2$ in $A_1(q^6)$, q^8+q^4+1 in $A_2(q^4)$ and q^6+1 in $B_2(q^3)$ and ${}^2A_3(q^2)$, while T is self centralizing in $F_4(q)$, excluding these groups. On the other hand, $G_2(q^2)$ contains a cyclic maximal torus of order q^4+q^2+1 [9], while there are no elements of that order in $F_4(q)$ [38]. In the Ree groups in characteristic 3, the exponent of 3 is always odd, so that ${}^2G_2(q^2)$ does not exist. Finally in characteristic 2 neither the Suzuki groups ${}^2B_2(q^3)$ nor the Ree groups ${}^2F_4(q)$ have elements of order q^4-q^2+1 (remember $q\neq 2$). This leaves the three possibilities $F_4(q)$, ${}^3D_4(q)$ and ${}^2A_2(q^2)$ as candidates for H.

To handle the last cases, we have to make use of the other classes in the class structure. Namely, in ${}^2A_2(q^2)$ the centralizer order of an element of order $q+1$ is always divisible by $q^2+1=\Phi_4(q)$, while $|\mathscr{C}_G(\sigma)|$ is not divisible by $\Phi_4(q)$ by Lemma 1. 5, excluding ${}^2A_2(q^2)$. If $p \neq 2$, ${}^3D_4(q)$ has a single class C of involutions [15], [16]. Furthermore, if $H={}^3D_4(q)$ then this class must fuse into the class C' of $\sigma^{(q+1)/2}$, which was chosen so that it has centralizer structure B_4. From [16] we calculate $n(C, C, C_T)_{{}^3D_4}=1$, while $n(C', C', C_T)_G=0$ (the values of the characters not vanishing on $T^{\#}$ at C' are determined with the Deligne-Lusztig formula). This contradiction shows $H \neq {}^3D_4(q)$, and the only possibility left is $H=F_4(q)$, proving the theorem. ■

For the groups $F_4(3^n)$ the class structure consisting of three semisimple classes from [31] will be used. This avoids having to know the Green functions in characteristic three. The notation for the conjugacy classes of G is taken from [38]. Let $C_2=[h_2]$ be a class of involutions of G central in a Sylow 2-subgroup. Further, let $C^+=[h_{10}^2]$ if $q \equiv 1 \pmod 4$, respectively $C^-=[h_9^2]$ if $q \equiv -1 \pmod 4$, be a class of elements of order $(q+\varepsilon)/2$ with $q \equiv \varepsilon \pmod 4$ (by Table 8 in [38], elements of that type exist in G for all $q \geqq 9$), and finally denote by $C_T=[h_{99}]$ a class of elements of order $\Phi_{12}(q)=q^4-q^2+1$.

Theorem 5. 2. *The groups* $F_4(q)$, $q=3^n$, $n \geqq 2$, *occur as Galois groups over* $\mathbb{Q}^{ab}$ *for the ramification structure* $\mathfrak{C}_\varepsilon^*=(C_2, C^\varepsilon, C_T)^*$ (*the corresponding classes containing elements of orders* $(2, (q+\varepsilon)/2, q^4-q^2+1)$). *More precisely, a proper field of definition* $K(q)$ *is the compositum of the maximal real subfield of* $\mathbb{Q}(\zeta_{(q+\varepsilon)/2})$ *with a field of index* 12 *in* $\mathbb{Q}(\zeta_{q^4-q^2+1})$.

Proof. By the same arguments as in the proof of Proposition 5. 1, the only irreducible characters of G not vanishing on at least one of the three classes are among the twelve unipotent characters χ_i mentioned there. Their values were either already calculated in Proposition 5. 1, or for the class C_2 are easily obtained from the Deligne-Lusztig formula for the values of characters at semisimple elements. Namely the centralizer of an involution in C_2 has a Weyl group of type B_4. The conjugacy classes of this group $W(B_4)$ are enumerated in [6], part G. The fusion into classes of $W(F_4)$ is determined with the permutation character of $W(B_4) < W(F_4)$. In the notation of [8], p. 413, the latter is equal to $\chi_{1,1}+\chi_{2,1}$. Now the formula of Lemma 1. 8 can be evaluated, and we get $n(\mathfrak{C})=1$ (see Table 5. 5 in [31]).

As for generation, we again mimick the proof in characteristic $p \geqq 5$. This applies to the local subgroups, and to the exceptional almost simple groups. As for Lie groups in characteristic 3, the eleven possibilities mentioned in the proof of Theorem 5. 1 are easily ruled out as demonstrated in the proof of that theorem. Again elements of order $q+1$ in ${}^2A_2(q^2)$ have centralizer order divisible by $\Phi_4(q)$, which is not true for elements in C^ε. So we are left to consider the triality group ${}^3D_4(q)$. By [16], the conjugacy classes of elements of orders $(q-1)/2$ and $(q+1)/2$ (for $q \geqq 9$) have representatives s_3^2, s_5^2, s_6^2 and s_7^2, s_{10}^2, s_{15}^2 respectively. The centralizer orders of s_3 and s_7 in ${}^3D_4(q)$ are divisible by q^6-1, but not the one of $\sigma^\varepsilon \in C^\varepsilon$ in G. Moreover in ${}^3D_4(q)$ there exists only one class of involutions and one type of classes of elements of order q^4-q^2+1 (with representatives s_2 and s_{14}). From [16] and [41] the following normalized structure constants of ${}^3D_4(q)$ are calculated:

$$\begin{aligned}
n(s_2, s_5^2, s_{14}) &= q^6+2q^4+q^3+2q^2+1,\\
n(s_2, s_{10}^2, s_{14}) &= q^6+2q^4-q^3+2q^2+1,\\
n(s_2, s_6^2, s_{14}) &= q^8+q^7+2q^6+3q^5+4q^4+3q^3+2q^2+q+1,\\
n(s_2, s_{15}^2, s_{14}) &= q^8-q^7+2q^6-3q^5+4q^4-3q^3+2q^2-q+1.
\end{aligned}$$

This shows that for all possible fusions of classes of ${}^3D_4(q)$ into those of $\mathfrak{C}$ in G, the structure constant is too large. Consequently, the group generated by a triple from $\mathfrak{C}$ has to be $F_4(q)$, and the theorem holds by Lemma 1. 1. ■

The class structures for $F_4(q)$ introduced above do not exist in $F_4(2)$ and $F_4(3)$. Here different class structures have to be used. Let $C_4 := [h_{10}]$ be a class of elements of order four in $F_4(3)$ and as above, C_2 the class of involutions with centralizer structure B_4. For the classes of $F_4(2)$ we take the Atlas names.

Theorem 5. 3. *The group $F_4(2)$ occurs as a Galois group over $\mathbb{Q}(\sqrt{17})$ for the ramification structure $\mathfrak{C}_1^* = (2A, 8A, 17A)^*$.*

The group $F_4(3)$ occurs as a Galois group over a field of index 12 *in $\mathbb{Q}(\zeta_{73})$ for the ramification structure $\mathfrak{C}_2^* = (C_2, C_4, C_T)^*$.*

Proof. From the Atlas [11] one has $n(\mathfrak{C}_1) = 1$. All maximal subgroups of $F_4(2)$ are enumerated in [11]. The only ones with order divisible by 17 are two groups $S_8(2)$. But the permutation characters for these subgroups are easily determined to be $\chi_1 + \chi_4 + \chi_6 + \chi_{10} + \chi_{12}$, $\chi_1 + \chi_3 + \chi_6 + \chi_9 + \chi_{11}$, respectively. They take value zero on the class $8A$, which proves that a triple of $\mathfrak{C}_1$ can only generate all of $F_4(2)$. The field of definition is clear from the character table.

The characters not vanishing on the t.i.-subgroup T of $F_4(3)$ were already determined in the proof of Proposition 5. 1. The two other classes in the class structure are semisimple, so the values of the unipotent characters at those elements are computable by the Deligne-Lusztig formula. With that we get $n(\mathfrak{C}_2) = 1$. Remains the proof of generation. Because of the structure of T, the group H generated by a triple from $\bar{\Sigma}(\mathfrak{C}_2)$ has one of the structures described in Lemma 1. 3. The orders of the three elements are (2, 4, 73). Thus, H cannot be r-local for $r \geqq 5$. Again, no parabolic subgroup of $F_4(3)$ has order divisible by $|T| = \Phi_{12}(3)$. Since 2-rank$(F_4(3)) \leqq 8$, H is not 2-local either. None of the exceptional groups in Lemma 5. 1 has order divisible by 73, nor any of their automorphism groups.

Besides $H = F_4(3)$, only the possibility $K \leqq H \leqq \mathrm{Aut}(K)$, with K simple of Lie type in characteristic three remains. As in the proof of Theorem 5. 1, only ${}^3D_4(3)$ and ${}^2A_2(3^2) = U_3(9)$ are not immediately excluded. As $|\mathrm{Out}({}^3D_4(3))| = 3$, if $H \leqq \mathrm{Aut}({}^3D_4(3))$, we would already have $H = {}^3D_4(3)$. But in the proof of Theorem 5. 1 we had seen by calculating the structure constant $n(C_2, C_2, C_T)$ in ${}^3D_4(q)$ and in G that C_2 can not contain involutions of ${}^3D_4(3)$.

The Atlas table [11], p. 79, finally shows that all elements of order four in $U_3(9) \cdot 2$ have centralizer order divisible by 5. This contradicts

$$|\mathscr{C}_G(\sigma)| = 3^4 (3+1)(3^2-1)^2 (3^3+1).$$

So H is forced to be equal to $F_4(3)$. The theorem now follows from Lemma 1. 1, using that C_4 is a rational class. ■

The cyclic subgroup of order 17 in $F_4(2)$ indeed generalizes to a t.i.-subgroup of order $\Phi_8(q) = q^4 + 1$ in $F_4(2^n)$. But for class structures with a class containing such elements, the possibility of the generated group to be contained in $B_4(2^n)$ is not easily ruled out. In the case $F_4(2)$ this was only possible because of the knowledge of the permutation characters of such subgroups.

Theorems 5. 1 through 5. 3 complete the realization of all groups $F_4(q)$ with $p \geqq 3$ or $q=2$ as Galois groups over $\mathbb{Q}^{ab}$. It turns out that it is possible to choose a class structure of $F_4(p)$ for certain p such that the field of definition is $\mathbb{Q}$. This will be shown in the next section.

