On the size and structure of finite linear groups.

Boris Weisfeiler

Pennsylvania State University
University Park, PA 16802

Supported by NSF.

1. Introduction.

Our object here is to study linear, and, except in Section 14, finite groups. Our results concern mostly the size of such groups although some other, structural, results are obtained as well. The departure point for the present work was a result of M. Nori [ ] which can be considered as a conceptual refinement of Jordan's theorem on linear groups. It turned out that the methods used in [MVW] and [V] (and based on classification of finite simple groups) can be used to generalize, extend, and strengthen both Nori's [Proposition 21] and Jordan's theorem. Most of the present work is dedicated to obtaining the best bounds for our version of Jordan's theorem. This turned out to be quite difficult, especially because of necessity to specially handle groups in small dimensions. A qualitative result is much easier to obtain, see B. Weisfeiler [NAS].

Before going on to the statements of our results let us introduce some terminology. For a field k we denote by $p(k)$ the characteristic exponent of k, that is $p(k) = \text{char } k$ if $\text{char } k > 0$ and $p(k)=1$ if $\text{char } k = 0$. A 1-group and a group of Lie 1-type are both trivial. If $p\neq 1$ is a prime then a group of Lie p-type is a group of Lie type of characteristic p (see Section 4 for more detail). A group is said here to be centrally simple if its quotient by the center is simple. Two groups are centrally isomorphic if their quotients by the centers are isomorphic. $O_p(G)$ is, as usual, the largest normal p-subgroup of G.

Let k denote an algebraically closed field of characteristic exponent p. Our version of Jordan's theorem is

(1.1) Theorem (see (13.1)). Let G be a finite subgroup of $GL_n(k)$. Then G contains

(i) a normal subgroup $T \supseteq O_p(G)$,

(ii) a normal subgroup $L \supseteq T$

such that

(a) $T/O_p(G)$ is a commutative p'-group isomorphic to a product of $\leq n$ cyclic groups;

(b) L/T is isomorphic to a direct product of finite simple groups of Lie p-type;

(c) $|G/LT| \leq \begin{matrix} n^4(n+2)! & \text{if} & n \leq 63 \\ (n+2)! & \text{if} & n > 63 \end{matrix}$

If $p=1$ then $O_p(G) = 1$ and $L/T = 1$ and we obtain the usual statement of Jordan's theorems:

Theorem. If $p=1$ then G contains a normal commutative subgroup B that $|G/B| \leq f(n)$.

The best $f(n)$ known until our paper (B. Weisfeiler [ ]) was obtained by G. Frobenius (see A. Speiser [, Satz 201]); it was $f(n)=n!n\ 12^{n(\pi(n+1)+1)}$ where $\pi(n)$ is the number of primes $\leq n$. Recall that $\pi(n) \sim n/\ell n\ n$. Thus our estimate is of the type $n^{\text{const}\cdot n}$ and G. Frobenius' is of the type $n^{\text{const}\cdot n^2/(\ell n\ n)^2}$.

When $p\neq 1$ our result implies that of R. Brauer and W. Feit:

Theorem (see W. Feit [book, Theorem X1.1.2]). If p^m is the order of the Sylow p-subgroup of G then G contains a normal commutative p'-subgroup B such that $|G/B| \leq f(p,m,n)$ for an appropriate function of three variables.

Our Theorem (1.1) gives the above theorem with $f(p,m,n)=p^{3m}\cdot n^4\cdot (n+2)!$ (see (13.2)). This, of course, improves the estimate of R. Brauer and W. Feit. But it seems also noteworthy that our function $f(p,m,n)$ shows once again that the deviation of characteristic >0 case from characteristic 0 case is concentrated in the p-subgroup. Thus our $f(p,m,n)$ is a product of the cube of the order of the Sylow p-subgroup with a function independent of p and m.

Following H. Bass [J. Alg.] and using results of J. Tits [Free] and very recent classification of periodic simple linear groups (see, e.g., S. Thomas[vol. 41]) we can obtain the following structure result

(1.2) Theorem (see (14.1)). Let G be a subgroup of $GL_n(k)$. Then G contains

(i) a triangulizable normal subgroup T,

(ii) a normal subgroup $P \supseteq T$

(iii) a normal subgroup $F \supseteq T$

(iv) a normal subgroup $L \supseteq T$

such that

(a) the Zariski closures of P/T and F/T are connected and semi-simple,

(b) P/T is simple periodic of Lie p-type,

(c) $[P,F] \subseteq T$ and F has a certain minimality property,

(d) L/T is simple finite of Lie p-type,

(e) $|G/PFL| \le n^4(n+2)!$

An interesting feature of this result (except for the estimate) is that it exhibits a decomposition of linear groups into P and F parts.

A version of (1.1) for primitive groups is more precise:

(1.4) Theorem (see(11.1)). Let G be a primitive subgroup of $GL_n(k)$ with center C. Then G contains

(i) a normal subgroup A isomorphic to a direct product of alternating groups Alt_{m_i}, $m_i \ge 10$,

(ii) a normal perfect subgroup L centerally isomorphic to a direct product of finite simple groups of Lie p-type, such that

$$|G/ACL| \le n^{2\log_2 n+5}.$$

In other words this theorem says that unlimited growth of $|G/C|$ comes from groups of Lie p-type and the growth of type $n^{c\cdot n}$ comes from the alternating groups. The order of the remaining part is only of the type $n^{c\cdot \ell n\, n}$, i.e., incomparably smaller. This result should be, perhaps, compared with a result of P. Cameron [, Theorem 6.1], where one sees an estimate $n^{c\cdot \ell n \ell n\, n}$ on the order of a primitive group, other than some specified groups.

Our proof of (1.4) begins with a study of centrally simple linear groups.

(1.5) Proposition (see ( )). Let G be a finite centrally simple non-commutative subgroup of $GL_n(k)$. Suppose that G is not of Lie p-type and not isomorphic to an alternating group. Then

$$|\mathrm{Aut}\ G| \le n^4(2n+1)^{2\log_3(2n+1)+1}$$

This result has relevance to the study of maximal subgroups of finite groups of Lie p-type, $p > 1$ or, the same, of the primitive permutation representations of the latter). In particular, one can combine (1.5) with the results of M. Aschbacher [ ] and M. Liebeck [ ]. (I am grateful to M. Liebeck for making his paper available to me before publication):

(1.6) Theorem. Let H_0 be a classical simple group of Lie p-type ${}^cX_a(q^c)$ and H a subgroup of $\mathrm{Aut}\ H_0$ with $H \supseteq H_0$. Let G be a maximal subgroup of H. Then one of the following holds:

(a) G is "known" (a list, called $\mathcal{C}_H$, of these G is given in M. Aschbacher [ ]),

(b) the socle of G is simple of Lie p-type and $|G| \le q^{3cn}$, where n is the dimension of the natural representation of ${}^cX_a$,

(c) the socle of G is an alternating group,

(d) the socle of G is simple and $|G| \le n^4(2n+1)^{2\log_3(2n+1)+1}$

Note that the estimate in (b) has the type $q^{\mathrm{const}\cdot n} = n^{\mathrm{const}\cdot n/\ell n\, n}$ (with the latter constant increasing with q). Thus again there is a wide gap between the estimates in (b) and (d). Of course, the type of the estimate in (b) can not be substantially improved. Thus it seems desirable to separate cases (b), (c), and (d).

Another implication for maximal subgroups gives the follwing, rougher

(1.7) Proposition. Let H_0 be a simple group of Lie p-type ${}^cX_a(q^c)$ and H a subgroup of Aut H_0 with $H \supseteq H_0$. Let G_0 be a perfect centrally simple group and G a subgroup of Aut G_0 with $G \supseteq G_0$. If G is a maximal subgroup of H then one of the following holds

(a) G_0 is of Lie p-type,

or (b) G_0 is an alternating group,

or (c) $|G| \le r^4(2r+1)^{2\log_3(2r+1)+1}$

where r =	$n+1$	$2n$	$2n+1$	7	26	27	56	248
if X_a =	A_n	$C_n, \mathcal{D}_n$	B_n	G_2	F_4	E_G	E_7	E_8

This follows directly from (1.5) applied to the composite of $G_0 \to {}^cX_a(\bar{\mathbb{F}}_p) \to GL_r(\bar{\mathbb{F}}_p)$. Since, when q varies, the tower of groups ${}^cX_a(q^c)$ is infinite, it follows that groups in (b) and (c) can be maximal only for finitely many q:

(1.8) Theorem (see). In the assumptions of (1.7) there exists r, depending on ${}^{c}X_{a}$ (and not on p), such that if $q > p^{r}$ and G (as in (1.7)) is maximal in H then G_{0} is of Lie p-type.

We give in ( ) explicit values for r when H is of classical type.

2. Notation and preliminaries.

(2.1) Some of terminology and notation was introduced in Section 1.

(2.2) If M is a group and X a subset of M then $Z_M(X)$ (resp. $N_M(X)$, $C(M)$, Aut M, Aut_c M, Out M) denotes the centralizer of X in M (resp. the normalizer of X in M, the center of M, the group of automorphisms of M, the group of authomorphisms of M trivial on $C(M)$, the group of outer automorphisms of M). Occasionally we also write $NZ_M(X)$ for $N_M(X)/Z_M(X)$ and, in the case when X is a group, $\overline{NZ}_M(X)$ for $N_M(X)/X\cdot Z_M(X)$.

(2.3) The symmetric and alternating groups on n letters (resp. on a set X) are denoted Sym_n and Alt_n (resp. Sym X and Alt X).

(2.4) $\mathbb{N}$ is the set of non-negative integers. $\mathbb{Z}/a$ is the cyclic group of order a.

(2.5) $\log x$ (resp. $\ell n\ x$) denotes $\log_2 x$ (resp. the natural logarithm of x). $\Gamma(x)$ denotes the Γ-function of x, so that $\Gamma(n+1)=n!$ when $n \in \mathbb{N}$. We often use notation $f(x)$ for

$$f(x) = (2x+1)^{2\log_3(2x+1)+1} ;$$

it is one of our main functions.

(2.6) Our notation for the parameter of twisted groups of Lie type agrees with that of R. Steinberg [ ] and, therefore, differs from that of other authors, see (4.1.1) below.

(2.7) In our study we will need repeatedly the precise knowledge of centrally simple groups having faithful linear representations of the given degree. These are listed below in Table T2.7. In this table $a \cdot G$ denotes a perfect central extension of G by $\mathbb{Z}/a$; however, if $a \cdot G$ appears in characteristic p with $p \mid a$ then it should be read as $(a/p) \cdot G$; $a \cdot G(p=\ell)$ means that this group appears only in characteristic ℓ. This Table is compiled from W. Feit [Nice , §8.4] and A. Zalessky [1987, §13]. See Table T6.3 for different isomorphisms.

Table 2.7.

Centrally simple linear groups of small degree.

n	$G \le GL_n(k)$, $p(k) = p$		
	(almost) any p	sporadic p	Lie p-type
2	$2 \cdot Alt_5$		$A_1(p^a)$
3	Alt_5, $6 \cdot Alt_6$, $\bar{A}_1(7)$	$3 \cdot Alt_7(p=5)$	$A_2(p^a)$, $\bar{A}_1(p^a)$, ${}^2A_2(p^{2a})$
4	$Alt_5(p \ne 5)$, $6 \cdot Alt_6$, $2 \cdot Alt_7$	$Alt_6(p=2)$, $Alt_7(p=2)$	$A_3(p^a)$, ${}^2A_3(p^{2a}$, $B_2(p^a)$,
	$2 \cdot Alt_5$, $2 \cdot \bar{A}_1(7)$, $2 \cdot \bar{B}_2(3)$	$4 \cdot \bar{A}_2(4)(p=3)$	${}^2B_2(2^{2a+1})(p=2)$, $A_1(p^a)(p>3)$
			$\bar{A}_1(p^a)(a \ge 2)$
5	$Alt_5(p \ne 2)$, $Alt_6(p \ne 2,3)$, $\bar{A}_1(11)$, $\bar{B}_2(3)$	$Alt_7(p=7)$, $M_{11}(p=3)$	$A_4(p^a)$, ${}^2A_4(p^{2a})$, $\bar{B}_2(p^a)$
			$\bar{A}_1(p^a)(p \ge 5)$

3. Estimates for the alternating groups.

Let k be a field and $p=p(k)$ its characteristic exponent. We quote here some results of I. Schur, L. E. Dickson, and A. Wagner.

(3.1) Proposition. Let $H \simeq \mathrm{Alt}_m$. Let $\varphi : H \to GL_n(k)$ be a faithful irreducible representation.

(i) If $p=1$ and $m \geq 4$, $m \neq 5$, then $n \geq m-1$; for $m=5$, $n \geq 3$;

(ii) if $m \geq 9$ or $p\neq 2$ and $m \geq 7$ then $n \geq m-2$; moreover, if $p \nmid m$ then $n \geq m-1$;

(iii) if $m=5$ (resp. 6,7,8) then $n \geq 2$ (resp. 3,4,4).

Proof. (3.1 (i)) is a result of I. Schur [, §44]; (3.1) (ii) and (iii) are results of A. Wagner [,] (although essentially known from L. E. Dickson [ ]). See G. D. James [, Theorem 6 (ii)] for (ii) when $m \geq 10$. When $m=9$ see A. Wagner [,] and when $p\neq 2$, $m \geq 7$, see A. Wagner [ ]. To see (iii) we note that $\mathrm{Alt}_5 \simeq SL_2(\mathbb{F}_4)$ and has therefore a 2-dimensional representation in characteristic 2; $\mathrm{Alt}_6 \simeq PSL_2(\mathbb{F}_9)$ and has therefore an irreducible 3-dimensional (= adjoint) representation in characteristic 3, but it does not have, by Table T2.7 (the list of linear groups of small degree), representations of dimension 2; $\mathrm{Alt}_8 \simeq \mathcal{D}Sp_4(\mathbb{F}_2)$ and has therefore a representation of dimension 4 in characteristic 2, but, again by Table T2.7 it does not have smaller representations; Alt_7 has by above a 4-dimensional representation in characteristic 2, but by Table T2.7 it has no smaller representations.

(3.2) Coroolary. Let H, φ, and n be as in (3.1). If $n \geq 8$ then $|H| \leq (n+2)!/2$.

(3.3) Proposition. Let $H \simeq Alt_m$. Let $\varphi : H \to PGL_n(k)$ be a faithful projective irreducible reprsentation. Suppose that φ does not lift to a linear representation of H.

(i) If $p=1$, $m \geq 4$, $m \neq 6$, then $m \leq 2 + 2 \log n$; if $p=1$, $m=6$, then $n \geq 3$;

(ii) for all p and $m > 7$ we have $m \leq (81 + 32 \log n)/15 \leq 5.4 + 2.134 \log n$

(iii) for all p and $4 \leq m \leq 16$ we have

m	4	5	6	7	8	9	10	11	12	13	14	15	16
n≥	2	2	3	3	8	8	8	16	16	16	32	32	128

Proof. (3.3) (i) is a result of I. Schur [, §44]. To prove (ii) and (iii) write $m = 2^{w_1} + 2^{w_2} + \ldots + 2^{w_s}$, $w_1 > \ldots > w_s$, for the 2-adic decomposition of m. Then by A. Wagner [Theorem 1.3 (ii)] we see that $2^{[\frac{m-s-1}{2}]} | n$ if $m > 7$. For $7 < m \leq 16$, $m \neq 11$, this gives us the estimate in (iii). For m=5,6,7 the estimates in (iii) follow from Table 2.7 (of linear groups of small degree). For m=4 clearly $n \geq 2$ since Alt_4 is not commutative. For m=11 we get s=3 whence $8|n$. Suppose n=8. Consider in $H \simeq Alt_{11}$ the subgroup $H_1 \times H_2 \simeq Alt_8 \times Alt_3$. We know that φ lifts to a linear representation $\tilde{\varphi} : \widetilde{Alt}_{11} \to GL_8(k)$ where $\widetilde{Alt}_{11}$ is the (non-split) double cover of Alt_{11} (I. Schur [§5, Theorem II]). Let $\pi : \widetilde{Alt}_{11} \to Alt_{11}$ be the covering map. Then the relations (I. Schur [, §5, relations (IV)]) show that $\pi : \pi^{-1}(H_1) \to H_1$ is the non-split double cover of Alt_8. Since n=8 the representation will be irreducible for H_1 (by (3.1)(iii) with m=8). Since $H_2 \simeq \mathbb{Z}/3$ and $\text{Ker}\,\pi \simeq \mathbb{Z}/2$ it follows that $\pi^{-1}(H_2) \simeq \mathbb{Z}/3 \times \mathbb{Z}/2$. Therefore $\tilde{\varphi}(\pi^{-1}(H_2))$ commutes with $\tilde{\varphi}(\pi^{-1}(H_1))$. Since the latter is irreducible, $\tilde{\varphi}(\pi^{-1}(H_2)) \subseteq k\mathrm{Id}_8$. But then $\tilde{\varphi}(\pi^{-1}(H_2))$ is in the center of $\tilde{\varphi}(\pi^{-1}(H))$, an impossibility. Returning to the general m we see that $s \leq \log(m+1)$. Since

$\log(x+1)$ is a convex function it is bounded from above by a tangent line at any point. Thus $s \le \log(m+1) \le (m+49)/16$ (where we took the tangent at $x=15$.

Thus $n \ge 2^{[\frac{m-\log(m+1)-1}{2}]}$, or $[\frac{m-\log(m+1)-1}{2}] \le \log n$ or $2 + 2\log n \ge m - \log(m+1) \ge m - (m+49)/16 = (15m-49)/16$. This gives $m \le (81 + 32\log n)/15$ whence (ii).

(3.4) Corollary. Let H, φ, n, m be as in (3.3). If $n \ge 2, m \ge 4$, then $|\mathrm{Aut}\, H| \le (2n+1)^{2\log_3(2n+1)+1}$.

Proof. Recall that $\mathrm{Aut\,Alt}_m \simeq \mathrm{Sym}_m$ if $m \ge 4, m \ne 6$, (see B. Huppert [ ]) and $|\mathrm{Aut\,Alt}_6| = 2 \cdot 6!$. Now our claim is verified directly for cases of (3.3) (iii) using Table TA (values of functions for small arguments). If $m > 16$ we have by (3.3)(ii) that

$$|\mathrm{Aut}\, H| = m! \le m \cdot (m/e)^m = e \cdot (m/e)^{m+1} \le 2.72 \cdot (2+0.8\log n)^{6.4+2.134\log n}.$$

So it is sufficient to check that

$$2.72(2 + 0.8\log n)^{6.4+2.134\log n} < (2n+1)^{2\log_3(2n+1)+1}$$

for $n \ge 128$.

Now $\log_3 x = \log x/\log 3$. Therefore

$$(2n+1)^{2\log_3(2n+1)+1} > (2n+1)^{1.26\log(2n+1)+1}$$

$$> (2n)^{1.26\log(2n)+1} = (2n)^{1.26\log n + 2.26} =$$

$$2^{2.26} \cdot n^{1.26} \cdot n^{1.26 \log n + 2.26} > 4.79\, n^{1.26 \log n + 3.52}$$

$$> 4.79\, n^{1.26(\log n + 2.79)}.$$

On the other hand

$$2.72(2 + 0.8 \log n)^{6.4+2.134 \log n} < 2.72(2 + 0.8 \log n)^{2.3(\log n+2.79)}$$

Thus it suffices to establish that

$$2.72(2 + 0.8 \log n)^{2.3(\log n+2.79)} < 4.79\, n^{1.26(\log n + 2.79)}$$

or $$(2 + 0.8 \log n)^{2.3} < n^{1.26}$$

or $2 + 0.8 \log n < n^{0.547}$. This holds for $n=128$. On the other hand if $f(x) := 2 + 0.8 \log x - x^{0.547}$ then $f'(x) = 0.8/x - 0.547\, x^{-0.453} < 0$ for $x \geq 128$. Thus $f(x) < 0$ for $x \geq 128$ whence our claim.

4. Recollections and preliminaries about groups of Lie type.

We use R. Steinberg [ ] as basic reference for groups of Lie type. In particular, we denote by ${}^cX_a(m^c)$ the universal group of Lie type ${}^cX_a(m^c)$. As usual when $c = 1$ we just write $X_a(m)$. The groups $\mathcal{D}{}^cX_a(m^c)$ are also considered of Lie type (see (4.3.1)(b) below).

(4.1) Here m is the parameter associated to our group. This m is an integral power $m = q^s$ of a prime q if ${}^cX_a(m^c) \simeq G(\mathbb{F}_m)$ for some simply connected algebraic $\mathbb{F}_m$-group. For groups of type ${}^2B_2 = {}^2C_2$, ${}^2F_4$, and ${}^2G_2$ m^c is an <u>odd</u> power of a prime, $m = q^s$, $2s \in \mathbb{N}$, $s \notin \mathbb{N}$.

