The Hilbert-Siegel Problems
and Group Theory solving cases of them
by Michael D. Fried
Preprint remnant from 1986
from when I left UC Irvine to work
with John Thomson at Univ. of Florida
All other pieces of this preprint have now
appeared elsewhere (9/28/15)

Now we turn to the Hilbert-Siegel problems. Let K be a number field and let $f(x,y) \in K[x,y]$ be an absolutely irreducible polynomial. Define:

$$\mathcal{R}(f;\mathcal{O}_K) = \{x_0 \in \mathcal{O}_K \mid f(x_0,y) \text{ is reducible in } K[y]\}.$$

For $g \in K(y)$ define $V(g;\mathcal{O}_K) = \{x_0 \in \mathcal{O}_K \mid$ there exists $y_0 \in K$ with $g(y_0) = x_0\}$.

LEMMA 1.1. <u>There exist</u> $g_1,\cdots,g_\ell \in K(y)$ <u>with these properties</u>:

(1.1). a) $\mathbb{P}^1_y \xrightarrow{\varphi(g_i)} \mathbb{P}^1_x$ <u>has at most two places over</u> $x = \infty$, $i = 1,\cdots,\ell$; <u>and</u>

b) $\mathcal{R}(f;\mathcal{O}_K) = V(g_1;\mathcal{O}_K) \cup \cdots \cup V(g_\ell;\mathcal{O}_K) \cup V'$ <u>where</u> V' <u>is a finite set</u>.

<u>Proof</u>. This is a slight generalization of [Fr,4; Theorem 1] and a special case of [Fr,1; Theorem 1.1]. ∎

Assume in Lemma 1.1 that $g_1,\cdots,g_\ell$ is a minimal set of rational functions satisfying (1.11). Then $g_1, \cdots, g_2$ is a complete list, up to linear fractional changes of the variables, of the rational functions g satisfying these properties: $\sigma(g)$ satisfies (1.1)a); $f(x, g(y))$ is reducible; and for $g = g^{(1)}(g^{(2)})$ with $\deg(g^{(2)}) > 1$, $f(x, g^{(1)}(y))$ is not reducible. For the rest of this section consider the case $f(x,y) = h(y) - x$. Then, according to Lemma 1.1, the study of $\mathcal{R}(h(y) - x; \mathcal{O}_K)$ reduces to this:

THE 1ST HILBERT-SIEGEL PROBLEM: Describe explicitly, for all n and m

(1.2) $\{(h,g) \mid h \in \mathbb{C}[y]$ of degree n, $g \in \mathbb{C}(z)$ of degree m, $\mathcal{V}(h,g)$ is newly reducible and (1.1)a) holds for $\sigma(g)\}$.

[References in this paragraph refer to the basic result that reduces to whether the Galois closure of h, g covers are the same in [Fr, 7]

In terms of group theory this means that we have a group $G(\sigma)$ for which expressions (1.7) a) and b), and (1.8) a) and b) hold, and (from Lemma 1.3) either $n = m$ ((1.7) c)) or $T_2(\sigma(r))$ is a product of an m_1-cycle and an m_2-cycle with $m_1 + m_2 = m$ and n is the least common multiple of m_1 and m_2. Further special cases:

(1.3) a) $\{(h,g)$ that satisfy (1.2) with $g = g_1/g_2$ the ratio of relatively prime polynomials of degree $2 \cdot n$, g_2 a power of a quadratic with distinct zeros$\}$; and

b) $\{(h,g)$ that satisfy (1.3)a) with h indecomposable$\}$.

THEOREM 1.2. For $h(y) \in \mathbb{Z}[y]$ of degree unequal to 5, the collection of $x_0 \in \mathbb{Z}$ for which $h(y) - x_0$ is reducible consists of $V(h; \mathbb{Z})$ and a finite set. The exceptional cases of degree 5 include all polynomials that satisfy

(1.14) a) $\frac{d}{dy}(h(y)) = (y-a)\cdot(y-b)\cdot(y-c)\cdot(y-d)$, a,b,c and d distinct, and

b) $h(a) = h(b)$.

Reduction to §2.c) From [Fr,4; Corollary 2] this follows from the classification of those h for which there exists g with (h,g) satisfying (1.13)b). In turn, from expression (1.7), the result follows from the classification of double degree representations - §2.c). Example 1.5 for $n = 5$ consists of polynomials which are exceptional for the statement of the theorem, but the general exceptional case is given by condition (1.14). This corresponds to $((1\,2)(3\,4), (1\,5), (5\,3), (1\,2\,3\,4\,5)^{-1})$ as a description of the branch cycles for $\mathbb{P}^1_y \xrightarrow{\varphi(h)} \mathbb{P}^1_x$. To get a specific example with coefficients in $\mathbb{Q}$, take $a = -b = \sqrt{2}$, so

$$h(y) = (1/5)\cdot y^5 - ((c+d)/4)\cdot y^4 + ((c\cdot d - 2)/3)\cdot y^3$$

$$+ (c+d)\cdot y^2 - 2\cdot c\cdot d\cdot y \ .$$

Then $h(\sqrt{2}) = h(-\sqrt{2})$ together with the condition that the coefficients are in $\mathbb{Q}$ implies that $c\cdot d = -2/5$. ∎

§2. Doubly transitive representations.

§2.a) With an n-cycle.

Return to the case (1.9) b) of Davenport's problem: h is an indecomposable polynomial, and g is linearly inequivalent to h, but Kronecker conjugate to h. From [Fr,1; Theorem 2.1], in addition to conditions (1.7) a), b) and c) with T_1 replacing $T(h)$ and T_2 replacing $T(g)$,

(2.1) T_1 and T_2 are equivalent (but permutation inequivalent) group representations - both doubly transitive.

From [CuKanSe] the classification of finite simple groups ([Gor]) yields the classification of all simple groups with a faithful doubly transitive representation. In particular, their results imply

THEOREM 2.1. <u>If</u> (1.7) c) <u>and</u> (2.1) <u>hold, then either</u> $n = 11$ <u>and</u> $G(\underset{\sim}{\sigma}) = PSL(2, \mathbb{Z}/(11))$ <u>or</u> $PSL(K, \mathbb{F}(q)) \subseteq G(\underset{\sim}{\sigma}) \subseteq P\Gamma L(k, \mathbb{F}(q))$ <u>with</u> $n = (q^k - 1)/(q - 1)$ <u>for some</u> $k \geq 3$ <u>and</u> $q = p^t$ <u>for some prime</u> p. <u>If, in addition,</u> (1.7) a) (<u>and</u> b)) <u>hold, the allowable integers</u> n <u>are exactly</u> 7, 11, 13, 15, 21 <u>and</u> 31. <u>Thus, these are exactly the integers for which there is a newly reducible polynomial pair</u> (h, g) (§1.b)) <u>with</u> h <u>indecomposable</u>.

<u>Notation and collation of results from</u> [F,1,2,3] <u>and</u> [Fr,1]. The general linear group $GL(k, \mathbb{F}(q))$ acts on $\mathbf{F}(q)^k$. Denote the group generated by $GL(k, \mathbb{F}(q))$ and the pth power map on the coordinates by $\Gamma L(k, \mathbb{F}(q))$. Then $P\Gamma L(k, \mathbb{F}(q))$ is the quotient of $\Gamma L(k, \mathbb{F}(q))$ induced by the action of $\Gamma L(k, \mathbb{F}(q))$ on the points of

$\mathbb{P}^{k-1}(\mathbb{F}(q))$ - the points of projective k-1-space with coordinates in $\mathbb{F}(q)$. Finally, $PSL(k, \mathbb{F}(q))$ (resp., $PGL(k, \mathbb{F}(q))$ is the image in $P\Gamma L(k, \mathbb{F}(q))$ of the subgroup $SL(k, \mathbb{F}(q))$ of matrices of determinant 1 (resp., of $GL(K, \mathbb{F}(q)))$.

The first sentence of the theorem is from [CuKanSe]. The second sentence is outlined in [Fr,1; p.592] and completed in detail in [F,1; Theorem 4]. These include simple demonstrations that $\underline{\sigma} \in (S_n)^r$ with $r = 3$ or 4 and $r = 4$ only if $n = 7$ or 13. The groups that occur are these ([F,2]): $n = 11$ and $G = PSL(2, Z/(11))$; and $G = P\Gamma L(k,q)$ with $(k,q) = (3,2), (4,2), (5,2), (3,3)$ or $(3,4)$. The degree 11 (nonstandard) representations of $PSL(2, Z/(11))$ arise from an <u>Hadamard design</u> ([H,2; p.291, item #5 in Table 1]). The approach to the case $n = 13$ in the appendix avoids the [F,2] use of character tables; it is especially valuable in the case $n = 11$.

