JOURNAL OF ALGEBRA 111, 49–73 (1987)

On the Mumford–Tate Group of an Abelian Variety with Complex Multiplication*

B. DODSON

Department of Mathematics, Lehigh University,
Bethlehem, Pennsylvania 18015

Communicated by Walter Feit

Received November 10, 1984

Let (K, Φ) be a primitive CM-type with $[K: \mathbb{Q}] = 2n$ (for definitions and previous results see Section 1.1). Fix n, and consider the collection $S(n) = \{\text{Rank}(\Phi)\}$, where $\text{Rank}(\Phi)$ counts the number of independent translates of Φ under the Galois action and (K, Φ) ranges over all primitive types. The smallest element of $S(n)$, denoted by $B(n)$, is referred to as the *sharp lower bound* for the rank in dimension n. As was brought to the author's attention by Ribet, bounds on $B(n)$ of the form $p+1$, for p a prime dividing n, follow directly from the proof of Ribet's Nondegeneracy Theorem [21]. This is recorded as Theorem 1.4. Ribet's method also gives bounds of the form $2q$ for q a prime with q^2 dividing n, as is observed in Theorem 1.12. When combined with the author's constructions of Abelian varieties in [8, 9], we obtain the precise value of $B(n)$ for many values of n (Corollaries 1.5 to 1.8 and 1.13).

We recall that these constructions use the analytic method of Weil and Shimura, together with new results on the reflex field from an investigation suggested to the author by Shimura. The interest of the rank comes from the theory of complex multiplication. If A is an Abelian variety of CM-type (K, Φ), then the *Kubota Rank* of A is Rank (Φ), and controls properties of the classfields constructed from A as in Kubota [16] and Ribet [20]. This is connected with the fact that the rank of Φ is also the dimension of the Mumford–Tate group of A, and with the relation of this group to the l-adic representations of A, as in Serre [24, 25].

The main body of the paper contains results that provide information on $S(n)$. The main result, Theorem 2.5, asserts that when n is odd there is a computable subset $S^1_{\text{solv}}(n)$ of $S(n)$ that accounts for the ranks of many CM-types on most CM-fields. More precisely, let K_0 be the maximal totally real subfield of K, and K_0^c be the Galois closure of K_0. We consider the per-

* This research was supported by a generous grant from the Reidler Foundation.

0021-8693/87 $3.00

mutation group G_0 determined by K_0 (e.g., by the action of the Galois group on the roots of the polynomial of a primitive generator of K_0). Then our condition on K is that G_0 must have a solvable subgroup that is transitive. Refinements in the group-theoretic methods of [8] lead to the observation that the computable case, where the CM-field is solvable and contains an imaginary quadratic subfield, gives most of the information when n is odd, since we may use the action of certain solvable transitive subgroups.

One of the questions raised by the above solvability condition is the problem of determining when a nonsolvable permutation group has a solvable transitive subgroup. In Section 3 the author attempts to show that this problem has some merit as a problem in pure group theory, and it is connected to the theory of permutation representations of simple groups. Finally, we treat the example $n = 9$ in Section 4 and make some preliminary observations on the case $n = p^2$.

1. Ribet's Method

1.1. *Definitions and Previous Results.* All number fields in this paper are regarded as subfields of the field $\mathbb{C}$ of complex numbers. A *CM-field* is a totally imaginary quadratic extension K of a totally real field K_0. Let $[K_0 : \mathbb{Q}] = n$, so that $[K : \mathbb{Q}] = 2n$. A *CM-type* is a pair (K, Φ), where K is a CM-field and Φ is a set of n embeddings $\{\phi_1, ..., \phi_n\}$ of K into $\mathbb{C}$ such that every embedding is among $\{\phi_1, \bar{\phi}_1, ..., \phi_n, \bar{\phi}_n\}$, with $\bar{\phi}_j$ the composite of ϕ_j with complex conjugation. We also refer to Φ as a type on K.

Let K^c denote the Galois closure of K over $\mathbb{Q}$. For a type Φ on K and for $g \in \mathrm{Gal}(K^c/\mathbb{Q})$, let Φ^g be the type on K containing the embeddings ϕ_j^g, $j = 1, ..., n$, with $\phi_j^g(x)$ obtained by applying g to the image of $x \in K$ under ϕ_j. Then the *rank* of Φ, $\mathrm{Rank}(\Phi)$, is the rank over $\mathbb{Z}$ of the submodule spanned by $\{\Phi^g$ such that $g \in \mathrm{Gal}(K^c/\mathbb{Q})\}$ inside the free $\mathbb{Z}$-module $\mathbb{Z}[\phi_1, \bar{\phi}_1, ..., \phi_n, \bar{\phi}_n]$. A direct proof that $\mathrm{Rank}(\Phi)$ coincides with the dimension of the Mumford–Tate group of Abelian varieties of type (K, Φ) has been described to the author by H. Pohlmann and may be found in [19].

For a CM-subfield K_1 of K, let Φ_1 be a CM-type on K_1. Then the *lift* of (K_1, Φ_1) to K is the type consisting of all embeddings of K into $\mathbb{C}$ whose restriction to K_1 belongs to Φ_1. Finally, the type (K, Φ) is said to be *primitive* if Φ is not the lift of any type on any CM-subfield of K. We recall that the Theorem of Schappacher [22] asserts that, with two exceptions, every CM-field has some primitive type.

The results of Kubota [16], Shimura [26], and Ribet [20, 21] may be collected to give the following:

THEOREM 1.0. (i) $n+1 \in S(n)$, *for every* n. (ii) $t \in S(n)$ *implies* $t \leqslant n+1$. (iii) $t \in S(n)$ *implies* $\log_2(n)+2 \leqslant t$. (iv) *For* $n=2^j$, $j \geqslant 2$, $\log_2(2^j)+2=B(2^j)$. (v) (*Ribet's Nondegeneracy Theorem*) *For* $n=p$, p *a prime*, $S(p)=\{B(p)\}=\{p+1\}$.

When n is composite, but $n \neq 2^j$, we use $[\log_2(n)]+3$ as a lower bound for $B(n)$, where [ ] denotes the greatest integer function, and refer to this as the *log$_2$-bound*. We recall that Φ is said to be *nondegenerate* when $\operatorname{Rank}(\Phi)=n+1$.

Remark 1.1. The author has shown in [8] that $B(n)<n+1$ whenever n is composite, so that $S(n)=\{B(n)\}$ holds only when n is prime. The results of [8, 9] give additional information on $S(n)$, and upper bounds on $B(n)$. Composite values for which the log$_2$-bound is the sharp lower bound include $n=9$, 10, and 35, although the lower bound for these cases is also given by the bounds in the present paper. More generally, for $n=\binom{d}{m}$ with d odd, $d>7$, we have $B(n) \leqslant d+1$, while the log$_2$-bound appears to be d. When d is a prime, this is accounted for by Corollary 1.6 below.

Finally, we recall in an explicit form that the proof of case (A) of the Theorem of [8, Sect. 3.3.1] gives the upper bound of the following:

PROPOSITION 1.2. *For* $n=p^j$, *with* p *an odd prime*, $B(p^j) \leqslant pj-j+2$.

Proof. The reflex type of the type in the proof (*loc. cit.*, with $k=p$ and $l=j$) has the required property. The hypothesis on the existence of the (solvable) totally real field has been established in [9].

1.2.1. *Ribet's Lower Bound.* To see that there is a large class of values for which the log$_2$-bound is not the sharp lower bound, consider the following:

DEFINITION 1.3. Let p_r be the largest prime dividing n. We say that n is divisible by a *sufficiently large prime* if $4n<2^{p_r}$.

Then, from the Proof of the Nondegeneracy Theorem, we have

THEOREM 1.4 (Ribet). *Let* p *be an odd prime dividing* n. *Then* $B(n) \geqslant p+1$. *In particular, the* log$_2$-*bound on* $B(n)$ *is not sharp whenever* n *has a sufficiently large prime factor.*

We include the proof below for completeness, since the same arguments are required for Theorem 1.12. (For the best lower bound given by this method, see Section 1.3.2.)

Proof (Ribet [21]). We first note that when Φ is a primitive type on K, no element of $\mathrm{Gal}(K^c/\mathbb{Q})$ fixes every element of the $\mathrm{Gal}(K^c/\mathbb{Q})$-orbit of Φ.

In fact, if some element y of $\mathrm{Gal}(K^c/\mathbb{Q})$ fixes every Φ^g then y is the identity on every conjugate $(K')^g$ of the reflex field K' of (K, Φ), and therefore on $(K')^c$. But then $(K')' \subseteq (K')^c$, so $(K')^c \neq K^c$ implies $(K')' \neq K$, contradicting a requirement on primitive types (cf. Shimura [27]).

Next we observe that since the prime p divides n, which divides the order of $\mathrm{Gal}(K^c/\mathbb{Q})$, there is an element g of order p in $\mathrm{Gal}(K^c/\mathbb{Q})$. Now let V be the $\mathbb{Q}$-linear space spanned by the orbit of Φ, as in the definition of the rank above. Then the action of $\langle g \rangle$ on the orbit of Φ induces an action of the ring $R = \mathbb{Q}[X]/(X^p - 1)$ on V. Since R has the structure $\mathbb{Q} \oplus \mathbb{Q}(\mu_p)$, for μ_p a pth root of unity, the R-module V completely reduces as a direct sum $V_0 \oplus V_1$, where g has trivial action on V_0 and nontrivial action on V_1, with dimension $\dim_{\mathbb{Q}}(V_1) = b(p-1)$ and $b \geqslant 1$.