5. 2. Realizations of some $F_4(p)$ over $\mathbb{Q}$. The orders of all groups $F_4(p)$ are divisible by thirteen. If p is a primitive root mod 13, the factor of the group order containing the thirteen is $\Phi_{12}(p)=p^4-p^2+1$. In this case we can hope to get $F_4(p)$ as Galois group over $\mathbb{Q}$. Namely in the class structure of Proposition 5. 1 for $F_4(q)$ replace the class C_T by the class of elements of order thirteen in T. Then most of the above arguments remain valid for the new class structure. Moreover we choose the second class to contain rational elements with centralizer structure $A_2+\tilde{A}_1$. For this it is useful to consider besides C_{p+1} also $C_{p-1}=[h_{15}]$. We now define $C_6:=[h_{16}^{(p+1)/6}]$ if $p \equiv -1 \pmod 3$, $C_6:=[h_{15}^{(p-1)/6}]$ if $p \equiv 1 \pmod 3$. Obviously C_6 contains elements of order six, and by [38] their centralizer structure is $A_2+\tilde{A}_1$ whenever $p \geqq 5$. Finally, let $C_{13}:=[h_{99}^{(q^4-q^2+1)/13}]$.

Theorem 5. 4. *The groups $F_4(p)$, $p \equiv 2, 6, 7, 11 \pmod{13}$, $p \geqq 19$, occur as Galois groups over $\mathbb{Q}$ for the ramification structure $\mathfrak{C}^*=(C_p, C_6, C_{13})^*$.*

Proof. The semisimple classes C_6, C_{13} contain elements with the same centralizer structure as elements of C_{q+1}, C_T respectively. By the Deligne-Lusztig formula, the values of the unipotent characters on those classes must therefore be the same as the values calculated in the proof of Proposition 5. 1. Hence we arrive at $n(\mathfrak{C})=1$.

As for the structure of the group H generated by a triple of elements from $\bar{\Sigma}(\mathfrak{C})$, we can invoke Lemma 1. 3, because the centralizer in G of the element of order thirteen is once more the t.i.-torus T. Case (1) of the lemma obviously cannot occur for the primes p chosen. One immediately verifies, that of the local cases, only the possibility of an elementary abelian subgroup of order 27 or 729, with T acting fixed point freely remains. But as the top simple composition factor of H has a $(p, k, 13)$ generating triple of elements, $k|6$, an element of order p must act nontrivially on Z_3^3 or Z_3^6. This forces $p \mid |GL_6(3)|$. All such p are smaller than 19, and so excluded in the theorem.

By Lemma 1. 3 and Lemma 1. 6, H must be a simple subgroup as in Lemma 5. 1. There are nine sporadic simple groups with order divisible by 13. Seven of them contain elements of order 11 conjugate to five or ten of their powers, which can happen in G only in characteristic 11, which was excluded. The two remaining sporadic groups, *Ru* and *Th*, contain elements of order 29, (resp. 31) conjugate to 14 (resp. 15) of their powers, which is possible only if $p=29$ (resp. $p=31$). But these primes do not satisfy the conditions of the theorem. Of the remaining exceptional groups in Lemma 5. 1, eleven have order divisible by 13. The only other primes dividing the orders of these groups are 5 and 7. Hence H, which contains elements of orders 13 and p, must be a group of Lie type in characteristic p. As 13 is a primitive divisor of $p^{12}-1$ for the congruences mentioned in the theorem, the arguments in the proof of Theorem 5. 1 apply. Namely, H is one of ${}^3D_4(p)$, ${}^2A_2(p^2)$ or $F_4(p)$. The first and the second case are excluded as in Theorem 5. 1, and the assertion of the theorem is proved. ■

§ 6. Groups $E_6(q)$ as Galois groups over $\mathbb{Q}^{ab}$

When trying to realize groups of type E_6 as Galois groups, a new obstacle is encountered. Namely the group of fixed points G^F of the reductive algebraic group G of type E_6 under the Frobenius F has either a nontrivial center (simply connected case) or a nontrivial commutator factor group (adjoint case) of order three if $q \equiv 1 \pmod 3$. The cases are distinguished by the subscript $E_6(q)_{\mathrm{sc}}$, $E_6(q)_{\mathrm{ad}}$ respectively. In the case of nontrivial center, the criterion of Matzat and Thompson does not apply. In the simple group $E_6(q)_{\mathrm{sc}}/Z(E_6(q)_{\mathrm{sc}}) \cong E_6(q)'_{\mathrm{ad}} =: E_6(q)$, the structure constants tend to be multiples of $(q-1, 3)^2$. This means that only in the case $q \equiv -1 \pmod 3$ good class structures are easily found. In the other case no rigid class structure could be determined.

First we will compile a list of possible simple subgroups of $E_6(q)$ to be able to handle the problem of generation. As ${}^2E_6(q)$ is defined as a subgroup of $E_6(q^2)$, we simultaneously obtain a list of possible simple subgroups of the twisted groups of type E_6. This will be needed in the next paragraph. As it is not the aim of this paper to determine the maximal subgroups of the exceptional groups of Lie type, no effort is made to exclude as many simple groups as possible. For the purpose of the main theorem in this paragraph, a rough idea of what the simple subgroups of $E_6(q)$ look like will be sufficient.

Lemma 6. 1. *A nonabelian simple subgroup of $E_6(p^n)$ or ${}^2E_6(p^n)$ is either a group of Lie type in characteristic p or one of the following:*

(1) *$L_2(r^m)$ with $r^m \in \{7, 8, 11, 13, 16, 17, 19, 25, 27, 37, 41, 49\}$ or*

(2) *$L_3(3)$, $L_3(4)$, $L_3(5)$, $L_4(3)$, $L_5(2)$, $S_4(3)$, $S_4(4)$, $S_4(5)$, $S_6(2)$, $S_6(3)$, $O_7(3)$, $U_3(3)$, $U_3(4)$, $U_3(5)$, $U_4(3)$, $U_5(2)$, $U_6(2)$, $O_8^+(2)$, $G_2(3)$, $O_8^-(2)$, ${}^3D_4(2)$, ${}^2F_4(2)'$, $Sz(8)$ or*

(3) *A_m with $5 \leqq m \leqq 18$ or*

(4) *a sporadic simple group.*

Proof. By Lemma 1. 7(3), $E_6(p^n)$ (and so ${}^2E_6(q)$ due to ${}^2E_6(p^n) < E_6(p^{2n})$) possesses abelian Sylow r-subgroups for all primes r different from the characteristic p and not dividing the order of the Weyl group $|W| = 2^7 3^4 5$. Simple subgroups of G of Lie type in characteristic r can thus only be of type $L_2(r^m)$. With the projective representation of G of degree 27 over $\overline{\mathbb{F}_p}$ and [26] all possible r^m are determined as usual. Moreover $L_2(r^m)$ with $r^m \in \{23, 31, 43, 47, 53\}$ can not occur inside G, because they contain elements of order 23, 31, 43, 47, 53 conjugate to 11, 15, 21, 23, 26 respectively of their powers. This is possible in G only for $r = p$ by Lemma 1. 7(2), as no subgroups of these orders are contained in $W(E_6)$. Groups of Lie type in characteristic $r = 2$, 3 or 5 having a projective representation of degree at most 27 over $\overline{\mathbb{F}_p}$, $r \neq p$, are found in [26] again. This leads to part (1), (2) or (3).

The alternating groups A_m with $m \geqq 19$ have a 17-cycle conjugate to all of its primitive powers by an element of order 16. As $W(E_6) \cong U_4(2) \cdot 2$ does not contain an element of order 16 by [11], p. 27, A_{19} may be a subgroup of G only in characteristic $p = 17$ by Lemma 1. 7(2). In this characteristic, we proceed as in the case of $F_4(q)$ (proof of Lemma 5. 1). The centralizers of elements of order three in G are known by the work of Mizuno [35]. Their nonabelian simple composition factors are of Lie type A and D (or twisted versions of these) in the same characteristic and of Lie rank at most 5. But all of those have a projective representation of degree at most 10 over $\overline{\mathbb{F}_p}$, while the smallest nontrivial representation of A_{12} in characteristic 17 has degree 11. This shows that even for $p=17$, only a group A_{14} can possibly occur in $E_6(q)$. With the classification of finite simple groups, this proves the lemma. ■

For the reasons explained above, we will only consider $q \equiv -1 \pmod 3$, $G := E_6(q)$, for rigidity. The classes of semisimple and unipotent elements were calculated by Mizuno [35]. His notation for the classes will be used here. Let C_p be the unipotent class $[x_1]$ (the class A_1 in [5] and [8], p. 402) with centralizer order $q^{36}(q^2-1)(q^3-1)(q^4-1)(q^5-1)(q^6-1)$, C_{q^2-1} a class of elements of order q^2-1 with centralizer structure ${}^2A_2(q)+A_1(q^2)$, and C_T a class of elements of order $q^6+q^3+1=\Phi_9(q)$.

Proposition 6. 1. *For $\mathfrak{C}=(C_p, C_{q^2-1}, C_T)$ of $E_6(q)$, $q=p^n \equiv -1 \pmod 3$, $p \geqq 5$, we have $n(\mathfrak{C})=1$.*

Proof. From the list of centralizers in [35] one sees that an element $\tau \in C_T$ generates a cyclic Hall subgroup T of G with the property (*) of Section 1. 2. We apply the lemma of Feit to this t.i.-torus. As $(\mathcal{N}_G(T): T)=9$ (see for example [6], G-17), there exist $(q^6+q^3)/9$ exceptional characters Λ_i for T, while all other irreducible characters of G are constant on $T^{\#}$. The equations of Lemma 1. 4 hold. From the list of degrees of unipotent characters of G in [8], p. 480, exactly nine are prime to $|T|=\Phi_9(q)$. It was already pointed out in the case of F_4 that therefore these are the nonexceptional χ_i not vanishing on $T^{\#}$. The Weyl group of the centralizer of an element in the semisimple class C_{q^2-1} has the structure $W({}^2A_2+A_1) \cong S_3 \times Z_2$. The maximal tori of this centralizer are described in Table 6. 1 of [31]. The values of the unipotent χ_i on C_{q^2-1} are now calculated according to Lemma 1. 8. For the unipotent classes we have the results of Beynon and Spaltenstein [5] giving the values of the Green functions for large enough p and q (indeed for all good p by [30]). From them, with the theorem of Lusztig [29] the unipotent character values on C_p can be computed for $p \geqq 5$. This completes Table 6. 2 in [31], containing the characters not vanishing on $T^{\#}$. With the centralizer orders

$$|\mathscr{C}_G(\sigma)| = q^5(q^2-1)^2(q^3+1)(q^4-1), \quad \sigma \in C_{q^2-1}, \quad |\mathscr{C}_G(T)| = q^6+q^3+1,$$

and

$$|G| = q^{36}(q^2-1)(q^5-1)(q^6-1)(q^8-1)(q^9-1)(q^{12}-1),$$

we now get $n(\mathfrak{C})=1$. ■

Theorem 6. 1. *The groups $E_6(q)$, $q=p^n \equiv -1 \pmod 3$, $p \geqq 5$, occur as Galois groups over $\mathbb{Q}^{ab}$ for the ramification structure $\mathfrak{C}^* = (C_p, C_{q^2-1}, C_T)^*$ (with the corresponding classes containing elements of orders (p, q^2-1, q^6+q^3+1)). More precisely a proper field of definition $K(q)$ is the compositum of the maximal real subfield of $\mathbb{Q}(\zeta_{q^2-1})$ with a field of index 9 in $\mathbb{Q}(\zeta_{q^6+q^3+1})$.*