One final point about the case $n = 31$. The elimination of the case $(k,q) = (3,5)$ goes something like this: In the action of the group on $\mathbb{P}^2(Z/(5))$, [Fr,1; p.592] shows that we may assume that $r = 3$, $\sigma(1)$ is of order 2 and $\sigma(2)$ is of order 3, and $\text{ind}(\sigma(1)) = (31-5)/2 = 13$. From (1.7) a) conclude $\text{ind}(\sigma(2)) = 17$, a contradiction to $\sigma(2)$ being of order 3. Thus the case $n = 31$ arises from collineations acting on the points of $\mathbb{P}^4(Z/(2))$. We easily find elements $\sigma(1)$ and $\sigma(2)$ of order 2 and 3 whose indices correctly sum to 30. With a little additional work we can guarantee that they generate a transitive group. From these two conditions an easy lemma shows that $\sigma(1)\cdot\sigma(2) = \sigma(3)^{-1}$ is an n-cycle. The alternative procedure of [F,2] uses the character table to show that in certain conjugacy classes represented by elements $\sigma(1)$ and $\sigma(2)$ of order 2 or 3 there are elements $\sigma(1)'$ and $\sigma(2)'$ whose product is an n-cycle. This method has the advantage that it automatically identifies $G(\underset{\sim}{\sigma})$ as a particular subgroup of $P\Gamma L(k, \mathbb{F}(q))$. ∎

§2.b) With a double degree representation.

Recall the notation $G(T_1,1) = \{\sigma \in G \mid (1)T_1(\sigma) = 1\}$.

Def.2.2. Call a triple (G,T_1,T_2) a double degree representation of degree n if T_1 and T_2 are faithful representations of G of respective degrees n and $2\cdot n$, and the following conditions hold:

(2.2) a) T_1 is doubly transitive and T_2 is not doubly transitive;

b) there exists $\sigma \in G$ with $T_1(\sigma)$ an n-cycle and $T_2(\sigma)$ a product of two n-cycles;

c) $G(T_1,1)$ contains none of $G(T_2,j)$, $j = 1,\cdots,2\cdot n$; and

d) the restriction of T_2 to $G(T_1,1)$ is intransitive.

Let (G,T_1,T_2) be a double degree representation of degree n . Let χ_i be the group character of T_i , for $i = 1,2$, and write $\chi_i = 1 + \theta_i$. Then θ_1 is an irreducible character of G ([H,1;p.279, Th.16.6.5]). If $n = 3$, then $G(T_2,1) = \langle Id.\rangle$ and if $n = 4$, $G(T_2,1)$ (of index 8 in G) must be contained in one of the subgroups of S_4 isomorphic to S_3 . In both cases these contradict (2.2) c), so $n \geq 5$.

The next lemmas consider separately the possibilities that T_2 is primitive and imprimitive. In this subsection we apply them (to Proposition 2.5) somewhat frivolously: to the case that $n = p$ is a prime ≤ 23 . In Theorem 2.6, however, we apply Lemma 2.3 in the case that $G = A_n$ or S_n . Since we require §3 for a full proof of Lemma 2.3 our perspective on the result could be misleading. Finally, as we comment in §2.c), an easier argument than Lemma 2.4 suffices for

Proposition 2.7 (and therefore Theorem 1.10). But, other applications (of §4) do seem to require the full lemma.

LEMMA 2.3. <u>Suppose</u> T_2 <u>is primitive. Then the following hold:</u>

(2.3) a) $2\cdot n = \ell^2 + 1$ <u>for some positive integer</u> ℓ ;

b) $G(T_2,1)$ <u>has orbits of length</u> $\ell\cdot(\ell-1)/2$ <u>and</u> $\ell\cdot(\ell+1)/2$ <u>on</u> $\{2,\cdots,2\cdot n\}$;

c) $G(T_2,1)$ <u>acts faithfully on the orbit of b) of length</u> $\ell\cdot(\ell+1)/2$, <u>and if</u> $n \neq 5$, <u>also on the orbit of length</u> $\ell\cdot(\ell-1)/2$; <u>and</u>

d) $\theta_2 = \chi + \eta$ <u>for characters</u> χ <u>and</u> η <u>of</u> G <u>with</u> $\eta(\mathrm{Id.}) = n$.

<u>Reduction to</u> §3.b). Consider the representation T_3 of G acting on the ordered pairs of integers (i,j) , $1 \le i \le n$, $1 \le j \le 2\cdot n$ by the following formula:

$$(i,j)T_3(\sigma) = ((i)T_1(\sigma)\ ,\ (j)T_2(\sigma))\ ,\quad \sigma \in G\ . \qquad (2.4)$$

From (2.2) d), T_3 is intransitive. The Lemma is therefore exactly the statement, described as an unpublished result, of the opening paragraph of [Sco,3]. For $n = p$, a prime, this appears in [Wie,1] which also gives an indication for general n of how (2.3)d) implies the remaining results. An improvement for p prime, showing that ℓ cannot be a prime, appears in [Sco,2]. ∎

LEMMA 2.4. <u>Suppose that</u> T_2 <u>is imprimitive. If</u> n <u>is a prime, then either</u> G <u>has a subgroup of index</u> 2 <u>or</u> G <u>is one of the groups that appears in the statement of Theorem 2.1</u>.

Proof. There exists a subgroup H of G with $G(T_2,1) \subsetneq H \subsetneq G$. As n is a prime, either $(G:H) = 2$ or $(G:H) = n$. Assume G has no subgroup of index 2. Let $T^H_{G(T_2,1)}$ be the permutation representation of H given by the right cosets of $G(T_2,1)$. Denote its group character by $1^H_{G(T_2,1)}$. In the rest of our arguments we use the Frobenius reciprocity theorem ([H,1;p.284, Theorem 16.7.3]). In particular, $1^H_{G(T_2,1)}$ is $1_H + \alpha$ where α is a character of H, and $\alpha(Id) = 1$.

Now consider α^G, the character induced by α on G. Recall: If $G = H \cup H\cdot g_1 \cup \cdots \cup H\cdot g_n$ are the right cosets of H in G, then $\alpha^G(g) = \sum_{i=1}^{n} \bar{\alpha}(g_i\cdot g\cdot g_i^{-1})$ where

$$(2.5)\qquad \bar{\alpha}(g_i\cdot g\cdot g_i^{-1}) = \begin{cases} 0 & \text{if } g_i\cdot g\cdot g_i^{-1} \notin H \\ \alpha(g_i\cdot g\cdot g_i^{-1}) & \text{if } g_i\cdot g\cdot g_i^{-1} \in H \end{cases} \qquad \text{([H,1;Theorem 16.7.1])}.$$

We claim that the subgroup H induces a coset representation T^G_H of G that is equivalent as a group representation to T_1. Indeed, we have only to show that $1^G_H = 1_G + \theta_1$ (in the notation prior to Lemma 2.3). Divide the remainder of the proof into parts.

Part 1. θ_1 appears in $1^G_{G(T_2,1)}$. Use the inner product $(\ ,\ )_{G(T_2,1)}$ to compute. For α' a character of G let $res_{G(T_2,1)}(\alpha')$ be the restriction of α' to $G(T_2,1)$. Since $1_G + \theta_1$ is the character of T_1, and since restriction of T_1 to $G(T_2,1)$ breaks up into a sum of at least two permutation representations, this restriction contains the character $1_{G(T_2,1)}$ with multiplicity at least 2. That is

$$(2.6)\qquad (1_{G(T_2,1)}, res(1_G + \theta_1))_{G(T_2,1)} \geq 2 .$$

From Frobenius reciprocity, the expression on the left of (2.6) equals

(2.7) $(1^G_{G(T_2,1)}, 1_G + \theta_1)_G = (1^G_{G(T_{2,1})}, 1_G)_G + (1^G_{G(T_2,1)}, \theta_1)_G$.

Again, by Frobenius reciprocity, $(1^G_{G(T_2,1)}, 1_G)_G = 1$, so $(1^G_{G(T_2,1)}, \theta_1)_G \geq 1$. This statement means that θ_1 appears in $1^G_{G(T_2,1)}$.