Finally, the elements $N_X\Phi = \Phi + \Phi^g + \cdots + \Phi^{g^{p-1}}$ and $\Phi + \bar{\Phi}$ both belong to V_0, and are linearly independent, which we see by considering a relation of the form $N_X\Phi = c(\Phi + \bar{\Phi})$. Adding the coefficients of the embeddings on both sides, we obtain $c(2n) = pn$ (since Φ is a type), so $c = p/2$ is not an integer for p odd. But this contradicts $N_X\Phi$ in $\mathbb{Z}[\phi_1, ..., \bar{\phi}_n]$, since $\Phi + \bar{\Phi}$ is the vector with all coefficients equal 1. Thus we obtain $\mathrm{Rank}(\Phi) = \dim_{\mathbb{Q}}(V) = \dim_{\mathbb{Q}}(V_0) + b(p-1) \geqslant 2 + 1(p-1) = p+1$.

The remaining observation is merely that when p_r is sufficiently large, $\log_2(4n) < p_r$, so $[\log_2(n)] + 3 < p_r + 1$.

Examples of integers without sufficiently large prime factors are given by 2^a3^b and 3^a5^b. However, when n is written in the form $n = n_1 p_r$, the cofactor n_1 must satisfy the condition $n_1 < (1/p_r)(2^{p_r - 2})$, which grows rapidly with p_r.

1.2.2. *Values of $B(n)$.* The corollaries below give values of n for which the bound $p_r + 1$, for p_r the largest prime dividing n, is the sharp lower bound $B(n)$. The proofs give the reference for the construction of Abelian varieties with complex multiplication for which the sharp lower bound occurs. In cases for which n occurs in several corollaries, the field of complex multiplication has distinct Galois-theoretic structure in each occurrence. We recall that giving a CM-type is sufficient to obtain an Abelian variety, by the analytic construction of Sections 6 and 12.4 of Shimura and Taniyama [29].

COROLLARY 1.5. *Let $n = 2p$ with p a prime larger than 3; or, more generally, let $n = pt$ with t dividing $p-1$ and $t < p-1$. Then $B(n) = p+1$.*

Proof. When $p > 7$, we use the reflex of the type in Proposition 2.3.1 [9]. For $p = 5$ and 7, see [8].

COROLLARY 1.6. *Let n be a binomial coefficient, $n = \binom{p}{m}$, with p a prime larger than 3 and $2 \leqslant m \leqslant (p-1)/2$. Then $B(n) = p+1$.*

Proof. The existence here follows from the existence of a totally real field with Galois group the symmetric group S_p over $\mathbb{Q}$. (Cf., e.g., [8] or Section 2.1 of [9].)

COROLLARY 1.7. *Suppose the ideal* (2) *decomposes into primes of degree* f *in the* pth *cyclotomic field. Let* l *be an integer with* $1 \leqslant l \leqslant g-1$, *where* $g=(p-1)/f$. *Then* $B(n)=p+1$ *for* $n=2^{fl}p$.

Proof. The construction is given in the Theorem of Section 3.2.2 of [8].

COROLLARY 1.8. *Let* p *be a prime such that* $p>100$, $p \neq 151$. *Suppose that* 2 *is a quadratic residue* $(\operatorname{mod} p)$. *Then* $B(n)=p+1$ *for* $n=2^{(p-1)/2}pt$ *with any* t *dividing* $(p-1)/2$.

Proof. The reflex type of the type constructed in [9, Corollary 2.3.4] has the required rank, so we must verify the hypothesis on the existence of a prime k with $2<k<\frac{1}{2}p^{1/2}$ such that k does not divide $p-1$. We first consider large primes. Let p_j be the jth largest prime. Suppose p_1 up to p_s divide $p-1$, but p_{s+1} does not. Then $p \geqslant p_1 p_2 \cdots p_s$, so $\frac{1}{2}(p_1 \cdots p_s)^{1/2} > p_{s+1}$ will suffice, since then we take $k=p_{s+1}$.

Now we need to have at least $s+1$ primes smaller than $\frac{1}{2}(p_1 \cdots p_s)^{1/2}$. Using $a=\frac{1}{2}$ as the lower bound in the Prime Number Theorem, $a(\frac{1}{2}(p_1 \cdots p_s)^{1/2})/\log(\frac{1}{2}(p_1 \cdots p_s)^{1/2}) > s+1$ will suffice. We therefore show that

$$a(p_1 \cdots p_s)^{1/2}/(\log(p_1 \cdots p_s)+1) > s+1. \tag*{(*)}$$

First, we observe that the inequality (*) holds with $s_0=6$. Then we note that the function $f(y)=ay^{1/2}/(\log y+1)$, defined for $y>0$, is increasing and satisfies $f(16y)>f(y)+2$ for $y \geqslant p_1 \cdots p_6$. We then obtain (*) by induction for $s \geqslant s_0=6$, and establish our conclusion for $p \geqslant p_1 \cdots p_6+1=30,031$.

Now consider primes p in the range $2311 \leqslant p < 30{,}031$. Then $\frac{1}{2}p^{1/2} \geqslant \frac{1}{2}(2311)^{1/2} > 24$, so one of 3, 5, 7, 11, 13, or 17 will give a choice for k. Next, for $211 \leqslant p < 2311$, $\frac{1}{2}p^{1/2} > 7$, so either one of 3, 5, or 7 gives a choice for k, or else p is of the form $p=m(210)+1$. But we take $k=11$ for $p \geqslant 631$, and observe that 2 is not a quadratic residue for $p=211$ or 421, so there is a choice for all $p \geqslant 211$. The same method applies in the range $p>100$, $p \neq 151$, giving our conclusion.

Remark 1.9. The above proof confirms an observation of Professor Assmus. Recall from [9] that, except for a set of primes of density 0 (with, e.g., $\sum p^{-1/2} < \infty$), the method of Corollaries 1.7 and 1.8 can at most apply to values of the form $n=2^{fl}pt$ with t dividing $p-1$ and f, l as in Corollary 1.7. The above Corollary most likely holds with $p \geqslant 17$; however, we recall that the coding theory restriction of t dividing $(p-1)/2$ cannot be removed for some primes.

As a final case from the previous papers we have the following:

COROLLARY 1.10. *Let q_0 be an odd prime, and suppose $q_0^2+q_0+1$ is a prime p. Then a sufficient condition for $B(n)=p+1$ with $n=pq_0^2$ is that there exists a totally real field with Galois group the projective linear group $PSL(3, q_0)$ over the rationals.*

Proof. Subject to the existence of the totally real field, the construction follows from Proposition 2.4.1 of [9].

Remark 1.11. In support of an interest in the dimension of the Mumford–Tate group, we refer to Serre [24], especially Section 4, as well as to Deligne *et al.* [7]. The most direct explanation of the specific interest in the sharp lower bound $B(n)$ is in connection with Ribet's Theorem [20] on the rate of growth of the field of pth division points. Thus the above bound, and the bound in Theoem 1.12 below, asserts that this rate is often never as small as allowed by the $\log_2$-bound, while the Corollaries assert that, for the previously constructed Abelian varieties, the rate of growth for the degree of the field of pth division points is the slowest possible. We also refer here to Lang's book [17, Chap. 4 and 6] and to Katz and Lang [15].

Since the rate of growth in Ribet's Theorem depends upon the number of distinct prime factors of n and the Kubota rank, our question of how the factorization of n affects the rank arises naturally. We emphasize that these motivations complement, rather than replace, the motivations in the author's earlier papers.

1.3.1. *An Application of Ribet's Method.* If a serious study of the arithmetic function $B(n)$ is to be proposed, one of the problems is to decide whether the interplay between group theory and number theory that gives the above values is actually required by the values of $B(n)$, or only by the methods. As an example, we ask whether $B(n)$ for $n=pt$ with $t<p-1$ actually depends upon whether t divides $p-1$ or not; and we ask whether the value for $n=2^kp$, with $k<p-1$, actually depends upon k. A substantial necessary condition for an integer n with a sufficiently large prime factor to have $B(n)=p_r+1$ is given by the following:

THEOREM 1.12. *Let q be an odd prime for which q^2 divides n. Then $B(n)\geqslant 2q$.*

Proof. We consider the necessary modifications of the proof of the above Theorem 1.4. Since q^2 divides n and q is a prime, $\mathrm{Gal}(K^c/\mathbb{Q})$ has a subgroup of order q^2. First, we dispose of the case where there is an element x of oder q^2. Since x^q must have nontrivial action on the orbit of types, there must be a type whose orbit under x has length q^2. Examining the ring $\mathbb{Q}[X]/(X^{q^2}-1)$, we obtain a submodule of dimension $q(q-1)$ corresponding to the cyclotomic field generated by a primitive root of unity μ_{q^2} and establish our lower bound.

Next, we consider an elementary Abelian subgroup of order q^2, with generators g and h. Let $x \in \langle g, h\rangle$, and $y \in \langle g, h\rangle$, with $\langle x, y\rangle = \langle g, h\rangle$. Our proof relies upon the assertion that if there is an element in the span of the orbit of types for which x has trivial action, but y has nontrivial action, then we obtain our bound. In fact, we observe that under this hypothesis, the trivial submodule for the action of $\langle x\rangle$ has dimension at least $2+(q-1)$, while x has nontrivial action, so there is a complementary subspace of dimension at least $(q-1)$ and our rank is then at least $2q$. Note that the linear independence relation of the previous proof holds in this case, to give the bound on the dimension of the trivial subspace.