(4.1.1) N.B. Some authors to whom we refer (Gorenstein, Landazuri, and Seitz among them) use m differently. For them "${}^cX_a(m)$" is our ${}^cX_a(m^c)$ except when ${}^cX_a = {}^2B_2, {}^2F_4, {}^2G_2$. For these latter groups their notation ${}^2X_a(m^2)$ coincides with ours but then they write all related expressions (e.g. the order) as functions of m^2 (and not of m as we do).

(4.2) When m^c is a power of a prime q we say that q is a characteristic of ${}^cX_A(m^c)$ or of a perfect group centrally isomorphic to ${}^cX_a(m^c)$ and $\mathcal{D}{}^cX_a(m^c)$ or that these are of Lie q-type. Note that q generally depends not on the central isomorphism class of (an abstract group) ${}^cX_s(m^c)$ but on its representation as ${}^cX_a(m^c)$, see (4.3.2) below. We write $q = q({}^cX_a(m^c))$, $q = q(\mathcal{D}{}^cX_a(m^c))$ etc.

(4.3) We denote by ${}^c\overline{X}_a(m^c)$ the central quotient of ${}^cX_a(m^c)$.

(4.3.1) ${}^{c}\overline{X}_a(m^c)$ is simple non-commutative except in the following cases

(a) $\overline{A}_1(2)$, $\overline{A}_1(3)$, ${}^{2}\overline{A}_2(4)$, ${}^{2}\overline{B}_2(2)$ are solvable;

(b) the derived group of $B_2(2)$, $G_2(2)$, ${}^{2}F_4(2)$, ${}^{2}G_2(3)$ is simple non-commutative of prime index q (where q is as in (4.2)).

See R. Steinberg [, Theorems 5 and 34 and comments on them].

(4.3.2) The central quotients of the following groups are (sporadically) isomorphic to groups of Lie type in different characteristic or to alternating groups:

$$A_1(4),\ A_1(5),\ A_1(7),\ A_1(8),\ A_1(9),$$
$$A_2(2),\ A_3(2),\ B_2(3),\ {}^{2}A_2(9),\ {}^{2}A_3(4).$$

The isomorphisms are given in Table T6.3.

See R. Steinberg [, Theorem 37].

When ${}^{c}\overline{X}_a(m^c)$ is simple non-commutative we denote by ${}^{c}\widetilde{X}_a(m^c)$ the universal cover of ${}^{c}\overline{X}_a(m^c)$. The kernel of the canonical map ${}^{c}\widetilde{X}_a(m^c) \to {}^{c}X_a(m^c)$ is called the Schur multiplier.

(4.3.3) (a) ${}^{c}\widetilde{X}_a(m^c)$ is isomorphic to ${}^{c}X_a(m^c)$ except in the following cases

$A_1(4)$, $A_1(9)$, $A_2(2)$, $A_2(4)$, $A_3(2)$,

$B_2(2)$, $B_3(2)$, $B_3(3)$, $D_4(2)$, $F_4(2)$,

$G_2(2)$, $G_2(4)$, ${}^2A_3(4)$, ${}^2A_3(9)$,

${}^2A_5(4)$, ${}^2E_6(4)$

(b) In any case (exceptional or not) the kernel of ${}^c\tilde{X}_a(m^c) \to {}^cX_a(m^c)$ is a q-group where $m^c = q^s$ and q is a prime. It holds for any q for which ${}^c\overline{X}_a(m^c)$ happens to be of Lie q-type.

See R. Steinberg [, 1] or D. Gorenstein [, Table 4.1, p. 302], where the kernel of ${}^c\tilde{X}_a(m^c) \to {}^c\overline{X}_a(m^c)$ is also explicitly given.

Table T4.4

${}^{c}X_a$	$d(X_a)$	b	A_g	A_d	upperbound on
	see 4.4.1	see 4.4.2	see 4.5	see 4.5	$c\|A_d\|\|A_g\|$
A_1	3	1	1	$\mathbb{Z}/(2,m-1)$	2
$A_n, n\geq 2$	n^2+2n	n	$\mathbb{Z}/2$	$\mathbb{Z}/(n+1,m-1)$	2(n+1)
$B_2, q=2, m\neq 2$	10	2.5	$\|A_g\|=2$	1	2
$B_n, q\neq 2, n\geq 2$	$2n^2+n$	2n-2	1	$\mathbb{Z}/2$	2
$C_n, q=2, n\geq 3$	$2n^2+n$	2n-2.3	1	1	1
$C_n, q\neq 2, n\geq 3$	$2n^2+n$	n	1	$\mathbb{Z}/2$	2
D_4	28	5	Sym_3	$(\mathbb{Z}/(2,m-1))^2$	24
$D_n, n\geq 5$	$2n^2-n$	2n-3	$\mathbb{Z}/2$	$\begin{cases}(\mathbb{Z}/(2,m-1))^2, n \text{ even}\\ \mathbb{Z}/(4,m^n-1), n \text{ odd}\end{cases}$	8
E_6	78	11	$\mathbb{Z}/2$	$\mathbb{Z}/(3,m-1)$	6
E_7	133	17	1	$\mathbb{Z}/(2,m-1)$	2
E_8	248	29	1	1	1
F_4	52	10	$\begin{cases}\|A_g\|=2 \text{ if } q=2\\ 1 \quad \text{if } q\neq 2\end{cases}$	1	2
G_2	14	3	$\begin{cases}\|A_g\|=2 \text{ if } q=3\\ 1 \quad \text{if } q\neq 3\end{cases}$	1	2
${}^2A_n, n\geq 2$	n^2+2n	n	1	$\mathbb{Z}/(n+1,m+1)$	2(n+1)
${}^3D_4$	28	5	1	1	3
${}^2D_n$	$2n^2-n$	2n-3	1	$\begin{cases}(\mathbb{Z}/(2,m+1))^2, n \text{ even}\\ (\mathbb{Z}/(4,m^n+1)), n \text{ odd}\end{cases}$	8
${}^2E_6$	78	15	1	$\mathbb{Z}/(3,m+1)$	6
${}^2B_2$	10	3	1	1	2
${}^2F_4$	52	10	1	1	2
${}^2G_2$	14	4	1	1	2

(4.4) For a group ${}^cX_a(m^c)$ of Lie type we denote by $d = d(X_a)$ the dimension of the corresponding algebraic group of type X_a. The numbers $d = d(X_a)$ are listed in Table T4.4.

(4.4.1) $$|{}^cX_a(m^c)| \le m^d.$$

This is known (and can be easily checked by looking at a table of the orders e.g. in D. Gorenstein [, Table 2.4, p. 135]).

For groups not listed in (4.3.2) we denote by $\ell = \ell({}^cX_a(m^c))$ the smallest degree of centrally faithful irreducible representations of ${}^c\tilde{X}_a(m^c)$ (or, the same, faithful irreducible projective representations of ${}^c\overline{X}_a(m^c)$) over all fields of characteristic different from $q = q({}^cX_a(m^c))$.

(4.4.2) Except for cases listed below $\ell({}^cX_a(m^c)) \ge (m^b-1)/2$ where $b = b({}^cX_a(m^c))$ is the number of given in the 3rd column of Table T4.4

Exceptions: $A_1(4)$, $A_1(9)$, $A_2(4)$, $B_2(2)$, $B_3(3)$, $D_4(2)$, $F_4(2)$, ${}^2A_3(9)$, ${}^2B_2(8)$, ${}^2E_6(4)$.

This can be readily deduced from V. Landazuri and G. Seitz [, p. 419]. The estimates we give are generally worse than the ones given there. The advantage (for us) of our form for degrees is that they are given by a uniform expression.

Using Table T4.4 one can verify now that (with d and b as in (4.4.1) and (4.4.2))

(4.4.3) (a) $d \le 2b^2 + b$

(b) $d \leq b^2 + 2b$ if either ${}^cX_a$ is different from $C_n(C_2=B_2, C_1=A_1)$ or m^c is even.

(4.5) Suppose that ${}^cX_a(m^c)$ is not listed in (4.3.1)(a). Let $A = A({}^cX_a(m^c))$ denote the group $\mathrm{Out}({}^cX_a(m^c))$ of outer automorphisms of ${}^c\overline{X}_a(m^c)$ i.e. $A := (\mathrm{Aut}({}^cX_a(m^c)))/{}^c\overline{X}_a(m^c)$. By R. Steinberg [ ] (see D. Goremstein and R. Lyons [, 7] for explicit information) we know that A contains two subgroups (possibly trivial): A_d and A_f, and a subset A_g.

A_g is the set of graph automorphisms of ${}^cX_a$ (see R. Steinberg [, Corollary to Theorem 29, Theorem 36, and subsequent remarks to both]); A_q is given in column 4 of Table T4.4; it is a group unless ${}^cX_a$ is B_2, F_4 or G_2 and characteristic is 2,2, or 3 respectively in which case A_gA_f is a cyclic group generated by the non-trivial element of A_g;

A_d, the group of diagonal automorphisms (see R. Steinberg [, Lemma 58 and proof of Theorem 36]); A_d is given in column 5 of Table T4.4;

A_f, the group of field automorphisms, (see R. Steinberg [, just above Theorem 30]).

(4.5.1)(a) A_f is isomorphic to the Galois group of $\mathbb{F}_{m^c}$ over its prime field $\mathbb{F}_q$,

(b) $A_f \simeq \mathbb{Z}/s$ where $s = c \cdot \log_q m$.

Proof. (a) is the definition. Writing $m^c = q^s$ we get (b).

(4.5.2)(a) $A = A_dA_fA_g$;

(b) A_d is normal in A

(c) A_g can be taken to commute with A_f.

(d) $\mathcal{D}^3 A = \{1\}$, and $\mathcal{D}^2 A = \{1\}$ unless ${}^cX_a = D_4$.

Proof. (a) is known from R. Steinberg [, Theorems 30 and 36]. (b) is evident from definitions (since A_d can always be chosen to come from a maximal twist-invariant torus, see J.Tits [ ]). Since $A_g \neq 1$ implies that $c = 1$ we can assume in the proof of (c) that $X_a(m) = G(\mathbb{F}_m)$ where G is defined over the prime field $\mathbb{F}_q$. Then $A_g \subseteq (\mathrm{End}\ G)(\mathbb{F}_q)/(\mathrm{Inn}G)(\mathbb{F}_q)$ whence (c) evidently follows. Now (d) follows from (c) if one inspects columns 4 and 5 of Table T4.4

(4.5.3) $$|{}^cX_a(m^c)| = |{}^c\overline{X}_a(m^c)| \cdot |A_d|$$

See R. Steinberg [, Exercise (b) in the end of §10 and Corollary to Theorem 35] or D. Gorenstein and R. Lyons [, (7-1)(g)]

(4.5.4) In the notation of (4.4.2) we have except for groups from (4.3.1) (a):

(a) $$|A| \leq \begin{cases} 4.8 \log((m^b-1)/2) & \text{if } {}^cX_a = D_4 \text{ and } q = 2 \\ 3.03 \log((m^b-1)/2) & \text{if } {}^cX_a \neq D_4 \text{ or } q \neq 2 \\ 2 & \text{if } m^b \leq 8 \end{cases}$$

(b) $$|A_gA_f| \leq \begin{cases} 1.2 \log((m^b-1)/2 & \\ 2 & \text{if } m^b \leq 8 \end{cases}$$

Proof. Set $x := (m^b-1)/2$. Comparing columns 3 and 6 of Table T4.4 we see that

$$c|A_d|\cdot|A_g| \le \begin{cases} 4.8b & \text{if } {}^cX_a = D_4 \\ 3b & \text{otherwise} \end{cases}.$$

For ${}^cX_a = D_4$ we have $c|A_d||A_g| = 4.8b = 4.8\log_m(2x+1)$. Therefore using (4.5.1)(b) we have

$$|A| = |A_f||A_d||A_g| = c\log_q m \cdot |A_d||A_g|$$

$$= 4.8(\log_q M)\log_m(2x+1) = 4.8\log_q(2x+1)$$

$$\le \begin{cases} 4.8\log(2x+1) & \text{if } q = 2 \\ 4.8\log_3(2x+1) & \text{if } q \ge 3. \end{cases}$$

Since $4.8\log_3(2x+1) = (4.8/\log 3)\log(2x+1) < 3.03\log(2x+1)$ we have (for ${}^cX_a = D_4$)

$$|A| \le \begin{cases} 4.8\log(2x+1) & \text{if } q = 2 \\ 3.03\log(2x+1) & \text{if } q \ge 3. \end{cases}$$

If ${}^cX_a \ne D_4$ then $c|A_d||A_g| \le 3b$ whence $c|A_d||A_g| \le 3\log_m(2x+1)$ and

$$|A| = |A_f||A_d||A_g| = c\log_q m\ |A_d||A_f|$$

$$\le 3(\log_q m)\log_m(2x+1) = 3\log_q(2x+1) \le 3\log(2x+1).$$

This establishes the first two lines of (a).

The cases $m^b \leq 8$ for exception of those listed in (4.3.1)(a) are treated in Table T4.5.4 below which directly follows from Columns 4, 5, and 3 of Table T4.4. The remaining part of (a) follows from Table T4.5.4

Table T4.5.4

G	$A_1(4)$	$A_1(5)$	$A_1(7)$	$A_2(2)$	$B_2(2)$	$A_3(2)$	$G_2(2)$	${}^2A_3(4)$
A	A_f	A_d	A_d	A_g	A_g	A_g	$\{1\}$	A_f
$\|A\|$	2	2	2	2	2	2	1	2
x	1.5	2	3	1.5	1.5	3.5	3.5	3.5

To prove (b) we procede similary. We have $c|A_g| \leq 1.2b = 1.2 \log_m(2x+1)$ by comparing columns 3 and 4 of Table T4.4. Then

$$|A_gA_f| = |A_f||A_g| = (c \log_q)|A_g| \leq$$

$$1.2(\log_q m)(\log_m(2x+1))$$

$$= 1.2 \log_q(2x+1) \leq 1.2 \log(2x+1).$$

This together with a glance at Table T4.5.4 proves (b).

(4.5.5) Corollary. In the notations of (4.4.2) we have, except for groups from (4.3.1)(a):

(a) $|A| < ((m^b-1)/2)^2$

(b) $|A_gA_f| \leq (m^b-1)/2$ except for $A_1(4)$, $A_2(2)$, $B_2(2)$.

Proof. Set $x = (m^b-1)/2$. The inequality $4.8 \log(2x+1) < x^2$ for $x \geq 4$ (i.e. $m^b \geq 9$) together with a glance at Table T4.5.4 implies (a). Similarly, the inequality $1.2 \log(2x+1) < x$ for $x \geq 4$ and another glance at Table T4.5.4 yield (b).

(4.5.6) Remark. (4.5.5) is much rougher than (4.5.4). However when we try to extend our estimates to products of groups (in Section 9) the use of logarithmic estimates for factors still leads (at least by our methods) to power estimates for the product.

5. Estimates for groups of Lie type in their characteristic.

Let k be an algebraically closed field of characteristic $p \geq 2$ and $L \simeq {}^{c}X_a(m^c)$, $m^c = p^s$, a universal finite group of Lie p-type.

Consider a non-trivial irreducible representation $\varphi : L \to GL_n(k)$ and set $N := N_{GL_n(k)} L$. We have the following chain of natural homomorphisms:

$$N \to \text{Aut } L \to \text{Out } L \to A_f$$

(where we use the notation of (4.5)). Let N_f be the image of N in A_f.

(5.1) Proposition. $n \geq d^t$ where d is given in Table T5.1 below and $t := \max\{1, |N_f|/c\}$.

Table T5.1

X_a	A_a	B_a	C_a	D_a	E_6	E_7	E_8	F_4	G_2
d	a+1	2a	2a	2a	27	56	240	24	6

(5.2) Corollary. The image of N in Out L has order $\leq \begin{cases} 6 & \text{if } X_a = A_2,\ n=3 \\ n \log n & \text{otherwise} \end{cases}$

Proof. By (5.1) we have $|N_f|/c \leq \log_d n$. Therefore by (4.52)

$$|N| \leq |A_d| \cdot |A_g| \cdot |N_f| \leq c\ |A_d|\ |A_g| \cdot \log_d n.$$

Comparing tables T4.4 (where we have to take n=a) and T5.1 we see

$$c|A_d|\ |A_g| \leq \begin{cases} 3d & \text{if } X_a = D_4 \\ 2d & \text{otherwise} \end{cases}$$

Thus for $X_a = D_4$ we have

$$|N| \leq 3d \log_d n = 24 \cdot \log_8 n = (24/\log 8)\log n = 8 \log n \leq n \log n.$$

In the remaining cases

$$|N| \leq 2d \log_d n = 2(d/\log d)\log n \leq (2/\log d)\ n \log n$$

When $d \geq 4$ this gives $|N| \leq n \log n$. If $d=3$ then the type is A_2 and $|N| \leq 2(d/\log d)\log n = (2/\log 3)\ 3 \log n$

$$\begin{cases} = 6 & \text{if } n = d = 3 \\ \leq (2/\log 3) \cdot (3n/4)\log n < n \log n & \text{if } n \geq 4. \end{cases}$$

Finally, if $d=2$ then the type is A_1 and $c|A_d||A_g| = 2$ whence $|N| \leq 2 \log n \leq n \log n$. This concludes the proof of (a).

(5.3) Lemma. Let G be an algebraic k-group of type X_a and $\varphi : G \to GL_n$ its non-trivial irreducible rational representation over k. Then $n \geq d$ where d is as in Table T5.1.

Proof. Let b be the highest weight of φ and let $R := R(\varphi)$ be the set of all weights of φ. Then the Weyl group of G acts on R and, therefore, $|Wb| \leq |R| \leq n$. Let P be a parabolic subgroup of G corresponding to b (the stabilizer of the weight space of weight b) and W_P the subgroup of W corresponding to P. Then W_P is the stabilizer of b. Hence $n \geq |W/W_P|$. An easy case analysis gives that $\min\{|W/W_P|,\ P \text{ parabolic}\} = d$ whence our claim.

(5.4) Proof of 5.1. For a representation φ of $L := {}^cX_a(m^c)$ and a homomorphism $\alpha : \mathbb{F}_{m^c} \to k$ (such α is, automatically, a power of the Frobenius $\mathbb{F}r$) one can define a new (in general) representation $\varphi \circ \alpha$ of L by $\varphi \circ \alpha(\ell) = \varphi(\alpha(\ell))$ (see R. Steinberg [, 5] or [, 12.13]).

By R. Steinberg [, Theorems 7.4, 9.3, 12.2] there exists a set M of irreducible representations of L over k such that every other representation φ can be uniquely obtained as a tensor product $\varphi \simeq \bigotimes_{i=0}^{r} \varphi_i \circ \mathbb{F}r^i$, where $\varphi_i \in M$, $i=0,1,\ldots,r$ and $r=(s/c)-1$ unless ${}^cX_a = {}^2B_2, {}^2F_4, {}^2G_2$, and in this latter case $r=s-1$.

Now let $\bar{x}$ be a generator of N_f and x its preimage in N. The x acts on L as $y \cdot \mathbb{F}r^z$ where $y \in \operatorname{Ker}(N \to A_f)$ and $0 \leq z \leq s$. It is clear that replacing in the above decomposition $\varphi = \otimes \varphi_i \circ \mathbb{F}r^i$ the maps $\mathbb{F}r^i$ by $y_i \circ \mathbb{F}r^i$ where y_i are fixed (for every $i=0,1,\ldots,r$) automorphisms of L from $\operatorname{Ker}(\operatorname{Aut} L \to A_f)$ does not affect the claim. Thus there is still uniqueness and existence of decompositions $\varphi = \bigotimes_{i=0}^{r} \varphi_i \circ y_i \circ \mathbb{F}r^i$.

Let us take φ to be our representation from the beginning of this Section. Every $i=0,1,\dots,r$ we write as $i=i_1+zi_2$ with $0 \le i_1 < z$. Then we set $y_i \circ \mathbb{F}r^i := (y \circ \mathbb{F}r^z)^{i_2} \circ \mathbb{F}r^{i_1}$. Since the action of x normalizes φ and in view of uniqueness of the tensor product decomposition we must have $\varphi_{j_1} \simeq \varphi_{j_2}$ of $j_1 \equiv j_2 \pmod z$ and $0 \le j_1, j_2 \le r$. This shows that the tensor product, if non-trivial, contains at least as many non-trivial as there are integral multiples of z between 0 and r. In view of the expression for r given above we see that this number is $\ge z/c$.