Part 2. θ_1 appears in 1^G_H. Since $1^G_{G(T_2,1)} = (1_H + \alpha)^G = 1^G_H + \alpha^G$, the irreducible representation θ_1 appears either in 1^G_H or in α^G . If θ_1 appears in α^G , then $\alpha^G = \theta_1 + \beta$ for some character β of G . But $\alpha^G(\mathrm{Id.}) = (G:H)\cdot\alpha(\mathrm{Id.})$ and $\theta_1(\mathrm{Id.}) = n-1$, so $\beta(\mathrm{Id.}) = 1$. Thus β is a rational degree 1 character. Either the kernel of β is a subgroup of G of index 2, contrary to our initial assumption that G has no such group, or $\beta = 1_G$, contrary to the appearance of 1_G in $1^G_{G(T_2,1)}$ with multiplicity exactly 1. Conclude there is no such β , and that θ_1 appears in 1^G_H .

Write $1^G_H = 1_G + \theta_1 + \lambda$ with λ a character of G . Since $\lambda(\mathrm{Id.})$ is the degree of λ , clearly $\lambda = 0$. So, the permutation representation T_H is group equivalent to T_1 . But, from (2.2)c) these representations are permutation inequivalent. ∎

PROPOSITION 2.5. <u>Let</u> (G,T_1,T_2) <u>be a double degree representation of degree</u> n . <u>Then either</u>

(2.8) a) $A_n \subseteq G \subseteq S_n$, <u>or</u>

b) $PSL(k,\mathbb{F}(q)) \subseteq G \subseteq P\Gamma L(k,\mathbb{F}(q))$

for some $k \geq 2$ with $n = (q^k - 1)/(q - 1)$ and T_1 the representation of G on the points of $P^{k-1}(\mathbb{F}(q))$ (notation as in Theorem 2.1.).

Proof. First exclude the possibility that G is a solvable group. Double transitivity implies that such a group is of prime power degree ([Bu,2;p.202 - Burnside notes that this appears in the letter of May 29th, 1832, from Galois to his friend Chevalier]). But, since $T_1(\sigma)$ is an n-cycle for some $\sigma \in G$, $n = p$ a prime or $n = 4$ and $G = A_4$ ([Ri;p.27]). Further, if $n = p$, then a p-sylow is normal. Deduce that $|G(T_1,1)| = p - 1$, $|G(T_2,1)| = (p - 1)/2$ and $G(T_1,1)$ contains some conjugate of $G(T_2,1)$ contrary to (2.2)c).

Since G is not solvable, [CurKanSe] implies that the Proposition holds or G is one of the following: (i) $PSL(2,\mathbb{Z}/(11))$, $n = 11$; (ii) the Mathew group of degree 11; or (iii) the Mathew group of degree 23. In cases (i),(ii) and (iii), since $2 \cdot n$ is not of the form $1 + \ell^2$, Lemma 2.3 implies that T_2 is imprimitive. These are simple groups, so they contain no subgroups of index 2. Thus, Lemma 2.4 implies that G has a permutation representation equivalent, but permutation inequivalent to T_1. This excludes (ii) and (iii) (Theorem 2.1). Also, a subgroup of index 22 of $PSL(2,\mathbb{Z}/(11))$ would be of order 30. This is impossible, however: in a group of order 30 the 3-sylow and 5-sylow centralize each, so there is an element of order 15. In the action of this element on the 12 points of $\mathbb{P}^1(\mathbb{Z}/(11))$, its 3rd power would fix more than 3 points, and so would be the identity. This leaves only the groups in the statement of the proposition. ∎

§2.c) Proof of Theorem 1.10.

First, a serious application of Lemma 2.3 to improve Proposition 2.5.

THEOREM 2.6. *For* (G, T_1, T_2) *a double degree representation of degree* $n \neq 5$, $PSL(k, \mathbb{F}(q)) \subseteq G \subseteq P\Gamma L(k, \mathbb{F}(q))$.

Proof. We must eliminate case (2.8) a) from Proposition 2.5. Assume $n \geq 6$. Since A_n is simple, a subgroup H of index $1 < k < n$ in A_n would give an embedding of A_n in S_k, a clear impossibility. Thus A_n has no subgroup of index less than n. Consider two cases.

Case 1. T_2 is primitive. From Lemma 2.3, $|G(T_2,1)| \leq (\ell \cdot (\ell-1)/2)!$ with $2 \cdot n = \ell^2 + 1$. But $|G(T_2,1)| \geq n!/4 \cdot n = (1/4) \cdot ((\ell^2 - 1)/2)!$. Thus, $\ell \leq 3$ and $n \leq 5$, contrary to assumption.

Case 2. T_2 is imprimitive. If $G(T_2,1) \subsetneq H \subsetneq G$, then either $(G:H) = 2$ or $1 < (A_n : A_n \cap H) \leq n$. In either case A_n has a subgroup of index n containing $G(T_2,1)$. For $n > 6$, any subgroups of A_n (or S_n) of index n are conjugate ([Bu,2;p.208]). So, contrary to (2.2)c), $G(T_2,1)$ is contained in a conjugate of $G(T_1,1)$. If $n = 6$, then $G = A_6$ has a subgroup of index 12, and thus a subgroup of order 30; an impossibility by the same argument that appears at the end of proof of Proposition 2.5. This leaves only the elimination of the case $G = S_6$. We outline this interesting exercise.

Note that S_5 has 6 cyclic subgroups of order 5. Denote the normalizers of these, groups of order 20, by $N_1 = N(\langle(12345)\rangle)$, $N_2, \cdots, N_6$. Let S_5 act on these by conjugation to give an embedding $H(1)$ of S_5 in S_6. Let $H(1), \cdots, H(6)$ be the conjugates of $H(1)$

and let $G(1),\cdots,G(6)$ be the conjugates of the standard copy of S_5 in S_6. Any subgroup K of index 6 in S_6 would have a subgroup of order 20 in common with each of $H(1),\cdots,H(6)$, $G(1),\cdots,G(6)$. So the elements of K of order 3 would be distinct from those of $H(1),\cdots,G(6)$ - contrary to an easy computation. Conclude that an imprimitive subgroup of S_6 of index 12 is a conjugate of $A_6 \cap H(1)$ or $A_6 \cap G(1)$. Now apply Lemma 2.3 and the observation that $A_6 \cap H(1)$ is a transitive subgroup of S_6. ∎

Proof of Theorem 1.10. From Theorem 2.6 we need only consider the possibility that $PSL(k, \mathbb{F}(q)) \subseteq G \subseteq P\Gamma L(k, \mathbb{F}(q))$. For the first time, however, we need the conditions $G = G(\underset{\sim}{\sigma})$ where - (1.7) -

$$(2.9) \quad \sum_{j=1}^{r-1} \mathrm{ind}(T_1(\sigma(j))) = 2\cdot(n-1), \quad T_1(\sigma(r)) \text{ is an } n\text{-cycle and}$$
$$\sum_{j=1}^{r-1} \mathrm{ind}(T_2(\sigma(j))) = 2\cdot n .$$

We divide the proof into parts.

Part 1. Elimination of the case $k = 2$ and q odd. Here T_1 is the representation of G on the points of the projective line $P^1(\mathbb{F}(q))$, $n = q+1$. If we let the integer 1 correspond to the point at ∞, then $G(T_1,1)$ is the group of semi-linear transformations on $A^1(\mathbb{F}(q)))$ in G. Clearly, $G(T_1,1)$ is $N_G(P)$, the normalizer in G of the p-sylow group P of translations by elements of $\mathbb{F}(q)$.

Suppose H is a group for which $P \subset H \subseteq P\Gamma L(2,\mathbb{F}(q))$. Compute easily that either H is a subgroup of $N_G(P)$, or else H contains $PSL(2,\mathbb{F}(q))$. If q is odd, then, with no loss, assume that $G(T_2,1)$ contains P. Since T_2 is faithful, $PSL(2,\mathbb{F}(q)) \not\subseteq G(T_2,1)$. So $G(T_2,1) \subseteq N_G(P) = G(T_1,1)$, contrary to condition (1)d). If $p = 2$

and $P \subseteq G(T_2,1)$ conclude again that $G(T_2,1) \subseteq G(T_1,1)$. Thus we may assume that $p = 2$ and $P \not\subseteq G(T_2,1)$.