Proof. In Proposition 6. 1, $n(\mathfrak{C})=1$ was shown. So let (ϱ, σ, τ) be a triple in $\bar{\Sigma}(\mathfrak{C})$ for which generation will be studied. The Hall property of $\langle \tau \rangle = T$ leads to the cases of Lemma 1. 3. The first possibility is immediately excluded because H is nonsolvable by Lemma 1. 6 while $\mathcal{N}_G(T) = T \cdot 9$. The order of the Weyl group $|W| = 2^7 3^4 5$ is prime to $o(\tau) = q^6+q^3+1$ (here we use $q \equiv -1 \pmod 3$). Thus by Lemma 1. 7(2) H cannot be r-local for $r \notin \{2, 3, p\}$. Further, by studying subgroups of the form $(q-1)^6 \cdot W$ in $E_6(q)$ the following estimates are obtained: 2-rank$(E_6) \leqq 11$ and 3-rank$(E_6) \leqq 9$ in characteristic $p \neq 2, 3$. But τ has order at least $\Phi_9(5) = 15751$, while on the other hand

$2^{11}=2048$ and $3^9=19683$. Consequently T cannot act fixed point freely on a 2- or 3-local subgroup either, which excludes these local cases. Finally none of the parabolic subgroups of $E_6(q)$ has order divisible by $\Phi_9(q)$.

By Lemmas 1. 6 and 1. 3, H has to be one of the nonabelian simple groups in Lemma 6. 1. The order $o(\tau)\geqq 15751$ of τ is larger than any of those occurring in the exceptional groups in the lemma. Therefore the discussion can be confined to groups of Lie type K in the same characteristic. From the formulae for the orders of the groups of Lie type and the conditions $|K| \mid |E_6(q)|$ and $\Phi_9(q) \mid |K|$ and using Lemma 1. 5 we arrive at the 17 cases $A_1(q^{9/2})$, $A_2(q^3)$, $A_3(q^3)$, ${}^2A_2(q^{3/2})$, ${}^2A_3(q^{3/2})$, $B_2(q^{9/4})$, $B_3(q^{3/2})$, $B_4(q^{3/2})$, $C_3(q^{3/2})$, $C_4(q^{3/2})$, $D_4(q^{3/2})$, ${}^2D_4(q^{3/2})$, ${}^3D_4(q^{3/4})$, $G_2(q^{3/2})$, $F_4(q^{3/4})$, ${}^2E_6(q^{1/2})$ and $E_6(q)$. Of these, all but $A_2(q^3)$, $A_3(q^3)$ and $E_6(q)$ do not possess elements of order q^6+q^3+1. In $A_3(q^3)$, an element of order q^6+q^3+1 has centralizer order $q^9-1>|T|$. An element of order q^2-1 in $A_2(q^3)$ has centralizer order divisible by q^6-1, which is not the case for the element σ from the class C_{q^2-1} in G. Thus H has to be equal to $E_6(q)$, and the assertion follows with Lemma 1. 1. ■

§ 7. Groups ${}^2E_6(q)$ as Galois groups over $\mathbb{Q}^{ab}$

The results of the last paragraph of the groups $E_6(q)$ can easily be transferred to the very similar groups ${}^2E_6(q)$. In contrast to the situation for $E_6(q)$, the groups ${}^2E_6(q)$ possess a nontrivial Schur multiplier if $q\equiv -1 \pmod 3$. Therefore we will restrict our attention to $q\equiv 1 \pmod 3$, the other case not being tractable at the moment.

A classification of the unipotent classes of ${}^2E_6(q)$ for large enough p and q is to be found in [5], Section 4. Namely it is shown that they correspond to the unipotent classes of the untwisted group $E_6(q)$, with the centralizer order obtained by replacing q by $-q$ in the respective order in $E_6(q)$. The conjugacy classes of semisimple elements are enumerated in [15], Table 4. Let C_p be the unipotent class of ${}^2E_6(q)$ with centralizer order $q^{36}(q^2-1)(q^3+1)(q^4-1)(q^5+1)(q^6-1)$, C_{q+1} a class of semisimple elements of orders $q+1$ and centralizer structure ${}^2A_2+2A_1$ ([15], Table 4) and C_T a class of elements of order $\Phi_{18}(q)=q^6-q^3+1$.

Proposition 7. 1. *For $\mathfrak{C}=(C_p, C_{q+1}, C_T)$ of ${}^2E_6(q)$, $q=p^n\equiv 1 \pmod 3$, p and q large enough, we have $n(\mathfrak{C})=1$.*

Proof. From the centralizer orders in Table 4 of [15] it is seen that an element $\tau\in C_T$ generates a cyclic Hall subgroup of $G={}^2E_6(q)$ with the property (*) of Section 1. 2. Moreover $(\mathcal{N}_G(T):T)=9$ (see [15]), whence the existence of $(q^6-q^3)/9$ exceptional characters Λ_i for T, and the equations of Lemma 1. 4 apply. Exactly nine of the degrees of unipotent characters of G are prime to $|T|=\Phi_{18}(q)$ (see [8], p. 481). Consequently these are all the nonexceptional characters of ${}^2E_6(q)$ not vanishing on $T^\#$.

To calculate the values of these characters on the semisimple classes C_{q+1} and C_T, we have to make some modifications to the formula in Lemma 1. 8. Namely, the classes of maximal tori in G are now classified by F-conjugacy classes of $W(E_6)$, which are different from the ordinary conjugacy classes of $W(E_6)$. This makes the expression $\chi(w)$ in Lemma 1. 8 not well defined. But in [28], Theorem 1. 15, the calculation of $\langle \varrho, R_w\rangle$ in this case is described. If we take

$$\tilde{R}_\chi := |W|^{-1} \sum_{w\in W} \chi(ww_0) R_w,$$

then we have $\langle \varrho, \tilde{R}_\chi \rangle_{^2E_6} = \varepsilon_\varrho \langle \varrho', R_\chi \rangle_{E_6}$. Here $\varrho \leftrightarrow \varrho'$ is a suitable bijection, detailed in [28], from the unipotent characters of $^2E_6(q)$ onto the ones of $E_6(q)$, and w_0 denotes the longest element of W. Again this formula holds only for large enough q. We can now calculate the values of the unipotent characters on the semisimple classes in the class structure. The classes of maximal tori $[T_w]$ of the centralizer with structure $^2A_2 + 2A_1$ and the fusion of the ww_0 in $W(E_6)$ are given in Table 7. 1 of [31]. The values on the unipotent class C_p may be obtained from the information in [5], Section 4, for p and q large enough. (Unfortunately, no lower bound for p or q can be given.) They are the ones for $E_6(q)$, with q replaced by $-q$. The irreducible characters not vanishing on $T^{\#}$ are listed in Table 7. 2 of [31].

With the centralizer orders

$$|\mathscr{C}_G(T)| = q^6 - q^3 + 1, \quad |\mathscr{C}_G(\sigma)| = q^5(q+1)^2\,(q^2-1)^3\,(q^3+1)$$

and

$$|G| = q^{36}(q^2-1)\,(q^5+1)\,(q^6-1)\,(q^8-1)\,(q^9+1)\,(q^{12}-1)$$

one gets $n(\mathfrak{C}) = 1$. ■

Theorem 7. 1. *The groups $^2E_6(q)$, $q = p^n \equiv 1 \pmod 3$, $p \geqq 5$, p and q large enough, occur as Galois groups over $\mathbb{Q}^{ab}$ for the ramification structure $\mathfrak{C}^* = (C_p, C_{q+1}, C_T)^*$ (with the respective classes containing elements of orders $(p, q+1, q^6 - q^3 + 1)$). More precisely, a proper field of definition $K(q)$ is the compositum of the maximal real subfield of $\mathbb{Q}(\zeta_{q+1})$ with a field of index nine in $\mathbb{Q}(\zeta_{q^6-q^3+1})$.*

Proof. The similarity between $^2E_6(q)$ and $E_6(q)$ is reflected in the proof of the theorem, which consists more or less of the proof of Theorem 6. 1, with only minor modifications. Let (ϱ, σ, τ) be a triple in $\bar{\Sigma}(\mathfrak{C})$. Using the Hall property of the maximal torus $T = \langle \tau \rangle < H := \langle \varrho, \sigma \rangle$, we can invoke Lemma 1. 3. The local cases are disposed of exactly as in the proof of Theorem 6. 1 due to $(|T|, p|W|) = 1$ and $|T| \geqq \Phi_{18}(7) = 117307$. Thus H must be one of the simple groups in Lemma 6. 1 by Lemmas 1. 3 and 1. 6. The order of τ excludes all exceptional cases of the lemma, leaving the groups of Lie type in characteristic p. The divisibility criterion of Lemma 1. 5 leads to a list of cases as in § 6, with q replaced by $-q$ (i.e. A_l replaced by ^2A_l). Besides $H = G$, only $^2A_2(q^3) \cong U_3(q^3)$ remains as a candidate. But an element of order $q+1$ in $U_3(q^3)$ lies in a maximal torus of this group of order $(q^3+1)^2$ or $q^6 - 1$. No such tori exist in $\mathscr{C}_G(\sigma)$ ([31], Table 7. 1). Therefore we have $H = {}^2E_6(q)$ and the theorem follows with Proposition 7. 1. ■

The restriction "p and q large enough" seems to be of a more technical nature; it is needed for the classification of the unipotent classes and for the determination of the Green functions. In both cases, the results should be uniform for all good p. At least this is so for the untwisted groups [30].

§ 8. Groups $E_7(q)$ as Galois groups

For groups of type E_7, the methods of the preceding paragraphs are not immediately applicable. First, $E_7(q)$ contains no cyclic selfcentralizing t.i.-Hall subgroup. Second, for odd prime powers q the group G^F of fixed points of the algebraic group under the Frobenius map is not simple — the problem which was already encountered with $E_6(q)$ for $q \equiv 1 \pmod 3$ now arises for all $p \neq 2$. The Rationality Criterion and Lemma 1. 1 are only applicable to groups with trivial center.