Thus $\dim \varphi \ge \max (d_1^{z/c}, d_1)$ where d_1 is the minimal dimension of a non-trivial irreducible k-representation of L. By R. Steinberg [, Theorem 43] each irreducible k-representation of L is a restriction of one of G (where G is as in (5.3)) whence by (5.3) $d_1 \ge d$ and (5.1) is proved.

(5.5) Our proof gives an apparently stronger statement. Define the action of Out L on the set of equivalence classes of representations of L by $(\varphi\circ\alpha)(\ell) := \varphi(\tilde{\alpha}(\ell))$ for φ an representation, $\alpha \in \text{Out } L$, $\ell \in L$; here $\tilde{\alpha}$ is a lift of α to Aut L. Let $(\text{Out } L)_\varphi$ be the stabilizer of the equivalence class of φ in Out L.

Proposition. In the notation of (5.1)

$$|(\text{Out } L)_\varphi| \le \begin{cases} 6 & \text{if } X_a = A_2,\ n=3 \\ n \log n & \text{otherwise.} \end{cases}$$

6. Estimates for groups of Lie type in non-equal characteristic.

Let k be an algebraically closed field of characteristic exponent $p=p(k)$. Let G be a finite simple group of Lie q-type, $q\neq p$, q a prime. To avoid trouble with different characteristics (see (4.3.2)) we fix an isomorphism $G \simeq {}^c\bar{X}_a(m^c)$ and write $m^c=q^s$. Set $H := \mathcal{D}G$. Set $f(t) := (2t+1)^{2\log_3(2t+1)+1}$.

(6.1) Proposition. Let $\varphi : H \to PGL_n(k)$ be a faithful irreducible projective representation. Then

(a) $|H| \leq f(n)$ except for the cases

$H \simeq {}^2\bar{A}_3(9)$ and $n=6$ when $|H| \leq 1.58\, f(6)$;

and $H \simeq D_4(2)$ and $n=8$ when $|H| \leq 4.62\, f(8)$

(b) $|\text{Aut } H| \leq n\, f(n)$ except for the following cases

$n =$	2	2	4	6	8
$H \simeq$	Alt_6	$A_1(8)$	$\bar{A}_2(4)$	${}^2\bar{A}_3(9)$	$D_4(2)$
$\lvert\text{Aut } H\rvert \leq$	2.6f(2)	2.71f(2)	4.1f(4)	12.61f(6)	27.69f(8)

(c) $|\text{Out } H| \leq n^2$;

(d) $|N_{PGL_n(k)}(\varphi(H))| \leq n\, f(n)$ except when $H \simeq D_4(2)$ and $n=8$

(6.2) Lemma. If H is not centrally isomorphic to one of the groups listed in (4.3.1), (4.3.2), and (4.4.2) then

$$|{}^cX_a(m^c)| \leq f(n)$$

Proof. By (4.4.2) $n \geq (m^b-1)/2$, i.e. $m^b \leq 2n+1$. Since ${}^2B_2(2)$, ${}^2F_4(2)$, and ${}^2G_2(3)$ are excluded by (4.3.1) we have $m \geq 2$ and, therefore, $b \leq \log(2n+1)$. If we exclude type C_r, $r \geq 2$, in odd characteristic we have by (4.4.1) and (4.4.3) (b)

$$|{}^cX_a(m^c)| \leq m^d \leq m^{b^2+2b} = (m^b)^{b+2} \leq (2n+1)^{\log(2n+1)+2}$$

For the type C_r, $r \geq 2$, in odd characteristic we have $m \geq 3$ whence $b \leq \log_3(2n+1)$ whence by (4.4.1) and (4.4.3) (a)

$$|{}^cX_a(m^c)| \leq m^d \leq m^{2b^2+b} = (m^b)^{2b+1} \leq (2n+1)^{2\log_3(2n+1)+1}$$

Note that the first occurrences of this latter case are for $(r,m) = (2,3)$ (resp. (2,5), (3,3)), $(m^b-1)/2 = 4$ (resp. 12, 13).

In general we have, therefore, that $|{}^cX_a(m^c)| \leq \max\left\{(2n+1)^{2\log_3(2n+1)+1}, (2n+1)^{\log(2n+1)+2}\right\}$. One easily sees that $(2n+1)^{2\log_3(2n+1)+1} \geq (2n+1)^{\log(2n+1)+2}$ if $n \geq 7$. For $n \leq 6$ the difference can come only from groups of type C_r, $r \geq 2$, in odd characteristic. As we remarked the first such groups occur at n=4,12,13. One has $|B_2(3)| = 2 \cdot 25{,}920 \leq f(4)$. Therefore both functions give valid estimates for $n < 12$. Therefore $f(n)$ can be taken for an estimate for all n.

Table T6.3

Group M	M is centrally isomorphic to	Order modulo center	min n	LS estimate	Adjusted estimate	min non-Lie-p-type n	Out M	Schur multiplier of M/center
$A_1(4)$	$A_1(5)$, Alt_5	60	2	2	2	2	$\mathbb{Z}/2$ $(=A_f)$	$\mathbb{Z}/2$
$A_1(5)$	$A_1(4)$, Alt_5	60	2	2	2	2	$\mathbb{Z}/2$ $(=A_d)$	$\mathbb{Z}/2$
$A_1(7)$	$A_2(2)$	168	2	$3(p\neq 7)$	$2^{b)}$	$3^{d)}$	$\mathbb{Z}/2$ $(=A_d)$	$\mathbb{Z}/2$
$A_1(8)$	$\mathcal{D}(^2G_2(3))$	504	2	$7(p\neq 2)$	$2^{b)}$	7	$\mathbb{Z}/3$ $(=A_f)$	$\mathbb{Z}/2$
$A_1(9)$	$\mathcal{D}B_2(2)$, Alt_6	360	2	$3(p\neq 3)$	$2^{b)}$	3	$\mathbb{Z}/2\times\mathbb{Z}/2$ $(=A_d\times A_f)$	$\mathbb{Z}/2\times\mathbb{Z}/3$
$A_2(2)$	$A_1(7)$	168	2	$2(p\neq 2)$	$2^{b)}$	$3^{d)}$	$\mathbb{Z}/2$ $(=A_g)$	$\mathbb{Z}/2$
$A_3(2)$	Alt_8	20,160	4	$7(p\neq 2)$	$4^{c)}$	7	$\mathbb{Z}/2$ $(=A_g)$	$\mathbb{Z}/2$
$\mathcal{D}B_2(2)$	$A_1(9)$, Alt_6	360	2	$2(p\neq 2)$	$2^{b)}$	$3^{d)}$	$\mathbb{Z}/2\times\mathbb{Z}/2$ $(=A_g\times(H/\mathcal{D}H))$	$\mathbb{Z}/2$
$B_2(3)$	$^2A_3(4)$	25,920	4	$4(p\neq 3)$	$4^{b)}$	$4^{d)}$	$\mathbb{Z}/2$ $(=A_d)$	$\mathbb{Z}/2$
$\mathcal{D}G_2(2)$	$^2A_2(9)$	6,048	3	$3(p\neq 2)^{a)}$	$3^{b)}$	$6^{d)}$	$\mathbb{Z}/3$ $(=H/\mathcal{D}H)$	1
$^2A_2(9)$	$\mathcal{D}G_2(2)$	6,048	3	$3(p\neq 3)$	$3^{b)}$	$6^{d)}$	$\mathbb{Z}/3$ $(=A_f)$	1
$^2A_3(4)$	$B_2(3)$	25,920	4	$4(p\neq 2)$	$4^{b)}$	$4^{d)}$	$\mathbb{Z}/2$ $(=A_f)$	$\mathbb{Z}/2$
$\mathcal{D}(^2G_2(3))$	$A_1(8)$	504	2	$2(p\neq 3)^{a)}$	2^{b}	7	$\mathbb{Z}/3$ $(=H/\mathcal{D}H)$	$\mathbb{Z}/2$

Table T6.3 cont.

$A_2(4)$	20,160	4	$4(p\neq 2)$	same as LS	same as LS	$Sym_3 \times \mathbb{Z}/2 (=A_d A_g A_f)$	$\mathbb{Z}/3 \times \mathbb{Z}/4 \times \mathbb{Z}/4$
$B_3(3)$	$9.17 \cdot 10^9$	13	$27(p\neq 3)$	"	"	$\mathbb{Z}/2\ (=A_d)$	$\mathbb{Z}/2 \times \mathbb{Z}/3$
$D_4(2)$	$1.74 \cdot 10^8$	10	$8(p\neq 2)$	same as LS	8[f]	$Sym_3\ (=A_g)$	$\mathbb{Z}/2 \times \mathbb{Z}/2$
$F_4(2)$	33.10^{15}	33	$44(p\neq 2)$	"	same as LS	$\mathbb{Z}/2\ (=A_g)$	$\mathbb{Z}/2$
$G_2(4)$	$2.5 \cdot 10^8$	10	$12(p\neq 2)$[e]	"	"	$\mathbb{Z}/2\ (=A_f)$	$\mathbb{Z}/2$
${}^2A_3(9)$	$3.26 \cdot 10^6$	7	$6(p\neq 3)$	"	6[d]	$\mathbb{Z}/4 \cdot \mathbb{Z}/2\ (=A_d \cdot A_f)$	$\mathbb{Z}/4 \times \mathbb{Z}/3 \times \mathbb{Z}/3$
${}^2B_2(8)$	29,120	4	$8(p\neq 2)$	"	same as LS	$\mathbb{Z}/3\ (=A_f)$	$\mathbb{Z}/2 \times \mathbb{Z}/2$
${}^2E_6(4)$	$2.3 \cdot 10^{23}$	88	$1500(p\neq 2)$	"	"	$\mathbb{Z}/2\ (=A_f)$	$\mathbb{Z}/3 \times \mathbb{Z}/2 \times \mathbb{Z}/2$
$\mathcal{D}({}^2F_4(2))$	$1.8 \cdot 10^7$	8	$8(p\neq 2)$[a]	"	"	$\mathbb{Z}/2\ (=H/\mathcal{D}H)$	1

(6.3) Proof of (6.1)(a) for the cases omitted in (6.2) is contained in Table T6.3 and for the case $D_4(2)$ which requires special attention in (6.3.2). The upper portion of Table T6.3 handles groups of Lie type which can appear in two different characteristics (see (4.3.2)) or are isomorphic to alternating groups. The lower portion treats groups for which LS-estimates (LS stands for Landazuri-Seitz, see (4.4.2)) do not have the form $(m^b-1)/2$ with b from Table T4.4 (see exceptions in (4.4.2)). Column 4 gives minimal n for which $|M/\text{center}| \le f(n)$ (see (6.3.1) below for explicit formula). Column 6 gives an adjusted estimate on dimensions of projective representations of M; explanantions are given in notes a)-c) below. If Column 6 is larger than min n then (6.1)(a) holds for M/(center). Column 7 gives an estimate (still from below) on dimensions of projective representations of M in such characteristics p for which M/(center) is not isomorphic to a group of Lie p-type; explanations are given in notes below.

Explanations:

a) We took an estimate for G in V. Landazuri and G. Seitz [, p. 419] and divided it by $|G/\mathcal{D}G|$ to obtain an estimate for M = G.

b) The estimate is the minimum over isomorphic groups on the same line as M.

c) See (5.1).

d) See Table T2.7 (groups of small degree).

e) The estimate given in V. Landazuri and G. Seitz [, p. 419] is incorrect for $G_2(4)$. The correct estimate is 12 (personal communication of G. Seitz who also explained how a slip in the proof of Lemma 5.6(b) of the above paper should be corrected).

f) $D_4(2)$ has an 8-dimensional projective representation as the derived group of the Weyl group of E_8, see R. Steinberg [, §11, after Theorem 37].

(6.3.1) Lemma. $\min n$ is the smallest integer $\geq (3^x-1)/2$ where

$$x := \frac{1}{4}\left(-1 + \sqrt{0.5 + 8 \log_3 |M/\text{center}|}\right)$$

Proof. Setting $x=2n+1$ we have to solve $2x^2+x \leq \log_3 |M/\text{center}|$ whence our claim.

(6.3.2) Lemma. $D_4(2)$ does not have faithful irreducible projective representations of dimension 9 over fields of characteristic $p \neq 2$.

Proof. Suppose $\varphi : \tilde{D}_4(2) \to GL_9(k)$, $p \neq 2$, is an irreducible representation. Since the center of $\varphi(\tilde{D}_4(2))$ will be contained then in the center of $SL_9(k)$ which is isomorphic to a subgroup of 9-th roots of 1 and since the center of $\tilde{D}_4(2)$ is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$, it follows that the center of $\varphi(\tilde{D}_4(2))$ is trivial. Thus φ is, in fact, a representation of $D_4(2)$. But then the proof of V. Landazuri and G. Seitz [, Lemma 3.3(2)] gives that $D_4(2)$ has no representations over k of degree ≤ 27, whence our claim.

(6.4) To prove (6.1)(b) we use (4.5.3). Except when H is in the Table T6.3 this gives us that $|\text{Aut } H| = |H| \cdot |A_d| \cdot |A_f| \cdot |A_g| = |{}^cX_a(m^c)| \cdot |A_f||A_g|$ whency by (4.5.5)(b), (4.4.2) and (6.2) $|\text{Aut } H| \leq n\, |{}^cX_a(m^c)|$ whence (6.1)(b). When H is in the Table T6.3 one has to verify (6.1)(b) directly (see Table TA for values of $f(n)$ for small n).

(6.5) The claim of (6.1)(c) is contained in (4.5.4)(a) when (4.4.2) holds for H. In the remaining cases one uses Table T6.3 to verify the claim directly.

(6.6) Of course, (6.1)(d) follows from (6.1)(b) for all but four cases. Set $N := |NZ_{PGL_n(k)}(\varphi(H))|$.

Lemma.

If	$n = 2$	2	4	6
and	$H \simeq Alt_6$	$A_1(8)$	$\bar{A}_2(4)$	$^2\bar{A}_3(9)$
then	$N \leq 720$	504	40,320	6,531,840

(6.6.1) If $H \simeq Alt_6$ and $n=2$ then comparing rows $A_1(9)$ and $\mathcal{D}B_2(2)$ of Table T6.3 we see that $p=3$ so that ours is the natural representation of $SL_2(\mathbb{F}_9)$. The normalizer of $SL_2(\mathbb{F}_9)$ is $GL_2(\mathbb{F}_9) \cdot k^*$, whence $NZ_{PGL_2(k)}\varphi(H) \simeq PGL_2(\mathbb{F}_9)$ and $N = 2|H|$.

(6.6.2) If $H \simeq A_1(8)$ and $n=2$ then comparing rows $A_1(8)$ and $\mathcal{D}(^2G_2(3))$ of Table T6.3 we see that $p=2$ and ours is the natural representation of $SL_2(\mathbb{F}_8)$. The normalizer of $SL_2(\mathbb{F}_8)$ is $GL_2(\mathbb{F}_8) \cdot k^*$ whence $N = |H|$.

(6.6.3) Let now $n=4$ and $H^\sim \subseteq GL_4(k)$ be a perfect group centrally isomorphic to $H \simeq \bar{A}_2(4) \simeq PSL_3(\mathbb{F}_4)$. By Table T2.7 (groups of small degree) we have $p=\text{char } k=3$. Then H contains a subgroup T isomorphic to $\text{Ker}\{N_{\mathbb{F}_{64}/\mathbb{F}_4} : \mathbb{F}_{64}^* \to \mathbb{F}_4^*\}$. Clearly $T \simeq \mathbb{Z}/7$ and $N_H(T)/T$ acts on T as $Gal(\mathbb{F}_{64}/\mathbb{F}_4) \simeq \mathbb{Z}/3$. Let $T^\sim$ be the 7-component of the preimage of T in $H^\sim$. Since $T^\sim$ is a Sylow 7-subgroups of $H^\sim$ we have (by Frattini argument that $N_{GL_4(k)}(H^\sim) = H^\sim \cdot N_{GL_4(k)}(T^\sim)$. We have that $NZ_{GL_n(k)}(T^\sim)/T^\sim$ contains $\mathbb{Z}/3$ and is contained in $\mathbb{Z}/6$. By representation theory of Frobenius groups we have that $|NZ(T^\sim)/T^\sim| \leq 4$ whence $|NZ(T^\sim)/T^\sim| = 3$ and $NZ(T^\sim) \subseteq H$. Since A_g can be assumed to be the transpose-inverse on T we have that then the image of $NZ(T^\sim)$ in $\text{Out } H^\sim = A_d \cdot A_g \cdot A_f$ does not contain A_g. Thus this image is a subgroup of $A_d \cdot A_f \simeq Sym_3$. If it is the whole group $\simeq Sym_3$ then $Z_{GL_4(k)}(\tilde{T})$ contains a subgroup centrally isomorphic to Sym_3. Since all eigenspaces of $\tilde{T}$ are 1-dimensional this is impossible so that the image S of $NZ(\tilde{T})$ in $\mathrm{Out}\ \tilde{H}$ is of order 2 or 3.

If $|S| = 3$ then take the 3-component $\tilde{S}$ of the preimage of S in H. It commutes with $\tilde{T}$ whence by multiplicity 1 of eigenspaces of $\tilde{T}$ we have that $\tilde{S}$ is diagonalizable. But since $|\tilde{S}| = 3$ and char $k = 3$ it follows that $\tilde{S}$ is unipotent. Thus $\tilde{S}=\{1\}$.

(6.6.4) Let $n=6$ and let $\tilde{H} \subseteq GL_6(k)$ be a perfect group centrally isomorphic to $H \simeq {}^2\bar{A}_3(9) \simeq PSU_4(\mathbb{F}_9)$. We have $|H| = 2^7 \cdot 3^6 \cdot 5 \cdot 7 = 3{,}265{,}920$. We assume that $p \neq 3$, i.e., char $k \neq 3$.

Let $\tilde{H} \simeq {}^2\tilde{A}_3(9)$. Then $Z := \mathrm{Ker}({}^2\tilde{A}_3(9) \to {}^2A_3(9)) \simeq (\mathbb{Z}/3)^2$. By D. Gorenstein and R. Lyons [, (7-8)(3)] $\mathrm{Out}\ \tilde{H} \simeq (\mathbb{Z}/4) \cdot (\mathbb{Z}/2)$ (the dihedral group) acts faithfully on Z. It is easy to check then, using elementary representation theory of $\mathrm{Out}\ \tilde{H}$ on Z (: = the dual of Z), that the stabilizer of a point $z \in Z$ in $\mathrm{Out}\ \tilde{H}$ is isomorphic to $\mathbb{Z}/2$.

Let $\varphi : \tilde{H} \to GL_6(k)$, char $k \neq 3$, be an irreducible representation. If $\varphi(Z) = \mathrm{Id}$ then the 3-Sylow subgroup of $\varphi(\tilde{H})$ is the same as that of $H \simeq PSU_4(\mathbb{F}_9)$ and it contains an extraspecial 3-subgroup P of order 3 (consisting of matrices $\begin{bmatrix} 1 & & & 0 \\ a & 1 & & \\ b & 0 & 1 & \\ c & \bar{b} & \bar{c} & 1 \end{bmatrix}$, $a, b \in \mathbb{F}_9$, $c \in \mathbb{F}_3$, in an appropriate basis). By representation theory of P any of its irreducible faithful representations is of degree $9 > 4$. Thus the case $\varphi(Z)=\mathrm{Id}$ is impossible.

Since $\varphi(\tilde{H})$ is irreducible it follows then that $\varphi(Z) \simeq \mathbb{Z}/3$ and consists of scalar matrices. In particular, $\varphi(Z)$ is in the center of $N := N_{GL_6(k)}(\varphi(\tilde{H}))$

whence the image S of N in Out $H^{\sim}$ acts trivially on $\varphi(Z)$ whence $\varphi|Z(\in Z^{\vee})$ is stable under S. By one of the remarks above we have then $|S| \leq 2$, as desired.