Now we claim that the above always holds. Take a (primitive) type Φ in the $\mathrm{Gal}(K^c/\mathbb{Q})$-orbit on which g has nontrivial action. Writing the action on the left, we set $N_{\langle x\rangle}(\Phi) = \Phi + x\Phi + \cdots + x^{q-1}\Phi$, for x of order q. If h fixes the type Φ on which g has nontrivial action, h also fixes $g\Phi$ (since g and h commute), so the above argument establishes our bound. Similarly, we obtain that the type Φ has an orbit of order q^2 under $\langle g, h\rangle$. Now we consider the elements $N_{\langle h\rangle}(\Phi)$, $N_{\langle gh\rangle}(\Phi)$, ..., $N_{\langle g^{q-1}h\rangle}(\Phi)$. If g is nontrivial on any of these, the above applies; so we consider the case where equations $g\{N_{\langle g^j h\rangle}(\Phi)\} = N_{\langle g^j h\rangle}(\Phi)$ hold for $j=0, 1, ..., q-1$. We add these q equations together, and observe that the terms may be rearranged so that the right-hand side satisfies

$$\begin{aligned} &N_{\langle h\rangle}(\Phi) + N_{\langle gh\rangle}(\Phi) + \cdots + N_{\langle g^{q-1}h\rangle}(\Phi) \\ &\quad = q(\Phi) + hN_{\langle g\rangle}(\Phi) + h^2 N_{\langle g^2\rangle}(\Phi) + \cdots + h^{q-1} N_{\langle g^{q-1}\rangle}(\Phi) \\ &\quad = q(\Phi) + (q-1)(N_{\langle g\rangle}(\Phi)). \end{aligned}$$

In fact, $N_{\langle g^j\rangle}(\Phi) = N_{\langle g\rangle}(\Phi)$, and h^j must have trivial action, or else the above applies. But then, on the left-hand side, a similar rearrangement gives $gN_{\langle h\rangle}(\Phi) + \cdots + gN_{\langle g^{q-1}h\rangle}(\Phi) = q(g(\Phi)) + (q-1)\, N_{\langle g\rangle}(\Phi)$, so $g(\Phi) = \Phi$, which contradicts our choice of Φ.

From Proposition 1.2 above we have immediately the following:

COROLLARY 1.13. *$B(n) = 2p$ when $n = p^2$ for p an odd prime.*

1.3.2. *Postcript: The p-Sylow Bound.* When n is divisible by a large prime power, Ribet's method gives substantially stronger lower bounds. As in the proof of Theorem 1.4, a primitive CM-type gives a faithful linear representation defined over the rationals of the group $G = \mathrm{Gal}(K^c/\mathbb{Q})$. A necessary condition for $\mathrm{Rank}(\Phi) = r$ is then that G must be isomorphic to a (finite) subgroup of $GL_{r-1}(\mathbb{Q})$, since we may split off a 1-dimensional trivial representation corresponding to $\Phi + \bar{\Phi}$. We immediately obtain the following:

THEOREM 1.14 (p-sylow Bound). (1) *Factor n as $n = p_1^{e_1} \cdots p_r^{e_r}$ with $p_i \neq p_j$* for *$i \neq j$, with $i, j = 1, \ldots, r$. For $p = p_j$, let $R(p, n)$ denote the smallest integer d such that there exists a finite subgroup of $GL(d, \mathbb{Q})$ with p-Sylow subgroup of order $\geqslant p_j^{e_j}$. Then*

$$B(n) \geqslant L(n) = \max_p \left(R(p, n) + e_p\right),$$

where $e_p = 2$ if p is odd, $e_p = 1$ if p is even.

(2) *If K is a given CM-field of degree $2n$, and G is the group* $\mathrm{Gal}(K^c/\mathbb{Q})$, *then for every primitive CM-type Φ on K*

$$\mathrm{Rank}(\Phi) \geqslant L(|G|),$$

where $L(|G|)$ is defined as in (1) with n replaced by the order of G.

Finally, if p^e is the exact power of p dividing n, then $R(p, n)$ is known, and satisfies the asymptotic estimate

$$R(p, n) > e(p-1)^2/p, \qquad \textit{if } p \textit{ is odd and } R(2, n) > e/2.$$

Proof. Let P be the p-Sylow subgroup of G. Then the value of e_p for p odd follows from the independence of the norm $N_P(\Phi) = \sum_{g \in P} \Phi^g$ from $\Phi + \bar{\Phi}$, which depends upon p being odd. For the value of $R(p, n) = R(p, p^e)$, we consider the arithmetic function $r(x, y)$ in Exercises 6 and 7 of Chapter 3 of Bourbaki [1]. Then $R(p, n) = d$ when $e > r(p, d+1)$ but $e \leqslant r(p, d)$. We have that when p is odd

$$r(p, y) = \left[\frac{y}{p-1}\right] + \left[\frac{y}{p(p-1)}\right] + \left[\frac{y}{p^2(p-1)}\right] + \cdots,$$

where [ ] denotes the greatest integer function. The asymptotic estimate is then given by the inequalities

$$\begin{aligned} r(p, y) &< \left[\frac{y}{p-1}\right]\left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \\ &< (y/(p-1))(p/(p-1)). \end{aligned}$$

The same method is used to estimate the given value for $r(2, y)$.

Parts (1) and (2) of the above result were observed by the author in June 1985, along with an elementary estimate for $R(p, n)$. In fact, if $e \leqslant p$ we have $d = e(p-1)$, but for $e > p$ the term $[d/p(p-1)]$ is nonzero. The correct estimate, and then the above reference, was brought to the author's attention by H. W. Lenstra, Jr. The author also acknowledges the comments and subsequent letter of V. Kumar Murty.

The interest of the bound given in (2) above is the restriction on the possible CM-fields that could have a type of rank $L(n)$, since we may have $L(|G|) > L(n)$. We also record Lenstra's remark that if a p-Sylow subgroup P of G has a central element of order p^2 then $\operatorname{Rank}(\Phi) > R(p, |G|)$. A closer examination of Exercise 6, e, f (*loc. cit.*) shows that when the maximum value giving $L(n)$ occurs for an odd prime then a necessary condition for $B(n) = L(n)$ is that the p-Sylow subgroup of G must have the precise structure given there. These remarks clarify the role of the type in Proposition 1.2, since the p-Sylow subgroups used there are Abelian or have just one wreath product.

2. A Solvability Condition on CM-Fields

2.1.0. *The Action on Types.* We recall the notation of [8], which is used to specify types and the $\operatorname{Gal}(K^c/\mathbb{Q})$-action on types. As the group-theoretic properties are somewhat intricate, we restate our intention to obtain simplifications under restrictive conditions. Let K_0 be the maximal totally real subfield of K and K_0^c be the Galois closure of K_0 over $\mathbb{Q}$. Let G_0 be a permutation representation of $\operatorname{Gal}(K_0^c/\mathbb{Q})$ for which $\operatorname{Gal}(K_0^c/K_0)$ corresponds to the stabilizer of a letter, which we take to be 1.

Then our method requires that we begin by specifying a permutation representation of $\operatorname{Gal}(K^c/\mathbb{Q})$. We do this by taking G_0 to act on the symbols $\{1, ..., n\}$ and giving an action on symbols $\{\pm 1, ..., \pm n\}$ under the conditions that

(1) every set $\{\pm j\}$ is mapped to a set $\{\pm k\}$, and

(2) the induced action on the sets $\{\pm j\}$ coincides with the action of G_0 on $\{1, ..., n\}$ under the identification of $\{\pm j\}$ with j.

We recall that such an action is said to have n sets of imprimitivity of order 2 and has been shown to be necessary in [8, Sect. 1].

Next, we must specify the kernel of the induced action in (2). Let $(Z_2)^n$ denote the group generated by the transpositions $(+j, -j)$. We specify $(+j, -j)$ by a 1 in the jth coordinate of $(Z_2)^n$. Let $\sigma \in G_0$ act on $(Z_2)^n$ by sending $(+j, -j)$ to $(+\sigma(j), -\sigma(j))$. Then we give

(3) a subgroup C of $(Z_2)^n$ such that (a) C contains the permutation $(+1, -1) \cdots (+n, -n)$ and (b) C is preserved by the action of G_0.

Here we recall that C is referred to as a (linear) code, and that the largest subgroup of S_n preserving C under the above action is referred to as the automorphism group of the code. The distinguished permutation in (3a), also denoted by $(1, ..., 1)$, or by ρ, represents the field automorphism given by complex conjugation. We refer to the code given by $\langle \rho \rangle$ as the *trivial code.*

Finally, we must give a choice of coset representatives for the projection (2). For $e \in (Z_2)^n$ and $\sigma \in S_n$ let (e, σ) denote the permutation of the set $\{\pm 1, ..., \pm n\}$ given by applying e and then applying the map $\tilde{\sigma}$ sending $+j$ to $+\sigma(j)$ and $-j$ to $-\sigma(j)$. Then we give

(4) a map $s: G_0 \rightarrow (Z_2)^n$ such that the composite with the projection onto $(Z_2)^n/C$ is a 1-cocycle.

