THE STRUCTURE OF GALEOIS GROUPS OF CM-FIELDS

BY

B. DODSON

ABSTRACT. A CM-field K defines a triple (G, H, p), where G is the Galois group of the Galois closure of K, H is the subgroup of G fixing K, and p ∈ G is induced by complex conjugation. A "p-structure" identifies CM-fields when their triples are identified under the action of the group of automorphisms of G. A classification of the p-structures is given, and a general formula for the degree of the reflex field is obtained. Complete lists of p-structures and reflex fields are provided for [K: Q] = 2n, with n = 3, 4, 5 and 7. In addition, simple degenerate Abelian varieties of CM-type are constructed in every composite dimension. The collection of reflex fields is also determined for the dihedral group G = D_{2n}, with n odd and H of order 2, and a relative class number formula is found.

Let K be a CM-field with [K: Q] = 2n, and let K^c be the Galois closure of K over Q, where Q is the field of rational numbers. In the theory of complex multiplication, the reflex field K' of a CM-type is a fundamental notion. Recall that a CM-type (K, Φ) specifies a set Φ = {φ_1, ..., φ_n} of n embeddings of K into C so that every embedding is among {φ_1, φ_1, ..., φ_n, φ_n}. It is known that [K': Q] depends upon [K: Q] and Φ in a rather complex way. When K/Q is Abelian, K' is a subfield of K. Shimura has shown that there exist CM-fields such that the maximal degree [K': Q] = 2^n occurs, and that there are cases with K ⊆ K'. A general formula for the degree of the reflex field given in §1, is one of our main results.

An Abelian variety A with complex multiplication of type (K, Φ) is called degenerate when the rank τ(Φ), defined in §3, is less than the maximal value of n + 1. The problem of computing the rank was proposed by Kubota, and in the case K/Q Abelian, Lemma 2 of Kubota [8] gives a formulation in terms of group characters. The Theorem of §3.1.1 reduces the calculation of the rank to linear algebra when K has an imaginary quadratic subfield, a case emphasized in this context by Weil [24]. While several degenerate cases with A simple have been constructed, Ribet [15] proves that there are no such examples with n = p, for p a prime. In §3 a converse to Ribet's Theorem is proved by constructing simple degenerate Abelian varieties in every composite dimension.

Shimura's Theorem 2.5 of [21] gives (n + 1 - τ(Φ)) algebraic relations among certain transcendental numbers arising as the periods of Abelian integrals, so the actual values of τ(Φ) are of special interest (cf. [1]). The present result is that when n

Received by the editors August 24, 1982 and, in revised form, May 5, 1983.

1980 Mathematics Subject Classification. Primary 14K22, 12A55; Secondary 20B25.

Key words and phrases. Complex multiplication of Abelian varieties, reflex field, nondegenerate Abelian variety of CM-type, imprimitive permutation groups, relative class number.

©1984 American Mathematical Society
0025-5726/84 $1.00 + $.25 per page
has a factorization $n = kl$, $k > 2$, $l \geq 2$, there is a type $\Phi$ with $t(\Phi) = n - l + 2$ for the cyclotomic fields $K$, with $\text{Gal}(K/\mathbb{Q}) = \langle \rho \rangle \times \mathbb{Z}_n$, where $\mathbb{Z}_n$ denotes the cyclic group of order $n$, and $\rho$ is the automorphism induced by complex conjugation. Further, when certain non-Abelian totally real fields exist, the same rank occurs for $K/\mathbb{Q}$ non-Galois, and smaller ranks are obtained when $n$ is even or divisible by a square.

Suppose the Galois groups of the Galois closures of the totally real fields of degree $n$ are known, and consider, for example, the problem of listing the values of $n'$ that occur as $n' = \frac{1}{2}[K':\mathbb{Q}]$ for the reflex field $K'$ of a $CM$-type for a $CM$-field of degree $2n$; or the problem of listing the values of $t(\Phi)$, for primitive types $\Phi$, when $n$ is composite. Group theoretic techniques are introduced in §§1 and 2 to obtain such information. Generating permutations and defining relations for the distinct permutation groups of degree $n$ that occur is sufficient information about the groups of totally real fields (cf. the Classification Theorem of §2.3). The relation of these calculations to the structure of the group of automorphisms of the Galois group $\text{Gal}(K^c/\mathbb{Q})$ is described in §6.