To remove the first obstacle, the full results of the Deligne-Lusztig character theory of reductive groups have to be used. Until now, this was avoided so as to keep the exposition reasonably straightforward. The second problem can be solved by a suitable choice of the three classes in $E_7(q)_{\mathrm{ad}}$ and descent to the commutator factor group, which is the simple group in question.

8. 1. The Lusztig character theory. For the calculation of a normalized structure constant in $E_7(q)_{\mathrm{ad}}$, the complete Lusztig character theory, as described in [29], will be needed. One of the most important results is the so called Jordan decomposition of the irreducible characters of G^F for a connected reductive algebraic group G with connected center. In § 1. 5, the generalized characters $R_{T,\theta}$ of the group G^F were mentioned. As the Deligne-Lusztig characters belonging to pairs (T, θ), (T', θ') which are not geometrically conjugate do not have any irreducible component in common, and on the other hand every irreducible character occurs as a component of some $R_{T,\theta}$ ([8], Corollary 7. 5. 8), this defines a partition of the irreducibles of G^F into disjoint families, parametrized by the classes of pairs (T, θ) modulo geometric conjugation. To describe these families, a simple classification of the classes (T, θ) under geometric conjugation is needed. In [8], Theorem 4. 4. 6, a bijective correspondence between these and the semisimple classes of the dual G^{*F^*} of G^F is proved. (For the type $G^F = E_7(q)_{\mathrm{ad}}$, the dual group G^{*F^*} is isomorphic to $E_7(q)_{\mathrm{sc}}$, [8], p. 120.) Each irreducible character χ of G^F is a component of a unique class of $R_{T,\theta}$, thus it corresponds to exactly one F-stable semisimple conjugacy class $[s]$ of G^*. If χ belongs to the class of $s \in G^*$, we write $\chi \in \mathscr{E}_{(s)}$. The unipotent characters for example were defined as the components of the $R_{T,1}$, and $(T, 1)$ belongs to the identity element of G^*, so the unipotent characters lie in $\mathscr{E}_{(\iota)}$.

The second step to the Jordan decomposition of the complex irreducible characters of G^F is the description of the characters belonging to one class $\mathscr{E}_{(s)}$. Lusztig proved a bijection from the characters χ of G^F in $\mathscr{E}_{(s)}$ to the unipotent characters of the group dual to $\mathscr{C}_{G^*}(s)$, which will be called H. The results of § 1. 5 show that the knowledge of the values of the χ on the semisimple elements of G^F is equivalent to the knowledge of the multiplicities $(\chi, R_{T,\theta})$ for all $R_{T,\theta}$ of G^F. Again, these multiplicities were determined by Lusztig. As each χ is contained in just one $\mathscr{E}_{(s)}$ (belonging to the geometric conjugacy class of (T, θ)), we can get nonzero multiplicities only for those $R_{T,\theta}$. If in the bijection mentioned above χ corresponds to the unipotent character ϱ of $H = \mathscr{C}_{G^*}(s)^*$ (the group dual to the centralizer in G^{*F^*} of s; this can again be interpreted as a subgroup of G^F), then $(\chi, R_{T,\theta})$ is equal to $(\varrho, R_{T',1})_H$ up to sign. Here $R_{T',1}$ denotes a Deligne-Lusztig character of H. Furthermore the sign only depends on the class of s. It can be obtained from the condition $\chi(\iota) > 0$. Thus the degree of the irreducible character $\chi \in \mathscr{E}_{(s)}$ is the product of the degree of the corresponding unipotent character ϱ of H with $|(G^F : H)|_{p'}$. This complete classification of the χ resembles the Jordan decomposition of the elements of G^F into semisimple and unipotent part. The above results are contained in Theorem 4. 23 and Chapter 8 of [29]. A short form can be found on pages IX—X of the same book.

The formula for the calculation of the values of unipotent characters at semisimple elements in § 1. 5 holds with suitable changes for all irreducible characters χ of G^F. So one obtains

$$\chi(t)=\varepsilon_t|\mathscr{C}_G^0(t)^F|_p^{-1}\cdot\sum_{T^F\ni t}\varepsilon_T\cdot\sum_{\theta\in\widehat{T^F}}\theta(t)^{-1}(\chi, R_{T,\theta}).$$

With a knowledge of the (T,θ) belonging to $s\in G^{*F^*}$, the value of $\chi\in\mathscr{E}_{(s)}$ at every semisimple element $t\in G^F$ can be computed.

8. 2. Proof of $\boldsymbol{n}(\mathfrak{C})=1$. Now let $G:=E_7(q)_{\mathrm{ad}}$ with $q=p^n$. As the values of the unipotent characters at unipotent classes are at present only known in good characteristic [30] and the class structure will contain a unipotent class, let $p\geqq 5$. A class with some similarity to the t.i.-Hall classes used until now is C_T^δ, containing elements of order $(q-\delta)(q^6+\delta q^3+1)$ with $q\equiv-\delta\ (\mathrm{mod}\ 3)$. Define C_p to be the unipotent class $4A_1$ in [5] or [8], p. 403. To assure generation of G, choose the third class so as to contain involutions from $G\backslash G'$. According to [6], Part F, §§ 11 and 12, those have centralizer structure A_7 or ${}^2A_7$. More precisely, in case $q\equiv 1\ (\mathrm{mod}\ 4)$ an involution with centralizer ${}^2A_7(q)$ is not contained in G', in case $q\equiv-1\ (\mathrm{mod}\ 4)$ the one with centralizer $A_7(q)$. Let the class C_2 consist of such elements. (The condition in [14], p. 201, for the existence of elements with centralizer structure A_7 or ${}^2A_7$ is not quite correct.)

Proposition 8. 1. *For the class structure* $\mathfrak{C}=(C_p, C_2, C_T^\delta)$ *of* $E_7(q)_{\mathrm{ad}}$, $p\geqq 5$, $q\equiv-\delta\ (\mathrm{mod}\ 3)$, *we have* $n(\mathfrak{C})=1$.

Proof. Contrary to the situation in the preceding paragraphs, $\tau\in C_T$ does not generate a cyclic t.i.-subgroup of G. In particular, Lemma 1. 4 about the exceptional characters does not apply. But nevertheless the theory of Lusztig enables us to get a survey of all irreducible characters of G not vanishing on C_T. From [14] we see that the elements τ of order $(q-\delta)(q^6+\delta q^3+1)$ are *regular* (i.e. contained in just one maximal torus T_τ of G, the one generated by τ). This simplifies the formula for character values from the first section to

$$\chi(\tau)=\varepsilon_\tau\varepsilon_{T_\tau}\sum_{\theta\in\widehat{T_\tau}}\theta(\tau)^{-1}(\chi, R_{T_\tau,\theta}).$$

Thus, the irreducible character χ of G will not vanish on τ only if it occurs as a component of some $R_{T_\tau,\theta}$. The classes of pairs (T_τ,θ) are classified by semisimple conjugacy classes $[s]$ in the torus of order $(q-\delta)(q^6+\delta q^3+1)$ in $G^*=E_7(q)_{\mathrm{sc}}$ dual to T. These can be found in Table 1 of [14].

The characters for $s=\iota$ are the unipotent characters of G. Equally many characters with the same degrees belong to the element of order two lying central in G^*. The computations will show that these take the same values at the elements of G' as the corresponding unipotent characters, while their values at elements from $G\backslash G'$ are negated. This is not surprising, because both families of characters originate from the unipotent characters of G' by induction to G. To the elements s with $o(s)\,|\,(q-\delta)$, $o(s)\neq 1, 2$, there exist another $(q-2-\delta)/2$ families of irreducibles, each parametrized by the unipotent characters of $E_6^\delta(q)$. (Here we denote $E_6^+(q):=E_6(q)$ and $E_6^-(q):={}^2E_6(q)$.

For the relevant congruences, $E_6^\delta(q)_{\mathrm{ad}}$ and $E_6^\delta(q)_{\mathrm{sc}}$ coincide.) Finally remain the regular $s \in T_\tau^*$, i.e. those elements of the cyclic torus T_τ^* whose order does not divide $q-\delta$. As $\mathscr{C}_{G^*}(s) = T_\tau^*$ has only one unipotent character, namely the trivial one, the corresponding $(q-\delta)(q^6+\delta q^3)/18$ families consist of just one irreducible of G. These correspond to the exceptional characters in the earlier examples. The following table collects the families of characters not vanishing on τ:

$o(s)$	number	$\mathscr{C}_{G^*}(s)^*$	$\lvert\mathscr{E}_{(s)}\rvert$	$\theta(\tau)$
1	1	G	76	1
2	1	G	76	-1
$\mid(q-\delta), \neq 1, 2$	$(q-2-\delta)/2$	$(q-\delta)\cdot E_6^\delta(q)$	30	$\zeta_{q-\delta}$
$\nmid(q-\delta)$	$(q-\delta)(q^6+\delta q^3)/18$	T_τ	1	$\zeta_{(q-\delta)(q^6+\delta q^3+1)}$

By the result of Lusztig, we now also know the degrees of those characters. The classes of pairs (T, θ) belonging to the semisimple classes $s \in T_\tau^*$ each possess a representative (T_τ, θ) with $\theta(\tau)$ as in the table ([8], Section 4. 4 and 4. 5). Now we are ready to calculate the values of the $\chi \in \mathscr{E}_{(s)}$ at τ, because the multiplicities $(\chi, R_{T_\tau,\theta})$ are known for $\theta = 1$ by [28]; in the general case they coincide with $(\varrho, R_{T',1})$ for some unipotent ϱ of $H := \mathscr{C}_{G^*}(s)^*$ (where in our case H is either $E_6^\delta(q)$ or the torus, so that again [28] and [1] can be used). We get that only eighteen characters from the first two families do not vanish on τ. Of the thirty characters in the families of the third type, only nine take nonzero values at τ. The tables of these values are not reproduced here, they can be found in [31] (Tables 8. 2 and 8. 3). The fourth type of families will vanish at one of the other classes, so we need not consider it here.

Next, the values of the remaining characters χ at $\sigma \in C_2$ shall be determined. The classes of maximal tori of the groups $A_7(q)$ and ${}^2A_7(q)$ may be obtained according to [6], Part G, and are given in Table 8. 1 in [31]. For the unipotent $\chi \in \mathscr{E}_{(\iota)}$, we proceed with Lemma 1. 8. As σ was chosen to lie in $G \backslash G'$, it cannot be a square in G. Consequently, the θ in the class of (T, θ) with $s \in T^*$ and $o(s) = 2$ take value -1 at σ. With the formula of the first section we therefore get that the characters of the second family take the negative of those of the unipotent ones on σ. As the centralizer order of σ is not divisible by $q^6 + \delta q^3 + 1$, σ is not contained in T_τ, and the characters of the fourth type (the "exceptional" characters for T_τ) vanish at the second class. (This could also be deduced from the description of these characters in 7. 3. 5 and of their values in 7. 5. 3 of [8].) Finally the evaluation of the formula for the characters χ of the third type is possible. The complete results are given in [31].