Part 2. The case $k = 2$ and $q = 2^e$. Consider the group $H_1 = PSL(2,\mathbb{F}(q)) \cap G(T_2,1)$. If $q = 2^e$, then $|H_1| = 2^{e-1}\cdot(q-1)\cdot k$ where k divides $q+1$. If K is a proper subgroup of $PSL(2,\mathbb{F}(2^e))$ which contains no conjugate of the 2-sylow P , then K satisfies one of the following conditions ([Bu,3] and [Bu,2;p.452]):

(2.10) a) $K \simeq PSL(2,\mathbb{F}(2^f))$ for some f dividing e ;

b) K contains a cyclic subgroup C with either $|C| = 2$ or odd, and $(K:C) \leq 2$; or

c) $|K| = 12, 24$ or 60.

Take K to be H_1 . Conclude: If (2.10)a), then $H \simeq PSL(2,2^{e-1})$ with $e-1 \mid e$, so $e = 2$; if (2.10)b) and $|C| = 2$, then $2^{e-1} \mid 4$ and $n = 3$, contrary to assumptions; and if (9)b) and $|C|$ is odd, then $e = 2$. Finally, consider case by case the possibilities of (2.10)c). If $|H_1| = 24$, then $e = 4$ and $2^4 - 1 \mid |H_1|$, which is not the case. And if $|H_1| = 12$ or 60 , then $e = 3$ and $2^3 - 1 \mid |H_1|$, which is not the case.

We have thus eliminated all cases except $q = 2^2$, $n = 5$. But $PSL(2,\mathbb{F}(4)) \simeq A_5$, as permitted by the statement of the proposition.

Part 3. Elimination of the case $k > 2$. Finally we use condition (2.9). A list of the possible cases appears in comments in Theorem 2.1. We identify these again to outline the analysis that preceeds from [F,2] to their elimination:

(i) $PSL(3,\mathbb{Z}/(2))$, $n = 7$; (ii) $PSL(3,\mathbb{Z}/(3))$, $n = 13$;

(iii) $PSL(4,\mathbb{Z}/(2))$, $n = 13$; (iv) $P\Gamma L(3,\mathbb{F}(4))$, $n = 21$; and

(v) $PSL(5,\mathbb{Z}/(2))$, $n = 31$.

For H a subgroup of G and T_H the associated permutation representation of G , decompose T_H as a direct sum $\sum_{i=1}^{r} c_i \cdot \Gamma_i$ of irreducible group representations Γ_i (with positive multiplicity c_i) of G . From [Bu,2;p.274], $\sum_{i=1}^{r} (c_i)^2$ equals the number of orbits of H in the representation T_H and c_i is the number of times the identity representation on H appears in the restriction of Γ_i to H . Also, $(G:H) = \sum_{i=1}^{r} c_i \cdot \deg(\Gamma_i)$. Thus, if the character table of G is handy, we may, on occasion, use it to exclude the existence of a subgroup of index equal to a specific integer n . List all positive linear combinations $\sum_{i=1}^{r} c_i \cdot \chi_i$ of $\mathbb{Q}$-valued characters for which $\sum_{i=1}^{r} c_i \cdot \deg(\chi_i) = n$. If the representation T_H is known to be non-doubly transitive, then $r \geq 3$ ([Bu,2;p.338]). These comments suffice to show that $PSL(5,\mathbb{Z}/(2))$ contains no subgroup of index 62 and that $PSL(4,\mathbb{Z}/(2))$ contains no subgroup of index 30 ([Li;p.267] and comments from [F,2;p.241-2]). This eliminates (iii) and (v).

Eliminate cases (i) and (ii) by applying Lemma 2.3 to conclude that T_2 is imprimitive, contrary, since $\deg(T_1)$ is prime, to [Fr,4; proof of Corollary 3]. This application of [Fr,4] uses (2.9), as we must also in case (iv). Follow the method of the Appendix in case (iv) ([F,2; Theorem 2]) to see that we may assume that $\sigma(1)$ is of order 2, $\sigma(2)$ is of order 4, $\mathrm{ind}(T_1(\sigma(1))) = 7$ and $\mathrm{ind}(T_1(\sigma(2))) = 13$. From the character table, however, compute that $\mathrm{ind}(T_2(\sigma(1))) = 21$ and $\mathrm{ind}(T_2(\sigma(2))) = 29$ ([F,2;Lemma 3.13]). This contradicts $\mathrm{ind}(T_2(\sigma(1))) + \mathrm{ind}(T_2(\sigma(2))) = 42$. ∎

Finally, note that we could have eliminated any use of Lemma 2.4 from the proof of Theorem 1.10 by applying [Fr,4; proof of Corollary 3].

§3. The rank of primitive double degree representations.

§3.a) Orbital characters.

This small subsection is primarily a survey. Let $T: H \to S_m$ be any transitive permutation representation. Consider the representation $T^{(2)}$ of H acting on the ordered pairs of integers (i,j), $1 \le i,j \le m$ by this formula:

$$(3.1) \qquad (i,j)T^{(2)}(\sigma) = ((i)T(\sigma), (j)T(\sigma)) \quad \text{for} \quad \sigma \in H .$$

Denote by $0_1, \cdots, 0_t$ the orbits of H under $T^{(2)}$ and order these so that $0_1 = \{(i,i) \mid 1 \le i \le m\}$.

Def.3.1. The jth orbital character, γ_j, is defined by the formula $\gamma_j(h) = |\{u \in \{1,2,\cdots,m\} \mid (u,(u)T(h)) \in 0_j\}|$, $h \in H$. Thus γ_1 is the character of T. Note that $\sum_{j=1}^{t} \gamma_j(h) = m$ and that $\gamma_j(h)$ is a sum of the lengths of certain of the orbits of the centralizer, $\mathrm{Cen}_H(h)$, of h in H under the representation T.

The centralizer ring, $V(H,T)$, of the representation T on H consists of the matrices of $\mathbb{M}(m,\mathbb{C})$ that commute with all permutation matrices arising from H through T. Define A_i, the matrix associated to the orbit 0_i by this formula: the $j \times k$ entry of A_i is 1 if $(j,k) \in 0_i$, 0 otherwise. The collection $\{A_i\}_{i=1}^{t}$ is a $\mathbb{Q}$-basis for $V(H,T)$. Also, by using idempotents of $V(H,T)$, there is a natural correspondence between isomorphism classes of indecomposable $\mathbb{C}[H]$ submodules of $\mathbb{C}^m$ and irreducible $V(H,T)$ submodules of $\mathbb{C}^m$ ([Sco,4; p.103]). Thus, to each irreducible character constituent, χ_s' of the character $\chi(T)$ of T, there is a corresponding character, Δ_s, of the centralizer ring. We may express the orbital characters in terms of the χ'_s's and the Δ_s's . More precisely:

LEMMA 3.2. For each i, $\gamma_i = \sum_s \Delta_s({}^{tr}A_i)\cdot\chi'_s$. Also, for each s, $\Delta_s(1)\cdot\chi'_s = (\chi'_s(1)/m)\cdot\sum_{i=1}^{t}(\Delta_s(A_i)/n(i))\cdot\gamma_i$ where

$$n(i) = |\{j \in \{1,\cdots,m\} \mid (1,j) \in O_i\}| .$$

Outline of proof. For $h \in H$, calculate that $\gamma_i(h)$ is the trace of ${}^{tr}A_i\cdot T(h)$ to get the first equation. Denote the centrally primitive idempotent associated to Δ_s by c_s . Write c_s as a general linear combination of the A_i's . Then multiply by A_i and take traces to calculate that

$$c_s = (\chi'_s(1)/m)\cdot\sum_i(\Delta_s(A_i)/n(i))\cdot{}^{tr}A_i . \tag{3.2}$$

The second formula follows by applying $T(h)$ on the right of both sides of (3.2). ∎

Certain orthogonality relations immediately follow by applying $\Delta_{s'}$ to expression (3.2):

$$\sum_i(\Delta_s(A_i)\cdot\Delta_{s'}({}^{tr}A_i))/n(i) = \begin{cases} m\cdot\Delta_s(1)/\chi'_s(1) & \text{if } s = s' \\ 0 & \text{otherwise} \end{cases} . \tag{3.3}$$

If we take $\chi_1 = 1$, then $\Delta_1(A_i) = n(i)$. As a special case of (3.3): $\sum_i \Delta_s(A_i)$ is m if $s = 1$, 0 otherwise.