From the information specified by (1)–(4) we obtain a permutation group G with elements given by $(es(\sigma), \sigma)$, where e ranges over C and σ ranges over G_0. Since we have shown in [8] that every Galois group of a CM-field has such a permutation representation, we use the data (G_0, C, s) to define the action on types. The reader interested in this "structure" may wish to consult [8, Sect. 2 and 6].

To obtain types, we normalize $s: G_0 \rightarrow Z_2^n$ to have first coordinate 0, and pick coset representatives τ_i for the stabilizer of 1 in G_0. Then $\mathbf{f} \in Z_2^n$, $\mathbf{f} = (f_1, ..., f_n)$, is used to specify the type on K given by restricting the maps corresponding to $(\rho^{f_i} s(\tau_i), \tau_i)$ to K, where $\rho = (1, ..., 1)$ corresponds to complex conjugation. Then the required action from [8] is given by writing $g \in \mathrm{Gal}(K^c/\mathbb{Q})$ as $g = (es(\sigma), \sigma)$ with $e \in C$, and recalling that for Φ given by $\mathbf{f}$, Φ^g is given by $\sigma^{-1}(\mathbf{f}es(\sigma))$, where the addition in Z_2^n is written multiplicatively. The choice of embeddings specified by $\mathbf{f}$ will also be viewed as a choice of cosets of $\mathrm{Gal}(K^c/K)$ in $\mathrm{Gal}(K^c/\mathbb{Q})$ as in Shimura [28, Sect. 5.5].

2.1.1. *A Nondegeneracy Result.* A case that illustrates the principle that certain Galois-theoretic properties of CM-types are determined by the Galois structure of the maximal totally real subfield of the CM-field is the generic case S_n included in the following:

PROPOSITION 2.1. *Let n be odd and suppose that K is a CM-field of degree $2n$ such that the maximal totally real subfield K_0 has* $\mathrm{Gal}(K_0^c/\mathbb{Q}) \cong A_n$ *or S_n. Then every primitive CM-type (K, Φ) is nondegenerate.*

Proof. By [9, Proposition 2.2.2] we have that either there is a single $\mathrm{Gal}(K^c/\mathbb{Q})$-orbit of types of order 2^n, in which case $\mathrm{Rank}(\Phi) = n + 1$ is clear, or else K contains an imaginary quadratic subfield. In the latter case, we take s to be identically 0, as usual, and note that in the action on types $e = 0$ or ρ. Then recall from Section 2.1 (*loc. cit.*) that for $n > 1$ there are only $(n-1)/2$ orbits of primitive types, where each orbit corresponds to $\mathbf{f} \in \mathbb{Z}_2^n$ having a fixed number of nonzero coordinates. For an orbit with k nonzero coordinates, $1 \leqslant k \leqslant (n-1)/2$, we select the n vectors $(10 \cdots 01 \cdots 1)$, $(010 \cdots 01 \cdots 1)$, ..., $(0 \cdots 01 \cdots 1)$, $(10 \cdots 0101 \cdots 1)$, $(010 \cdots 01101 \cdots 1)$, ..., $(0 \cdots 010 \cdots 01 \cdots 10)$, and observe that they are linearly independent in $\mathbb{Z}[Z_2^n]$. Then we conclude that $\operatorname{Rank}(\mathbf{f}) = n+1$ by the Constant Weight Criterion [8].

2.2.1. *The Minimal Group Method.* Let G and G_0 be as in Section 2.1.0 and consider a minimal permutation subgroup M_0 of G_0; that is, let M_0 be a transitive subgroup with the property that every proper subgroup of M_0 is intransitive. A transitive subgroup M of G is obtained by restricting the map s to M_0, so that we have $M = \{(es(\sigma), \sigma)$ such that $e \in C$ and $\sigma \in M_0\}$, where G is given by (G_0, C, s), as above. Then the G-orbit of $\mathbf{f}$ decomposes into a disjoint union of orbits of M. An element of an M-orbit defines a "type," regarded as a choice of n of the $2n$ cosets of the stabilizer in M of a letter, under the condition that only one coset is selected from each of the cosets paired by the action of ρ. Then we have the following:

PROPOSITION 2.2. *The rank of the type defined by* $\mathbf{f}$ *is bounded below by the ranks of types representing the orbits of* M, *for any choice of a minimal transitive subgroup* M_0. *Further, if* M_0 *is a primitive permutation group then* M_0 *must be a simple group with a maximal subgroup of index* n.

Proof. For the first assertion, recall the method used in the proof of the Minimal Weight Criterion [8, Sect. 3.1.1], where the types are regarded as elements of $\mathbb{Z}[Z_2^{2n}]$. Then the submodule spanned by the types for M is contained in the submodule spanned by the types for G when coset representatives for M_0 are used as coset representatives for G_0. The second assertion follows from [18, Proposition 4.4], which asserts that normal subgroups of primitive groups are transitive.

Remark 2.3. An example of a minimal permutation group that is primitive, non-Abelian, and simple is given by the Mathieu group M_{22}, with $n = 22$, as may be observed from Conway [4, Table 3]. A general class of examples is given by Proposition 3.3 below. However, we note that [3] (cf. Cameron [2]) shows that the set of integers n for which there is any primitive group in degree n aside from A_n and S_n has density 0. Further, A_n contains a regular subgroup unless $n \equiv 2 \pmod 4$; and in this last case the permutation group of [8, Sect. 3.3.1, Proof of (C)] is a solvable transitive subgroup.

2.2.2. *A Relative Solvability Condition.* Our group-theoretic condition is given by the following:

DEFINITION 2.4. Let n be a positive integer and let K_0 be a totally real field of degree n. Then the Galois closure K_0^c of K_0 is said to satisfy the *relative solvability condition* with respect to K_0 if the permutation group determined by the action of $\mathrm{Gal}(K_0^c/\mathbb{Q})$ on the cosets of $\mathrm{Gal}(K_0^c/K_0)$ in $\mathrm{Gal}(K_0^c/\mathbb{Q})$ has at least one solvable subgroup that is transitive.

Observe that K_0^c solvable over $\mathbb{Q}$ is sufficient to assure relative solvability with respect to any subfield. In particular, K_0 normal over $\mathbb{Q}$ is sufficient when n is odd, by the Theorem of Feit and Thompson. Second, if K_0^c over $\mathbb{Q}$ has the Galois group A_n, with n odd, $n \geqslant 5$, where K_0 is of degree n, then K_0^c is relatively solvable with respect to K_0 (Remark 2.3), so that our condition is weaker than solvability. An example that does not satisfy this solvability condition, with $n = 15$, is obtained from a totally real field with group A_5 over $\mathbb{Q}$, by taking K_0 to be the subfield fixed by a 2-Sylow subgroup.

We now have a stronger form of the orbit decomposition in Proposition 2.2 given by the following:

THEOREM 2.5. *Let (K, Φ) be a primitive CM-type, and let K_0 be the maximal totally real subfield of K. Suppose that $[K_0 \colon \mathbb{Q}] = n$ is odd, and that K_0^c is relatively solvable with respect to K_0. Then the* $\mathrm{Gal}(K^c/\mathbb{Q})$*-orbit of Φ is a union of orbits of a solvable subgroup M_1 whose action on types as in Section* 2.1.0 *is given by the trivial code $C = \langle \rho \rangle$ and the action of a transitive permutation group M_0 of degree n (i.e., the coset map s in* (4) *of Section* 2.1.0 *is identically* 0). *In particular, we may choose M_0 to be a minimal permutation group.*

Conversely, the orbits of types for the permutation groups M_1 occur for certain CM-fields of degree $2n$, and these CM-fields contain an imaginary quadratic subfield.

The computable subset $S^1_{\mathrm{solv}}(n)$ in the Introduction is the collection of ranks of primitive types on CM-fields of degree $2n$ that contain an imaginary quadratic subfield and have solvable Galois closure.

Proof. As in Proposition 2.2, we consider a transitive permutation subgroup M_0 of the permutation group determined by K_0. Then we obtain the orbit of types for $\mathrm{Gal}(K^c/\mathbb{Q})$ as a disjoint union of types for the permutation group M given by restricting the map s, associated with a permutation representation of $\mathrm{Gal}(K^c/\mathbb{Q})$, to M_0. By our assumption, we pick M_0 to be solvable.

Using P. Hall's extended Sylow Theorems for solvable groups, we pick a subgroup P_0 of M_0 having odd order and satisfying $|M_0| = 2^k\,|P_0|$. We then observe that P_0 is a transitive subgroup of M_0 by examining the stabilizer H_0 of a letter in the action of M_0 and checking that the indices satisfy $(M_0 \colon H_0) = (P_0 \colon P_0 \cap H_0)$, so that coset representatives for H_0 in M_0 may be selected from P_0.

Now taking M_0 to have odd order, the group extension

$$0 \to C \to M \to M_0 \to 1$$

splits, by the Theorem of Schur and Zassenhaus, since all elements of C are of order 2. Then we apply Lemma 2.2.1 of [9], noting that M_0 is of odd order, to obtain that the permutation structure of M is uniquely determined by the group extension. In particular, we may adjust the map s giving the action of $\mathrm{Gal}(K^c/\mathbb{Q})$ on types to arrange that s restricts to 0 on M_0 by extending the definition of a coboundary in $B^1(M_0, (Z_2)^n/C)$ to $\mathrm{Gal}(K_0^c/\mathbb{Q})$ (cf. [8, Sect. 2]). Finally, with s identically 0 on M_0, the subgroup $\langle \rho \rangle \times M_0$ of the semi-direct product $C \times_s M_0$ gives our transitive subgroup M_1 of $\mathrm{Gal}(K^c/\mathbb{Q})$.