The values of the R_χ, $\chi \in \widehat{W(E_7)}$ at the class C_p can be found in [5]. With this, the values of the unipotent characters at C_p can be computed as usual. By Corollary 7. 2. 9 of [8], the $R_{T,\theta}(u)$ for u unipotent are independent of θ, i.e. equal to the Green functions. For $s \in T_\tau^*$ with $o(s) = 2$ we have $H = \mathscr{C}_{G^*}(s)^* = G$. Accordingly, for χ of the second type $(\chi, R_{T,\theta})$ coincides with $(\varrho, R_{T,1})$ for some unipotent ϱ of G up to sign. Now $\iota \in G$ can be thought of as unipotent, and we have $\chi(\iota) > 0$. So we must have $(\chi, R_{T,\theta}) = (\varrho, R_{T,1})$ and together with $R_{T,\theta}(u) = R_{T,1}(u)$ even $\chi(u) = \varrho(u)$ for a suitable bijection $\chi \leftrightarrow \varrho$ (namely for a bijection preserving the degree $\chi(\iota) = \varrho(\iota)$). Again the characters of the third type cause the biggest computational difficulties. But the procedure in principle resembles the one for the second type. Namely, by [28], the knowledge of the multiplicities $(\chi, R_{T,1})$ already suffices to express χ as a linear combination of $R_{T,1}$, (and so $\chi(u)$ as a function of the $R_{T,1}(u)$). So we only have to determine the $R_{T,1}(u)$. They can be obtained from the R_χ in [5] with the formula for the multiplicities of the χ in the $R_{T,1}$ in [28] (and for small q in [30]). Those are then considered as Green functions of $E_6^\delta(q)$, leading to the determination of the values of the χ in the E_6^δ-families as in the preceding paragraphs. All character values are collected in Tables 8. 2 and 8. 3 of [31]. With them and with

$$|\mathscr{C}_G(\varrho)| = q^{51}(q^2-1)(q^4-1)(q^6-1),$$

$$|\mathscr{C}_G(\sigma)| = 2q^{28}(q^2-1)(q^3-1)(q^4-1)(q^5-1)(q^6-1)(q^7-1)(q^8-1)$$

and

$$|\mathscr{C}_G(\tau)| = (q-\delta)(q^6+\delta q^3+1)$$

for $(\varrho, \sigma, \tau) \in \mathfrak{C}$, we get $n(\mathfrak{C}) = 1$ in all cases. ■

8. 3. Proof of generation. Although none of the classes in the class structure for $E_7(q)_{\mathrm{ad}}$ contains generators of t.i.-subgroups (which would then have enabled us to invoke Lemma 1. 3), we still only need a list of possible simple subgroups of G to prove $l^i(\mathfrak{C}) = 1$. This is obtained from the classification in the usual way.

Lemma 8. 1. *A nonabelian simple subgroup of $E_7(p^n)_{\mathrm{ad}}$ (or $E_7(p^n)_{\mathrm{sc}}$) is either a group of Lie type in characteristic p or one of the following*:

(1) *$L_2(r^m)$ with $r^m \in \{7, 8, 11, 13, 16, 17, 19, 25, 27, 29, 31, 32, 37, 41, 49, 61, 81\}$ or*

(2) $L_3(3)$, $L_3(4)$, $L_3(5)$, $L_3(7)$, $L_4(3)$, $L_5(2)$, $L_6(2)$, $S_4(3)$, $S_4(4)$, $S_4(5)$, $S_4(7)$, $S_4(9)$, $S_6(2)$, $S_6(3)$, $S_8(2)$, $S_8(3)$, $O_7(3)$, $O_8^+(2)$, $F_4(2)$, $G_2(3)$, $U_3(3)$, $U_3(4)$, $U_3(5)$, $U_3(7)$, $U_3(8)$, $U_4(3)$, $U_4(4)$, $U_5(2)$, $U_6(2)$, $U_7(2)$, $O_8^-(2)$, ${}^3D_4(2)$, $Sz(8)$, ${}^2F_4(2)'$ *or*

(3) *A_m with $5 \leqq m \leqq 21$ or*

(4) *a sporadic simple group.*

Proof. For $r \notin \{2, 3, 5, 7, p\}$, the Sylow r-subgroups of $E_7(p^n) := E_7(p^n)'_{\mathrm{ad}}$ are abelian. Simple subgroups of Lie type in characteristic r therefore can only be groups $L_2(r^m)$. The normalizer of a Sylow r-subgroup in $L_2(r^m)$ is a Frobenius group of order $(r^m-1)r^m/2$. Thus, if $L_2(r^m)$ occurs as a subgroup of $E_7(q)$, by Lemma 1. 7 there must exist an element of order $(r^m-1)/2$ in $W(E_7)$. From the Atlas [11], p. 47, the maximal order of any element in $W(E_7) \cong 2 \times S_6(2)$ is 30. This forces $r^m - 1 \leqq 60$, and because of $(r^m-1) \mid 2|W(E_7)|$, only $r^m \in \{11, 13, 17, 19, 29, 31, 37, 41, 61\}$ remain (43 can be excluded because $W(E_7)$ does not contain elements of order 21). As $E_7(q)$ has a modular representation of degree 56 over $\mathbb{F}_q$, the results of [26] yield a list of possible simple subgroups in characteristic $r \in \{2, 3, 5, 7\}$, $r \neq p$. From this, we arrive at (1) and (2).

Now $2 \times S_6(2) \cong W(E_7)$ does not contain elements of order 16, so by the argument in § 6 for $E_6(q)$ we see that for $p \neq 17$ no alternating group A_{19} can be contained in $E_7(q)$. For $p = 17$ we again look at the centralizer of an element of order three. By [14], its composition factors are groups of Lie type A_l, D_l with $l \leqq 6$ or E_6 (possibly twisted versions). None of those contains A_m with $m > 18$ (this is shown for E_6 in the proof of Lemma 6. 1). As in the cases of F_4 and E_6 we can therefore deduce that at most an alternating group A_{21} can be a subgroup of $E_7(q)$.

The lemma is now immediate from the classification of finite simple groups. ■

We are now ready to formulate the main result:

Theorem 8. 1. *The groups $E_7(q)_{\mathrm{ad}}$, $q = p^n$, $p \geqq 5$, $q \equiv -\delta\,(\mathrm{mod}\,3)$, occur as Galois groups over $\mathbb{Q}^{ab}$ for the class structure $\mathfrak{C}^* = (C_p, C_2, C_T^\delta)^*$ (with the respective classes containing elements of orders $(p^?, 2, (q-\delta)(q^6 + \delta q^3 + 1))$). More precisely, a proper field of definition $K^\delta(q)$ has index eighteen in the abelian field $\mathbb{Q}(\zeta_{q^7 - \delta q^6 + \delta q^4 - q^3 + q - \delta})$.*

Proof. With Proposition 8. 1, only the generation of $G = E_7(q)_{\mathrm{ad}}$ by a triple $(\varrho, \sigma, \tau) \in \bar{\Sigma}(\mathfrak{C})$ remains to be proved. Now $T := \langle \tau^{q-\delta} \rangle$ forms a t.i.-Hall subgroup of G, so that $H := \langle \varrho, \sigma \rangle$ has one of the structures given in Lemma 1. 2. The stronger assertion of Lemma 1. 3 does not apply in this case though, because the centralizer of τ is not a Hall subgroup of G.

From the list of centralizers in [14] we immediately get that case (4) of Lemma 1. 2 cannot occur. Furthermore we have $|T| = q^6 + \delta q^3 + 1 \geqq \Phi_9(5) = 15751$, excluding (5). With this, only the local subgroups and the normalizers of simple subgroups remain to be considered. The normalizer of T in G has order $o(\tau) \cdot 18$. Due to $p \geqq 5$ this is prime to p, and we are not in the first case of Lemma 1. 2. For the second case, i.e. $H \leqq \mathcal{N}_G(Z_r^\nu)$, first assume $r \neq p$. The estimate for $|T|$ and Lemma 1. 7(2) show in this case that r either is one of the torsion primes 2 or 3, or we must have $\mu = 0$. As for F_4 and E_6, estimates 2-rank$(G) \leqq 7 + 8$ and 3-rank$(G') \leqq 7 + 3$ can be derived. But $2^{14} = 16384$, $2^{15} = 32768$, $3^9 = 19683$, $3^{10} = 59049$, while $|T| = 15751$ in case $q = 5$ or $|T| \geqq 117307$ for $q \geqq 7$, so we get $\mu = 0$ for all $r \neq p$. Namely, Z_r^ν is contained in $\mathscr{C}_G(T) = T \times Z_{q-\delta}$, whence $r | q - \delta$ and $\nu = 1$. From Table 1 in [14] we find that the centralizer of a subgroup Z_r with $r | q - \delta$ and $T \leqq \mathscr{C}_G(Z_r)$ contains a group $(q-\delta) \cdot E_6^\delta(q)$ (by the choice of δ the possibility $A_2^\delta(q^3)$ is excluded), with normalizer $N := (q-\delta) \cdot E_6^\delta(q) \cdot 2$. Assume $H \leqq N$. Then N contains a $(p^?, 2, (q-\delta)(q^6 + \delta q^3 + 1))$-system of elements. The Schur multiplier of $E_6^\delta(q)$ is trivial for the given congruences, consequently N has to have a normal subgroup isomorphic to $E_6^\delta(q)$. After factorization by this normal subgroup we are left with a dihedral group $(q-\delta) \cdot 2$ of order prime to p. The above triple of elements then reduces to one of the forms (1, 1, 1) or (1, 2, 2). In any case $E_6^\delta(q)$ would have to contain elements of order $(q-\delta)(q^6 + \delta q^3 + 1)/2$, which is not so by [35] for $q - \delta > 2$. This excludes Lemma 1. 2(2) for $r \neq p$.

On the other hand, a p-local H is contained in a maximal parabolic subgroup of G by Lemma 1. 7(1). The only maximal parabolics of G with order divisible by $(q^6 + \delta q^3 + 1)$ have the form $Q := P \cdot (q-\delta) \cdot E_6^\delta(q)$, where P denotes some p-group. If H is contained in Q, the same arguments as before apply. Namely, Q has a $(p^?, 2, (q-\delta)(q^6 + \delta q^3 + 1))$-system, which, after factoring out the p-group P, gives similar system for $(q-\delta) \cdot E_6^\delta(q)$. This was already shown to lead to a contradiction above.