(6.7) One may need (and we shall in Section 16) a variation of (6.1)(a):

Proposition. Let G be centrally simple perfect finite subgroup of $GL_n(k)$ of Lie q-type, $q \neq p$. Then $|G| \leq f(n)$ except in the following cases

n	=	2	4	6	8
G	$\simeq$	$2 \cdot \mathcal{D}B_2(2)$	$4 \cdot \bar{A}_2(4)$	$6 \cdot {}^2\bar{A}_3(9)$	$2 \cdot D_4(2)$
G	=	720	80720	$1.96 \cdot 10^7$	$3.48 \cdot 10^8$
p	=	3	$\neq 2$	$\neq 3$	$p \neq 2$
q	=	2	2	3	2

Proof. If G is not centrally isomorphic to a group from (4.3.3)(a) or from Table T6.3 then our claim follows from (6.2). Let $G^{\sim}$ be the universal cover of G. If G is in Table T6.3 one readily verifies that $|G^{\sim}| \leq f(n)$ except for the pairs $(\mathcal{D}({}^2\tilde{G}_2(3)), 2)$ (for $p=2$), $(\mathcal{D}\tilde{B}_2(2), 2)$ (for $p=3$), $(\tilde{A}_2(4), 4)$, $(\tilde{A}_2(4), 5)$, $({}^2\tilde{A}_3(9), 6)$, $({}^2\tilde{A}_3(9), 7)$, $({}^2\tilde{A}_3(9), 8)$, $(\tilde{D}_4(2), 8)$, $(\tilde{D}_4(2), 9)$, $(\tilde{D}_4(2), 10)$. Now note that since G is perfect, its center C is contained in the group of n-th roots of 1. Thus $C \simeq \mathbb{Z}/m$, where $m|(n/p^a)$ where p^a is the highest power of p dividing n. Applying this information to the pairs $(G^{\sim}, n)$ given above and taking into account (6.3.2) one is left only with pairs listed in (6.7).

Now it remains to check the groups from (4.3.3)(a) which are not contained in Table T6.3. These groups, their orders, their centers, and the estimates for the from V. Landazuri and G. Seitz [, p. 419] are

$\tilde{G}$	$\tilde{B}_3(2)$	$\tilde{G}_2(3)$	${}^2\tilde{A}_5(4)$
$\lvert\tilde{G}\rvert$	$2.9 \cdot 10^6$	$1.27 \cdot 10^7$	$1.1 \cdot 10^{11}$
Center $(\tilde{G})$	$\mathbb{Z}/2$	$\mathbb{Z}/3$	$\mathbb{Z}/3 \times \mathbb{Z}/2 \times \mathbb{Z}/2$
LS-estimate	7	14	21
f(LS-estimate)	$9.42 \cdot 10^6$	$2.67 \cdot 10^7$	$6.58 \cdot 10^{12}$

7. Estimates for sporadic groups.

Our purpose here is to obtain estimates from below on the minimal degrees of faithful irreducible projective representations of the 26 sporadic groups. This Section uses references which, often, are not used in other parts of the paper. For this reason we refered directly to many papers without placing them in the list of references at the end of the paper.

My knowledge of sporadic groups is very scanty and, in many cases, the literature on them contains enormous gaps covered by references to unpublished work, lectures, and personal communtications. I had good fortune of being helped in many cases where I was at loss by Robert Griess. I am extremely grateful to him; the arguments he supplied are marked so, some other data refers directly to his <u>personal communitcations</u>. However some of his suggestions were later superceded. Therefore we refer directly only to portion of the many arguments he offered.

We want to keep the estimate $f(x) := (2x+1)^{2\log_3(2x+1)+1}$. This is, however, impossible (as it was for ${}^2A_3(9)$ and $D_4(2)$, see (6.1)), for Suzuki's group Suz and Conway's groups $\cdot 1$ and $\cdot 2$. To give an estimate for these groups we introduce cumbersome functions $F(H,n)$. To define them we use notation (for $a_1, a_2, b \in \mathbb{R}$)

$$y_{a_1,a_2,b}(t) = \begin{cases} 1 & t < a_1 \\ b & a_2 > t \geq a_1 \\ f(t) & t \geq a_2 \end{cases}$$

We also use $\delta_{a,b}$ for the Christoffel symbol.

(7.1) Theorem. Let k be an algebraically closed field of characteristic exponent $p=p(k)$ and $\varphi : H \to PGL_n(k)$ a faithful irreducible projective representation of a sporadic simple group H.

(a) Unless H is centrally isomorphic to Suz, $\cdot 1$, $\cdot 2$, we have

$$|H| \le f(n)$$

(b) $|Suz| \le y_{12,18,\,Suz}(n) =: F(Suz,n)$

$$|\cdot 1| \le y_{24,49,|\cdot 1|}(n) =: F(\cdot 1,n)$$

$$|\cdot 2| \le y_{20,24,|\ 2|}(n) =: F(\cdot 2,n)$$

(7.2) Our proof of (7.1) is mostly contained in Table T7.2. In this table min n (resp. min $\tilde{n}$) is the smallest integer m such that $f(m) \ge |H|$ (resp. $m^{2 \log m + 4.32} \ge |H|$). We will need min n in §10. To obtain estimates we try to find two subgroups H_1 and H_2 and to use their lower estimate to estimate $Cd(H)$. Column "Subgroup" says what subgroups we use and the next column gives a reference to a source where existence of these subgroups is pointed out. The next three columns describe the estimate obtained from H_1 and H_2 and give a reason why such an estimate holds. The possible reasons are listed in 7.3 below. The "adjusted estimate" is generally equal to the minimum of the estimates for H_1 and H_2. If there is another reason for taking the indicated estimate it is given next to the "adjusted estimate". The next three columns describe precise results if such are known to me. The last column gives sometimes an indirect reference; e.g. c) [51] is paper [51] in the list of references of c).

Table 7.2

H	$\|H\|$ (:=b)	min n (=:a_2)	min $\tilde{n}$	Schur multiplier	subgroup	source	estimate	conditions	reason	adjusted estimate (=:a_1)	additional reasons	precise result when known to me	conditions	source
M_{11}	7920	4	4	1						5	see →	5	p=3	a)
M_{12}	$9.50 \cdot 10^4$	5	4	2						6	b)	6	p=3, proj	?
M_{22}	$4.43 \cdot 10^5$	6	5	12						6	b)	6	p=2, proj	Convey p242
M_{23}	$1.02 \cdot 10^7$	8	6	1						11	see →	11		a)
M_{24}	$2.45 \cdot 10^8$	10	7	1						11	see →	11		a)
J_1	$1.76 \cdot 10^5$	5	5	1						6	b)	56 7	p=1 Higman p=11	c) [71]
J_2	$6.05 \cdot 10^5$	6	5	2						6	b)	6	p=1 proj	Feit?
J_3	$5.02 \cdot 10^7$	9	7	1	$19 \cdot 9$ $A_1(16)$	c) p214	9 15	p≠19 p≠2	f) d)	9		85	p=1	c) [73]
J_4	$8.68 \cdot 10^{19}$	58	28	1	2^{1+12} $N(11^{1+2})$	c) pp215 238	64 110	p≠2 p≠11	e) e)	64				
HS	$4.44 \cdot 10^7$	9	7	2	${}^2A_2(25)$ M_{11}	c) p.220	20 10	p≠5 p≠3,11	d) a)	10		22	p=1 linear	c) [42]
Mc	$1.28 \cdot 10^8$	9	7	3	${}^2A_2(25)$ M_{11}	c) p.222	20 10	p≠5 p≠3,11	d) a)	10				
Suz	$4.48 \cdot 10^{11}$	18	11	G	$G_2(4)$ $5^2 \cdot (4 \times Sym_3)$	c) pp221, 222	12 12	p≠2 p≠5	r1) r2)	12		12 143	p=1, proj p=1, linear	c) [90] c) [154]
Ru	$1.46 \cdot 10^{11}$	16	11	2	${}^2A_2(25)$ ${}^2F_4(2)$	c) p224	20 16	p≠5 p≠2	d) d)	16				
He	$4.03 \cdot 10^9$	13	9	1	$7^2 \cdot A_1(7)$ $C_2(4)$	c) p. 221	48 18	p≠7 p≠2	f) d)	18				

Table 7.2 continued

H	$\|H\|$ (:=b)	min n (=:a_2)	min n	Schur multiplier	subgroup	source	estimate	conditions	reason	adjusted estimate (=:a_1)	additional reasons	precise result when known to me	conditions	source
Ly	$5.18 \cdot 10^{16}$	38	20	1	$G_2(5)$ $N(67)$	c) p.223	120 22	p≠5 p≠67	d) f)	110	m)	2480	p=1	c) [93]
ON	$4.61 \cdot 10^{11}$	18	11	3	$A_2(7)$ $31 \cdot 15$	ℓ1)p422 c)p225	48 15	p≠7 p≠31	d) f)	18	ℓ2)	10944 342	p=1, linear p=1, proj.	ℓ1)p461 ℓ1)p468
·1	$4.16 \cdot 10^{18}$	49	24	2	$2^{11} \cdot M_{24}$ $3^6 \cdot (2 \cdot M_{12})$	c)p217	24 24	p≠2 p≠3	g1) g2)	24		24 24	p≠2, proj. p=2, linear	
·2	$4.23 \cdot 10^{13}$	24	14	1	M_{23} $N(5^{1+9})$	c)pp216 217	22 20	p≠2,23 p≠5		20		23 22	p=1 p=2	
·3	$4.96 \cdot 10^{11}$	18	11	1	${}^2A_2(25)$ M_{23}	c)p216	20 21	p≠5 p≠2	d) a)	20		23	p=1	G)[34]
M(22)	$6.46 \cdot 10^{13}$	25	15	6	$B_3(3)$ $2^{10}M_{22}$	c)p218	27	p≠3 p≠2	d)			78	p=1 linear	c)[67]
M(23)	$4.09 \cdot 10^{18}$	49	24	1	$D_4(3)$ $2^{11} \cdot M_{23}$	c)p219	234	p≠3 p≠2	d)			782	p=1	c)[66]
$\mathcal{D}$M(24)	$7.38 \cdot 10^{22}$	83	37	3	$D_4(3)$ $2^{12}M_{24}$	c)p219	234 759	p≠3 p≠2	d) p)	234				
F_5	$2.73 \cdot 10^{14}$	27	16	1	${}^2A_2(64)$ $N(5^{1+4})$	c)p226	56 100	p≠2 p≠5	d) e)	56		133	p=1	c)[54]
F_3	$9.07 \cdot 10^{16}$	39	21	1	$2^{1+8} \cdot Alt_q$ $3^5 \cdot A_1(q)$	c)p225 o)p67	128 80	p≠2 p≠3	n) q)	80		248	p=1	c)[131]
F_2	$4.155 \cdot 10^{33}$	260	89	2	${}^2E_6(4)$ $N(3^{1+8})$	c)p219 o)p68	1536 594	p≠2 p≠3	d) m)	594		196 883 196 882	p 2,3, proj. p=2, linear	m)
F_1	$8.08 \cdot 10^{53}$	1472	343	1	2^{1+24} $3^8 \cdot {}^2D_4(9)$	k)p116	4096 2132	p≠2 p≠3	e) i)	2132		196 883		

(7.3) Reasons.

(a) For the groups M_i, i=11,12,22,23,24, the exact values of degrees of their faithful irreducible (linear) representations in all characteristics are given in

G. James, The modular characters of the Mathien groups, J. Algebra, 27(1973), 57-111.

(b) From the Table T2.7 (groups of small degree) we can obtain the exact value of Cd(H) if it is ≤ 5. Otherwise we have, of course, $Cd(H) \geq 6$.

(c) S. A. Syskin, Abstract properties of the simple sporadic groups, Russian Math. Surveys, 35 : 5(1980), 209-246.

(d) For a group of Lie type we obtain our estimates from V. Landazuri and G. Seitz [, p 419]. Note that the ones we need are, generally, listed as exceptions.

(e) For an extraspecial group (E of order) q^{1+2m}, $m \geq 1$, we have the estimate q^m if $q \neq p$ (see (8.1)). However if $N_H(q^{1+2m}) =: N(q^{1+2m})$ acts transitively on the center q of q^{1+2m} then the estimate becomes $(q-1)q^m$ because $N(q^{1+2m})$ permutes central characters of q^{1+2m} and our claim follows from Clifford theory. N. B. e) can be tricky to use if the Schur multiplier of H is divisible by q: in this case one has to trace what happens with q^{1+2m} after a central extension.

(f) If H contains a subgroup R which is the middle term of $1 \to E \to R \to M \to 1$ with $E = q^m$ (i.e. $E \simeq (\mathbb{Z}/q)^m$) with $p \neq q$ and q a prime which is prime to the Schur multiplier then by Clifford theory the faithful irreducible projective representations of R have degree not less than the minimal length of an orbit of M on the characters of E, i.e. on $E^{v}:=\mathrm{Hom}(E, \mathbb{F}_q)$.

Particular cases are: 1) $q \cdot r(:=(\mathbb{Z}/q) \times (\mathbb{Z}/r))$ then the orbits have length r, 2) M acts transitively on E^{v} (for example $M \supseteq SL_m(\mathbb{F}_q)$), and 3) M is isomorphic to a Mathien group M_i in which case non-trivial orbits have length $\geq i$.

(g1) We apply f) and h). Since M_{24} does not have subgroups of index ≤ 23, each orbit of M_{24} on 2^{11} has length 1 or ≥ 24. Since by a) M_{24} is irreducible on 2^{11} it follows by j) that for $\cdot 1$ (resp. for $\cdot 0$) orbits of length 1 all lie in the center whence our claim.

(g2) For $3^6 \cdot (2 \cdot M_{12})$ we again have from Table T2.7 that $2 \cdot M_{12}$ is irreducible on $E:=3^6 \equiv \mathbb{F}_3^{\,6}$. Then $2M_{12}$ acts on $\mathbb{P}(E) \simeq \mathbb{P}^5(\mathbb{F}_3)$ and, one easily sees, has only orbits of length ≥ 12. Since the center of $2M_{12}$ inverts the elements of 3^6 it follows from the above the $2M_{12}$ has on 3^6 only orbits of length $\geq 2 \cdot 12=24$.

h) We need several times the following argument: Suppose $q^m \cdot M$ is a subgroup of H with M irreducible on q^m and m odd. Suppose $\varphi : \tilde{H} \to H$ is a cover with central kernel $\mathbb{Z}/q$. Then the preimage of q^m in H is isomorphic to q^{m+1} (although the representation of $\varphi^{-1}(M)$ on q^{m+1} may not be completely reducible). Indeed, if the preimage $S:=\varphi^{-1}(q^m)$ is not commutative then the commutator map defines an alternating bilinear form on q^m with values in Ker φ. Since m is odd, the form must be degenerate and since it is (evidently) M-invariant and M is irreducible, this form is zero. Thus S is commutative. The map $x \to x^{v}$ on S is also invariant under $\varphi^{-1}(M)$ and, as above, must be trivial, whence our claim.

(i) We consider $E \times \Omega_8^-(\mathbb{F}_3)$ where $E \simeq \mathbb{F}_3^{\ 8}$ and $\Omega_8^-(\mathbb{F}_3) = \mathcal{D}(SO_8^-(\mathbb{F}_3))$. We have $E \simeq E$ as $\Omega_8^-(\mathbb{F}_3)$ - module since it possesses an invariant non-degenerate quadratic and, therefore, bilinear form. One easily derives from Witt's theorem that $\Omega_8^-(\mathbb{F}_3)$ acts transitively on the vectors of the same length; possible lengths are 0, 1, -1. The stabilizers of the corresponding vectors are: the commutator of a parobolic subgroup $\mathbb{F}_3^8 \cdot \Omega_6^-(\mathbb{F}_3)$, and (for both lengths $\neq 1$) $\Omega_7(\mathbb{F}_3)$. This gives lengths of orbits of $\Omega_8^-(\mathbb{F}_3)$ as 1, 2132 (isotropic), 2214 (for both anisotropic) whence our estimate in view of f).

(j) If H is an irreducible subgroup of $GL_u(k)$ with H perfect with center of order m then m/n. This is evident.

(k) R. L. Griess Jr., The structure of the "Monster" simple group, in "Proc. Conf. on Finite Groups", W. R. Scott, F. Gross, ed., Academic Press, New York, 1976, pp. 113-118.

(ℓ1) M. E. O'Nan, some evidence for the existence of a new simple group, Proc. London Math. Soc. 32(1976), 421-479.

(ℓ2) We have to show that $Cd(H) \geq 18$. We already have that $Cd(H) \geq 15$ and by use of $A_2(7)$ it is sufficient to consider the case p=7. So let $\varphi : H^{\sim} \to GL_n(k)$ be a centrally faithful irreducible representation of the universal cover $H^{\sim}$ of H. Let $C(\simeq \mathbb{Z}/3)$ be the center of $H^{\sim}$. $H^{\sim}$ contains (see D. Gorenstein and R. Lyons [, p. 61]) subgroup $E \simeq 3^{1+4}$ whose center is C. If $\varphi(C) \neq 1$ then it follows from (8.1) and from complete reducibility of $\varphi|E$ in characteristic 7 that $9|n$. Since $n \geq 15$ it imples that $n \geq 18$.

Thus it suffices to consider the case when $\mathrm{Ker}\ \varphi = C$. In this case the Sylow 3-subgroup $\varphi(E)$ of $\delta(\tilde{H}) \simeq H$ is isomorphic to $(\mathbb{Z}/3)^4$ and is, see D. Gorenstein, R. Lyons [, p 61], a self-dual $N_H(\varphi(E))/Z_H(\varphi(E))$-module. The structure of $N_H(\varphi(E))$ is given in ℓ1) p. 422. One sees from that that $N_H(\varphi(E))$ is transitive on $\varphi(E)=Id_n$ whence $n \geq 80$ in our case.

(m) R. L. Griess Jr., personal communication.

(n) (R. L. Griess) Since $2^{1+8} \cdot \mathrm{Alt}_9$ occuring in F_3 is the unique twisted holomorph, the estimate is 2^4 (from 2^{1+8}) times the degree of the smallest irreducible projective (and non-linear) representation of A_9. This latter is ≥ 8 by (3.1)(b). Thus the minimal degree in characteristic $\neq 2$ is $\geq 2^4 \cdot 8 = 128$.

(o) D. Gorenstein, R. Lyons,

(p) By p 245 of J. H. Conway (Three lectures on exceptional groups, pp. 215-247, in "Finite simple groups", Proc. Confer of London Math. Soc., M. B. Powell, G. Higman ed., Academic Press, London, 1971) we see that $\mathcal{D}M(24)$ contains a subgroup $A \cdot M_{24}$, $A \simeq 2^{12}$, (non-split) with the action of M_{24} on 2^{12} being dual to that of M_{24} on the Golay code (which is just another group 2^{12}). The orbits of M_{24} on the Golay code are of lengths 1, 759, 2576, 759, 1. Thus, if char $k \neq 2$, the shortest non-trivial orbit of M_{24} on $\mathrm{Hom}(A,k^*)$ is of length 759 whence our estimate by f).

(q) By o) p. 67 F_3 contains a subgroup $R \simeq 3^4 \cdot SL_2(\mathbb{F}_9)$ (which is contained in N(3C) in the notation of that paper). The action of $S:=SL_2(\mathbb{F}_9)$ on $E:=3^4$ can not be trivial. Thus we are dealing with a representation of S over $\mathbb{F}_3$. This representation can not be reducible, for all homomorphisms of $SL_2(\mathbb{F}_9)$ into $SL_2(\mathbb{F}_3)$ or $SL_3(\mathbb{F}_3)$ are trivial. Thus it is irreducible. Let φ be its extension to $\overline{\mathbb{F}}_3$. If φ is reducible then it is a sum of two conjugate 2-dimensional representations of $SL_2(\mathbb{F}_9)$, or in other words our representation is the natural 2-dimensional representation of $SL_2(\mathbb{F}_9)$ on $\mathbb{F}_9^2(\simeq E)$. In this case S acts transitively on $E-\{1\}$ (and also on $E-\{1\}$ where E is the set of characters of E). Thus in this case, by f), we have estimate $9^2-1=80$ on dimensions of representations of F_3.

If φ is irreducible then $\varphi \simeq \varphi_1 \otimes (\varphi_1\ Fr)$ where φ_1 is the natural 2-dimensional representation of $SL_2(\mathbb{F}_9)$. However in this case the center $C \simeq \mathbb{Z}/2$ of S acts trivially on E. But this is impossible because the centralizer of the only (conjugacy class) element of order 3 in F_3 does not contains $3 \times 3^4 \cdot SL_2(\mathbb{F}_9)$.

(r1) See comment e) to Table T6.3.

(r2) Since the primitive cube root of 1 is not in $\mathbb{F}_5$, the element of order 3 fixes no line of $5^2 \simeq \mathbb{F}_5^2$. Since the normalizer of every line permutes transitively the non-zero elements of this line (by o) p. 56) we see that $4 \times Sym_3$ has two orbits of length 12 and one of length 1 on 5^2 (and on its dual) whence by f) the estimate.

(7.4) Once the table is complete we see that $|H| \le f(n)$ if the "adjusted estimate" is $\geqq \min n$ for H. If this is not the case then $|H| \le y_{a_1,a_2,H}(n)$ where $a_2:=\min n$, $a_1:=$"adjusted estimate" or an estimates for one or both of the H_i, combined with the corresponding restrictions on p. Now inspection of Table T7.2 completes the proof of (7.1).