To illustrate the present methods, complete information is given for the reflex fields when $n = 3, 4, 5, \text{ and } 7$. The list for $n = 4$ uses the methods of group cohomology introduced in §2, while results for the other values of $n$ are obtained from the classical lists of permutation groups of degree $2n = 6, 10$ and $14$. The distribution of the values of $t(\Phi)$ is given for $n = 4$ by the Theorem of §3.3.2, and a procedure for the composite values with $n < 16$ is sketched in §5.3 with $n = 6$.

A related arithmetic topic is taken up for the example of the dihedral group $G = D_{2n}$, $n$ odd. The equivalence classes of reflex types introduced in Shimura [21, Remark 2.4] are also determined for this case. A formula relating the relative class numbers of Shimura [17, 20] is given in §4. Professor Shimura’s suggestion of a more general formula involving the equivalence classes of reflex types initiated the author’s interest in the present investigation.

The author wishes to acknowledge and express his appreciation for Professor Shimura’s comments and encouragement. In particular, Professor Shimura patiently explained the reflex principle to the author; brought the work of Ribet to the author’s attention; and suggested that the reflex fields for the dihedral group and the corresponding characters be examined. At several points in the investigation the author was influenced by the comments of Professor Weil. The author also wishes to thank Dr. Yoshida for his comments on an earlier manuscript and for providing several corrections. Finally, the author wishes to thank the referee for the observation that the results deserved to be rewritten.

1. The reflex degree theorem.

1.1. A $CM$-field is a totally imaginary quadratic extension of a totally real field $K_0$. Let $K^c_0$ be the Galois closure of $K_0$ over $\mathbb{Q}$.

**Proposition.** The Galois group of a $CM$-field of degree $2n$ is given by an exact sequence

$$0 \rightarrow (\mathbb{Z}_2)^v \rightarrow \text{Gal}(K^c/\mathbb{Q}) \rightarrow \text{Gal}(K^c_0/\mathbb{Q}) \rightarrow 1,$$

$1 \leq v \leq n$, where $(\mathbb{Z}_2)^v$ is identified with the subgroup $\text{Gal}(K^c/K^c_0)$ of $\text{Gal}(K^c/\mathbb{Q})$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Proof. By Galois theory only the identification of the normal subgroup \( \text{Gal}(K^c/K_0) \) with \((\mathbb{Z}_2)^v\) must be established. Write \( K = K_0((-\delta)^{1/2}) \), with \( \delta \in K_0 \), let \( \delta_1, \ldots, \delta_n \) be the conjugates of \( \delta \) over \( \mathbb{Q} \), and observe that \( K^c = K_0((-\delta_1)^{1/2}, \ldots, (-\delta_n)^{1/2}) \). Every automorphism \( \epsilon \) of \( K^c \) fixing \( K_0 \) is determined by the images \((-\delta_1)^{1/2} \rightarrow \epsilon_1(-\delta_1)^{1/2}, \ldots, (-\delta_n)^{1/2} \rightarrow \epsilon_n(-\delta_n)^{1/2} \), with \( \epsilon_j = \pm 1, \ j = 1, \ldots, n \). Then \( \text{Gal}(K^c/K_0) \) may be identified with the image in \((\mathbb{Z}_2)^n\) of the map \( \epsilon \rightarrow (\epsilon_1, \ldots, \epsilon_n) \in (\mathbb{Z}_2)^n \), with \( \epsilon_j \) defined by \( \epsilon_j = (-1)^{\delta_j}, j = 1, \ldots, n \). Note that the automorphism \( \rho \) of \( K^c \) induced by the complex conjugation has image \((1, \ldots, 1)\), so \( v \geq 1 \). \( \square \)