Hence only the cases (3) and (6) of Lemma 1. 2 remain. Obviously, none of the groups Aut(K), for K one of the exceptional groups in Lemma 8. 1, possesses elements of order exceeding 15750. The nonabelian simple group R of Lemma 1. 2 therefore has to be of Lie type in characteristic p. From the theory of primitive divisors in Lemma 1. 5, all such groups apart from $E_6^\delta(q)$, $A_2^\delta(q^3)$ and $E_7(q)$ can be excluded. Moreover this proves that case (6) of Lemma 1. 2 does not occur.

The orders of the elements in the three classes of $\mathfrak{C}$ now finally allow us to arrive at the desired conclusion. Namely, we already have $E_6^\delta(q)$ or $A_2^\delta(q^3)$ normal in H. The outer automorphism groups of those simple groups are either cyclic or dihedral. With an argument as in the local case we derive the contradiction that $E_6^\delta(q)$ or $A_2^\delta(q)$ contains elements of order $(q-\delta)(q^6+\delta q^3+1)$. This only leaves $H=E_7(q)_{\mathrm{ad}}$, proving the theorem. ■

It is an easy step to obtain Galois realizations for the simple groups $G' := E_7(q)'_{\mathrm{ad}}$. The arguments for the descent to this normal subgroup of index two in G can be found in [33] for example. This leaves the field of definition fixed, and we get

Theorem 8. 2. *The simple groups* $E_7(q)'_{\mathrm{ad}}$, $q=p^n$, $p \geqq 5$, $q \equiv -\delta \pmod 3$, *occur as Galois groups over* $\mathbb{Q}^{ab}$ *for the ramification structure* $\mathfrak{C}^* = (C_p, C_p, C_T^\delta)^*$ (*with the respective classes containing elements of orders* $(p^?, p^?, (q-\delta)(q^6+\delta q^3+1)/2)$. *More precisely a proper field of definition* $K^\delta(q)$ *has index eighteen in the abelian field* $\mathbb{Q}(\zeta_{q^7-\delta q^6+\delta q^4-q^3+q-\delta})$.

§ 9. Groups $E_8(q)$ as Galois groups

In $G := E_8(q)$ no class structure containing only semisimple classes and with class number one could be found. So a unipotent class has to be incorporated into the class structure. This leads to the problem that character values are at present only known in good characteristic, i.e. $p \geqq 7$. On the other hand, for certain congruences of the prime p, a rationally rigid class structure for $E_8(p)$ is determined, leading to realizations of these groups as Galois groups over $\mathbb{Q}$. Again, we first compile a list of possible simple subgroups of G.

Lemma 9. 1. *A nonabelian simple subgroup of* $E_8(p^n)$ *is either a group of Lie type in characteristic p or one of the following*:

(1) $L_2(r^m)$ *with* $r^m \in \{7, 8, 11, 13, 16, 17, 19, 25, 27, 29, 31, 32, 37, 41, 49, 61, 64, 81, 125, 128, 243, 343\}$ *or*

(2) $L_3(3)$, $L_3(4)$, $L_3(5)$, $L_3(7)$, $L_3(8)$, $L_3(9)$, $L_4(3)$, $L_4(4)$, $L_4(5)$, $L_5(2)$, $L_5(3)$, $L_6(2)$, $L_6(3)$, $L_7(2)$, $L_8(2)$, $S_4(3)$, $S_4(4)$, $S_4(5)$, $S_4(7)$, $S_4(8)$, $S_4(9)$, $S_6(2)$, $S_6(3)$, $S_6(5)$, $S_6(7)$, $S_8(2)$, $S_8(3)$, $S_{10}(2)$, $S_{10}(3)$, $O_7(3)$, $O_8^+(2)$, $O_8^+(3)$, $O_{10}^+(2)$, $F_4(2)$, $G_2(3)$, $G_2(4)$, $G_2(5)$, $U_3(3)$, $U_3(4)$, $U_3(5)$, $U_3(7)$, $U_3(8)$, $U_3(9)$, $U_3(16)$, $U_4(3)$, $U_4(4)$, $U_4(5)$, $U_5(2)$, $U_5(3)$, $U_5(4)$, $U_6(2)$, $U_6(3)$, $U_7(2)$, $U_8(2)$, $U_9(2)$, $O_8^-(2)$, $O_8^-(3)$, $O_{10}^-(2)$, ${}^3D_4(2)$, ${}^3D_4(3)$, $Sz(8)$, $Sz(32)$, ${}^2F_4(2)'$, *or*

(3) A_m *with* $5 \leqq m \leqq 24$ *or*

(4) *a sporadic simple group.*

Proof. For primes $r \notin \{2, 3, 5, 7, p\}$ dividing the order of $G := E_8(p^n)$, G has an abelian Sylow r-subgroup by Lemma 1. 7. Simple subgroups of Lie type must therefore have the type L_2. The normalizer of a Sylow r-subgroup in $L_2(r^m)$ is a Frobenius group of order $(r^m-1)r^m/2$. For $L_2(r^m)$ to be contained in $E_8(q)$, by Lemma 1. 7(2) there must exist an element of order $(r^m-1)/2$ in the Weyl group $W(E_8)$, $|W(E_8)| = 2^{14}3^5 5^2 7$. By the Atlas [11], p. 85, the maximal element order in $W(E_8) \cong 2 \cdot O_8^+(2) \cdot 2$ is thirty. So we have $r^m - 1 \leqq 60$, and because of the divisibility condition we are left with $r^m \in \{11, 13, 17, 19, 29, 31, 37, 41, 61\}$. A list of possible subgroups of Lie type in characteristic $r \in \{2, 3, 5, 7\}$, $r \neq p$, of G can be obtained from the fact that G has a representation of degree 248 over $\mathbb{F}_q$, using the result of [26]. Excluding those groups isomorphic to alternating groups, one arrives at the parts (1) and (2).

Alternating groups on 23 or more letters contain a Frobenius group of type $23 \cdot 11$, so by Lemma 1. 7(2) they cannot be contained in G in characteristic different from 23. The centralizer of a semisimple element of order three in $E_8(q)$ has as composition factors only groups of Lie type A and D of rank at most eight, E_6, ${}^2E_6$ or E_7, all in characteristic p. The latter contain at most an alternating group A_{21} (see Lemma 6. 1 and 8. 1), while the former have a projective representation of degree at most sixteen over $\overline{\mathbb{F}}_q$. With the argument cited already for F_4, one sees that even for $p = 23$ only A_m with $m \leqq 24$ can occur in G. This completes the proof of the lemma. ■

9. 1. Realizations over $\mathbb{Q}^{ab}$. The classes of semisimple elements in $E_8(q)$ and their centralizers can be found in Table 2 of the paper [14] of Deriziotis. Let C_2 denote the class of involutions with centralizer structure D_8, and C_T a class of elements of order $\Phi_{30}(q) = q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$. The classes of unipotent elements in $E_8(q)$ were determined in [36]: let $C_p := [z_{189}]$ (this corresponds to the class $4A_1$ in [5] and on p. 405 of [8]).

Proposition 9. 1. *For the class structure $\mathfrak{C} = (C_2, C_p, C_T)$ of $E_8(q)$, $q = p^n$, $p \geqq 7$, we have $n(\mathfrak{C}) = 1$.*

Proof. An element $\tau \in C_T$ generates a cyclic Hall subgroup T of G with the property (*) of § 1. 2, as can be seen from the centralizer orders in [14]. To this subgroup, the theory of exceptional characters according to Lemma 1. 4 is applied. Exactly $30 = (\mathcal{N}_G(T) : T)$ of the degrees of unipotent characters of E_8 are prime to $|T| = \Phi_{30}(q)$ ([8], p. 484). So together with the exceptional characters all irreducible characters of G not vanishing on $T^\#$ are found. The Weyl groups of E_8 and D_8 are sufficiently well known by [6], part G, and [20], hence the values of the unipotent characters $\chi_1, \ldots, \chi_{30}$ on the classes C_2 and C_T can be computed with Lemma 1. 8. For the classes of $W(D_8)$ and the fusion into the classes of $W(E_8)$, see Table 9. 1 in [31]. Of the 30 characters, exactly 18 take nonzero values on C_2, while the exceptional characters for T vanish on that class. The values of the unipotent characters on the unipotent class C_p are read off from the tables in [5], using [28], Theorem 1. 5, and [30]; four of them are zero. This leaves 14 irreducible characters of $E_8(q)$ not vanishing on any class of the class structure $\mathfrak{C}$ (see Table 9. 2 in [31]).

With the centralizer orders

$$|\mathscr{C}_G(\varrho)| = q^{100}(q^2-1)(q^4-1)(q^6-1)(q^8-1), \quad |\mathscr{C}_G(\tau)| = \Phi_{30}(q)$$

and

$$|\mathscr{C}_G(\sigma)| = q^{56}(q^2-1)(q^4-1)(q^6-1)(q^8-1)^2(q^{10}-1)(q^{12}-1)(q^{14}-1)$$

for $(\varrho, \sigma, \tau) \in \mathfrak{C}$ we finally have $n(\mathfrak{C}) = 1$. ■

Theorem 9. 1. *The groups $E_8(q)$, $q=p^n$, $p \geqq 7$, occur as Galois groups over $\mathbb{Q}^{ab}$ for the ramification structure $\mathfrak{C}^* = (C_2, C_p, C_T)^*$ (with the respective classes containing elements of orders $(2, p^7, \Phi_{30}(q))$)). More precisely, a proper field of definition $K(q)$ has index 30 in the abelian field $\mathbb{Q}(\zeta_{q^8+q^7-q^5-q^4-q^3+q+1})$.*

Proof. With the result of Proposition 9. 1, only the generation of $G = E_8(q)$ by a triple $(\varrho, \sigma, \tau) \in \bar{\Sigma}(\mathfrak{C})$ is left to be proved. As already mentioned, $T := \langle \tau \rangle$ is a self centralizing Hall subgroup of G. So $H := \langle \varrho, \sigma, \tau \rangle$ is one of the groups in Lemma 1. 3. Moreover by Lemma 1. 6, H is a perfect subgroup of G. Hence it cannot be contained in the solvable normalizer of the torus T. If H were p-local, by Lemma 1. 7(1) it would have to lie in a parabolic subgroup of G. But the orders of these are all prime to $|T| = \Phi_{30}(q)$. Moreover, T cannot act fixed point freely on an elementary abelian r-group for $r \notin \{2, 3, 5, p\}$ by Lemma 1. 7(2). The estimates $2\text{-rank}(G) \leqq 20$, $3\text{-rank}(G) \leqq 12$ and $5\text{-rank}(G) \leqq 10$ are obtained by consideration of suitable semisimple subgroups of G. As $o(\tau) \geqq \Phi_{30}(7) = 6568801$, H can not be 2, 3 or 5-local. (We have $2^{20}-1 = 1048575$, $3^{12}-1 = 531440$, $5^9-1 = 1953124$ and $5^{10}-1 = 9765624$.)