We may either replace our initial choice of M_0 by a minimal transitive subgroup, to obtain a restrictive collection of permutation groups of degree n for M_0, with considerable information on types, or else we may allow M_0 to range over all solvable permutation groups for which the subgroup M of $\mathrm{Gal}(K^c/\mathbb{Q})$ has trivial split structure, and therefore admits a transitive subgroup M_1 of the above from. The latter collection gives the larger collection of ranks of orbits, so we wish to show that all of these ranks do occur in $S(n)$. But Shafarevich's Theorem on the existence of totally real fields L_0 with arbitrarily given solvable Galois group (cf. [9, Theorem 1.1]) gives the existence of CM-fields L with Galois group isomorphic to M_1, for which the fixed field of M_0 is imaginary quadratic. Then a CM-field as required is given as the subfield of L fixed by the subgroup $0 \times H_0$, with H_0 the stabilizer of a letter in M_0

The reader might wish to refer to Section 4.1 to see how the sharp lower bound in dimension 9 occurs: the minimal (solvable) groups give only the values 8 and 10, and the sharp lower bound of 6 occurs (only) for solvable groups with orbits that avoid primitive types for the minimal groups and contain several orbits of reducible types. As to the actual computation of the above values, we note that the values obtained in Section 1 are all associated with non-Abelian groups (fields), and in each case the ranks are computed from the reflex type.

We use the above method to obtain some information on the solvable minimal groups in the following:

PROPOSITION 2.6. *For a minimal solvable permutation group M_0 of degree n, the set of primes dividing the order of M_0 coincides with the set of primes dividing n.*

Proof. Since n divides the order of M_0, we must show that every prime dividing the order of M_0 divides n. But if q is a prime dividing the order of

M_0 we again use solvability and the extended Sylow Theorems to obtain a complement to a q-Sylow subgroup of M_0. As above, we observe that this complement is transitive unless q divides n, so M_0 minimal implies that q divides n.

2.3. *The Prime Power Case.* There is one case where the above method applies to all CM-fields.

PROPOSITION 2.7. *Let $n=p^j$ with p a prime, and let G_0 be a permutation group of degree n. Then G_0 contains a minimal transitive subgroup that is a p-group. Further, for $n=p^2$, G_0 contains one of the two regular groups.*

In particular, the solvability condition required for Theorem 2.5 holds relative to each K_0 of degree $n=p^j$, with p an odd prime.

Proof. Let H_0 be the subgroup of G_0 fixing a letter, so that the index $(G_0: H_0)=p^j$. Consider a p-sylow subgroup P_0 of G_0. Observe that $(P_0: P_0 \cap H_0)=p^j$, so that coset representatives for H_0 in G_0 may be selected from P_0. Then P_0 is a transitive subgroup of G_0, and we obtain a minimal transitive subgroup of G_0 that is a p-group by picking a minimal transitive subgroup of P_0. Finally, p-groups are solvable, so the conditions for Theorem 2.5 hold.

For the case $n=p^2$, we use an argument suggested by the referee. If the group P_0 has exponent p^2, then pick any cyclic subgroup of order p^2 and observe it is transitive since it contains a p^2-cycle. Otherwise, let $z \neq 1$ be central. Since z does not belong to $P_1=H_0 \cap P_0$, we consider the group $L=P_1 \times \langle z \rangle$. Then for any $y \notin L$ we have a factorization $P_0=P_1 \cdot \langle z, y \rangle$. So $\langle z, y \rangle$ is transitive, and clearly regular.

Remark 2.8. We recall that a proper transitive subgroup always gives a factorization as in the above proof (cf. R. Scott, "Group Theory," Prentice-Hall, Englewood Cliffs, N.J., 1964). In particular, for p-groups, we have a factorization if and only if the subgroup fixing a letter is not a subgroup of the Fratini subgroup. Then an example of a nonregular minimal 2-group of degree 8 may be observed as the permutation group $G=32\Gamma_7 a_1$ with sets of imprimitivity permuted by $(Z_2)^2$ from [8, Sect. 5.2]. In fact, since the Fratini subgroup of G is $(Z_2)^3$, with subgroup $H=(Z_2)^2$ containing no nontrivial normal subgroup of G, we also obtain a nonregular minimal group of degree 16. Further examination of the tables and lattice diagrams of Hall and Senior shows that G is the unique nonregular minimal group of degree 8.

Remark 2.9. The present methods give an improvement of Theorem 2.1.1 of the author's paper [9]. We consider the values $2^{f_1}t$ listed in (*) 2. Applying the above results with a minimal cyclic group of prime order, the orbits of types contain $2mp$ or $2(mp+1)$ elements, depending upon whether the orbit contains $\langle \rho \rangle$ or not. Thus we would have

$2^{fl}t \equiv 0$ or 1 (mod p), where t divides $p-1$. But recalling that f was chosen so that $2^f \equiv 1$ (mod p), we obtain $t \equiv 1$ (mod p) and $t < p$, so $t = 1$. This argument may be used to replace Corollary 2.3.7 and Proposition 2.3.9 in the proof of Theorem 2.1.3, and removes the restriction $p \equiv 3$ (mod 4) in Theorem 2.1.3(b).

3. Nonsolvable Permutation Groups

3.0. *A Problem on Nonsolvable Permutation Groups.* The material of the present section is not required in Section 4. Recall that a transitive permutation group M, of degree n, is said to be a *minimal transitive group* of degree n if every proper subgroup of M is intransitive. We have the following:

Proposition 3.1. *Let M be a minimal transitive permutation group of degree n. Then exactly one of the folowing descriptions hold.*

(1) *M is regular, i.e., of order n.*

(2) *M is non–regular and primitive. In this case M is a non-Abelian simple group.*

(3) *M is non–regular, imprimitive, but still simple.*

(4) *M is non–regular and has a nontrivial proper normal subgroup N. In this case the orbits of N are sets of imprimitivity for M.*

Proof. Regular groups are clearly "minimal." If M is not simple, we obtain sets of imprimitivity by Wielandt [31, Proposition 7.1].

If we are to analyze the action of all permutation groups of some fixed degree n by use of the minimal transitive groups, we must first restrict our choice of n to control the regular groups. As remarked above, taking n odd assures that the regular groups are solvable. Next, we must select a value of n for which the simple groups of degree n can be analyzed; for example, where n is square free as in [12], or where n has just two distinct prime factors at least one of which is repeated. Heuristically, we regard the groups of case (4) above as the main nonregular case: there are many degrees for which A_n is the only simple group of degree n, but A_n is not minimal for $n > 3$. The following subsections on simple groups are relevant to a numerical version of this principle. For standard references and notation for simple groups, we refer to Gorenstein [10].

First, we consider the groups of case (4). We have the following:

Theorem 3.2. *Let M be a non-regular minimal transitive group of degree n, and suppose M has a nontrivial normal subgroup N. Let L be the* (*normal*) *subgroup of M fixing each orbit of N. Then M/L is a minimal transitive group on the set of orbits of N. The degree of this permutation representation divides n.*

Proof. If T/L acts transitively on the orbits of N, then T is transitive.

To see that there are many non-Abelian simple candidates for the quotient M/L above, consider the following:

PROPOSITION 3.3. *Let G be an abstract finite simple group, and let $d(G)$ be the minimal degree of the permutation representations of G. Let G_0 be a permutation group isomorphic to G, and let H_0 be the stabilizer of a letter in G_0. Suppose that the index n of H_0 in G_0 satisfies $n > |G|/d(G)$. Then G_0 is a group of degree n with no proper transitive subgroup.*

Proof. Suppose that $G_0 = H_0 M_0$ with M_0 transitive. Then the order of M_0 satisfies $|M_0| \geqslant n$. But $(G_0 \colon M_0) \geqslant d(G)$, so $|G| = |G_0| = (G_0 \colon M_0)|M_0| \geqslant d(G)\,n$. But now we have $n \leqslant |G|/d(G)$, which is contradictory.

We note that n is odd if and only if H_0 contains a 2-Sylow subgroup of G_0, and that every simple group occurs at leasst with n given as the index of a 2-Sylow of G, as well as with n the index of the "local" subgroup containing a 2-Sylow. As a prototypical example for the Proposition, consider the Suzuki groups $\mathrm{Sz}(q)$ $(= {}^2B_2(q))$, for which the list of maximal subgroups is given in Suzuki [30]. In particular, $n = 65$ is an odd value for which there definitely is a group of degree n with no solvable transitive subgroup. (The Mathieu group M_{22} in degree 22 has been previously mentioned.)

As an additional example, we mention N. Ito's paper (*Acta Sci. Math.* (*Szeged*) **15** (1953), 79–84), which shows that most subgroups of $PSL(2, q)$ do not occur in any factorization, and therefore we obtain minimal transitive groups as in Remark 2.8.

3.1. *Representations of the Simple Groups in Odd Degrees.* We consider the simple groups of Lie type. We separate our results depending upon whether our group is "exceptional" or classical, where the twisted groups are included as one or the other of these two cases. We use the method of Guralnick's paper [11], supplemented by the list of maximal parabolic subgroups for the groups of Lie rank 1 or 2.