8. Estimates for extraspecial groups.

Let k be an algebraically closed field of characteristic exponent $p := p(k)$. If $q \neq p$ is a prime then every extraspecial q-group E of ordre q^{1+2a} has faithful irreducible representations over k and they all have degree q^a (see D. Gorenstein [,]). Let $\mathrm{Aut}_c E$ denote the group of autormorphisms of E which are trivial on the center of E. We have $\mathrm{Aut}_c E \supseteq \mathrm{Inn}\, E$ and $\mathrm{Inn}\, E \simeq (\mathbb{Z}/q)^{2a}$. It is known (see e.g. B. Huppert [III.13.7 and III.13.8]) that $\mathrm{Aut}_c E/\mathrm{Inn}\, E \simeq Sp_{2a}(\mathbb{F}_q)$ if $q \neq 2$ and $\simeq O_{2a}(\mathbb{F}_2)$ if $q = 2$; here $\varepsilon = 0$ or 1 and O^{ε}_{2a} is the orthogonal group of a quadratic form on $\mathbb{F}_2^{2a}$ of Arf invariant ε. Recall that $|Sp_{2a}(\mathbb{F}_q)| \leq q^{2a^2+a}$ (see (4.4.1)) and $|O^{\varepsilon}_{2a}(\mathbb{F}_2)| = 2 \cdot |SO^{\varepsilon}_{2a}(\mathbb{F}_2)| \leq 2 \cdot 2^{2a^2-a}$ if $a > 1$ (see (4.4.1) and take into account lower-dimensional isomorphisms, (see R. Steinberg [, Theorem 37]). We have $|O^{\varepsilon}_2(\mathbb{F}_2)| \leq 6$ (see J. Diendonne [, II.10.3]).

For $d \in \mathbb{N}$ set

$$N(d,q) := \begin{cases} d^{2\log_3 d+3} & \text{if } q \neq 2 \\ 2d^{2\log d+1} & \text{if } q = 2,\ d > 2 \\ 24 & \text{if } q = 2,\ d \leq 2 \end{cases}$$

(8.1) Proposition. Let $\psi: E \to GL_d(k)$ be a faithful irreducible representation. Then

(a) $d = q^a$;

(b) $|\mathrm{Aut}_c E| \leq N(d,q)$

(c) $|\mathrm{Aut}\, E| \leq (q-1)N(d,q)$

(d) $|N_{GL_d(k)}(\psi(E))/Z_{GL_d(k)}(\psi(E))| \leq |Aut_c E|$

Proof. We have already given references for (a). Thus $a = \log_q d$. Note that, since ψ is irreducible the center C of E acts on k^d via a fixed character (with values in $\mu_q \subset k^*$). Therefore for $n \in N_{GL_d(k)}(\psi(E))$ we must have that $n\psi(C)n^{-1} = \psi(C)$ and then that $n\psi(c)n^{-1} = \psi(c)$ for any $c \in C$. Thus $N_{GL_d(k)}(\psi(E))$ induces on E automorphisms from $Aut_c E$. Thus (d) follows from (b). Since $Aut\ E/Aut_c E \simeq Aut\ C \simeq \mathbb{Z}/(q-1)$, (c) also follows from (b). If $q \neq 2$ then $q \geq 3$ so that $a \leq \log_3 d$. Therefore $|Aut_c E| = q^{2a}\,|Sp_{2a}(\mathbb{F}_q)| \leq q^{2a} \cdot q^{2a^2+a} = (q^a)^{2a+3} = d^{2a+3} \leq d^{2\log_3 d+3} = N(d,q)$.
If $q = 2$ then $a = \log d$ whence if $d > 2$ we have

$$|Aut_c E| \leq 2^{2a} \cdot 2 \cdot 2^{2a^2-a} = 2 \cdot 2^{2a^2+a}$$

$$= 2 \cdot (2^a)^{2a+1} = 2d^{2\log d+1} = N(d,2) \text{ for } d > 2.$$

Finally if $q = 2$, $a = 1$, then $d = 2$ and $|Aut_c E| \leq 2^2 \cdot 6 = 24 = N(2,2)$.

(8.2) Corollary. In the assumptions of (8.1) we have

n	2	3	4	5	7	8	9	11	13	16	17	19
$\|Aut_c E\| \leq$	24	216	1920	3000	16,464	$3.3\cdot10^6$	$4.2\cdot10^8$	$1.6\cdot10^5$	$3.7\cdot10^5$	$1\cdot10^{11}$	$1.4\cdot10^6$	$2.6\cdot10^6$
$\|Aut\ E\| \leq$	24	432	1920	12000	98,784	$3.3\cdot10^6$	$1.26\cdot10^7$	$1.6\cdot10^6$	$4.4\cdot10^6$	10^{11}	$2.2\cdot10^7$	$4.7\cdot10^7$
$2n^{21\ gn+1}$	16	195	2048	17616	778,230	$4.2\cdot10^6$	$2\cdot10^7$	$2.5\cdot10^8$	$4.5\cdot10^9$	$1.3\cdot10^{11}$	$3.9\cdot10^{11}$	$2.8\cdot10^{12}$

Moreover, $|\mathrm{Aut}\ E| \le 2n^{2\log n+1}$ for $n \ge 4$.

Proof. If $n = q^a$ is a power of an odd prime then $|\mathrm{Aut}_c E| = n^2\ |C_a(q)|$ and $|\mathrm{Aut}\ E| = (q-1) \cdot |\mathrm{Aut}\ E|$ whence by direct computation of $|C_a(q)|$ the expressions for the above n. If $n = 2^a$ then $|\mathrm{Aut}_c E| \le n^2 \cdot \max_{\pm} |O^{\pm}_{2a}(2)|$ and we use then expressions for $|O^{\pm}_{2a}(2)|$ from, say, J. Diendonné [, §II.10].

The estimate $n^{2\log_3 n+4} < 2n^{2\log n+1}$ holds for $n > 12$ and since the estimate $2n^{2\log n+1}$ applies by the table above to $4 \le n \le 12$, n a prime power, we obtain the concluding statement of (8.2).

(8.3) Corollary. In the assumptions of (8.1) assume also that $q \ne 2$. Then

$$|\mathrm{Aut}\ E| \le 2d^{2\log_3 d+1}.$$

Proof. The claim holds for $q = 3$. Assume $q > 3$. Let $d = q^a$ (by (8.1)(a)). Then from the proof of (8.1) we have $|\mathrm{Aut}\ E| = (q-1)\ |\mathrm{Aut}_c E|$ and $|\mathrm{Aut}_c E| \le d^{2\log_q d+3}$. We have thus to check whether $F(d) := 2d^{2\log_3 d+3}/(q-1)d^{2\log_q d+3}$ is ≥ 1. We have

$$\ln F(d) = \ln 2 - \ln(q-1) + 2(1/\ln 3 - 1/\ln q)\ln^2 d$$

$$\ge \ln 2 - \ln q + 2(1/\ln 3 - 1/\ln q)a^2\ln^2 q$$

$$= \ln 2 + \frac{2a^2 \ln^2 q}{\ln 3} - (2a^2+1)\ln q$$

$$\geq 0.69 + 1.82a^2 \ln^2 q - (2a^2+1)\ln q.$$

Thus $\ln F(d) > 1.82\, a^2 \ln q(\ln q - (2+\frac{1}{a^2})0.55)$

$$\geq 1.82a^2 \ln q(\ln q - 1.65).$$

This latter expression is > 0 if $q \geq 6$. Thus our claim follows for $q \geq 7$.
If $q = 5$ then $0.69 + 1.82a^2 \ln^2 q - (2a^2+1)\ln q \geq 1.49a^2 - 0.9 > 0$, whence (8.3).

85?

n	2	3	4	5	7	8	9	11	13	16	17	19
$\lvert Aut_c E\rvert \le$	24	216	1920	3000	16,464	$3.3\cdot 10^6$	$4.2\cdot 10^8$	$1.6\cdot 10^5$	$3.7\cdot 10^5$	$1\cdot 10^{11}$	$1.4\cdot 10^6$	$2.6\cdot 10^6$
$\lvert Aut\ E\rvert \le$	24	432	1920	12000	98,784	$3.3\cdot 10^6$	$1.26\cdot 10^7$	$1.6\cdot 10^6$	$4.4\cdot 10^6$	10^{11}	$2.2\cdot 10^7$	$4.7\cdot 10^7$
$2n^{21\ gn+1}$	16	195	2048	17616	778,230	$4.2\cdot 10^6$	$2\cdot 10^7$	$2.5\cdot 10^8$	$4.5\cdot 10^9$	$1.3\cdot 10^{11}$	$3.9\cdot 10^{11}$	$2.8\cdot 10^{12}$

9. Estimates for direct products of finite centrally simple groups.

Let k be an algebraically closed field of characteristic exponent $p=p(k)$. Let $G_1,\dots,G_m$ be finite perfect centrally simple universal (i.e., with trivial Schur multiplier) groups. Let $\varphi_i : G_i \to GL_{n_i}(k), i=1,\dots,m$, be non-trivial irreducible representations. Set $G := \Pi_{1\le i\le m} G_i$, $\varphi := \otimes_{1\le i\le m} \varphi_i$, $n := \Pi_{1\le i\le m} n_i$. Let C_i be the center of $G_i, i=1,..,m$.

We introduce the following subsets of the set of the i, $1\le i\le m$.

I_{Alt}, the set of i such that $\varphi_i(G_i)$ is isomorphic to Alt_{a_i}, $a_i \ge 10$;

$I_{Lie,\,p}$, the set of i such that G_i is isomorphic to a group of Lie p-type (see Table T6.3 for exceptional isomorphisms);

$I_{Lie,p'}$, the set of i such that G_i is isomorphic to a group of Lie p'-type but not isomorphic to any group of Lie p-type (see Table T6.3 for exceptional isomorphisms) and neither isomorphic to ${}^2A_3(9)$ or $D_4(2)$.

$I_{extrz\text{-}spor}$, the set of i such that G_i is centrally isomorphic to Suz,·1,·2, if $p\neq3$, to ${}^2A_3(9)$, and if $p\neq2$, to $D_4(2)$.

I_{rest} the set of the remaining indices; i.e. $\varphi_i(G_i)$ for $i \in I_{rest}$ is isomorphic to $\widetilde{Alt}_{a_i}$ for $a_i \ge 10$, or centrally isomorphic to Alt_7, Alt_9, or to one of the 23 sporadic groups not included in $I_{extra\text{-}spor}$.

These sets are pairwise disjoint.

Set $H:=\Pi_{i\notin I_{Lie,p}} G_i$, $L:=\Pi_{i\in I_{Lie,p}} G_i$, $A:=\Pi_{i\in I_{Alt}} G_i$, C = center of H, and for $R \subseteq GL_n(k)$ set

$$NZ(R) := N_{GL_n(k)}(R)/Z_{GL_n(k)}(R).$$

$$\overline{NZ}(R) := N_{GL_n(k)}(R)/R\cdot Z_{GL_n(k)}(R).$$

Thus NZ(R) "describes" the part of the automorphism group of R "realized" in $N_{GL_n(k)}(R)$ and $\overline{NZ}(R)$ the corresponding past of outer automorphism group.

Set $f(x) := (2x+1)^{2\log_3(2x+1)+1}$.

(9.1) Theorem. (a) $|H/C| \le \begin{cases} f(n) & \text{if } n<10,\ n\ne 6.8 \\ 1.58f(6) & \text{if } n=6 \\ 4.62f(8) & \text{if } n=8 \\ (n+2)! & \text{if } n\ge 10 \end{cases}$

$$|\mathrm{Aut}\ H| \le \begin{cases} nf(n) & \text{if } n=2,3,5,7,9,10,11 \\ 4.1\ f(4) & \text{if } n=4 \\ 12.61\ f(6) & \text{if } n=6 \\ 27.69\ f(8) & \text{if } n=8 \\ 231\ \ f(12) & \text{if } n=12 \\ (n+2)! & \text{if } n>12 \end{cases}$$

$$|\mathrm{Out}\ H| \le [\log n]!n^2 \quad \text{if} \quad n \ge 2$$

(b) if $I_{Alt}=\phi$ and

(i) $|I_{extra\text{-}spor}| \ne 1$,

or (ii) $\prod_{1\le i\le m,\ i\notin I_{extra\text{-}spor}} n_i \ge 4$,

or (iii) $m \ge 3$,

then $|H/C| \le f(n)$;

$$|\mathrm{Aut}\ H| \le \begin{cases} n\ f(n) & \text{if } n\ne 4 \\ 4.1\ f(4) & \text{if } n=4 \end{cases}$$

$$|\mathrm{Out}\ H| \le [\log n]!n^2$$

(c) if $m\le 2$, $I_{Alt}=\phi$, $|I_{extra\text{-}spor}|=1$ (assume $I_{extra\text{-}spor}=\{1\}$), and $n/n_1=1,2$, or 3 then

$$|H/\text{center}| \le \begin{cases} F(G_1,n) & \text{if } m=1 \\ 60F(\cdot 1,n) & \text{if } m=2,\ G_1 \simeq \cdot 0,\ 48 \le n \le 72 \\ f(n) & \text{otherwise} \end{cases}$$

$$|\mathrm{Aut}\ H| \le \begin{cases} F(G_1,n) & \text{if } m=1 \\ 3.05 \cdot 48\ f(48) & \text{if } m=2,\ G_1/C_1 \simeq \cdot 1,\quad n=48 \\ 1.43 \cdot 50\ f(50) & \text{if } m=2,\ G_1/C_1 \simeq \cdot 1,\quad n=50 \\ n\ f(n) & \text{in the remaining cases} \end{cases}$$

$$|\mathrm{Out}\ H| \le 32$$

where $F(G_1,n) = F(G_1/\text{center},n)$ is defined just before (A6).

The normalizer of $\varphi(G)$ in $GL_n(k)$ permutes the (isomorphic linear) groups $\varphi(G_i)$. Let $\bar{\varphi} : \overline{NZ}(\varphi(G)) \to \mathrm{Sym}_m$ be the corresponding homomorphism.

(9.2) Theorem. (a) $\mathrm{Ker}\ \bar{\varphi}$ is solvable with $\mathcal{D}^3(\mathrm{Ker}\ \bar{\varphi}) = \{1\}$;

(b) $|\mathrm{Ker}\ \bar{\varphi}| \le n^2$ and, therefore,

(c) $|\overline{NZ}(\varphi(G))| \le [\log n]! \cdot n^2$.

Remark. Of course, if G does not contain $D_4(m)$ then $\mathcal{D}^2(\mathrm{Ker}\ \bar{\varphi}) = \{1\}$.

(9.3) Lemma. If $|G_i/C_i| \le f(n_i)$ for $i=1,\ldots,m$ and $I_{\mathrm{Lie},p}=\phi$ then

(a) $|G/\text{center}| \le f(n)$

(b) $|\mathrm{Aut}\ G| \le \begin{cases} n\ f(n) & \text{if } n\ne 4 \\ 4.1\ f(r) & \text{if } n=4 \end{cases}$

(c) $|\mathrm{Out}\ G| \le [\log n]!n^2$

(d) $|\Pi\,\mathrm{Out}\ G_i| \le n^2$.

Proof. We have $|G/\text{center}|=\Pi|G_i/C_i| \le \Pi f(n_i) \le f(\Pi n_i) = f(n)$ (the last inequality by (A1)(a)). This proves (a).

Now we use (6.1)(b), (c). Note that the exceptions in (6.1)(b) are all, but $A_2(4)$ for n=4, excluded: Alt_6 and $A_1(8)$ do not have representations of dimension 2 unless they are of Lie p-type (see column 7 in Table T6.3) and ${}^2A_3(9)$ is excluded for n=6 by $|{}^3A_3(9)| > f(6)$, similarly $D_4(2)$. Thus we have $|\mathrm{Out}\ G_i| \le n_i^2$ and $|\mathrm{Aut}\ G_i| \le n_i f(n_i)$ unless $n_i=4$, $G_i \simeq \tilde{A}_4(2)$ when $|\mathrm{Aut}\ G_i| = 4.1f(4)$, if G_i is of Lie p'-type. For the remaining centrally simple groups: alternating of degree $\ne 6$ (recall $\mathrm{Alt}_6 \simeq \mathcal{D}B_2(2)$) and sporadic, we have $|\mathrm{Out}\ G_i| \le 2$. Thus $|\mathrm{Out}\ G_i| \le n_i^2$. This implies (d).

To prove (b) and (c) let us split the set $J = \{1,\dots,m\}$ of indices into the subsets $J_1,\dots,J_r$ such that $G_i \simeq G_j$ if and only if $i,j \in J_s$ for some s. Then $\mathrm{Aut}\ G = \mathrm{Aut}(\Pi G_i) = \Pi_{1\le i\le r}((\Pi_{j\in J_i} \mathrm{Aut}\ G_j) \rtimes \mathrm{Sym}\ J_i)$ where $\mathrm{Sym}\ J_i$ permutes the isomorphic G_j, $j \in J_i$. Let $t_i := |J_i|$. Let $\tilde{n}_i := \min\{n_j, j \in J_i\}$. Assume for definiteness that if some $G_j \simeq \tilde{A}_2(4)$ then $j \in J_1$. Write $|\mathrm{Aut}\ G_j| \le a_i \tilde{n}_i f(\tilde{n}_i)$ where $a_i=1$ unless $i=1$, $\tilde{n}_1=4$, and $G_j \simeq \tilde{A}_2(4)$ for $j \in J_1$, and $a_i=1.025$ otherwise, for $i=1,\dots,r$. If $n_j=2$ then $G_j \simeq \widetilde{\mathrm{Alt}}_5$ (see Table T2.7), i.e., $|G_j/C_j|=60$, $|\mathrm{Aut}\ G_j|=120$. Thus in notation of (A1) $|\mathrm{Aut}\ G_j| \le \tilde{n}_i \tilde{f}(\tilde{n}_i)$. Then by (A1) we have $|\mathrm{Aut}\ G| =$

$$\Pi_{1\le i\le r}(\Pi_{j\in J_i} |\mathrm{Aut}\ G_j|)(t_i!) \le (a_1^{t_1}\tilde{n}_1^{t_1}\tilde{f}(\tilde{n}_1)^{t_1} t_1!) \cdot \Pi_{i\ge 2}\tilde{n}_i^{t_i}\tilde{f}(\tilde{n}_i)^{t_i} t_i!$$

$$\le a_1^{t_1} \ \Pi\tilde{n}_i^{t_i}(\Pi\tilde{f}(n_i)^{t_i}(t_i!)) \le a_1^{t_1}\ n \cdot \Pi\tilde{f}(n_i^{t_i})$$

$$\le a_1^{t_1} n\tilde{f}(\Pi\tilde{n}_i^{t_i}) \le a_1^{t_1} n\tilde{f}(n) \le a_1^{t_1} nf(n).$$

This proves (b) if $a_1=1$. If $a_1=1.025$ and $t_1 \ge 2$ we use (A1)(d) to get that $a_1^{t_1} f(\tilde{n}_1)^{t_1} \le f(\tilde{n}_1^{t_1})$ and then the argument can be continued (from the middle) as above (but a_1-factor will be lost). If $a_1=1.025$, $t_1=1$, $m>1$ then the above $a_1 f(n)\Pi_{i\ge 2} \tilde{f}(\tilde{n}_i^{t_i}) \le a_1 f(4)\tilde{f}(n/n_1) \le f(n)$ by (A1)(c). This concludes the proof of (b).

Part (c) now follows as above:

$$|\mathrm{Out}\ G| = \Pi_i(\Pi_{j\in J_i} |\mathrm{Out}\ G_j|)t_i! = (\Pi_s \ \mathrm{Out}\ G_s)\ \Pi t_i! \le \Pi n_s^2 \cdot ((\Sigma\ t_i)!)$$

$$\le n^2([\log n]!)$$

Set $g(x) := \Gamma(x+3)$; recall that $\Gamma(n+3)=(n+2)!$ for $n \in \mathbb{N}$.

(9.4) Lemma. If $G_i \simeq \widetilde{Alt}_{m_i}$, $m_i \geq 10$, for $i=1,\ldots,m$ then

(a) $|Aut\ G| \leq (n+2)!$

(b) $|Out\ G| \leq n \cdot ([\log n]!)$

Proof. By (3.1)(a) we have $m_i \leq n_i+2$, so that $|G_i/center| \leq 1/2(n_i+2)!$. Since $Alt_r = Sym_r$ for $r \geq 7$ (see D. Gorenstein [, p. 304]) we have $|Aut\ G_i| \leq (n_i+2)!$ Now the same argument as in the proof of (9.3) yields $|Aut\ G| \leq \Pi_j(Aut\ G_j) \cdot \Pi_i t_i!$ where $\Sigma_i t_i \leq \log n$. Then (A2) gives (a). To get (b) note that $|Out\ G| = \Pi_i Out\ G_j \cdot \Pi_i t_i! \leq 2^{\log n} \cdot [\log n]!$ as claimed.