Observe that $V(H,T)$ is commutative precisely when $\chi(T)$ is multiplicity free, or, equivalently, when $\Delta_s(1) = 1$ for all s . There are two further orthogonality relations, the second of which requires that $V(H,T)$ be commutative, as a result of taking the trace, respectively, of A_i and of $A_i \cdot {}^{tr}A_j$:

(3.4) a) $$\sum_s \chi'_s(1)\cdot\Delta_s(A_i) = \begin{cases} m & \text{if } i = 1 , \\ 0 & \text{otherwise; and} \end{cases}$$

b) $$\sum_s \chi'_s(1)\cdot\Delta_s(A_i)\cdot\Delta_s({}^{tr}A_j) = \begin{cases} m\cdot n(i) & \text{if } i = j \\ 0 & \text{otherwise} \end{cases} .$$

In addition, $\Delta_s(A_i)$ is an algebraic integer. For $\sigma \in G(\bar{\mathbb{Q}}/\mathbb{Q})$, $\Delta_s(A_i)^\sigma = \Delta_{s'}(A_i)$ whenever $(\chi'_s)^\sigma = \chi'_{s'}$, and $\Delta_s({}^{tr}A_i)$ is the complex conjugate of $\Delta_s(A_i)$.

Finally, crucial to the proof of Proposition 3.6 is an inequality from [HiN].

LEMMA 3.3. <u>For each</u> i , $|\Delta_s(A_i)/n(i)| \le \Delta_s(1)$, <u>with equality for</u> $i \neq 1$ <u>only when</u> G <u>is imprimitive</u>.

§3.b) <u>Proof of Lemma</u> 2.3.

Return to the notation of §2.b): (G,T_1,T_2) is a double degree representation with $\chi_i = 1 + \theta_i$ the group character of T_i . Denote by $\sigma(\infty)$ the element of G for which $T_1(\sigma(\infty))$ is an n-cycle and $T_2(\sigma(\infty))$ is a product of two n-cycles. From Part 1 of the proof of Lemma 2.4,

(3.5) $$\theta_1 \text{ is a constituent of } \chi_2 .$$

Let $U = \langle\sigma(\infty)\rangle$ be the group generated by $\sigma(\infty)$.

The next lemma allows us to use expression (3.4)b).

LEMMA 3.4. <u>If T_2 is primitive, then the nonidentity constituents of χ_2 are faithful. In particular χ_2 is multiplicity free. Therefore the centralizer ring $V(G,T_2)$ is commutative.</u>

<u>Proof</u>. Let χ' be an irreducible constituent of χ_2, $\chi' \neq 1$. Suppose that $\ker(\chi')$, the kernel of the homomorphism of G into the endomorphism space afforded by χ', is nontrivial. Since T_2 is faithful, $\mathrm{Ker}(\chi')$ is not contained in $G(T_2,1)$. And, as T_2 is primitive, $G = G(T_2,1)\cdot\ker(\chi')$. Clearly, therefore, the restriction, $\mathrm{res}_{G(T_2,1)}(\chi')$, of χ' to $G(T_2,1)$ is still irreducible. Now apply Frobenius reciprocity (as in Lemma 2.4):

$$(3.6)\quad (1^G_{G(T_2,1)}, \chi')_G = (1_{G(T_2,1)}, \mathrm{res}_{G(T_2,1)}(\chi'))_{G(T_2,1)} = 0 \quad .$$

Since $1^G_{G(T_2,1)} = \chi_2$, this contradicts that χ' appears in χ_2, and thus $\ker(\chi')$ is trivial.

In particular, the above paragraph shows that χ_2 contains no 1-dimensional character (excluding 1). Now use (3.5). If the irreducible representation θ_1 occurs with multiplicity 2, then $\chi_2 - 2\cdot\theta_1 - 1$ is a dimension one character, contrary to our previous conclusion. Otherwise, the restriction of $\chi_2 - \theta_1 - 1$ to U consists of 1-dimensional characters, each of multiplicity 1. In particular, $\chi_2 - \theta_1 - 1$, and therefore χ_2, is multiplicity free. ∎

The restriction of χ_2 to U contains the identity character on U with multiplicity 2. Let $\chi_1' = 1$, $\chi_2' = \theta_1$ and χ_3' the unique irreducible constituent of χ_2, different from 1, whose restriction to U contains 1. Apply the notation of §3.a). Since χ_2' and

χ_3' are $\mathbb{Q}$-valued, $\Delta_2(A_i)$ and $\Delta_3(A_i)$ are in $\mathbb{Z}$ for all i.

LEMMA 3.5. *For each* $i = 1,\cdots,t$ *, and each* $\sigma \in U$, $\gamma_i(\sigma) = 0, n$ *or* $2\cdot n$. *For some value of* i, $\gamma_i(\sigma) \neq 0$. *If* $\gamma_i(\sigma) = n$ *there is a unique* $j \neq i$ *with* $\gamma_j(\sigma) = n$; *and if* $\gamma_i(\sigma) = 2\cdot n$, *then* $\gamma_j(\sigma) = 0$ *for all* $j \neq i$.

There is at most one value of i *for which* $\gamma_i(\sigma) = 2\cdot n$ *for some* $\sigma \neq \mathrm{Id.}$ *in* U. *For such an* i, $n(i) = n-1$ *and* $\Delta_2(A_i) = -1$.

Proof. The first part is immediate from $\gamma_i(\sigma)$ being the sum of certain orbit lengths of $\mathrm{Cen}_G(\sigma)$, and the formula $\sum_i \gamma_i(\sigma) = 2\cdot n$. For the last paragraph of the lemma apply Lemma 3.2 to find χ_2' in terms of the γ_i's. Since $1 + \chi_2'$ is the regular character on U, $\chi_2'(\sigma) = -1$. So

$$(3.7) \qquad -1 = (n-1)\cdot\Delta_2(A_i)/n(i) \quad \text{or} \quad n(i) = (n-1)\cdot(-\Delta_2(A_i)) .$$

If $n(i) = 2\cdot(n-1)$, then there would be $j \neq 1$ with $n(j) = 1$. This contradicts the primitivity of χ_2. Hence $n(i) = n-1$ and $\Delta_2(A_i) = -1$. Similarly, the index i is unique. ∎

If $\gamma_i(\sigma) = 2\cdot n$ for some $\sigma \neq \mathrm{Id.}$ in Lemma 3.5, call i "bad." Otherwise call i "good."

PROPOSITION 3.6. *If all* $i \neq 1$ *are good, then* $\sum_{i=2}^{t} \Delta_3(A_i)/n(i) = r-3$. *In particular,* $r = 3$, *and Lemma 2.3 holds*.

Proof. Among the constituents of χ_2, only χ_1' and χ_3' contain 1 when restricted to U. For any i, Lemma 3.2 implies that

$$(\gamma_i,1)_U = \Delta_1(A_i) + \Delta_3({}^{tr}A_i) = n(i) + \Delta_3(A_i) \quad .$$

If i is "good," then γ_i takes only the values 0 or n on U. Clearly, therefore, $(\gamma_i,\gamma_i)_U = n\cdot(\gamma_i,1)_U = n\cdot(n(i)+\Delta_3(A_i))$. But Lemma 3.2 gives another expression for this:

$$(\gamma_i,\gamma_i)_U = \sum_{s,s'} \Delta_s({}^{tr}A_i)\cdot\Delta_{s'}(A_i)\cdot(\chi_s',\chi_{s'}')_U \quad .$$

Divide by $n(i)$ and sum over all i to get

$$(3.8) \quad \sum_{i=1}^{t}(\gamma_i,\gamma_i)_U/n(i) = \sum_{s,s'}(\chi_s',\chi_{s'}')_U\cdot\sum_i \Delta_s({}^{tr}A_i)\cdot\Delta_{s'}(A_i)/n(i) =$$

$$= \sum_s(\chi_s',\chi_s')_U\cdot(2\cdot n)/\chi_s'(1) = t\cdot 2\cdot n \quad .$$

Recall that $\gamma_1 = \chi_2$ and therefore that $(\gamma_1,\gamma_1)_U = 4\cdot n$. Use the assumption that all $i \neq 1$ are "good" (and the first expression for $(\gamma_i,\gamma_i)_U$) to recompute (3.8):

$$(3.9) \quad \sum_{i=1}^{t}(\gamma_i,\gamma_i)_U/n(i) = 4\cdot n + \sum_{i=2}^{t}(1+\Delta_3(A_i)/n(i))\cdot n \quad .$$

Combine (3.8) and (3.9) to get $\sum_{i=2}^{t}\Delta_3(A_i)/n(i) = r-3$.