Consequently, H must be a nonabelian simple group. None of the exceptional groups of Lemma 9. 1 has elements of order at least $10^6 < \Phi_{30}(7) \leqq \Phi_{30}(q) = o(\tau)$. So H is a simple group of Lie type in characteristic p. Only those of Lie rank at most eight need to be considered (see the proof of Theorem 5. 1). As $T \leqq H$, we must have $\Phi_{30}(q) \mid |K|$. A look at the order formulae for groups of Lie type produces the following list of possibilities: $A_1(q^{15})$, $A_2(q^{10})$, $A_4(q^6)$, ${}^2A_2(q^5)$, ${}^2A_3(q^5)$, ${}^2A_4(q^3)$, ${}^2A_5(q^3)$, $B_2(q^{15/2})$, $B_3(q^5)$, $B_5(q^3)$, $C_3(q^5)$, $C_5(q^3)$, $D_4(q^5)$, $D_6(q^3)$, ${}^2D_4(q^5)$, ${}^2D_5(q^3)$, ${}^3D_4(q^{5/2})$, $G_2(q^5)$, $F_4(q^{5/2})$ and $E_8(q)$. But except for $E_8(q)$, none of these groups contains a *self centralizing* subgroup of order $|T| = \Phi_{30}(q)$, so that they cannot be subgroups of G. The statement of the theorem is now immediate from Lemma 1. 1. ■

9. 2. Realizations over $\mathbb{Q}$. In the groups $F_4(p)$ the t.i.-torus of order $\Phi_{12}(p)$ contains rational elements of order 13 for infinitely many primes p. While the tori $\Phi_9(p)$ in $E_6(p)$ and $\Phi_7(p)$ in $E_7(p)$ do not contain such rational elements, there exist rational elements in the torus T of order $\Phi_{30}(p)$ of $E_8(p)$ for certain congruence classes of p. Namely, because $(\mathcal{N}_G(T) : T) = 30$ an element of order 31 in T is conjugate to all its primitive powers, so it is rational. We have $31 \mid \Phi_{30}(p)$ exactly if p is a primitive root modulo 31. This happens for about one fourth of all primes. There is another suitable t.i.-torus T in $E_8(p)$, of order $\Phi_{15}(p)$, which contains rational elements of order 31 if p is the square of a primitive root modulo 31. Thus for about half of all primes (in the sense of the theorem of Dirichlet), Galois realizations of $E_8(p)$ over $\mathbb{Q}$ can be obtained. To ease notation, let

$$\mathcal{P}_1 := \{p \in \mathbb{P} \mid p \equiv 3, 11, 12, 13, 17, 21, 22, 24 \pmod{31}\}$$

and

$$\mathcal{P}_2 := \{p \in \mathbb{P} \mid p \equiv 7, 9, 10, 14, 18, 19, 20, 28 \pmod{31}\},$$

i.e. $\mathcal{P}_1$ (resp. $\mathcal{P}_2$) contains all primes such that $31 \mid \Phi_{30}(p)$ ($31 \mid \Phi_{15}(p)$ respectively). Define $C_{31} := [\tau^{o(\tau)/31}]$, where τ generates a maximal torus of order $\Phi_{30}(p)$ if $p \in \mathcal{P}_1$ (of order $\Phi_{15}(p)$ if $p \in \mathcal{P}_2$ respectively). The other classes are taken from the first section.

Proposition 9. 2. *For the class structure $\mathfrak{C} = (C_2, C_p, C_{31})$ of $E_8(p)$, $p \geqq 7$, $p \in \mathcal{P}_1 \cup \mathcal{P}_2$, we have $n(\mathfrak{C}) = 1$.*

Proof. In the case of $p \in \mathscr{P}_1$ this was already proved in Proposition 9. 1, because then an element of C_{31} is contained in a maximal torus T of order $\Phi_{30}(p)$. The irreducible characters of $G := E_8(p)$ different from the exceptional characters are constant on $T^{\#}$. So $n(\mathfrak{C}) = 1$ follows from the values calculated in the proof of Proposition 9. 1.

In the case $p \in \mathscr{P}_2$ one first convinces oneself with the list of centralizers in [14], Table 2, that $\langle \tau \rangle =: T$ is a Hall subgroup with the property (*) of Section 1. 2. Applying Lemma 1. 4, a comparison with the list of degrees of unipotent characters of G in [8], p. 484, leads to thirty nonexceptional irreducible characters of G not vanishing on C_{31}. Their values on the three classes are calculated in the usual way with Lemma 1. 8, Table 9. 1 of [31] and with the help of a computer. The results for those characters not vanishing on any of the three classes are given in Table 9. 3 of [31]. Again we find $n(\mathfrak{C}) = 1$. ■

The proof of generation becomes a bit more delicate in comparison with the first section, because now we lack the semisimple element of large order. Only the order of the unipotent elements in the class C_p gets larger for increasing p. For small p we therefore can not expect to prove generation. Let $\mathscr{P} := \{p \in \mathscr{P}_1 \cup \mathscr{P}_2 \mid p \geqq 43 \text{ and } p \neq 127\}$.

Theorem 9. 2. *The groups $E_8(p)$, $p \in \mathscr{P}$, occur as Galois groups over $\mathbb{Q}$ for the ramification structure $\mathfrak{C}^* = (C_2, C_p, C_{31})^*$ (with the respective classes containing elements of orders $(2, p^7, 31)$).*

Proof. We already know that $T := \mathscr{C}_G(\tau)$ has the structure of a cyclic t.i.-Hall subgroup of $G := E_8(p)$. Therefore the assertion of Lemma 1. 3 applies to the present situation.

The order of the Weyl group $|W| = 2^{14} 3^5 5^2 7$ of G is not divisible by $|T| = 31$. Furthermore, for the given congruences, 31 is a primitive divisor of $\Phi_{30}(p)$ or $\Phi_{15}(p)$ in the sense of Lemma 1. 5. This excludes the parabolic subgroups of G as possibilities for $H := \langle \varrho, \sigma, \tau \rangle$, $(\varrho, \sigma, \tau) \in \bar{\Sigma}(\mathfrak{C})$. By Lemmas 1. 3 and 1. 6, H must either be one of the simple groups of Lemma 9. 1 or a r-local subgroup for $r \in \{2, 3, 5\}$. But 31 does not divide any $3^m - 1$ for $m \leqq 12$, and so τ can not act fixed point freely on an elementary abelian 3-group. If H is 2- or 5-local with socle $E := Z_r^m$, then $\mathscr{N}_G(E)/\mathscr{C}_G(E) =: \bar{H}$ is generated by a $(2, p^7, 31)$-system of elements. Moreover the simple top factor K of a composition series for $\bar{H}$ must also have a $(2, p^7, 31)$-system. In particular, the order of K is divisible by p and 31, and therefore K acts nontrivially on E. This means that p must divide some $2^{5k} - 1$, $k \leqq 4$, or $5^{3k} - 1$, $k \leqq 3$. But the only prime factors of these numbers greater than 41 are 151 and 829. Both of these do not lie in $\mathscr{P}$. Therefore H is no local subgroup of G.

Hence H is one of the nonabelian simple groups in Lemma 9. 1. The Lie groups in characteristic different from p may be excluded by divisibility properties, namely, none of them has order divisible by 31 and by some $p \in \mathscr{P}$. Because 31 does not divide the order of any A_n, $n \leqq 23$, H is none of the alternating groups in Lemma 9. 1. Only six sporadic simple groups have orders divisible by 31; they are $O'N$, Ly, Th, J_4, B and M. Of these, J_4, B and M possess elements of order 23 conjugate to 11 or 22 of their primitive powers, which is only possible in $E_8(23)$, but $p = 23$ was excluded. The only prime $r \geqq 43$ dividing the orders of the remaining three groups is $r = 67$, but this is not contained in $\mathscr{P}$. Again, we are left with the groups of Lie type in the same characteristic. As already mentioned, 31 is a primitive divisor of $\Phi_{30}(p)$, $\Phi_{15}(p)$ respectively. The arguments in the proof of Theorem 9. 1 carry over immediately to exclude all cases but $H = E_8(p)$. The theorem then follows from Lemma 1. 1. ■

§ 10. Concluding remarks

It was already mentioned in the introduction that the only simple groups which are not known to be Galois groups over abelian number fields are those exceptional groups of Lie type not treated in this work. This illuminates the importance of the Rationality Criterion of Matzat and Thompson given in § 1. 1. It might now be asked whether the remaining cases can be handled with the same criterion. We will give some heuristic arguments why this may not be possible, at least not so for the Suzuki groups

$$^2B_2(2^{2n+1}) = Sz(2^{2n+1}).$$

To explain this, we first have to tell which considerations lead to the choices for the class structures $\mathfrak{C}$ in the previous paragraphs. The aim was always the proof of $n(\mathfrak{C}) = 1$ and then the application of Lemma 1. 1. The character theoretic formula for $n(\mathfrak{C})$ consists of a sum over all irreducible characters of G, multiplied by a factor, namely the order of G divided by the three centralizer orders. At least one of the summands in the character sum is known: the one coming from the trivial character $\chi = 1$ obviously takes value 1. Assuming that, for large q, this is the dominant term of the sum, we have to choose $\mathfrak{C}$ such that the extra factor also equals 1 for $q \longrightarrow \infty$. Writing the group order and the centralizer orders as polynomials in q, this means that the degrees of the centralizer order polynomials must add up to the degree of the polynomial giving the group order. Indeed, for all examples in this work, the three classes were chosen in this way, and no case was found with $n(\mathfrak{C}) = 1$ for an infinite family of values for q where this condition was not satisfied. Thus, for class structures according to this heuristic condition, asymptotically the trivial character often yields the relevant part of the character sum.