(9.5) Lemma. For a group G_i, $i \in I_{rest}$, we have

(a) $|G_i/C_i| \leq f(n_i)$;

(b) $|Aut\ G_i| \leq 2f(n_i)$

(c) $|Out\ G_i| \leq 2$

Proof. When G_i is centrally isomorphic to a sporadic group (a) is contained in (7.1). If G_i is centrally isomorphic to Alt_7 or Alt_9 we see from Table T2.7 (groups of small degree) that Alt_7 has no non-trivial projective representations of dimension 2 and one easily sees that $|Alt_7| = 2520 < f(3)$. For Alt_9 we see from the same Table T2.7 that it does not have non-trivial projective representations of dimension ≤ 4 and then $|Alt_9| = 781{,}440 < f(5)$.

If G_i is isomorphic to $\widetilde{Alt}_a$, $a \geq 10$, then (a) is contained in (3.4).

Finally, (c) is known, see D. Gorenstein [, p. 304].

(9.6) Proof (9.1)(a) and (9.2). (9.1)(a) follows directly from (9.3), (9.4) and (A3) and (A6) since the estimates for one G_i hold by (3.1), (6.1), (7.1), and (9.5). To prove (9.2) note that, similarly to the proofs of (9.3)(b), (c) and (9.4), we have that $\mathrm{Ker}\ \bar{\varphi}$ is a subgroup of $\Pi\overline{NZ}(\varphi_i(G_i))$. Then: by (6.1)(c) $|\overline{NZ}(\varphi_i(G_i))| \le n_i^2$ if G_i is of Lie p′-type; by (5.1), $|\overline{NZ}(\varphi_i(G_i))| \le 2n_i \log n_i \le n_i^2$ if G_i is of Lie p-type; and by D. Gorenstein, [, p.304] we have $|\overline{NZ}(\varphi_i(G_i))| \le 2 \le n_i^2$ in the remaining cases. Thus $|\overline{NZ}(\varphi(G))| \le (\Pi n_i^2)\cdot(m!) = n^2\cdot(m!) \le n^2([\log n]!)$. This proves (9.2)(c); and (b) was also implicitly proved above. To prove (9.2)(a) recall that $\mathcal{D}^3(\mathrm{Out}\ \tilde{G})$ for every simple group $\tilde{G}$ of Lie type and $|\mathrm{Out}\ \tilde{G}| \le 4$ in the remaining cases.

(9.7) Proof of (9.1)(b). If $|I_{\text{extra-spor}}| > 1$ (and $I_{\text{Alt}}=\phi$) then (A6), (A1), and (9.5) imply that $|H/C| \le f(n)$. The same argument as in the proof of (9.3) together with the fact that $|\mathrm{Out}\ G_i| \le 2 \le n_i^2$ for sporadic groups, $|\mathrm{Out}\ {}^2A_3(9)| = 8 < 36 \le n_i^2$ if $G_i \simeq {}^2\tilde{A}_3(9)$, and $|\mathrm{Out}\ D_4(2)| = 6 \le 64 \le n_1^2$ if $G_i \simeq \tilde{D}_4(2)$ gives $|\mathrm{Out}\ H| \le ([\log n]!)n^2$. The estimates on $|\mathrm{Aut}(\ )|$ in (9.3), (9.5) together with evident estimates $|\mathrm{Aut}\ G_i| \le F(G_i,n_i)$ for $i \in I_{\text{extra-spor}}$, combined with (A1) and (A6) give that $|\mathrm{Aut}\ H| \le nf(n)$.

If $I_{\text{extra-spor}}=\phi$ then the above proof works again but the reference to (A6) is not needed anymore.

If $|I_{\text{extra-spor}}| = 1$ and (9.1)(b)(iii) holds then so does (9.1)(b)(ii). So assume that $I_{\text{extra-spor}}=\{1\}$, $n/n_1 \ge 4$. Then $\mathrm{Aut}\ H = \mathrm{Aut}(H/G_1) \times \mathrm{Aut}\ G_1$. We have by above $|\mathrm{Aut}(H/G_1)| \le \begin{cases} (n/n_1)f(n/n_1) & \text{if } n/n_1 \ne 4 \\ 4.1\ f(4) & \text{if } n=4n_1 \end{cases}$.

Now $|\mathrm{Aut}\ G_1| \le F(G_1,n)$ and the claim follows from (A6).

(9.8) The proof of (9.1)(c) is also similar. If $m=1$ then we are done in view of (7.1) and of definition of $F(G,n)$. If $m=2$ then $n_2=n/n_1=2$ or 3. If $2 \notin I_{Lie,p}$ then from Table T2.7 (groups of small degree) G_2 is isomorphic to $\widetilde{Alt}_a$ for $a=5,6$, or 7, or $\tilde{A}_1(7)$. First, $|\mathrm{Out}\ G_2| \le 4$ (and $=4$ if $G_2 \simeq \widetilde{Alt}_6$) and $|\mathrm{Out}\ G_1| \le 8$ (and $=8$ if $G_1 \simeq {}^2\tilde{A}_3(9)$), whence the estimate on Out H.

Now if $n_2=2$ then $|G_2/C_2| = 60$ and $|H/C| \le 60\ F(G_1,n_1)$. If $n_2=3$ then $|G_2/C_2| \le 2{,}520$ and $|H/C| \le 2{,}520\ F(G_1,n_1)$.

We now refer to Table TA6 and use notation therefrom. We have $F(G_1,n_1) \ge F(G_1,a_1) = |G_1/C_1|$. We see from the Table that $60F(G_1,a_1) \le F(G_1,2a_1) = f(2a_1)$ and $2{,}520\ F(G_1,a_1) \le F(G_1,3a_1)=f(3a_1)$ unless $G_1 \simeq \cdot 0$. If $G_1/C_1 \simeq \cdot 1$ we establish by direct calculations that $2{,}520\ F(G_1,n_1) \le F(G_1,3n_1) = f(3n_1)$ if $n_1 \ge 25$ and $60\ F(G_1,n_1) \le F(G_1,2n_1) \le f(G_1,2n_1) = f(2n_1)$ if $n \ge 31$. The remaining part of the estimate on $|H/C|$ is then verified by direct calculations again.

If, finally, $2 \in I_{Lie,p}$ then we have to check weaker inequalities $F(G_1,n_1n_2) \ge |\mathrm{Aut}\ G_1|$ which, of course, hold if the ones above hold.

The estimate on $|\mathrm{Aut}\ H|$ holds if $m=1$ holds by the definition of $F(G,n)$ and if $m=2$ by (A6) except when $m=2$, $G_1 \simeq \cdot 0$.

We assume now that $m=2$, $G_1/C_1 \simeq \cdot 1$. Then $\mathrm{Aut}\ G_1 = G_1/C_1$. If $n_2=2$ we see that $120 \cdot |\cdot 1| \le 2n_1 f(2n_1)$ if $n_1 \ge 26$; for $n_1=24,25$ we have values given by (9.1)(c). If $n_2=3$ then $5040 \cdot |\cdot 1| \le 3n_1 f(3n_1)$ if $n_1 \ge 24$.

That $|\mathrm{Aut}\ H| \le nf(n)$ holds in the remaining cases is easily seen from Table TA6.

10. Estimates for direct products of centrally simple and extraspecial groups.

Let k, m, the G_i, φ_i, n_i, $i=1, \ldots, m$, φ, H, and L have the same meaning as in §9. Recall $f(n)=(2n+1)^{2\log_3(2n+1)+1}$. Set

$$f_H(n) = \begin{cases} F(G_1,n) & \text{if } H=G_1,\ G_1/C_1 \simeq {}^2\bar{A}_3(9), D_4(2), \text{Suz}, \cdot 1, \text{ or } \cdot 2. \\ 1.025\ f(4) & \text{if } m=1,\ H/C \simeq \bar{A}_2(4) \\ 3.05\ f(48) & \text{if } m=2,\ G_1/C_1 \simeq \cdot 1,\ n=48 \\ 1.43\ f(50) & \text{if } m=2,\ G_1/C_1 \simeq \cdot 1,\ n=50 \\ f(n) & \text{in the remaining cases.} \end{cases}$$

Let $E_1,\ldots,E_r$ be extraspecial groups of orders $p_1^{1+2a_1},\ldots,p_r^{1+2a_r}$ where $p_1 < p_2 < \ldots < p_r$, $p_i \neq p$ for $i=1,\ldots,r$, and $a_i \geq 1$ for $i=1,\ldots,r$. Let $\varphi_i : E_i \to GL_{d_i}(k)$ be faithful irreducible representations. By (8.1) we have $d_i=p_i^{a_i}$. Set $\psi := \otimes_{1\leq i\leq r}\, \psi_i$, $d := \Pi_{1\leq i\leq r}\, d_i$, $E := \Pi_{1\leq i\leq r}\, E_i$ and, if $p_1=2$, set also $\bar{E} := \Pi_{2\leq i\leq r}\, E_i$, $\bar{\psi} := \otimes_{2\leq i\leq r}\, \psi_i$, $\bar{d} := \Pi_{2\leq i\leq r} d_i$.

Set $G := L\times H\times E$, $\omega := (\otimes\varphi_i)\otimes\psi$, $n := (\Pi n_i)d$, $N := |\text{Aut }(H\times E)|$, $d := (\log 3-1)/2 \leq 0.2925$, $\beta := \log_{24} |\cdot 1| - 2 \log 24 \leq 4.32$.

(10.1) Theorem.

(a) $$|\text{Aut }(H\times E)| \quad \begin{cases} n\ f(n) & \text{if } n=2,3,5,7,9,10,11 \\ 4.1\ f(4) & \text{if } n=4 \\ 12.61\ f(6) & \text{if } n=6 \\ 27.69\ f(8) & \text{if } n=8 \\ 231\ f(12) & \text{if } n=12 \\ (n+2)! & \text{if } n > 12 \end{cases}$$

(b) If $I_{Alt} = \phi$ and $|E/\bar{E}| = 2^{1+2a}$ then $|Aut(H \times E)| \leq 2^{2a^2+1}\, n\, F_H(n/2^a)$.

(10.2) Corollary. If $I_{Alt} = \phi$, $E \neq \{1\}$ then

(a) $N \leq n\, f(n)$ if any one of the following holds

(i) $p_1 \neq 2$;

(ii) $p_1=2$, $1 \leq a_1 \leq 5$;

(iii) $p_1=2$, $a_1 \geq 2$, $n \geq 2^{(\alpha+1)a_1}$

(b) $N \leq 2\, n^{2 \log n + 1}$ otherwise.

(10.3) Corollary. If $I_{Alt} = \phi$ then

(a) $|Aut(H \times E)| \leq \max(nF_H(n),\ 2n^{2 \log n + 1})$

(b) $|Aut(H \times E)| \leq n^{2 \log n + 5}$ for $n \geq 2$

(c) $|Aut(H \times E)| \leq 2\, n^{2 \log n + 1}$ if $n \geq 39$.

(10.4) Proof of (10.1). Note that since the E_i are not isomorphic and none of them is isomorphic to a quotient of H we have

(10.4.1) $|Aut(H \times E)| = |Aut\ H| \cdot \Pi_{1 \leq i \leq r} |Aut\ E_i|$

Since one easily sees that $2n^{2 \log n + 1} < (n+2)!$ for $n > 12$ and $\leq f(n)$ for $n < 14$ one gets (a) from (A1)(a), (A2)(a), (8.2), and (9.1)(a).

To prove (b) note first that $n^{2 \log_3 n + 3} \leq f(n)$ by (A7)(a). Therefore by (9.1)(b), (c)

$$|Aut(H \times \bar{E})| \leq (n/2^a)\ F_H\ (n/2^a).$$

Assuming that $a \neq 0$ (otherwise we are done) we have $p_1 = 2$ and $|\mathrm{Aut}\ E_1| = 2 \cdot (2^a)^{2a+1} = 2^{2a^2+a+1}$ whence (b) follows, in view of (10.4.1).

(10.5) Proof of (10.2). We have $I_{Alt} = \phi$, $E \neq \{1\}$.

(10.5.1) Assume first that

$$|\mathrm{Aut}\ H| \leq (\Pi n_i) f(\Pi n_i).$$

If $p_1 \neq 2$ then by (10.4.1), (8.3), and (A7)(a)

$$\begin{aligned} |\mathrm{Aut}(H \times E)| &\leq (\Pi n_i) f(\Pi n_i) \cdot \Pi\ 2\ d_j^{2\ \log_3 d_j + 3} \\ &\leq (\Pi n_i) f(\Pi n_i)\ \Pi f(d_j) \leq n f(\Pi n_i\ \Pi d_j) \\ &\leq n f(n), \end{aligned}$$

whence (10.2)(a)(i).

If $p_1 = 2$ but $1 \leq a_1 \leq 5$ then $24 < f(2)$ and $2 d_1^{2 \log d_1 + 1} \leqq d_1 f(d_1)$ (direct verification). Therefore (10.4.1), (10.1)(b) and (A1) give

$$|\mathrm{Aut}(H \times E)| \leq n f(d_1) f(n/d_1) \leq n f(n)$$

whence (10.2)(a)(ii).

Now let $p_1 = 2$, $a_1 \geq 2$, $n \geq 2^{(\alpha+1) a_1}$. Then by (A5) $2\ 2^{2a_1^2 + a_1} f(n/2^{a_1}) \leq f(n)$ whence by (10.4.1) and (10.1)(b) we get (10.2)(a)(iii).

For (b) we note that the "otherwise" condition implies $a_1 \geq 6$. Now (b) follows from (A7)(c).

(10.5.2) Now we consider the remaining case when $|\mathrm{Aut}\ H| \geq (\Pi n_i) f(\Pi n_i)$. It follows then from (9.1)(b),(c) that either $m=1$ and $H=G_1$ is centrally isomorphic to Suz, ·1, ·2, ${}^2A_3(9)$, $D_4(2)$ or $A_2(4)$ or $m=2$, $n=48$ or 50, and G_1/C_1 or G_2/C_2 is isomorphic to ·1.

Assume first that $\bar{E} \neq \{1\}$. Then by (8.3),(A7)(a): $|\mathrm{Aut}\ \bar{E}| \leq \Pi 2d_i^{\,2\log_3 + 3} \leq f(\bar{d})$ whence $|\mathrm{Aut}(H \times \bar{E})| \leq |\mathrm{Aut}\ H| \cdot f(\bar{d})$. Using one of (A1)(c) or (A6)(c), (d) we get, therefore that $|\mathrm{Aut}(H \times \bar{E})| \leq \bar{d}(\Pi n_i) f(\bar{d}\Pi n_i)$ unless $m=1$, $G_1/C_1 \simeq$ ·1 and $\bar{d}=3$. In this latter case we have $|\mathrm{Aut}\ \bar{E}| = 432$ (by (8.2)) and Aut ·1 = ·1. Then

$$|\mathrm{Aut}(H \times \bar{E})| = 432 \cdot 4.16 \cdot 10^{18} \sim 1.8 \cdot 10^{21} \leq (3.24) f(3.24) \sim 4.10^{23}$$

and since $nf(n) \geq 72 f(72)$ if $n \geq 72$ it follows that in all cases (if $\bar{E} \neq \{1\}$) $|\mathrm{Aut}(H \times \bar{E})| \leq \bar{d}(\Pi n_i) f(\bar{d}\Pi n_i)$.

Now (10.2) follows as in (10.5.1).

(10.5.3) Now we can assume that $\bar{E}=\{1\}$ so that $E=E_1 \simeq 2^{1+2a}$, $a := a_1 \geq 1$. If $a \leq 5$ then $|E| \leq f(d)$ and the argument of (10.5.2) works except when $d=2$. When $d=2$, $m=1$, $G_1 \simeq A_2(4)$ we still get our claim by (A1)(c). In the remaining cases we have to check that $24 \cdot |\mathrm{Aut}\ H| \leq 2 \cdot (\Pi n_i) f(2\Pi n_i)$. If $m=1$ this is readily seen (except for ·1) from Table TA6 (compare lines $F(G, 2a_1)$ and $24\ |\mathrm{Aut}\ G|$). If $m=1$ and $G_1 \simeq$ ·1 then one has $|\mathrm{Aut}(H \times E)| = 10^{20}$ and $48 f(48) \geq 1.63 \cdot 10^{20}$ whence the desired estimate holds in this case as well. The cases $m=2$ and $n=48$ (resp. 50) and $|\mathrm{Aut}\ H| \leq 3.05 \quad 48 f(48)$ (resp $\leq 1.43 \cdot 50 f(50)$) are verified directly.

(10.5.4) We now assume that $a \geq 6$ (and the assumptions of (10.5.2) and (10.5.3) hold). Suppose first that $|\mathrm{Aut}\ H| \leq d \cdot \Pi n_i\ f(\Pi n_i)$ and $n \geq 2^{(1+\alpha)a}$. Then (by (10.4.1) and (A5))

$$|\mathrm{Aut}(H \times E)| \leq 2d^{2 \log d + 1}(d\Pi n_i)f(\Pi n_i) \leq (d\Pi n_i)f(d\Pi n_i)$$
$$\leq nf(n).$$

This gives (10.2)(a)(iii). The condition $|\mathrm{Aut}\ H| \leq d\Pi n_i f(\Pi n_i)$, $d \geq 64$, evidently (from expressions in (9.1)(c)) holds if $m=2$. If $m=1$, $G_1/C_1 \simeq A_2(4)$ (resp ${}^2\bar{A}_3(9)$, $D_4(2)$ Suz, $\cdot 1$, $\cdot 2$) then $n_1 \geq 4$ (resp. 6,8,12,24, 20 (by Table T7.2)) and (10.2)(a)(iii) follows from the comparison of lines $64a_1 f(a_1)$ and $|\mathrm{Aut}\ G|$ in Table TA6, except, of course, when $G_1/C_1 \simeq \cdot 1$. In this case it holds if $d \geq 4096 = 2^{12}$. Thus it is sufficient to check (10.2)(a)(iii) for $m=1$, $G_1/C_1 \simeq \cdot 1$, $d=2^a$, $6 \leq a \leq 11$, directly. We have

a	6	7	8	9	10	11
$\|\mathrm{Aut}\ E\| = 2^{2a^2+a+1}$	$6 \cdot 10^{23}$	$8.1 \cdot 10^{31}$	$1.7 \cdot 10^{41}$	$6 \cdot 10^{51}$	$3.3 \cdot 10^{63}$	$2.9 \cdot 10^{76}$
$\|\cdot 1\| \cdot \|\mathrm{Aut}\ E\|$	$2.5 \cdot 10^{42}$	$3.4 \cdot 10^{50}$	$7.1 \cdot 10^{59}$	$2.5 \cdot 10^{70}$	$1.4 \cdot 10^{82}$	$1.2 \cdot 10^{95}$
$f(2^a\ 24)$	$2.9 \cdot 10^{54}$	$9 \cdot 10^{63}$	$1.5 \cdot 10^{74}$	$1.5 \cdot 10^{85}$	$9 \cdot 10^{96}$	$3 \cdot 10^{109}$.

Thus (10.2)(a)(iii) holds in all cases.

(10.5.5) It remains to prove (10.2)(b) in the case when the conditions of (10.5.2), (10.5.3) and (10.5.4) hold. So $|E| = 2^{1+2a}$, $a \geq 6$. We have to check

$$|\mathrm{Aut}\ E| \cdot |\mathrm{Aut}\ H| \leq r^{2 \log r + 1}$$

where $r=2^a \cdot s$, $s=\Pi n_i$. Substituting $|\mathrm{Aut}\ E| \le 2^{2a^2+a+1}$ and taking log we see that it suffices to check

$$\log_{10} |\mathrm{Aut}\ H| \le (2/\log_{10}2)\log_{10}^2 s + (4a+1)\log_{10}s.$$

Noting that $a \ge 6$, i.e., $4a+1 \ge 25$ we easily see that $(4a+1)\log_{10}s$ supplies a power of 10 sufficient to overcome $|\mathrm{Aut}\ H|$ (here, of course, $s \ge 4$ (resp 6,8,12,24,20) if $m=1$ and $G_1/C_1 \simeq \bar{A}_2(4)$ (resp. ${}^2\bar{A}_3(9)$, $\bar{D}_4(2)$, Suz, $\cdot 1$, $\cdot 2$) and $s=48$ or 50 if $m=2$ and G_1/C_1 or $G_2/C_2 \simeq \cdot 1$). This proves (10.2)(b).