PROPOSITION 3.4. *Let G be a simple exceptional group of Lie type defined over a finite field with q elements and characteristic q_0. Suppose that G has a permutation representation of degree n with n odd. Then either q_0 divides $2n$ or else $G = E_6(q)$, and n is divisible by $(q^9 - 1)(q^{12} - 1)/(q-1)(q^4 - 1)$. In any case, $q^3 < n$.*

Suppose in addition that n is relatively prime to 3 and 5. Then either q is odd or else $G = E_7(q)$ with $q = 2^{8k}$, and n is divisible by $(q^9+1)(q^5+1)(q^{14}-1)/(q-1)$. Further, for $G = E_6(q)$, the above exception occurs only when $q = 3^k$.

Proof. If q_0 does not divide n, we have by the Lemma of Seitz and Tits [23] that G has a maximal parabolic subgroup P with the index $(G: P)$ dividing n. If, in addition, q_0 is odd, we check the list of maximal parabolics and find that $(G: P)$ is even with the exception of a single pair of parabolics for $E_6(q)$ with the given index.

With the additional assumption that n is prime to 3, we observe that the given index for E_6 is divisible by 3 whenever $q \equiv \pm 1 \pmod 3$, since there is a factor of the form $m^4 + m^2 + 1$ with $m = q^2$. Rechecking the indices with q even shows that the same fact holds for these cases, except for $\mathrm{Sz}(q)$, where the odd degrees are divisible by 5, and the above case for E_7.

Finally, the estimate on q may be found in [3]. (To remove any possible confusion regarding the Chevalley groups, we may check that the assertions of the Proposition hold for the simple group of Tits using [5].)

For the classical groups, the formulae giving the indices of the maximal parabolic subgroups are less tractable. We have the following:

PROPOSITION 3.5. *Let G_0 be a classical simple group defined over a field with q elements and characteristic q_0. Suppose that G has a representation of degree n with n odd. Then one of the following holds.*

(1) *$G = PSL(2, q)$ with either* (a) *q even and $q+1$ dividing n or* (b) *q odd and q_0 dividing n. In either case $q < n$.*

(2) *$G = PSL(3, q)$ with either* (a) *q^2+q+1 dividing n or* (b) *q_0 dividing n. In either case $q^2 < n$.*

(3) *G is a classical group aside from the above two, and either q_0 divides n or else n is divisible by one of the values on the list of indices of the maximal parabolic subgroups below. In any case $q^3 < n$.*

(3a) $$\frac{\prod_{j=1}^{m}(q^j-1)}{\prod_{j=1}^{k}(q^j-1)\prod_{j=1}^{m-k}(q^j-1)}$$ *for $PSL(m, q)$.*

(3b) $$\frac{\prod_{j=1}^{m}(q^{2j}-1)}{\prod_{j=1}^{k}(q^j-1)\prod_{j=1}^{m-k}(q^{2j}-1)}$$ *for $PSp(2m, q)$ and $\Omega(2m+1), q)$.*

(3c) $$\frac{\prod_{j=0}^{2k-1}(q^{n-j}-(-1)^{n-j})}{\prod_{j=1}^{k}(q^{2j}-1)}$$ *for $U_n(q)$.*

(3d) $$\frac{\prod_{j=0}^{k-1}(q^{m-2j}-e)(q^{m-2j-1}+e)}{\prod_{j=1}^{k}(q^j-1)}$$ *for $\Omega^{\varepsilon}(2m, q)$, $e = \varepsilon 1$, $\varepsilon = \pm$.*

Proof. Parts (1) and (2) are well known. Part (3) results from the Lemma referred to in the proof of Proposition 3.4, combined with Cooperstein [6], which lists the above indices and gives the minimal degree for permutation representations.

Lists of maximal subgroups have long been available for $PSL(2, q)$, $PSL(3, q)$, $U_3(q)$, and, when q is odd, $PSp(4, q)$ (see the references in Cooperstein [6]). The reader can easily locate examples from among these that occur in degrees with no small prime factor (Definition 3.6 below), which are extreme examples of degrees that are odd and prime to $3 \cdot 5$. While our lists could be extended to give, for example, the cases up to $q^5 < n$, hard information on the maximal subgroups of odd index in the groups Lie type has recently been obtained by Kantor [14], so we defer further numerical consideration of the parabolic case.

3.2. *Degrees without Small Divisors.* As remarked above, there is no shortage of examples, so we consider the case of the following:

DEFINITION 3.6. Let n be an odd integer with at least two distinct prime divisors. Let p_1 denote the smallest prime dividing n. We say that n has *no small prime divisors* if $4n < 2^{p_1}$.

For the alternating groups we observe that when n has no small divisors we may specify precisely when an alternating group aside from A_n in degree n can occur.

PROPOSITION 3.7. *Suppose n is without small prime divisors. Let A_m be an alternating group with a permutation representation of degree n. Then either $n = m$ or else there is a binomial coefficient $\binom{m}{k}$, $1 < k < m/2$, that has no small prime divisors and divides n.*

Proof. We follow a simplification suggested by the referee. Let H be the subgroup of A_m stabilizing one of the n letters and consider the action of H on the m letters corresponding to $A_m \subset S_m = \mathrm{Aut}(\{1, 2, ..., m\})$. If H is intransitive on these m letters, H has an orbit of size k with $1 \leqslant k < m/2$. If $k \neq 1$, $\binom{m}{k}$ divides n, this being the index of a maximal subgroup containing H. If $k = 1$ the result follows by induction, so we may suppose H acts transitively on the m letters.

If the action of H is imprimitive, m has a factorization $m = st$, and considering a maximal subgroup M containing H, n is divisible by $(A_m: M) = (st)!/(s!)^t\,(t!)$. Observe that this number and the number obtained by switching the role of s and t have a prime factor p_a with p_a in the interval $[\max(s, t), 2\max(s, t)]$. We therefore consider the smaller of these two numbers, i.e., we suppose $t \geqslant s$. Checking for small prime factors, we may suppose $t \geqslant 5$. With $t = 5$, we verify that $(st)! > (s!)^t\, t! 2^{p_a - 2}$, for each $s = 1, \ldots, 5 = t$. We therefore obtain this inequality in general by induction, delaying the case $s = t$ to the last step. Then p_a is a small prime factor, contradicting our assumption that n has no small prime factors.

Finally, if H is primitive, we observe that the small divisor 3 must not divide n, so H contains a 3-Sylow subgroup of A_m. But then H contains a 3-cycle, so $H = A_m$ by Wielandt [31].

Next we consider the sporadic groups, under the same condition on n. During corrections to the final version of the paper, we have completed the following:

PROPOSITION 3.8. *Suppose that n has no small prime divisors and that a sporadic simple group has a representation of degree n. Then* $n = 11 \cdot 23$, *G is the Mathieu group* M_{23}, *and G has one of the two possible permutation structures.*

Professor Gorenstein has informed us that a forthcoming paper by M. Aschbacher, to appear as an AMS Memoir, includes a solution for all odd n as a special case. The present result illustrates our divisibility assumption.

Proof. Several of the sporadic groups have orders with no divisor being without small prime factors. These are the Mathieu groups M_{11}, M_{12}, and M_{22}, the Janko group J_2, the McLaughlin group, the Higman–Sims group, and Held's group. We observe that if every primitive representation has a small prime factor then we are done, since the degree of any imprimitive representation is divisible by the degree of a primitive representation. The sporadic groups whose maximal subgroups have been classified now at least include all but seven of the sporadic groups, as in [5].

For the remaining groups, we resort to the available information on the characters. Thus we must have $n = 1 + \sum e_v f_v$, where the f_v are degrees of nontrivial irreducible characters and the e_v are the multiplicities, as in Higman [13]. We use the degrees of the irreducible characters given in the tables of [5] to complete our analysis.

In the earlier version of this paper the author located some degrees n so that n is of the form $n = pq$, with p and q distinct primes, and the only simple group of degree n is A_n. We will observe that the recent paper by Guralnick and Wales [12] settles this question (without supposing that n has no small prime divisors). In response to examples of parabolic subgroups found by the author, Guralnick asserts that the list of Table 1 (*loc. cit.*) is complete after the following minor corrections:

(1) the comment on when $(l^r - 1)/(l - 1)$ has exactly two prime factors should require only that l is necessarily a prime or the square of a prime;

(2) $L_4(2)$ ($\cong A_8$) occurs in degree $5 \cdot 7$ for a unique conjugacy class of subgroups (stabilizing a plane), and $L_5(2)$ occurs in degree $5 \cdot 31$ for two classes with the same character (stabilizing a lane and a 3-space); and,

(3) $\Omega_{2m}^{+}(2)$, with subgroup $H =$ stabilizer of a singular line, occurs in degree $(2^m - 1)(2^{m-1} + 1)$, which has only 2 prime factors when m is a Fermat prime, $2^{m-1} + 1$ is a Fermat prime, and $2^m - 1$ is a Mersenne prime (e.g., $m = 5$ or 17).

We record our observation as a

Corollary of Guralnick and Wales. *Let $n = pq$ be the product of two distinct prime factors. Then A_n is the only simple primitive transitive permutation group of degree n if and only if n is not given by*

(a) $n = p(p \pm 1)/2$;

(b) $n = (l^r - 1)/(l - 1)$;

(c) $n = (2^m - 1)(2^{m-1} + 1)$ *with m a Fermat prime*; or

(d) $n = 22, 35, 3 \cdot 19, 7 \cdot 11, 5 \cdot 31,$ *or* $7 \cdot 29$.