From the inequality $1 = (\chi_3',1)_U \geq (n-1+\chi_3'(1))/n$, conclude that $\chi_3'(\sigma) \leq 0$ for some $\sigma \neq \mathrm{Id.}$ in U . From Lemma 3.5 there exist distinct i and j with $\gamma_i(\sigma) = \gamma_j(\sigma) = n$. Apply Lemma 3.2 to χ_3' to get $0 \geq (\chi_3'(1)/2)\cdot(\Delta_3(A_i)/n(i) + \Delta_3(A_j)/n(j))$. From the expression of the last paragraph, (3.10) $$\sum_{k\neq 1,i,j} \Delta_3(A_k)/n(k) \geq r-3 \quad .$$

The left side of (3.10) has $r-3$ terms, so there exists k with $\Delta_3(A_k)/n(k) \geq 1$ if $r > 3$. Since χ_2 is primitive, conclude that $r = 3$ from Lemma 3.3. Now conclude Lemma 2.3 from [Wie,1]. ∎

In the remainder of the subsection we assume that there exists a "bad" value of i; let it be $i = 2$. This leads to a contradiction which, combined with Proposition 3.6, concludes the proof of Lemma 2.3. Note that, since $n(i) = n-1$ only for $i = 2$, $A_i = {}^{tr}A_i$.

LEMMA 3.8. For each $\sigma \in U$, $\gamma_2(\sigma) = 0$ or $2\cdot n$.

Proof. Use Lemmas 3.1 and 3.2 to calculate:

$$(\gamma_2,\gamma_2)_U = \sum_{s,s'} \Delta_s(A_2)\cdot\Delta_{s'}(A_2)\cdot(\chi'_s,\chi'_{s'})_U =$$

$$\sum_s \Delta_s(A_2)\cdot\Delta_s(A_2)\cdot\chi'_s(1) + 2\cdot\sum_{s\neq 2}\Delta_2(A_2)\cdot\Delta_s(A_2)\cdot\chi'_s(1) +$$

$$(-2\cdot\Delta_2(A_2)\cdot\Delta_2(A_2)\cdot(n-1) - 2\cdot\Delta_2(A_2)\cdot\Delta_3(A_2) - 2\cdot\Delta_2(A_2)\cdot\Delta_1(A_2))$$

$$+ 2\cdot\Delta_1(A_2)\cdot\Delta_3(A_2) = 2n\cdot(n-1) + 0 - 2\cdot(-1)^2\cdot(n-1)$$

$$+ 2\cdot\Delta_3(A_2) + 2\cdot(n-1) = 2\cdot n\cdot(n-1+\Delta_3(A_2)) \quad .$$

Thus $(\gamma_2,\gamma_2)_U = 2\cdot n\cdot(\gamma_2,1)_U$. But, if α (resp., β) is the number of times that γ_2 takes the value n (resp., $2\cdot n$) on U, then

$$\alpha + 2\cdot\beta = (\gamma_2, 1)_U \ , \text{ or } \ \alpha\cdot n + 4\cdot\beta\cdot n = (\gamma_2, \gamma_2)_U \ .$$

Conclude that $\alpha = 0$ - the conclusion of the lemma holds. ∎

LEMMA 3.9. For $j > 2$,

$$(3.11) \quad 0 = n\cdot(\Delta_2(A_j) + \Delta_3(A_j)) + (\Delta_3(A_2) + 1)\cdot(n(j) - \Delta_2(A_j)) \ .$$

Proof. From Lemma 3.5 combined with Lemma 3.8, $(\gamma_2, \gamma_j)_U = 0$. On the other hand, a direct calculation of $(\gamma_2, \gamma_j)_U$, as in Lemma 3.8 gives the result. ∎

LEMMA 3.10. For $\sigma \in U - \{Id.\}$ and $a = \chi_3'(1)\cdot\Delta_3(A_2)/(n-1)$, either $\gamma_2(\sigma) \neq 0$ and $\chi_3'(\sigma) = a$, or $\gamma_2(\sigma) = 0$ and $\chi_3'(\sigma) = -a$.

Proof. If $\gamma_2(\sigma) \neq 0$ then $\gamma_2(\sigma) = 2\cdot n$ (Lemma 3.8). So $\gamma_j(\sigma) = 0$ for $j \neq 2$, and the result follows from an application of the second formula of Lemma 3.2 to χ_3' .

If $\gamma_2(\sigma) = 0$, Lemma 3.5 produces unique i and j with $\gamma_i(\sigma) = \gamma_j(\sigma) = n$, $2 \neq i \neq j$. Again apply Lemma 3.2:

$$(3.12) \quad \chi_3'(\sigma) = (\chi_3'(1)/2)\cdot(\Delta_3(A_i)/n(i) + \Delta_3(A_j)/n(j)) \ .$$

Use Lemma 3.9 on each of the terms on the right side of expression (3.12):

$$(3.13) \quad 0 = n\cdot(\Delta_2(A_i)/n(i) + \Delta_2(A_j)/n(j) + \Delta_3(A_i)/n(i) + \Delta_3(A_j)/n(j))$$

$$+ (\Delta_3(A_2) + 1)\cdot(2 - \Delta_2(A_i)/n(i) - \Delta_2(A_j)/n(j)) \ .$$

Since $-1 = ((n-1)/2)\cdot(\Delta_2(A_i)/n(i) + \Delta_2(A_j)n(j))$ (use Lemma 3.2 on χ_2'), (3.13) gives

$$0 = \bar{n}\cdot((-2/(n-1)) + \Delta_3(A_i)/n(i) + \Delta_3(A_j)/n(j) + (\Delta_3(A_2)+1)\cdot(2+2/(n-1)) \,. \tag{3.14}$$

A little rearrangement of (3.14) plugged into the right side of expression (3.12) concludes the lemma. ∎

The conclusion of Lemma 3.10 is the key to the remaining argument. It, together with the multiplicity free $\mathbb{Q}$-valued restriction of χ_3' to U, will force $\chi_3'(1)$ to be 1, $n-1$ or n. The first two cases contradict Lemma 3.4 since they imply that χ_2 has a nontrivial degree constituent. If $\chi_3'(1) = n$, then the conclusion of Proposition 3.6 holds, anyway; although this contradicts Lemma 3.5 as $\gamma_i(\sigma)$ must be nonzero for at least two values of $i > 2$ for some $\sigma \in U$.

PROPOSITION 3.11. <u>Let</u> ξ <u>be a multiplicity free</u> $\mathbb{Q}$-<u>valued character on a finite cyclic group</u> U <u>of order</u> n. <u>Let</u> a' (<u>resp.</u>, a) <u>be the g.c.d of all values of</u> ξ <u>on</u> U (<u>resp.</u>, <u>of all values of</u> ξ <u>on</u> $U-\{\mathrm{Id.}\}$). <u>Then</u> $a' \mid n$ <u>and there exists a character</u> ψ <u>on the subgroup of index</u> a' <u>in</u> U <u>such that</u> $\xi = \psi^U$, <u>the character induced on</u> U <u>by</u> ψ.

<u>Similary, if</u> ξ <u>is not the regular representation of</u> U, <u>then</u> $a \mid n$ <u>and</u> $\xi = \psi^U$ <u>where</u> ψ <u>is a character of the subgroup of index</u> a. <u>In either situation, if</u> a' (<u>resp.</u>, a) > 1, <u>then</u> ξ <u>vanishes on any generator of</u> U.

Proof. If $a' = 1$ we are done. Otherwise let p be a prime divisor of a'. Then $\xi \bmod p \equiv 0$, so $p \mid n$. Write $U = U(1) \times U(2)$ where $U(1)$ is a p-sylow of U, and let $U(0)$ be the subgroup of $U(1)$ of index p. We divide the rest of the proof into parts.

Part 1. Properties of characters of $U(1) \times U(2)$. The general irreducible rational character of $U(1) \times U(2)$ is $\mu \cdot \varphi$ where μ (resp., φ) is a rational irreducible character of $U(1)$ (resp., $U(2)$). In addition, μ is either 1 or the form $1_L^{U(1)} - 1_K^{U(1)}$ with $L \subseteq K$ subgroups of $U(1)$ and $(K:L) = p$: an easy combinatorial consequence of counting that this gives the correct number of irreducible rational characters of $U(1)$.