(10.6) Proof of (10.3). If $I_{alt}=\phi$, $E=\{1\}$ then (10.3)(a) follows from (9.1)(b), (c) (and the definition of $F_H(n)$). If $E\ne\{1\}$ it follows from (10.2).

We have $F(G,n) \le 2\cdot n^{2\log n + 4.32}$ for all sporadic G (since min $\tilde{n} \le$ (adjusted estimate) in Table T7.2). We have $5-4.32=0.68$ and $12^{0.68}=5.42 > 2$. Thus $|\mathrm{Aut}\ G| \le n^{2\log n + 5}$ for a sporadic G. We also have $f(n) \le n^{2\log n + 5}$ if $n \ge 4$ by (A7)(b), $4.1 \cdot f(4) < 4^{2\log 4 + 5}$, $12.61 f(6) < 6^{2\log 6 + 5}$, $27.69 f(8) < 8^{2\log 8+5}$ whence (10.3)(b) holds (by (10.1)(a)) for all $4 \le n \le 12$. If $n=2$ or 3 then by Table 2.7 (groups of small degree) $|\mathrm{Aut}(H\times E)| \le 120$ (resp. 5040) which $\le 2^7$ (resp. $3^{8.17}$), whence (b) holds also for $n=2$ and 3. If $E=\{1\}$ it leaves (in view of (9.1)(b), (c)) only the case when $m=2$, $n_1n_2=48$ or 50 and $|\mathrm{Aut}\ H|/n_1n_2f(n_1n_2) \le 3.05$. One verifies that then $|\mathrm{Aut}\ H| \le (n_1n_2)^{2\log(n_1n_2)+5}$.

Thus $E\ne\{1\}$. In this case our claim follows from (10.2) in view of (A7)(c) and the evident inequality $2n^{2\log n + 1} < n^{2\log n + 5}$ for $n \ge 2$.

To prove (10.3)(c) note that by (A7)(c) $nf(n) \le 2n^{2\log n + 1}$ for $n \ge 37$ and, in addition, one verifies directly that $|\mathrm{Aut}\ G| \le 2 \cdot 39^{2\log 39 + 1}$ for any sporadic G. Further one verifies that $3.05 \cdot 48 \cdot f(48) < 2 \cdot 48^{2\log 48 + 1}$ and $1.43 \cdot 50 f(50) < 2 \cdot 50^{2\log 50 + 1}$. These remarks together with (9.1)(b), (c) and (10.2) imply (10.3).

11. Estimates for finite quasi-primitive group.

Let k be an algebraically closed field of characteristic exponent $p=p(k)$, M a finite subgroup of $GL_n(k)$, and C the center of M. Recall (see R. Brauer [, p. 64, where q should be K]) that M is quasi-primitive if it is irreducible and if for every normal subgroup N of M, any two irreducible constituents are equivalent. Of course, any irreducible representation of a centrally simple group is quasi-primitive. Let $\bar{S}$ be the socle of M/C and S its preimage in M. Recall that $f(n) = (2n+1)^{2\log_3(2n+1)+1}$.

(11.1) Theorem. Suppose that M is quasi-primitive. Then M contains

(i) a normal subgroup A isomorphic to a direct product of alternating groups Alt_{m_i}, $m_i \geq 10$;

(ii) a normal perfect subgroup L centrally isomorphic to a direct product of finite simple groups of Lie p-type;

(iii) a normal subgroup E isomorphic to a direct product of extra-special groups whose orders are powers of distinct primes q with $q|n$, $q \neq p$;

such that

$$
\text{(a)} \qquad |M/CL| \leq \begin{cases} nf(n) & \text{if } n=2,3,5,7,9,10,11 \\ 4.1\, f(n) & \text{if } n=4 \\ 12.61\, f(6) & \text{if } n=6 \\ 27.69\, f(8) & \text{if } n=8 \\ 231\, f(12) & \text{if } n=12 \\ (n+2)! & \text{if } n > 12 \end{cases}
$$

(b) $|M/ACL| \le n^{2 \log n + 5}$ if $n \ge 2$

and $\le 2n^{2 \log n + 1}$ if $n \ge 39$

(c) $|M/S| \le [\log n]!\, n^2 \cdot |N_M(E)/Z_M(E) \cdot E|$

(11.2) Lemma. S is a central product of C with centrally simple groups $G_1,\dots,G_m$ and extraspecial groups $E_1,\dots,E_r$ with $|E_i| = p_i^{1+2a_i}$, $a_i > 0$, $p_i \ne p$, $p_i | n$, $p_i \ne p_j$ if $i \ne j$, $i,j=1,\dots,r$.

Proof. $\bar{S}$ is a direct product of simple groups. Write $\bar{S} = \bar{G}_1 \times \dots \times \bar{G}_m \times \bar{E}_1 \dots \times \bar{E}_r$ where the $\bar{G}_i$ are simple non-commutative and $\bar{E}_i$ are elementary abelian, $|\bar{E}_i| = p_i^{b_i}$, $p_i \ne p_j$ if $i \ne j$. Let $\tilde{G}_i, i=1,\dots,m,$ be the preimage of $\bar{G}_1$ in M. Then $G_i := [\tilde{G}_i, \tilde{G}_i]$ is centrally simple.

Let $\tilde{E}_i, i=1,\dots,r,$ be the preimage of $\bar{E}_i$ in M. Note that since M is primitive every normal commutative subgroup of M is central. The pairing $\bar{E}_i \times \bar{E}_i \to C$ given by $[\bar{x},\bar{y}]=[x,y]$ where x,y are preimages of x and y in $\tilde{E}_i$ does not depend on the choice of x and y. Let $\bar{F}_i := \{x \in \bar{E}_i | [x,E_i]=\{1\}\}$ and F_i the preimage of $\bar{F}_i$ in E_i. Then F_i is commutative. As it is a characteristic subgroup of $\tilde{E}_i$ and, therefore, of M, it is normal. Therefore $F_i \subseteq C$, i.e., $\bar{F}_i=\{1\}$. Thus our pairing is non-degenerate. It follows now from D. Gorenstein [ ] that $\tilde{E}_i=E_i \cdot C, i=1,\dots,r,$ where the E_i are extraspecial, $|E_i| = p_i^{1+2a_i}, p_i \ne p_j$ if $i \ne j$. The center of E_i is of order p_i and is contained in scalar matrices of degree n. Therefore $p_i | n, i=1,\dots,r$. Finally, $p_i \ne p$ $i=1,\dots,r,$ since the p-subgroup of C is trivial (k contains only trivial p-th roots of 1).

(11.3) Proof of (10.1). Let V be an irreducible component of the action of S on k^n and V and $v := \dim V$. Let, further, D be the product of the G_i

which are isomorphic neither to alternating groups Alt_a, $a \geq 10$, nor to groups of Lie p-type. Let U (resp. W) be an irreducible component of the action of ADE (resp. DE) on V (resp. U). Let $w := \dim W$, $u := \dim U$. We have by (10.1)(a) that Aut ADE is bounded as claimed by (11.1)(a) with n replaced by u. Let F(n) denote the right-hand side of (11.1)(a). Thus $|\text{Aut ADE}| \leq F(u)$.

Write $V = U \otimes \bar{U}$ where $\bar{U}$ is an irreducible representation of L. Let $N := N_{GL_n(k)}(L)/L \cdot Z_{GL_n(k)}(L)$. Then N can be identified with a subgroup of Out L. Since k^n is a multiple of $\bar{U}$ as the L-module (as k^n is primitive) it follows that N, acting on the irreducible representations of L by $\varphi^n(\ell) := \varphi(\tilde{n}\ell\tilde{n}^{-1})$, where $\tilde{n}$ is a lift of n to $N_{GL_n(k)}(L)$, preserves the equivalence class of φ. Then (5.5) together with the argument of the proof of (9.2) shows therefore that $|N| \leq [\log \bar{u}]!\ \bar{u}^2$.

The action of M on S induces automrophisms of A,D,E,L. Let us denote by ω_A and $\bar{\omega}_A$ (resp. ω_D, etc) the corresponding maps $\omega_A : M \to \text{Aut } A$ and $\bar{\omega}_A : M \to \text{Out } A$ etc. We have $\bar{\omega}_L(M) \subseteq N$ whence $|\bar{\omega}_L(M)| \leq [\log \bar{u}]!\bar{u}^2$. Clearly $\text{Ker } \omega_L \cap \omega_{ADE} \subseteq Z_M(S) = C$. Therefore $|M/CL| \leq |\bar{\omega}_L(M)| \cdot |\omega_{ADE}(M)| \leq |\bar{\omega}_L(M)| \cdot |\text{Aut ADE}| \leq [\log \bar{u}]!\bar{u}^2 \cdot F(u)$. One checks easily that $\bar{u}u \leq n$ implies $|M/CL| \leq F(n)$, thus proving (11.1)(a).

For (b) we have by (10.3)(b) that $|\text{Aut DE}| \leq w^{2 \log w + 5}$. We have also $|\bar{\omega}_A(A)| \leq [\log u/w]!2^{\log u/w} = [\log u/w]!u/w$ and $\text{Ker } \omega_A \cap \text{Ker } \omega_L \cap \text{Ker } w_{DE} = \{1\}$ whence as above

$$|M/AC| \leq |\bar{\omega}_A(M)| \cdot |\omega_L(M)| \cdot |\text{Aut DE}|$$
$$\leq [\log \bar{u}]!\bar{u}^2[\log u/w]!\ u/w\ \ w^{2 \log w + 5}$$

From $\bar{u} \cdot (u/w) \cdot w \leq n$ it follows that this $\leq n^{2 \log n + 5}$, as desired.

For the second estimate in (b) we have as above

$$|M/ACL| \le [\log \bar{u}]!\ \bar{u}^2 \cdot [\log u/w]!\ u/w \cdot |\mathrm{Aut}\ DE|.$$

If $w \ge 39$ we have by (10.3)(c) that $|M/ACL| \le 2w^{2 \log w + 1}$ which together with the above and the inequality $\bar{u} \cdot (u/w) \cdot w \le n$ implies the desired inequality. Assume that $s := \bar{u} \cdot u/w = 2$ (resp. 3) and $38 \ge w \ge [39/s]$. Then $|M/ACL| \le s^2 |\mathrm{Aut}\ DE|$ and one verifies using (10.2)(a) and (9.1)(c) that our claim holds in this case as well. If $s \ge 4$ then we can use $[\log \bar{u}]!\bar{u}^2[\log u/w]!u/w \le f(s)$ and invoke (A6) to conclude the proof.

Finally (c) is an evident corollary of the estimate in (9.1)(c) on Out H, the estimate we established on $(\mathrm{Out}\ L)_{\bar{U}}$ and of an evident estimate on the contribution of $N_M(E)$ to Out E.

12. Estimates for irreducible finite groups.

Let now k be an algebraically closed field of characteristic exponent $p=p(k)$.

(12.1) Theorem. Let H be an irreducible finite subgroup of $GL_n(k)$. Then H contains

(i) a commutative normal diagonalizable subgroup B;

(ii) a normal perfect subgroup L centrally isomorphic to a direct product of simple groups of Lie p-type

so that

(a) $|H/BL| \leq \begin{matrix} n^4(n+2)! & \text{if } n \leq 63 \\ (n+2)! & \text{if } n > 63 \end{matrix}$

Moreover

(b) for all $n \geq 2$

$$|H/BL| \leq (n+2)! \cdot n^{4020/((n-20)^2+1000)}$$

(c) for $n \leq 63$ we have

$$|H/BL| \leq (n+2)!\ n^{4\alpha_{irr}}$$

where α_{irr} is given by Table T12.1.

Table T12.1

	α_{irr}	α_{all}		α_{irr}	α_{all}
2	.34	.34	33	.83	.83
3	.7	.7	34	.53	.61
4	.78	.78	35	0	.6
5	.37	.53	36	.77	.77
6	.81	.81	37	0	.55
7	.67	.76	38	.47	.54
8	.88	.88	39	.71	.71
9	.89	.89	40	.44	.48
10	.58	.79	41	0	.47
11	.1	.81	42	.64	.64
12	.94	.94	43	0	.41
13	0	.81	44	.37	.4
14	.62	.77	45	.57	.57
15	.97	.97	46	.34	.34
16	.93	.93	47	0	.32
17	0	.77	48	.49	.49
18	.98	.98	49	0	.25
19	0	.81	50	.26	.26
20	.89	.89	51	.41	.41
21	.97	.97	52	.22	.22
22	.63	.78	53	0	.16
23	0	.75	54	.32	.32
24	.95	.95	55	0	.07
25	0	.75	56	.13	.13
26	.61	.73	57	.23	.23
27	.92	.92	58	.09	.09
28	.74	.74	59	0	0
29	0	.69	60	.13	.13
30	.88	.88	61	0	0
31	0	.67	62	0	0
32	.64	.65	63	.04	.04

(12.2) Proof. Set $V := k^n$ and let $V = \oplus_{i=1}^m V_i$ be an imprimitivity system for H on V. Let $H_i := \{h \in H \mid hV_i = V_i\}$. Then H_i is primitive on V_i. Let L_i be the largest perfect normal subgroup of H_i centrally isomorphic to a direct product of finite simple groups of Lie p-type and C_i the center of H_i. Then

(12.2.1) $|H_i/L_iC_i|$ satisifies (11.1)(a).

Let $\varphi : H \to \mathrm{Sym}_m$ be the homomorphism defined by $h(V_i)=V_{\varphi(h)i}$ and let $M := \mathrm{Ker}\ \varphi$. Then $MV_i=V_i$ for $i=1,\dots,m$. In particular, we have homorphisms $\omega_i : M \to H_i$. Set $M_i := \omega_i(M)$, $i=1,\dots,m$. Since M is normal in H we have that M_i is normal in H_i. Therefore each perfect factor of L_i either it is contained in M_i or M_i intersects it in its center. Let L_i' be the largest perfect normal subgroup of M_i which is centrally isomorphic to a direct product of finite simple groups of Lie p-type and let C_i' be the center of M_i. Then since $M_iL_iC_i/L_iC_i \simeq M_i/(L_iC_i \quad M_i)$ and since by the above comments $C_iL_i \cap M_i = C_i'L_i'$ we get

(12.2.2) $|M_i/L_iC_i| \leq |H_i/L_iC_i|$

Let $L := \cap_{i=1}^m \omega_i^{-1}(L_i')$, $B := \cap_{i=1}^m \omega_i^{-1}(C_i)$; clearly L and B are normal. Consider the evident homomorphism $\omega := \oplus_{i=1}^m \omega_i : M \to \Pi_{i=1}^m M_i$. Note that

(12.2.3) $\mathrm{Ker}\ \omega = \{1\}$.

We have $\omega(B) \subseteq \Pi_{i=1}^{m} C_i'$. This and (12.2.3) give that

(12.2.4) B is a commutative normal subgroup of M.

We also have $\omega(L) \subseteq \Pi_{i=1}^{m} L_i'$. Moreover, since $\operatorname{Ker} \omega = \{1\}$ and the projection of $\omega(L)$ on each L_i' is the whole L_i' it follows that

(12.2.5) L is perfect and centrally isomorphic to a direct of finite simple groups of Lie p-type. Clearly, $\omega(L)=\omega(M) \cap \Pi_{i=1}^{m} L_i'$. Thus

$$\omega(M)\Pi_{i=1}^{m} L_i'C_i'/\Pi_{i=1}^{m} L_i'C_i' \simeq \omega(M)/\omega(M) \cap \Pi_{i=1}^{m} L_i'C()$$
$$= \omega(M)/\omega(LB) \simeq M/LB.$$

Since evidently

$$|\omega(M)\ \Pi_{i=1}^{m}\ L_i'C_i'/\Pi_{i=1}^{m} L_i'C_i'| \leq |\Pi_{i=1}^{m} M_i/\Pi_{i=1}^{m} L_i'C_i'|$$

we get from (12.2.2):

$$|M/LB| \leq \Pi_{i=1}^{m}\ |H_i/L_iC_i|$$

Since H is irreducible on V it follows from Clifford theory that $H_i \simeq H_j$ for $i,j=1,\ldots,m$. Thus $\Pi_{i=1}^{m}\ |H_i/L_iC_i| = |H_1/L_1C_1|^m$. Since $M=\operatorname{Ker}\{H \to \operatorname{Sym}_m\}$ this implies

(12.2.6) $\quad |H/LC| \leq m!\ |H_1/L_1C_1|^m$

If now $n/m(= \dim V_1) > 12$ then (A9)(i) implies that $|H/BL| \le (n+2)!$ Thus it is sufficient to consider the cases when $n/m \le 12$. Set $r := n/m$. For $2 \le r \le 12$ values we use the estimate $|H_1/L_1C_1| < t_r$ where t_r is from Table T12.2. For $r=2,3,4,5$ we get a good estimate because all possible simple groups H_1 are known from Table T (groups of small degree) and we get good estimates on their normalizers from W. Feit [, p. 76] for $r=2$ and 3 (maxima are respectively for $H_1 \simeq Alt_5$ and $\simeq Alt_7$), from Zalessky [, p. 95] for $r=4$ and 5 (maxima in both cases are for Aut $B_2(3)$). For $6 \le r \le 11$, $r \ne 8$, we take $t_r = rf(r)$ (use (6.1)(d) to justify). For $r=8$ (resp. 12) we take $t_8 = |\mathrm{Aut}\ D_4(2)|$ (resp. $t_{12} = |\mathrm{Aut}(Suz)|$). Of course, it has to be verified that admitting central products for H_1 lowers the estimate, but this is straightforward in our range.

Set $F(m,r,t) := t^m(m!)/(rm+2)!$. For each $r \le 12$ we find, using a computer, the first m such that $F(m,r,t_r) < 1$, $F(m+1,r,t_r) \ge 1$. We denote this m by m_r; it is given in Table T12.2.

It is then easy to see that $F(m,r,t_r)$ 1 for all $m > m_r$. Namely

$$F(m+1,r,t_r) = F(m,r,t_r) \cdot t_r \cdot (m+1)/(rm+3)(rm+4)\dots(rm+r+2).$$

It is evident that $F_1(m,r,t_r) := t_r(m+1)/(rm+3)\dots(rm+r+3)$ decreases when m increases. By the definition of m_r we have $F_1(m_r,r,t_r) < 1$. Thus the same holds for all $m \ge m_r$.

Note that maximum of rm_r, $2 \le r \le 12$, is 63. Thus $|M| < (n+2)!$ if $n > 63$. For each $n \le 63$ the computer takes for an estimate on $|M|$ the maximum of $(n+2)!$ and all $t_r^m(m!)$ such that $r \le 12$, $mr=n$. One then checks, on the computer again, that these maxima satisfy the inequalities claimed in (12.1).

Table T12.2

r	2	3	4	5	6	7	8	9	10	11	12
t_r	60	2520	51840	51840	$1.24\cdot10^7$	$6.6\cdot10^7$	$1.05\cdot10^9$	$1.22\cdot10^9$	$4.47\cdot10^9$	$1.5\cdot10^{10}$	$9\cdot10^{11}$
m_r	30	21	13	4	7	5	3	3	2	2	1

13. Estimates for arbitrary finite linear groups.

Let k be an algebraically closed field of characteristic exponent $p=p(k)$.

(13.1) Theorem. Let G be a finite subgroup of $GL_n(k)$. Then G contains

(i) a triangulizable normal subgroup T, $T \supseteq O_p(G)$,

(ii) a normal subgroup L such that $L \supseteq O_p(G)$ and $L/O_p(G)$ is perfect and centrally isomorphic to a direct product of finite simple groups of Lie p-type

so that

(a) $|G/LT| \le \begin{cases} n^4 (n+2)! & \text{if } n \le 63 \\ (n+2)! & \text{if } n > 63 \end{cases}$

Moreover

(b) for all $n \ge 2$

$$|G/LT| \le (n+2)!\; n^{4020/((n-20)^2 + 1000)}$$

(c) for $n \le 63$ we have

$$|G/LT| \le (n+2)!\; n^{4\alpha_{all}}$$

where α_{all} is given in Table T12.1.

(13.2) This result implies one of R. Brauer and W. Feit [ ].

