17. Splitting fields

Let k be an algebraically closed field of characteristic $p>1$. For a finite group H we denote by $e(H)$ its exponent, the smallest integer e such that $h^e = 1$ for all $h \in H$. By C. Curtis and I. Reiner [, (70.24)] every representation of H over $\mathbb{F}_p(\sqrt[e]{1})$ ($\subseteq \mathbb{F}_{p^{\varphi(e)}}$, where $\varphi(e)$ is the Euler function) is absolutely irreducible. In other words if $H \subseteq GL_n(k)$ then a conjugate of H is contained in $GL_n(\mathbb{F}_p(\sqrt[e]{1}))$. Let e_0 be the least common multiple of the exp[illegible]ts of the universal central extensions of the sporadic simple groups [illegible] groups of Lie type having [illegible]al extensions (see (4.3.3) for a list).

For a field K and a finite group G we denote by $I(KG)$ a set of representatives of the equivalence classes of the irreducible K-representations of G. For $f \in I(KG)$ we denote by $K_0(f)$ the extension of the prime field K_0 of K given by $K_0(f) := K_0(\mathrm{Tr}\, f(G))$, meaning the field generated by the character values of the $g \in G$ under f.

(17.1) **Theorem.** Let G be a centrally simple finite group not isomorphic to a group of Lie p-type and $f : G \longrightarrow GL_n(k)$ an irreducible representation. Then

$$[\mathbb{F}_p(\mathrm{Tr}\, f) : \mathbb{F}_p] \leq \max(2, \varphi(e_0), n^2)$$

If n is sufficiently large ($n \geq \sqrt{|F_1|}$, e.g. $n \geq 9 \cdot 10^{26}$ would suffice) then

$$[\mathbb{F}_p(\mathrm{Tr} f) : \mathbb{F}_p] \leq \max(2, n^2).$$

(17.2) **Corollary.** Let $H_0 = {}^c\bar{X}_a(p^{rc})$ be a classical finite simple group of Lie p-type and let $H \geq H_0$, $H \subseteq \mathrm{Aut}\, H_0$. Suppose that $r > \max(2, \varphi(e_0), (2a+1)^2)$. Let M be a maximal subgroup of H. Then either

(a) M is one of the groups on the M Aschbacher [ ] list $\underset{\sim}{\mathcal{C}}_H$

or (b) the socle of M is simple of Lie p-type.

(17.3) Remark. Actually (17.2) can be sharpened by adding divisibility properties. For example, let $M_1, \dots, M_{N(n)}$ be the list of universal central extensions of simple groups which can have a representation of degree n.

For each such M_i and $f \in I(\mathbb{C}M_i)$ let a_f be the degree of a maximal cyclic subextension of $\mathbb{Q}(\mathrm{Tr} f)$. Let $a_1, \dots, a_{R(n)}$ be the collection of all numbers a_f for the M_i, $i = 1, \dots, N(n)$, and $f \in I(\mathbb{C}M_i)$. Then the conclusion of (17.2) holds if

$$r \geq \max_{1 \leq i \leq R(n)} (\mathrm{LCD}(r, a_i), 2).$$

Proof of (17.3). M. Aschbacher [ ] states that unless M belongs to $\underset{\sim}{C}_H$ the socle G of M is simple and can not be written in field smaller than $\mathbb{F}_{p^r}$. Since H_0 can be embedded into $GL_n(\overline{\mathbb{F}}_p)$, $n \le 2a+1$ (see, e.g., beginning of (16.3)) our claim follows from (17.1).

17.4) Proof of (17.1). First let us consider an ordinary representation $g : G \longrightarrow GL_m(\mathbb{C})$. Suppose $K := \mathbb{Q}(\mathrm{Tr}\, g)$.