The Suzuki groups $Sz(2^{2n+1})$ have a very transparent structure. Their character table and their maximal subgroups were determined by Suzuki more than 25 years ago. Thus all ingredients for the application of Lemma 1. 1 are known. But one immediately finds out that the heuristic condition on the centralizer orders of elements from three classes can only be satisfied if two of the classes contain involutions. But then the generated group is known to be dihedral. So no "good" class structure exists. In $G := Sz(q)$ there exist only six different types of conjugacy classes. This makes it possible to compute $n(\mathfrak{C})$ for all triples of conjugacy classes in G. And, as should be expected by the above heuristic, the structure constants are polynomials in q of degree at least one. Furthermore it is not hard to prove that the contribution to these structure constants coming from proper subgroups are too small to diminish this growth rate for $l^i(\mathfrak{C})$. (The parts of $n(\mathfrak{C})$ coming from the maximal subgroups of type $Sz(2^{2m+1})$ are known inductively; they grow not as quickly as $n(\mathfrak{C})$.) From this it can be seen that the Suzuki groups cannot be realized as Galois groups with the help of Lemma 1. 1. A better criterion is needed.

However in the smallest group, $Sz(8)$, there exists a class structure with class number one. The notation for the classes is taken from [11].

Theorem 10. 1. *The group $Sz(8) = {}^2B_2(8)$ occurs as a Galois group over the field of index four in $\mathbb{Q}(\zeta_{13})$ for the ramification structure $\mathfrak{C}^* = (2A, 13A, 13B)^*$.*

Proof. With [11], p. 28, one has $n(\mathfrak{C}) = 1$. The only maximal subgroup of $Sz(8)$ containing elements of order 13 is the normalizer of such an element of type $13 \cdot 4$. But this cannot have a (2, 13, 13)-system, so the generation is clear as well. ■

The next open case after the Suzuki groups are the Ree groups ${}^2F_4(2^{2n+1})$ in characteristic 2. For them, not enough is known about the character table at the moment. Only in the smallest case, the Tits group ${}^2F_4(2)'$, a Galois realization was found.

Theorem 10. 2. *The group* $Ti = {}^2F_4(2)'$ *occurs as a Galois group over* $\mathbb{Q}(\sqrt{13})$ *for the ramification structures* $\mathfrak{C}_1^* = (2A, 3A, 13A)^*$ *and* $\mathfrak{C}_2^* = (2A, 5A, 13A)^*$.

Proof. With the character table on p. 75 of [11] we check $n(\mathfrak{C}_1) = n(\mathfrak{C}_2) = 1$. The maximal subgroups of $G := {}^2F_4(2)'$ are also given there. Only $L_3(3) \cdot 2$ and $L_2(25) \cdot 2$ possess orders divisible by 13. As the group generated by a triple $(\varrho, \sigma, \tau) \in \bar{\Sigma}(\mathfrak{C}_j)$ is perfect by Lemma 1. 6, only the groups $L_3(3)$ and $L_2(25)$ themselves remain as candidates. Both contain exactly one class of involutions, which therefore fuses into $2A$ of G. But because of $A_5 \cong L_2(5) < L_2(25)$, $L_2(25)$ has a (2, 3, 5)-system, while $n(2A, 3A, 5A)_G = 0$. This excludes $L_2(25)$. The group $L_3(3)$ contains elements of order six which must fuse into $6A$ of G. But in G we have $(6A)^3 = 2B$. So every triple in $\bar{\Sigma}(\mathfrak{C}_j)$ generates G and the assertion follows. ■

References

[1] *T. Asai*, Unipotent characters of exceptional groups over $\mathbb{F}_q$ with small q, Comm. Algebra **11** (1983), 2203—2220.

[2] *M. Aschbacher, D. Gorenstein, R. Lyons, M. O'Nan, L. Sims, W. Feit* eds., Proceedings of the Rutgers group theory year, 1983—1984, Cambridge 1984.

[3] *G. V. Belyi*, On Galois extensions of a maximal cyclotomic field, Math. USSR-Izv. **14** (1980), 247—256.

[4] *G. V. Belyi*, On extensions of the maximal cyclotomic field having a given classical Galois group, J. reine angew. Math. **341** (1983), 147—156.

[5] *W. M. Beynon, N. Spaltenstein*, Computation of the Green functions of simple groups of type E_n ($n = 6, 7, 8$), Computer Centre Report no. 23, University of Warwick, England.

[6] *A. Borel* et al., Seminar on algebraic groups and related finite groups, Lect. Notes in Math. **131**, Berlin-Heidelberg-New York 1970.

[7] *A. Borel, J. Tits*, Éléments unipotents et sous-groupes paraboliques de groupes réductifs, Invent. Math. **12** (1971), 95—104.

[8] *R. W. Carter*, Finite groups of Lie type: Conjugacy classes and complex characters, Chichester 1985.

[9] *B. Chang*, The conjugate classes of Chevalley groups of type (G_2), J. Algebra **9** (1968), 190—211.

[10] *B. Chang, R. Ree*, The characters of $G_2(q)$, Symposia Mathematica **XIII**, London (1974), 395—413.

[11] *J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson*, Atlas of finite groups, Oxford 1985.

[12] *B. N. Cooperstein*, Maximal subgroups of $G_2(2^n)$, J. Algebra **70** (1981), 23—36.

[13] *P. Deligne, G. Lusztig*, Representations of reductive groups over finite fields, Ann. of Math. **103** (1976), 103—161.

[14] *D. I. Deriziotis*, The centralizers of semisimple elements of the Chevalley groups E_7 and E_8, Tokyo J. Math. **6** (1983), 191—216.

[15] *D. I. Deriziotis, M. W. Liebeck*, Centralizers of semisimple elements in finite twisted groups of Lie type, J. Lond. Math. Soc. **31** (1985), 48—54.

[16] *D. I. Deriziotis, G. Michler*, Character table and blocks of finite simple triality groups ${}^3D_4(q)$, Trans. Am. Math. Soc. **303** (1987), 39—70.

[17] *H. Enomoto*, The conjugacy classes of Chevalley groups of type (G_2) over finite fields of characteristic 2 or 3, J. Fac. Sci. Univ. Tokyo **16** (1970), 497—512.

[18] *H. Enomoto*, The characters of the finite Chevalley group $G_2(q)$, $q = 3^f$, Japan J. Math. N.S. **2** (1976), 191—248.

[19] *W. Feit, P. Fong*, Rational rigidity of $G_2(p)$ for any prime $p > 5$, in [2].

[20] *J. S. Frame*, The characters of the Weyl group E_8, Computational Problems in Abstract Algebra, Oxford (1970), 111—130.

[21] *G. Hoyden-Siedersleben, B. H. Matzat*, Realisierung sporadischer einfacher Gruppen als Galoisgruppen über Kreisteilungskörpern, J. Algebra **101** (1986), 273—286.

[22] *B. Huppert*, *N. Blackburn*, Finite groups III, Berlin-Heidelberg-New York 1982.

[23] *N. Kawanaka*, Generalized Gelfand-Graev representations of exceptional simple algebraic groups over a finite field I, Invent. Math. **84** (1986), 575—616.

[24] *P. B. Kleidman*, The maximal subgroups of the Steinberg triality groups ${}^3D_4(q)$ and of their automorphism groups, J. Algebra **115** (1988), 182—199.

[25] *P. B. Kleidman*, The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree groups ${}^2G_2(q)$ and of their automorphism groups, J. Algebra, to appear.

[26] *V. Landazuri*, *G. M. Seitz*, On the minimal degrees of projective representations of the finite Chevalley groups, J. Algebra **32** (1974), 418—443.

[27] *M. W. Liebeck*, *J. Saxl*, Primitive permutation groups containing an element of large prime order, J. Lond. Math. Soc. **31** (1985), 237—249.

[28] *G. Lusztig*, On the unipotent characters of the exceptional groups over finite fields, Invent. Math. **60** (1980), 173—192.

[29] *G. Lusztig*, Characters of reductive groups over a finite field, Annals of Math. Studies **107**, Princeton 1984.

[30] *G. Lusztig*, On the character values of finite Chevalley groups at unipotent elements, J. Algebra **104** (1986), 146—194.

[31] *G. Malle*, Exzeptionelle Gruppen vom Lie Typ als Galoisgruppen, Dissertation, Karlsruhe 1986.

[32] *B. H. Matzat*, Konstruktion von Zahlkörpern mit der Galoisgruppe M_{12} über $\mathbb{Q}(\sqrt{-5})$, Arch. Math. **40** (1983), 245—254.

[33] *B. H. Matzat*, Konstruktion von Zahl- und Funktionenkörpern mit vorgegebener Galoisgruppe, J. reine angew. Math. **349** (1984), 179—220.

[34] *B. H. Matzat*, Zum Einbettungsproblem der algebraischen Zahlentheorie mit nicht abelschem Kern, Invent. Math. **80** (1985), 365—374.

[35] *K. Mizuno*, The conjugate classes of Chevalley groups of type E_6, J. Fac. Sci. Univ. Tokyo **24** (1977), 525—563.

[36] *K. Mizuno*, The conjugate classes of unipotent elements of the Chevalley groups E_7 and E_8, Tokyo J. Math. **3** (1980), 391—461.

[37] *H. Pahlings*, Some sporadic groups as Galois groups, Rendiconti del seminaro Mat. dell'Universita di Padova, to appear.

[38] *T. Shoji*, The conjugacy classes of Chevalley groups of type (F_4) over finite fields of characteristic $p \neq 2$, J. Fac. Sci. Univ. Tokyo **21** (1974), 1—17.

[39] *T. Shoji*, On the Green polynomials of a Chevalley group of type F_4, Comm. Algebra **10** (1982), 505—543.

[40] *W. Simpson*, *J. Frame*, The character tables for $SL_3(q)$, $SU_3(q)$, $PSL_3(q)$, $U_3(q)$, Can. J. Math. **25** (1973), 486—494.

[41] *N. Spaltenstein*, Caractères unipotents de ${}^3D_4(\mathbb{F}_q)$, Comment. Math. Helvetici **57** (1982), 676—691.

[42] *J. G. Thompson*, Finite groups with fixed-point-free automorphisms of prime order, Proc. Nat. Acad. Sci. U.S.A. **45** (1959), 578—581.

[43] *J. G. Thompson*, Some finite groups which appear as $\mathrm{Gal}(L/K)$, where $K \subseteq \mathbb{Q}(\mu_n)$, J. Algebra **89** (1984), 437—499.

[44] *J. G. Thompson*, Some finite groups of type G_2 which appear as Galois groups over $\mathbb{Q}$, preprint.

[45] *H. N. Ward*, On Ree's series of simple groups, Trans. Am. Math. Soc. **121** (1966), 62—89.

[46] *K. Zsigmondy*, Zur Theorie der Potenzreste, Monatsh. Math. **3** (1892), 418—443.

Fachbereich 3/Sekretariat MA 8-1, TU Berlin, Straße des 17. Juni 135, D-1000 Berlin 12

Eingegangen 12. Januar 1988