Corollary. Suppose that p^a is the highest power of p dividing $|G|$. Then G contains a normal commutative diagonalizable subgroup B such that

$$|G/B| \leq p^{3a}\ |G/L| \leq \begin{cases} p^{3a} n^4 (n+2)! & \text{if } n \leq 63 \\ p^{3a} (n+2)! & \text{if } n > 63 \end{cases}$$

Proof. Let p^c be the order of the Sylow p-subgroup of $L/O_p(G)$. Then one easily sees from (4.4.1) that $|L/O_p(G)| \leq p^{3c}$. Let $p^t = |O_p(G)|$. Write D for a p'-complement to $O_p(H)$ in T. Then D is commutative. The action of D by conjugation on $R := O_p(H)$ defines a linear action of D on a $\mathbf{F}_p$-vector space $\bar{R} := R/[R,R] \cdot R^p$, i.e., a homomorphism $\omega := D \to GL(\bar{R})$. Let $\bar{t} = \dim_{\mathbf{F}_p} R$ so that $GL(\bar{R}) \simeq GL_{\bar{t}}(\mathbf{F}_p)$. It is evident that every commutative p'-subgroup of $GL_{\bar{t}}(\mathbf{F}_p)$ has order $\leq p^{\bar{t}}$. Let $B := \mathrm{Ker}\ \omega$. By the above $|B| \geq |D|/p^{\bar{t}} \geq |D|/p^t$. By D. Gorenstein [ ] B (acting trivially on $\bar{R}$) acts trivially on R. Thus B is the p'-component of the center of T. In particular, it is a characteristic subgroup of T and, therefore, a normal subgroup of G. We have

$$|G/B| = |G/L| \cdot |L/R| \cdot |D/B| \cdot |R| \leq |G/L| \cdot p^{3c} \cdot p^t \cdot p^t$$

Since $p^t \cdot p^c$ is the order of a Sylow p-subgroup of L we have $t+c \leq a$. Thus the above gives

$$|G/B| \leq p^{3a}\ |G/L|$$

as claimed.

(13.3) Proof of (13.1). Set $V := k^n$. Let $V_1 := V \supseteq V_2 \supseteq \dots \supseteq V_m \supseteq V_{m+1} =: 0$ be a sequence of G-submodules of V such that $V_i \neq V_{i+1}$, $i=1,\dots,m$ and $W_i := V_i/V_{i+1}$ is irreducible for G for $i=1,\dots,m$. Set $n_i := \dim W_i$. The action of G on W_i defines a homomorphism $\omega_i : G \to GL(W_i) \simeq GL_{n_i}(k)$. Set $H_i := \omega_i(G)$.

Set $\omega := \oplus\omega_i : G \to \Pi GL_{n_i}(k)$. The kernel of ω is a unipotent subgroup of G. Since each H_i is irreducible it has no unipotent normal subgroups and, therefore, Ker ω is the largest unipotent normal subgroup of G. Since G is finite this latter is just $O_p(G)$. Thus

(13.3.1) $\quad \operatorname{Ker} \omega = O_p(G)$.

Set $H := G/O_p(G)$ and let $\bar{\omega}_i : H \to H_i$ be the map induced by $\omega_i, i=1,\dots,m$. Set $\bar{\omega} := \oplus\, \bar{\omega}_i$. We have

(13.3.2) $\quad \operatorname{Ker} \bar{\omega} = \{1\}$.

Let L_i and B_i be the subgroups claimed in (12.1) for H_i. Let $L' := \bigcap_{i=1}^m \bar{\omega}_i^{-1}(L_i)$, $B' := \bigcap_{i=1}^m \bar{\omega}_i^{-1}(B_i)$. As in the proof of (12.2.4) and (12.2.5) we get

(13.3.3) B' is a commutative normal subgroup of H.

(13.3.4) L' is perfect and centrally isomorphic to a direct product of finite simple groups of Lie p-type.

We also have

$$\bar{\omega}(H)\ \Pi_{i=1}^{m}\ L_iB_i/\Pi_{i=1}^{m}\ L_iB_i \simeq \bar{\omega}(H)/\bar{\omega}(H)\ \cap\ \Pi_{i=1}^{m}L_iB_i$$
$$\simeq \bar{\omega}(H)/\omega(L'B') \simeq H/L'B'.$$

Since

$$|\bar{\omega}(H)\ \Pi_{i=1}^{m}L_iB_i/\Pi_{i=1}^{m}L_iB_i| \le |\Pi_{i=1}^{m}H_i/\Pi_{i=1}^{m}L_iB_i|$$

we have that

(13.3.5) $$|H/L'B'| \le \Pi_{i=1}^{m}\ |H_i/L_iB_i|.$$

If now all $n_i \ge 64$ then our claim follows from (A9)(ii). In the remaining cases we use estimates on $|H_i/L_iB_i|$ for $n_i \le 63$ obtained by the computer as described in (12.2). For each pair m_1, m_2, $2 \le m_1, m_2 \le 64$ we take for a new estimate for m_1+m_2 the maximum of the estimate obtained before for m_1+m_2 and of the product of these estimates for m_1 and m_2. We repeat this procedure until it stabilizes. It turns out that it gives new (compared with §12) values only for $n \le 55$. Then one checks using the computer that the estimates claimed in (13.1) for $n \le 126$ hold for $|H/B'L'|$. The case when some $n_i \le 63$ and some ≥ 64 is handled as follows. If I is a subset of $1,\ldots,m$ and $\Sigma_{i\in I}n_i \le 126$ then, as remarked, the computer establishes the required estimate.

In view of (A9)(ii) it remains to show that if A is the estimate (hold by the computer) for $r \le 64$ and if $d \ge 64$ is such that $r+d > 126$ then

$$A(d+2)! \le (r+d+2)!$$

We know (by a check on a computer) that this holds for $d=64$. By induction suppose it holds for some d. Then for $d := d+1$ we have

$$A(d+3)! = A(d+2)!\,(d+3) \leq (r+d+2)!\,(d+3) < (r+d+3)!$$

whence our present claim:

(13.3.6) The estimates of (13.1) hold for H.

Let now L be the preimage of L in G and T the preimage of B. Since B is diagonalizable T is triangulizable. This concludes our proof of (13.1).

14. Extension to infinite linear groups.

Let K be an algebraically closed field of characteristic exponent $p=p(k)$. For a subgroup H of $GL_n(k)$ let H^c denote its Zariski closure and set $H^\circ := H \cap (H^c)^\circ$. When H^c is semi-simple it contains, by J. Tits [, Theorems 3 and 4], a smallest (automatically connected) normal subgroup such that $H/H \cap \mathcal{F}$ is periodic; we call this $\mathcal{F}$ the Tits subgroup of H^c.

(14.1) Theorem. Let G be a subgroup of $GL_n(k)$. Then there exist

(i) a normal triangulizable subgroup T of G,

(ii) normal subgroups F, P, L of G with $T=F \cap P \cap L$,

such that

(a) P^c/T^c and F^c/T^c are connected, semi-simple and commute,

(b) F^c/T^c is the smallest among normal subgroups $\mathcal{H}$ of G^c/T^c such that $\mathcal{H} \cap G/T$ projects onto the image of $(G/T)^\circ$ in the Tits subgroup of $(G/T)^c$,

(c) $FP \supseteq \mathcal{D}G^\circ$ and G°/FP is finite commutative; in particular, $F^cP^c=(G^c)^\circ$.

(d) P/T is direct product of infinite simple groups of Lie p-type,

(e) L/T is a direct product of finite simple groups of Lie p-type

(f) $|G/PFL| \le \begin{matrix} n^4(n+2)! & \text{if } n \le 63 \\ (n+2)! & \text{if } n \ge 64 \end{matrix}$

Moreover

(g) if G is finitely generated then $P=F$.

(14.2) Proof of (14.1). First, let us show how (g) follows from (a)-(f). By (c) FP is of finite index in G. Therefore FP is finitely generated if G is finitely generated. But then $P/T = PF/F$ is also finitely generated. This is not so if P/T is infinite (by (d)). Hence $P/T=\{1\}$ if G is finitely generated, whence (g).

(14.3) Now consider the case when Zariski-closure of G is connected and almost simple and G is periodic. By J. Tits [, Theorem 3 and 4(iv)] we have then $p > 1$ and G^c is defined over $\overline{\mathbb{F}}_p$. Let us fix a (rational) irreducible representation $g : G^c \to GL_d$. Since G^c is connected g is also primitive (for otherwise G^c would contain a subgroup of finite index preserving a decomposition of k^d into a direct sum).

Since G is irreducible and primitive on $V := k^d$ there exists a finitely generated (and, hence, finite) subgroup G_1 of G which is also irreducible and primitive. Write $G=\cup_{i=1}^{\infty}G_i$ where $G_{i+1} \supseteq G_i$ and $G_{i+1} \neq G_i$ (for example, $G_{i+1} = \langle x_i, G_i \rangle$ where $x_i \in G - G_i$). Let S_i be the preimage in G_i of the socle of G_i/center. Then S_i is a central product of centrally simple perfect groups $H_{i,1},\ldots,H_{i,m_i}$ and of extraspecial groups $E_{i1}\ldots,E_{i,r_i}$ of relatively prime power orders. It is clear that each $H_{i,j}$ is contained in some $H_{i+1,s}$. Similarly, $E_{i+1,j} \subseteq E_{i,s}$ if $E_{i+1,j}$ and $E_{i,s}$ have <u>not</u> relatively prime orders. Therefore

(14.3.1) there exists c such that $m_i=m_c$, $r_i=r_c$ for $i \geq c$ and $E_{i,j}=E_{c,s}$ for $i \geq c$ and appropriate j and s.

We can assume (after renumeration) that $c=1$, $H_{i+1,j} \supseteq H_{i,j}$, $E_{i+1,j}=E_{i,j}$ for $i \geq 1$. Then set $H_j := \cup_{i=1}^{\infty}H_{i,j}$, $E_j := E_{1,j}$. We have that the H_j and the E_s commute. Therefore so do H_j^c and the E_s. Clearly $\Pi_j H_j^c \cdot \Pi_s E_s$ is a normal subgroup of G^c. Since G^c is connected and almost simple this implies that $m_1=1$ and $r_1=0$ (that is, there is only one H_j and no E_s).

Set $H_i := H_{i,1}$, $P := \cup_{i=1}^{\infty}H_i$. Then

(14.3.2) H is centrally simple.

By a recent (overlapping) results of V. Belyaev [ ], A. Borovik [ ], N. Chernikov [ ], B. Hartley and B. Shute [ ], S. Thomas [ ] (see, for definiteness S. Thomas [, Theorem 2]) we get

(14.3.3) P is centrally simple of Lie p-type over a subfield K of $\overline{\mathbb{F}}_p$.

We have that P is normal in G and therefore, G acts by automorphisms on P. By R. Steinberg [, Theorems 30 and 36], any automorphism of P is a product of a diagonal, graph, field, and inner one. However, since G^c is connected and since graph automorphisms do not belong to G^c and field automorphisms do not induce automorphisms of G^c we get

(14.3.4) G/P consists of diagonal automorphisms.

This implies

(14.3.5) G/P is finite commutative; it is given in column A_d of Table T4.4.

(14.4) Assume now that $\mathcal{Y} := G^c$ is connected and semi-simple. Then by J. Tits [, Theorems 3 and 4(i)] $\mathcal{Y}$ contains a connected normal subgroup $\tilde{\mathcal{F}}$ which is the smallest such subgroup with the condition that the image of G in $\mathcal{Y}/\tilde{\mathcal{F}}$ is periodic. Write $\mathcal{Y}_1,\ldots,\mathcal{Y}_m$ for almost simple quotients of $\mathcal{Y}/\tilde{\mathcal{F}}$. Let G_i be the image of G in $\mathcal{Y}_i$, $i=1,\ldots,m$. Then (14.3) applies to G_i and we have by (14.3.5) and (14.3.3) that $\mathcal{D}G_i$ is centrally simple of Lie p-type. Set $P_i := \mathcal{D}G_i$. Let $\varphi_i : G \to G_i$ be the natural projection. Then $\tilde{P} := \cap_{i=1}^m \varphi_i^{-1}(P_i)$ satisfies

(14.4.1) $\varphi_i(\tilde{P})=P_i$, $\mathcal{D}G \subseteq \tilde{P}$, $|G/\tilde{P}| < \infty$

Let $\varphi : \mathcal{Y} \to \tilde{\mathcal{F}}/\text{center}$ be the natural projection and let $P := \text{Ker}\ \varphi \cap \tilde{P}$. Then $\varphi_i(P)$ is normal in P_i. Therefore, since P_i is centrally simple, $\varphi_i(P)$ is either in the center of P_i or contains $\mathcal{D}P_i$. Since P is a subgroup of $\mathcal{Y}_1 \ldots \mathcal{Y}_m$ it follows that

(14.4.2) P is centrally isomorphic to a direct product of some of the P_i.

Next, P is normal in $\tilde{P}$ and, by construction, $\tilde{P}$ induces only inner automrophism of P. Thus

(14.4.3) $\tilde{P} = P \cdot F$ where $F = Z_{\tilde{P}}(P)$.

Let $\mathcal{F} := F^c$, $\mathcal{P} := P^c$. Then in view of (14.4.1) and (14.4.3).

(14.4.4) $\mathcal{F} \cdot \mathcal{P} = G^c$

Now, if $\mathcal{H}$ is a smallest factor of $\mathcal{Y}$ such that $\mathcal{H} \cap G$ projects onto the image G in $\tilde{\mathcal{F}}$ then, clearly, $\mathcal{H} \subseteq \mathcal{F}$. If $\mathcal{H} \neq \mathcal{F}$ then $\varphi(G)/\varphi(\mathcal{H} \cap G)$ is isomorphic to the projection of G onto the complement to $\mathcal{H}$ in $\mathcal{F}$ and, in particular, is $\neq \{1\}$. Thus

(14.4.5) $\mathcal{F}$ is the smallest among normal subgroups $\mathcal{H}$ of G^c such that $\varphi(\mathcal{H} \cap G) = \varphi(G)$.

(14.4.6) Remark. Note that since G may induce non-inner (hence, diagonal, automorphisms of P there is no decompostion similar to (14.4.3) for G.

(14.4.7) Example. Let $H := PGL_n(\bar{\mathbb{F}}_p[t])$. For $c \in \mathbb{F}_p$ we have a specialization homomorphism $\varphi_c : t \to c$ of $\bar{\mathbb{F}}_p[t]$ to $\bar{\mathbb{F}}_p$. It induces an epimorphism $\varphi_c : H \to PGL_n(\bar{\mathbb{F}}_p)$. Let $c_1, \ldots, c_m \in \mathbb{F}_p$. Then we define a homomorphism $\varphi := id \times \Pi_{i=1}^m \varphi_{c_i} : H \to (PGL_n)^{m+1} =: \mathcal{Y}$ with $G := \varphi(H)$ Zariski-dense in $\mathcal{Y}$. The group $\tilde{\mathcal{F}}$ is then the first simple factor of $\mathcal{Y}$. Write $\mathcal{Y} = \tilde{\mathcal{F}} \times \Pi_{i=1}^m \mathcal{Y}_i$ where $\mathcal{Y}_i := (\varphi_{c_i}(H))^c$. Let $\mathcal{H}$ be a direct factor of $\mathcal{Y}$. If $\mathcal{F}$ is not a factor of $\mathcal{Y}_1$ then $G \cap \mathcal{Y}_1 = \{1\}$. If $\mathcal{H} = \tilde{\mathcal{F}} \times \Pi_{i \in I} \mathcal{Y}_i$ for I a subset of $\{1, \ldots, m\}$, then $G/G \cap \mathcal{H} \simeq \Pi_{i \notin I} \varphi_{c_i}(H)$. Thus $\mathcal{Y}$ itself is the smallest normal subgroup $\mathcal{H}$ of $\mathcal{Y}$ such that the projection of $G/G \cap \mathcal{H}$ on $\tilde{\mathcal{F}}$ is equal to that of G. So $\mathcal{F} = \mathcal{Y}$.

We conclude this example by pointing out that it is not necessary that all simple factors of $\mathcal{F}$ are of the same type. For example, replacing H by $\varphi_{c_1}^{-1}(PSO_n(\mathbb{F}_p))$ and then proceeding as above we get that $\mathcal{Y}_1 \simeq PSO_n$.

(14.5) Assume now that G is primitve. Let C be the center of G (so that $T=C$ in our case). Let $\mathcal{Y} := (G^c)^\circ$. Since G is primitive $\mathcal{Y}$ is semi-simple. Set $\mathcal{Y} = \mathcal{Y}_1 \ldots \mathcal{Y}_s$, an almost direct product of almost simple groups. The group $\tilde{N} := N_{GL_n}(\mathcal{Y})/Z_{GL_n}(\mathcal{Y})$ consists of permutations of factors and of outer (that is, graph) automorphisms of the $\mathcal{Y}_i$. By (14.4) G° contains normal subgroups P and F such that (14.1)(a)-(d) hold with $T=C$. Thus (since $P^cF^c = (G^c)^\circ$ and G°/PF consists of diagonal automorphisms of P) it follows that for $N := N_{GL_n(k)}(PF)/Z_{GL_n(k)}(PF)$ we have $|N| \leq |\tilde{N}| \cdot |$Outer diagonal automorphism group of $P|$. As in (4.5.4) this imples

(14.5.1) $\quad |N| \leq n^2 \log n$

It is, therefore, now remains to study $Z := Z_G(PF)$. This latter group is finite and, since G is primitive, it is completely reducible. An argument similar to ones we used in Sections 10 and 11 shows that Z contains a nromal subgroup L centrally isomorphic to a direct product of simple finite groups of Lie p-type such that Z/L satisfies the conclusions of (11.1).

Now a repetition of arguments of Sections 12 and 13 yields (14.1) in complete generality.

References

[A] M. ASCHBACKER, On the maximal subgroups of finite classical groups, Invent. Math. 76(1984), 469-514.

[Ba] H. BASS, Theorems of Jordan and Burnside for algebraic groups, J. Algebra 82(1983), 245-254.

[Be] V. BELYAEV,

[Bo] A. BOROVIK,

[Br] R. BRAUER, On finite projective groups, pp. 63-82 in "Contributions to Algebra", Academic Press, New York, 1977.

[BF] R. BRAUER and W. FEIT, An analogue of Jordan's theorem in characteristic p, Ann. of Math. 84(1966), 119-131.

[Cm] P. CAMERON,

[Ch] N. CHERNIKOV,

[Dc] L.E. DICKSON, "Linear Groups", Dover, New York, 1958.

[Dd] J. DIEUDONNÉ, "La Géométrie des Groupes Classiques", 3rd ed. Springer-Verlag, Berlin/Heidelberg/New York, 1971.

[F1] W. FEIT, The current situation in the theory of finite simple groups, pp. 55-93 Vol 1 Actes du Congrès International des Mathématiciens, Gauthier-Villars, Paris, 1971.

[F2] W. FEIT, "The Representation Theory of Finite Groups", North-Holland, Amsterdam 1980.

[G] D. GORENSTEIN, "Finite Groups", Chelsea, New York 1980.

[GL] D. GORENSTEIN and R. LYONS,

[HS] B. HARTLEY and G. SHUTE, Monomorphisms and direct limits of finite groups of Lie type, Quart. J. Math. 35(1984), 49-71.

[H] B. HUPPERT, "Endliche Gruppen", Springer-Verlag, Berlin/Heidelberg/New York 1967.

[J] G.D. JAMES,

[LS] V. LANDAZURI and G.M. SEITZ, On the minimal degrees of projective representations of finite Chevalley groups, J. Algebra 32(1974), 418-443.

[L] M. LIEBECK,

[MVW] C.R. MATTHEWS, L.N. VASERSTEIN AND B. WEISFEILER, Congruence properties of Zariski-dense subgroups, Proc. Lond. Math. Soc. 48(1984), 514-532.

[N] M. NORI, Subgroups of $SL_2(\mathbb{Z})$ and $SL_n(\mathbb{F}_p)$, preprint.

[Sc] I. SCHUR, Über die Darstellung der symmetrischen und der alternierenden Gruppe, J. reine angew Math. 139(1911), 155-250.

[Sp] A. SPEISER, Die Theorie der Gruppen von Endlicher Ordnung, Berlin, 1923.

[S1] R. STEINBERG, "Lectures on Chevalley Groups", Yale University Lecture Notes, 1968.

[S2] R. STEINBERG, Generators, relations and coverings of algebraic groups, II, J. Algebra 71(1981), 527-543.

[Th] S. THOMAS,

[Tt] J. TITS,

[V] L.N. VASERSTEIN,

[Wg] A. WAGNER,

[W1] B. WEISFEILER, Strong approximation for Zariski dense subgroups of semi-simple algebraic groups, Ann. of Math. 120(1984), 271-315.

[W2] B. WEISFEILER, A post-classification version of Jordan's theorem on finite linear groups, Proc. Nat. Acad. Sci. 81(1984), 5278-5279.

[W3] B. WEISFEILER, On the maximal subgroups of the finite classical groups (notes).

[Z] A.E. ZALESSKY, Linear groups, Russian Math. Surveys 36(1981), no. 5, 63-128.