Further, including simple imprimitive groups, the same conclusion holds with the addition that n is not given by

(e) $\left(\dfrac{l^d - 1}{l - 1}\right) q$ *with q dividing $l - 1$.*

Proof. The present assertion involves only an analysis the degrees in Table 1 Guralnick and Wales, noting that we have only corrected the use of elementary number theory referred to in [12, p. 108]. The main cases (a) and (b) occur (at least) for linear and alternating groups. The groups U_3, Sz, and Sp_4 also occur in degrees given by (b). The orthogonal case above is accounted for by (c), so we are left with 21 isolated examples, occurring in 14 distinct degrees. All of these but the 6 cases listed in (d) occur in degrees given by (a). Finally, for the imprimitive case (e), p must be a "special prime" as in [9], and $G = \mathrm{PSL}_d(l)$ occurs as in [12, Theorem 6.2(6), (7)].

To assist in the location of examples in degrees with more prime factors, we apply Propositions 3.4–3.8 to obtain the following:

Numerical Restrictions 3.9. Suppose $n < N$ with $N = 10^7$, and that n is without small prime divisors. Then a simple group G has a primitive permutation representation of degree n only if (a) $n = \binom{m}{k}$ and $G = A_m$, (b) $n = 11 \cdot 23$ and $G = M_{23}$, (c) $n = (q^m - 1)/(q - 1)$, (d) G is of Lie type of characteristic q_0 with q_0 dividing n, or (e) G is a classical group of characteristic 2. Further, in Proposition 3.5, (3b) is always divisible by $q + 1$ and therefore is even when q is odd.

4. An Example

4.1. *Minimal Group Calculations in Dimension* 9. This section is independent of the material in Section 3; we return to the analysis of CM-types. Recall that for a regular group R_0 the *holomorph*, $\mathrm{Hol}(R_0)$, of R_0 is the permutation group $R_0 \times_s A$, where A is the automorphism group of R_0. The notation R_0 will always denote a regular permutation group in this section. Also, for $\mathbf{f} \in Z_2^n$, recall that *weight*$(\mathbf{f})$ is the number of nonzero coordinates of $\mathbf{f}$.

Proposition 4.1. *Let* $\mathbf{f} \in Z_2^9$ *define a type on* $\langle \rho \rangle \times R_0$, *for* R_0 *one of the two regular groups of degree* 9. *Then the type defined by* $\mathbf{f}$ *is nondegenerate whenever* weight $(\mathbf{f})$ *is relatively prime to* 3.

Proof. Let $\mathrm{weight}(\mathbf{f}) = k$. Observe that if a subgroup of R_0 stabilizes $\mathbf{f}$ then the coordinates of $\mathbf{f}$ are constant on the orbits of the subgroup. But since the proper subgroups of the regular groups are $\frac{1}{2}$-transitive, this cannot occur unless $k = 0$, 3, 6, or 9. Thus, the orbit of $\mathbf{f}$ under R_0 is of order 9.

By the Constant Weight Criterion we are reduced to showing that the 9 elements in each orbit are linearly independent. Multiplying by $\rho = (1 \cdots 1)$ we may suppose that $k = 1$, 2, or 4. When $k = 1$, linear independence is clear, and we also check the 4 orbits of weight 2 directly.

Now, with $k = 4$, we apply the Lemma below to observe that checking representatives for the $\mathrm{Hol}(R_0)$-orbits of the R_0-orbits is sufficient. By explicit calculations we find that there are 4 such $\mathrm{Hol}(Z_9)$-orbits and 3 such $\mathrm{Hol}(Z_3^2)$-orbits. In either case, we pick representatives and check linear independence directly to verify that all R_0-orbits are nondegenerate.

Lemma 4.2. *Let* $G_0 \subset S_n$, *let* π *be an element of the normalizer* $N_{S_n}(G_0)$, *and let* $\mathbf{f} \in Z_2^n$ *define a type on* $\langle \rho \rangle \times G_0$. *Then* $\mathrm{Rank}(\mathbf{f}) = \mathrm{Rank}(\pi\mathbf{f})$. *In particular, when* G_0 *is regular, the rank of types on* G_0 *is constant on* $\mathrm{Hol}(G_0)$-orbits.

Proof. Observe that $\sum_{\sigma \in G_0} n_\sigma \sigma(\pi\mathbf{f}) = \sum_{\pi\sigma'\pi^{-1}} (n_{\pi\sigma'\pi^{-1}})(\pi\sigma'\pi^{-1})(\pi\mathbf{f}) = \sum_{\pi\sigma'\pi^{-1}} (n_{\pi\sigma'\pi^{-1}})\, \pi\sigma'\mathbf{f} = \pi[\sum_{\sigma'} (n_{\sigma'})(\sigma'\mathbf{f})]$; so, when π normalizes G_0, relations among elements of the G_0-orbits of $\pi\mathbf{f}$ induce relations in the G_0-orbit of $\mathbf{f}$, and conversely. The assertion on the holomorph follows, since $\mathrm{Hol}(G_0) = N_{S_n}(G_0)$.

Example 4.3. When $n = 9$ and $R_0 = Z_3^2$, we have $\mathrm{Aut}(Z_3^2) = GL(2, 3)$, the general linear group of 2-by-2 matrices. To obtain the $\mathrm{Hol}(Z_3^2)$-orbits of the Z_3^2-orbits in the proof of Proposition 4.1, we take Z_3^2 to be explicitly given as the group generated by (123)(456)(789) and (147)(258)(369). Then generators for $GL(2, 3)$ are explicitly given as automorphisms of Z_3^2 by (23)(56)(89), (2539)(4876), (2437)(5698), and (456)(798).

By the analysis in the proof of Proposition 4.1, we may now assume weight $(\mathbf{f})=3$ and restrict to representatives for the $\mathrm{Hol}(R_0)$-orbits of the R_0-orbits. The remaining information provided by the orbits of the minimal groups $\langle\rho\rangle\times R_0$ is collected in the following:

PROPOSITION 4.4. (1) *Suppose* $R_0=Z_9$ *and* $\mathrm{weight}(\mathbf{f})=3$. *Then the orbits of order* 9 *give types with* $\mathrm{rank}(\mathbf{f})=8$ *or* 10, *and these orbits account for all but three* $\mathbf{f}$, *in a single* Z_9*-orbit.*

(2) *Suppose* $R_0=Z_3^2$ *and* $\mathrm{weight}(\mathbf{f})=3$. *Then there are the following cases*: (a) *the orbits of order* 9 *give types with* $\mathrm{rank}(\mathbf{f})=8$ *and* (b) *there are twelve* $\mathbf{f}$ *in four* Z_3^2*-orbits of order* 3.

Further, in case (2b), *an orbit of types consisting of the union of any two orbits corresponds to types with rank* 6, *and such an orbit occurs for certain* G_0 *properly containing* $R_0=Z_3^2$. *Finally, the union of three orbits corresponds to types of rank* 8, *and the union of all four orbits corresponds to types of rank* 10.

Proof. (1) There are two distinct $\mathrm{Hol}(Z_9)$-orbits of Z_9-orbits of order 9, with respective ranks 8 and 10. We note here that three orbits of order 9 consist of types for which rank $(\mathbf{f})=8$.

(2) There is a single $\mathrm{Hol}(Z_3^2)$-orbit of Z_3^2-orbits of order 9, whose types have rank 8. The four Z_3^2-orbits of order 3 correspond to the four subgroups isomorphic to Z_3 in Z_3^2, and the ranks for the union of these orbits may then be checked directly. The rank 6 orbit is the one referred to in Proposition 1.2.

Remark 4.5. As a corollary of the above analysis of $\mathrm{Hol}(R_0)$-orbits, and of the existence of solvable CM-fields, we obtain the existence of simple Abelian varieties of dimension $n=18$, 27, 36, 54, and 72 with rank 10, i.e., $10\in S(n)$ for these n.

4.2. *A Characterization of the Rank in Dimension* 9. To complete the analysis of the rank of primitive types in dimension 9, we must examine unions of orbits of degenerate types, or of reducible types, for the minimal groups, as described in Section 2. Since a full characterization includes a criterion for each value of the rank to occur, we observe the following:

PROPOSITION 4.6. *Suppose A is a simple Abelian variety of dimension* 9 *and that A has complex multiplication. Let* (K,Φ) *be the CM-type of A, and suppose that* $\mathrm{Rank}(A)=6$. *Then the following properties hold*:

(i) (K,Φ) *is the reflex type of a CM-type* (K',Φ'), *where K' has degree* 12 *over* $\mathbb{Q}$; *and,*

(ii) *the maximal totally real subfield* K_0 *of K is not Galois over* $\mathbb{Q}$, $[K^c:K_0^c]=2$, *and* $\mathrm{Gal}(K_0^c/\mathbb{Q})$ *is isomorphic to one of the wreath products* $Z_3\wr Z_2$ *or* $S_3\wr Z_2$, *or else to one of two specific groups of order* 36 *that occur as index two subgroups in the latter group.*

Proof. Consider the number of elements in an orbit of types for $\mathrm{Gal}(K^c/\mathbb{Q})$. By Proposition 2.2 we must take unions of orbits of types for a permutation subgroup M over a minimal group M_0, so that none of the orbits have rank greater than 6. Since M is split with trivial structure over M_0, observe that M has a transitive subgroup M_1 of the form analyzed in Section 4.1, i.e., with $Z_2^v = \langle \rho \rangle$, and that the M-orbits are given as unions of M_1-orbits.