Part 2. $\xi|_{U(0) \times U(2)} = p \cdot \psi$. In the notation of Part 1, if $K \neq U(1)$, then the restriction of $1_L^{U(1)} - 1_K^{U(1)}$ to $U(0)$ is p times the character $1_L^{U(0)} - 1_K^{U(0)}$. Thus, $1_{U(1)}$ and $1_{U(0)}^{U(1)} - 1_{U(1)}$ are the only irreducible μ's whose restriction to $U(0)$ is not p times a character. These are the only μ's such that $\mu \bmod p \not\equiv 0$.

Since $\xi \bmod p \equiv 0$ and the φ's mod p are linearly independent, $(1_{U(0)}^{U(1)} - 1_{U(1)}) \cdot \varphi$ must appear in ξ whenever $1_{U(1)} \cdot \varphi$ does; and vice-versa. Of course, the restriction of their sum to $U(0) \times U(2)$ is p times $1_{U(0)} \cdot \varphi$. We are done.

Part 3. Conclusion of the properties of a'. From Part 2, $\xi \subseteq p \cdot \psi^U$. Since ξ is multiplicity free, $\xi \subseteq \psi^U$. But $\xi(1) = p \cdot \psi(1) = \psi^U(1)$ implies $\xi = \psi^U$. The properties of a' therefore follow by induction.

Part 4. Conclusion of the properties of a. Let ρ be the regular character of U. Then $\rho - \xi$ also satisfies the hypotheses. If

$(\xi,1) = 0$ then clearly a divides $\xi(1)$, and the conclusion of Part 3 applies.

Otherwise $(\rho-\xi,1)=0$ and Part 3 applies to $\rho-\xi$: $\rho-\xi=\psi^U$ where ψ is a character of the subgroup W of index a in U . So $\xi = \rho-\psi^U = 1^U - \psi^U = (1^W-\psi)^U$. As ψ is obviously multiplicity free, $1^W - \psi$ is a character. This completes the proof. ∎

To finish the section (as stated prior to Proposition 3.11) we need only show that $\xi = \chi_3'|_U$ has $\xi(1) = 1, n-1$ or n . Take a in Proposition 3.11 to be the value that is labeled a in Lemma 3.10.

If $a = 0$, then ξ is the regular character and $\xi(1) = n$. If $a \neq 0$, then Proposition 3.11 implies that $a = \pm 1$. Thus $(\xi,\xi) = \xi(1)$, $n-1+\xi(1)^2 = \xi(1)\cdot n$, and therefore $\xi(1)=1$ or $n-1$.

§4. Variants of the Hilbert-Siegel problem.

The precise result of Theorem 1.10 is a consequence of the hypotheses that $h(y)$ is an indecomposable polynomial with coefficients in $\mathbb{Q}$. Without the indecomposability condition (but h still in $\mathbb{Q}[y]$) we would be considering condition (1.12): $\mathscr{D}(h,g)$ is newly reducible with g a polynomial of the same degree as h or condition (1.13)a) holds. Let, however, $\underset{\sim}{\sigma}$ (§1.a)) be a description of the branch cycles for $\mathbb{P}^1_y \xrightarrow{\varphi(h)} \mathbb{P}^1_x$. We can no longer assert that $G(\underset{\sim}{\sigma})$ is doubly transitive (not even primitive) and therefore the classification of simple groups through [CuKanSe] would be of little immediate value unless we can understand $G(\underset{\sim}{\sigma})$ in terms of branch cycles for the covers given by composition factors of h. Actually, there are practical possibilities in this direction ([Fr,2; §5.3,c)]), but they do not yield results like Theorem 1.10. Therefore, in all the rest of our discussion we retain an indecomposability (i.e., primitive group) assumption.

<u>Replace</u> $\mathbb{Q}$ <u>by any number field</u> K. The analogous study to Theorem 1.10 would consider $\mathcal{O}_K$, the ring of integers of K, and those indecomposable $h \in \mathcal{O}_K[y]$ for which the set $\{x_0 \in \mathcal{O}_K$ with $h(y)-x_0$ reducible$\}$ consists of $V(h;\mathcal{O}_K)$ and a finite set. From Lemma 1.9 this is the study of condition (1.12). In that statement it is easy to draw a further conclusion about $T_2(\sigma(r))$:

LEMMA 4.1. *If* h *is indecomposable and condition* (1.12) *holds, then either* $T_2(\sigma(r))$ *is an* n-*cycle or* $T_2(\sigma(r))$ *is the product of an* n-*cycle and an* m_2-*cycle with* m_2 *a divisor of* n *greater than* 1 (*and* $\deg(T_2) = m = n + m_2$).

Proof. First suppose that $m_2 = 1$. Then, since $\deg(T_2) = n+1$ and $T_2(\sigma(r))$ is a product of a 1-cycle and an n-cycle, $G(\underset{\sim}{\sigma})$ is doubly transitive in the representation T_2. But $G(\underset{\sim}{\sigma})$ has an intransitive subgroup, $G(T_1,1)$, of index n according to condition (1.8). This contradicts an elementary lemma in group theory: A doubly transitive group has no intransitive subgroup of index less than its degree.

Suppose only that $T_2(\sigma(r))$ is not an n-cycle. The argument above shows that $\deg(T_2) = m_1 + m_2$ is at least as large as n. Since $\ell.c.m.(m_1,m_2) = n$, check that either m_1 or m_2 equals n. This concludes the lemma. ∎

If $T_2(\sigma(r))$ is an n-cycle, then the polynomials listed in Theorem 1.8 $(\deg(h) = 7,11,13,15,21,31$ - e.g., as in the appendix) give exceptional cases to a result analogous to Theorem 1.10. If $T_2(\sigma(r))$ is a product of two n-cycles, the degree 5 polynomials of Theorem 1.10 give the only additional exceptional cases (over any field K). The serious remaining question: Are there other exceptional polynomials h for which $T_2(\sigma(r))$ is a product of an n-cycle and an m_2-cycle with $m_2 < n$? We don't even know of any triples (G,T_1,T_2) as in Def. 2.2., with the relaxation on condition (2.2)b) that $T_2(\sigma)$ be a product of an n-cycle and an m_2-cycle with $m_2 < n$.

Variation of coefficients other than the constant term. Suppose $h \in Z[y]$ For $0 < i < n$ consider $\mathcal{R}(h(y) + x\cdot y^i; Z) = \{x_0 \in Z \mid h(y) + x_0\cdot y^i$ is reducible in $Z[y]\}$. In order to describe $\mathcal{R}(h(y) + x\cdot y^i; Z)$, Lemma 1.9 tells us to find those $g \in C(z)$ for which $\mathcal{J}(h(y)/y^i, g(z))$ is newly reducible where condition (1.11)a) holds for g. In terms of group theory we must find groups $G = G(\underset{\sim}{\sigma})$ with (1.7)a) and b), (1.8)a) and b), $T_1(\sigma(r))$ is a product of an i - cycle and an $(n-i)$ - cycle, and $T_2(\sigma(r))$ is a product of two $(m/2)$ - cycles. Thus $m/2$ is $\mathrm{l.c.m}(i, n-i)$. If i and n are relatively prime, indecomposability of $h(y)/y^i$ (i.e., primitivity of T_1) is an easy consequence. This case would not, however, include cases arising from the doubly transitive groups containing an n - cycle that appear in Theorem 2.1. Indeed, we would expect a similarly striking analogue to Theorem 1.10, but noone has worked out the group theory.

<u>Mordell analogue of Hilbert-Siegel problem</u>. The results above have all considered specialization of x to integer values. Consider, instead for $h(y) \in \mathbb{Q}[y]$, $\mathcal{R}(h(y) - x; \mathbb{Q}) = \{x_0 \in \mathbb{Q} \mid h(y) - x_0$ is reducible in $\mathbb{Q}[y]\}$. In order to get a result similar to Theorem 1.10 we <u>must</u> assume the Mordell conjecture: A nonsingular projective curve, of genus at least 2, defined over a number field K has only finitely many K - rational points. With this assumption we have a variant on Lemma 1.9.