Then the only possible orbits, aside from the order 12 orbits, obtained as $\theta \cup \theta\rho$ for θ an orbit of order 6 in Proposition 4.4(2b), are the union of one of these with the orbit $\{0, \rho\}$ of order 2. But we eliminate an orbit of order 14 since, by Section 5.1 of [8], there is no CM-field of degree 14 with a reflex field of degree 18. (Alternatively, we observe that such a type would have rank 8.)

As to the specific groups in (ii), observe that $[K' : \mathbb{Q}] = 12$, $[K : \mathbb{Q}] = 18$ with (K, Φ) primitive gives that $v = 1$ in the Reflex Degree Theorem applied to $(K')'$, and $K'^c = K^c$. Therefore, $[K^c : \mathbb{Q}] = 2m$, where m is the order of an abstract group H with transitive permutation representations of degree 6 and 9. But there are only 6 permutation groups of degree 6 with order divisible by 9, while A_6 and S_6 do not admit degree 9 representations, so at most the four groups referred to in (ii) occur.

Remark 4.7. Let A be a simple Abelian variety with complex multiplication, and suppose that the dimension of A is 9. Then $\mathrm{Rank}(A) = 6$, 8, or 10, and these three numbers do occur. This conclusion may be established by the present methods and has motivated a subsequent investigation by the author. As the new method is both simpler and more general, we omit the initial proof.

3.3. *A Preliminary Result with $n = p^2$.* Let $A(p^2)$ be the smallest value of the rank of the primitive CM-types (K, Φ) as K ranges over the CM-fields with K normal over $\mathbb{Q}$ of degree $2p^2$, and $\mathrm{Gal}(K/\mathbb{Q})$ Abelian. A general version of the result of Section 4.2 is given by the following:

PROPOSITION 4.8. *Suppose that (K, Φ) is a primitive CM-type on a CM-field K with $[K: \mathbb{Q}] = 2p^2$, for p an odd prime. Suppose that* $\mathrm{Rank}(\Phi) = t$ *with $t < A(p^2)$. Then the reflex field K' of the type (K, Φ) has degree $2n'$ with $n' = mp$ or $mp + 1$.*

Proof. Let K_0 be the maximal totally real subfield of K. By Proposition 2.7, the permutation group determined by K_0 must contain at least one of Z_{p^2} or Z_p^2 as a regular subgroup. Then by Theorem 2.5 the $\mathrm{Gal}(K^c/\mathbb{Q})$-orbit of the type Φ is given as a union of orbits of $M_1 = \langle \rho \rangle \times R_0$, for R_0 one of these two regular groups. Let Φ be given by $\mathbf{f}$ as usual, and observe that, if the $\mathrm{Gal}(K^c/\mathbb{Q})$-orbit of $\mathbf{f}$ contains any R_0-orbit of order p^2, then $\mathrm{rank}(\mathbf{f}) \geqslant A(p^2)$, since the orbits of order p^2 are precisely the orbits of the primitive types on the cyclotomic fields, up to multiplication by ρ. We therefore have that the orbit of $\mathbf{f}$ is a union or orbits of R_0 of order p, paired by multiplication by ρ, with the possible addition of $\{0, \rho\}$. This gives our conclusion, since the degree of the reflex field is the order of the orbit of the type.

Additional Remark. We describe here some subsequent developments relevant to the interest of the calculations of Section 4. The result of Proposition 4.1, taken together with the construction of [8] used to establish the converse of Ribet's Nondegeneracy Theorem, suggested to the author that a simple degenerate Abelian variety with a (minimal) cyclic transitive subgroup should be defined by a type with weight relatively prime to the dimension of the variety. H. W. Lenstra, Jr. gave a counterexample to this tentative conjecture at the Arcata Arithmetic Geometry conference. His examples have dimension 42 (even) and 385 (odd) and represent a theory that the author hopes to develop in a future investigation.

ACKNOWLEDGMENTS

The author wishes to thank Professor Shimura for his continuing support and for his suggestion that the topic was of sufficient interest that the best results should be obtained. The author also wishes to express his appreciation to Professor Ribet for the several conversations at the Arithmetic Geometry Conference at Storrs that led to the main results of the paper. Professor Ribet's comments have given a focus to the investigation and provided a deeper motivation for the subject. Since the results of [20, 21] formed a part of the initial motivation in [8], it is a pleasure to acknowledge his contribution to the present paper.

Note added in proof. The present version of this paper reflects several changes in viewpoint and the solution of some of the questions raised by the earlier version. For example, the lower bound of Section 1.3.2 is now best possible. While the Orbit Decomposition Theorem (Proposition 2.2 and Theorem 2.5) seemed significant to the author when the paper was first written, the subsequent solution of Ribet's Question, which is to appear elsewhere, confirms that the minimal transitive permutation groups introduced in the present paper have a definite role in the theory of Abelian varieties with complex multiplication. Finally, the author wishes to thank the referee for several improvements in the text.

REFERENCES

1. N. BOURBAKI, "Groupes et Algebres de Lie," Chaps. 2 et 3, Hermann, Paris, 1972.
2. P. CAMERON, Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* **13** (1981), 1–22.
3. P. CAMERON, P. NEUMANN, AND D. TEAGUE, On the degrees of primitive permutation groups, *Math. Z.* **180** (1982), 141–149.
4. J. CONWAY, Three lectures on exceptional groups, *in* "Finite Simple Groups" (Powell and Higman, Eds.), Academic Press, New York/London, 1971.

5. J. Conway, R. Curtis, S. Norton, and R. Wilson, "Atlas of Finite Groups," Oxford Univ. Press, London/New York, 1985.
6. B. Cooperstein, Minimal degree for a permutation representation of a classical group, *Israel J. Math.* **30** (1978), 213–235.
7. P. Deligne, J. Milne, A. Ogus, and K-y. Shih, "Hodge Cycles, Motives and Shimura Varieties," Lecture Notes in Mathematics, Vol. 900, Springer-Verlag, New York/Berlin, 1982.
8. B. Dodson, The structure of Galois groups of CM-fields, *Trans. Amer. Math. Soc.* **283** (1984), 1–32.
9. B. Dodson, Solvable and nonsolvable CM-fields, *Amer. J. Math.* **108** (1986), 79–93.
10. D. Gorenstein, "Finite Simple Groups: An Introduction to Their Classification," Plenum, New York, 1982.
11. R. Guralnick, Subgroups of prime power index in simple groups, *J. Algebra* **81** (1983), 304–311.
12. R. Guralnick and D. Wales, Subgroups inducing the same permutation representation, II, *J. Algebra* **96** (1985), 94–113.
13. G. Higman, Construction of simple groups from character tables, *in* "Finite Simple Groups" (Powell and Higman, Eds.), Academic Press, New York/London, 1971.
14. W. Kantor, Primitive permutation groups of odd degree, and an application to finite projective planes, *J. Algebra* **106** (1987), 15–45.
15. N. Katz and S. Lang, Finiteness theorems in geometric class field theory, *Ensign. Math.*, (1982), 285–314.
16. T. Kubota, On the field extension by complex multiplication, *Trans. Amer. Math. Soc.* **118** (1965), 113–122.
17. S. Lang, "Complex Multiplication," Springer-Verlag, New York, 1983.
18. D. Passman, "Permutation Groups," Benjamin, New York, 1968.
19. H. Pohlmann, On the image of an Abelian l-adic representation, lecture notes, Brown University, Providence, RI, 1985.
20. K. A. Ribet, Division fields of Abelian varieties with complex multiplication, *Mem. Soc. Math. France, 2e Ser.* Mem. No. 2 (1980), 75–94.
21. K. A. Ribet,"Generalization of a Theorem of Tankeev," Seminaire de Theorie des Nombres, Annee 1981–1982, Exposé No. 17, 5 Mars 1982.
22. N. Schappacher, Zur Existenz Einfacher Abelscher Varietaten mit Komplexer Multiplikation, *J. Reine Angew. Math.* **292** (1977), 186–190.
23. G. Seitz, Flag transitive subgroups of Chevalley groups, *Ann. of Math.* **97** (1973), 27–56.
24. J.-P. Serre, Representations l-adiques, *in* "Algebraic Number Theory" (S. Iyanaga, Ed.), International Symposium, Kyoto, 1976, Japan Soc. for Promotion of Science, Tokyo, 1977.
25. J.-P. Serre, "Abelian l-Adic Representations and Elliptic Curves," Benjamin, New York, 1968.
26. G. Shimura, On canonical models of arithmetic quotients of bounded symmetric domains, *Ann. of Math.* **91** (1970), 144–222.
27. G. Shimura, On the zeta function of an Abelian variety with complex multiplication, *Ann. of Math.* (2) **94** (1971), 504–533.
28. G. Shimura, "Introduction to the Arithmetic Theory of Automorphic Functions," Publ. Math. Soc. Japan, No. 11, Iwanami Shoten, Tokyo, and Princeton Univ. Press, Princeton, NJ, 1971.
29. G. Shimura and Y. Taniyama, "Complex Multiplication of Abelian Varieties and Its Application to Number Theory," Publ. Math. Soc. Japan, No. 6, 1961.
30. M. Suzuki, On a class of doubly transitive groups, *Ann. of Math.* **75** (1962), 105–145.
31. H. Wielandt, "Finite Permutation Groups," Academic Press, New York, 1964.