LEMMA 4.2. <u>Let</u> $V(h;\mathbb{Q}) = \{x_0 \in \mathbb{Q} \mid h(y_0) = x_0$ <u>for some</u> $y_0 \in \mathbb{Q}\}$. <u>Suppose that</u> $\underset{\sim}{\sigma}$ <u>is a description of the branch cycles of the cover</u> $\mathbb{P}^1_y \xrightarrow{\varphi(h)} \mathbb{P}^1_x$ (§1.a)), <u>and</u> $G = G(\underset{\sim}{\sigma}) \subseteq S_n$, <u>and that</u> $G(\underset{\sim}{\sigma})$ <u>has no subgroup</u> H <u>with these properties</u>:

(4.1) a) H <u>is an intransitive subgroup of</u> S_n;

b) <u>no conjugate of</u> $G(1) = \{\sigma \in G \mid (1)\sigma = 1\}$ <u>contains</u> H; <u>and</u>

c) $\sum_{i=1}^{r} \mathrm{ind}(T_H(\sigma(i))) = 2\cdot(G:H)$ <u>or</u> $2\cdot(G:H) - 2$.

<u>Then</u> $\mathcal{R}(h(y)-x;\mathbb{Q})$ <u>is the union of</u> $V(h;\mathbb{Q})$ <u>with a finite set</u>.

There are approximate converses (sic) to Lemma 4.2 ([Fr,2;§8.6]), but they naturally rely on number theory rather than pure group theory. Thus, in some sense, condition (4.1) is the best tool for investigating analogues of Theorem 1.10. But, for <u>every</u> integer n there are indecomposable polynomials h of degree n for which $\mathcal{R}(h(y)-x;\mathbb{Q}) - V(h;\mathbb{Q})$ is infinite. Indeed, these include polynomials h for which a description of the branch cycles of $\mathbb{P}^1_y \xrightarrow{\varphi(h)} \mathbb{P}^1_x$ is given by expression 1.9 of Ex.1.5.

REFERENCES

[BF] R. Biggers and M. Fried, Moduli spaces of covers and the Hurwitz monodromy group, J. für die reine und angewandte Mathematik, 1982.

[Bu,1] W. Burnside, On simply transitive groups of prime degree, Quart. J. Math. 37 (1906), 215-222.

[Bu,2] W. Burnside, Theory of groups of finite order, 2nd edition, Dover Publications, New York, 1955.

[Bu,3] W. Burnside, On a class of groups defined by Congruences, Proc. L.M.S. Vol. XXV (1894), 113-139.

[Ca] J. W. S. Cassels, Factorization of polynomials in several variables, Proc. 15th Scandinavian Congress Oslo, (1968), 1-17.

[Co] S. D. Cohen, The Galois group of a polynomial with two indeterminate coefficients, Pac. J. Math 90 (1980), 63-76.

[CuKanSe] C. W. Curtis, W. M, Kantor and G. M. Seitz, the 2-transitive permutation representations of the finite Chevalley groups, T.A.M.S. 218 (1976), 1-59.

[DLSc,1] H. Davenport, D. J. Lewis, and A. Schinzel, Equations of the form $f(x) = g(y)$, Quart. J. Math., Oxford (2) 12 (1961), 304-312.

[DLSc,2] H. Davenport, D. J. Lewis, and A. Schinzel, Polynomials of certin special types, Acta Arith. 9 (1964), 107-116.

[E] L. Ehrenfucht, Kryterium absolutnez hierokladnosci wielominow, Prace Mat. 2 (1958), 167-169.

[F,1] W Feit, Automorphisms of symmetric balanced incomplete block designs, Math. Zeit. 118 (1970), 40-49.

[F,2] W. Feit, On symmetric balanced incomplete block designs with doubly transitive automorphism groups, J. of Comb. Theory 14 (1973), 221-247.

[F,3] W. Feit, Some consequences of the classification of finite simple groups, Santa Cruz Conference on finite groups, Proceedings of Symposia in Pure Mathematics, AMS Rhode Island, 1980, 175-181.

[Fr,1] M. Fried, Exposition on an arithmetic-group theoretic connection via Riemann's existence theorem, The Santa Cruz Conference on finite groups, Proceeedings of Symposia in Pure Mathematics, Vol. 37 (1980), Providence R.I., 571-602.

[Fr,2] M. Fried, Application's of Riemann's existence theorem to arithmetic and algebraic geometry, manuscript in preparation.

[Fr,3] M. Fried, The field of definition of function fields and a problem in the reducibility of polynomials, Ill. J. Math. 17 (1973), 128-146.

[Fr,4] M. Fried, On Hilbert's irreducibility theorem, Vol. 6, No. 3 (1974), 211-232.

[Fr,5] M. Fried, On a theorem of MacCluer, Acta Arith. 25 (1974), 122-127.

[Fr,6] M. Fried, On a conjecture of Schur, Mich. Math. J. 17 (1970), 41-55.

[Fr,7] M. Fried, Fields of definition of function fields and Hurwitz families..., Comm. in Algebra 5 (1), 1977, 17-82.

[Gor] D. Gorenstein, Finite simple groups: an introduction to their classification, Academic Press, New York, 1982.

[H,1] M. Hall Jr., The theory of groups, MacMillan, N.Y., 1963.

[H,2] M. Hall Jr., Combinatorial theory, Blaisdell Pub. Co., Waltham Mass., 1967.

[Ha] H. Hasse, Bericht über neurere Untersuchungen und Probleme aus der theorie der algebraischen Zahlkorper, Jber. dt. Mat. Varein: Part I, 36 (1926), 1-55; Part Ia, 36 (1927), 233-311; Part II, Exg. Bb, 6 (1930), 1-204

[HiN] D. G. Higman and P. Neumann,

[Je] W. Jehne, Kronecker classes of algebraic number fields, J. No. Theory 9 (1977), 279-320.

[Kl,1] N. Klingen, Atomare KroneckerKlassen mit speziellen Galoisgruppen, Escheint in Abh. Math. Sem. Hamburg.

[Kl,2] N. Klingen, Zahlkörper mit gleicher Primzerlegung, J. fur die reine und angewandte Mathematik, 299/300 (1978), 342-384.

[Kro] L. Kronecker, Über die Irreductibilität von Gleichungen, Monatsber. Preuss. Akad. Wiss. (1880), 155-163 (Werke II, 85-93).

[Li] D. E. Littlewood, The theory of group charcters, Oxford Univ. Press, New York, London, 1940.

[Ri] J. Ritt, On algebraic functions which can be expressed in terms of radicals, T.A.M.S. 24 (1922), 21-30.

[S] C. L. Siegel, Über einige unwendungen diophantischer approximationen, Abh. Preuss. Akad. Wiss, Phys. - Math. Kl. 1 (1929), 14-67.

[Sc,1] A schinzel, Some unsolved problems, Mat. Bibl., 25 (1963), 63-70.

[Sc,2] A. Schinzel, Reducibility of polynomials of the form $f(x) - g(y)$, Coll. Math. 18 (1967), 213-218.

[Sc,3] A. Schinzel, Reducibility of polynomials, Actes Congress Intern. Math. 1970, Vol. 1, 491,496.

[Schu] V. Schulze, Die Vertielung der primteiler von Polynomen auf Restklassen, I, J. reine und angew. Math. 280 (1976), 122-133; II, J. reine und angew. Math. 281 (1976), 126-148.

[Sch] I. Schur, Zur theorie der einfach transitiven Permutationsgruppen, S. - B. Preuss. Akad. Wiss., Phys. - Math. Kl. (1933), 598-623.

[Sco,1] L. L. Scott, Uniprimitive Permutation Groups, in theory of finite groups, a symposium at Harvard University, W. A. Benjamin Inc., 1969, 55-62.

[Sco,2] L. L. Scott, On permutation groups of degree $2p$, Math. Z. 126 (1972), 227-229.

[Sco,3] L. L. Scott, On the n, $2n$ problem of Michael Fried, Proceedings of the conference of finite groups, Academic Press, New York, 1976, 471-472.

[Sco,4] L. L. Scott, Modular permutation representations, T.A.M.S. 175 (1973), 101-121.

[Sp] V.G. Sprindžuk, Reducibility of polynomials and rational points on algebraic curves, Seminar on Number Theory, Paris 1979-80, 287-309, Progress in Math. 12, Birkhaeuser, Boston, Mass., 1981.

[Tv] H. Tverberg, A study in irreducibility of polynomials, Dept. of Math., Univ. of Bergen, 1968.

[Wie,1] H. Wielandt, Primitive Permutationsgruppen von Grad 2p , Math. Zeit. 63 (1956), 478-485.

[Wie,2] H. Wielandt, Permutation groups through invariant relations and invariant functions, Lecture Notes, Dept. of Math., Ohio State Univ., Columbus, Ohio, 1969.