Let \( \text{Im}(n, 2) \subset S_{2n} \) denote the maximal imprimitive subgroup of the symmetric group \( S_{2n} \) admitting a specified \( n \) sets of order 2 as sets of imprimitivity. More explicit Galois theoretic information will be obtained from the following:

**Imprimitivity Theorem.** Let \( G \) be an abstract group with \( G \equiv \text{Gal}(K^c/\mathbb{Q}) \) for \( K \) a CM-field of degree \( 2n \). Then \( G \) may be represented as an imprimitive permutation group of degree \( 2n \) with \( n \) sets of imprimitivity of order 2 so that

\[
G = \bigcup_{\sigma \in G_0} (\mathbb{Z}_2)^v (s(\sigma), \sigma),
\]

where:

1. \( G_0 \equiv \text{Gal}(K_0^c/\mathbb{Q}) \) is given as a transitive permutation group of degree \( n \) and may be identified with the group of permutations of the sets of imprimitivity in the representation of \( G \);

2. \((\mathbb{Z}_2)^v \equiv \text{Gal}(K^c/K_0^c) \) is identified with the group of permutations preserving the sets of imprimitivity and is acted upon by \( G_0 \) by permutation of coordinates under an inclusion \( i: (\mathbb{Z}_2)^v \rightarrow (\mathbb{Z}_2)^n \); and

3. \((s(\sigma), \sigma) \in \text{Im}(n, 2) \equiv (\mathbb{Z}_2)^n \times S_n \), the semidirect product, is a lift of \( \sigma \in G_0 \), so that, for the mapping \( s: G_0 \rightarrow (\mathbb{Z}_2)^n \), the mapping \( j \circ s: G_0 \rightarrow (\mathbb{Z}_2)^n/(\mathbb{Z}_2)^v \) is a 1-cocycle, \( j \) being the projection mapping.

Proof. Fix the isomorphism \( G \equiv \text{Gal}(K^c/\mathbb{Q}) \) and let \( H \subset G \) be the subgroup corresponding to \( \text{Gal}(K^c/K) \). Note that, since \( K^c \) is the minimal Galois closure, the action of \( G \) on the coset space \( H \setminus G \) is effective. Since \( K/K_0 \) is a quadratic extension there is a subgroup \( S \) of \( G \) with \( H \subset S \) and indices \( (S : H) = 2, (G : S) = n \), giving that the action of \( G \) on \( H \setminus G \) admits the imprimitivity as asserted. Next observe that the kernel of the action of \( G \) on the coset space \( S \setminus G \) is the subgroup of \( G \) fixing all conjugates of \( S \), so that the identifications of (1) and (2) hold.

Identify \( G \) with the image of \( G \) under permutation representation on the cosets of \( H \), and let \( \text{Im}(n, 2) \) be the maximal subgroup of \( S_{2n} \) admitting the sets of imprimitivity given by using the \( n \) cosets of \( S \) to specify the \( n \) sets of cosets of \( H \). First note that \((\mathbb{Z}_2)^v \) is a subgroup of the maximal subgroup \((\mathbb{Z}_2)^n\) of \( \text{Im}(n, 2) \) preserving the \( n \) sets of imprimitivity. Next observe that the sequence \( 0 \rightarrow (\mathbb{Z}_2)^n \rightarrow \text{Im}(n, 2) \rightarrow S_n \rightarrow 1 \) has a splitting that may be explicitly given by lettering the sets of imprimitivity as \((\pm 1), \ldots, (\pm n)\) and lifting \( \sigma \in S_n \) by the mapping \( \sigma \rightarrow \sigma_+, \sigma_- \) defined by \( +j \rightarrow +\sigma(j), -j \rightarrow -\sigma(j), j = 1, \ldots, n \). The permutation action of \( G_0 \) then follows from...
the inclusion $G_0 \subseteq S_n$ and the $S_n$-action on $(\mathbb{Z}_2)^n$. Now, with
\[G \subseteq (\mathbb{Z}_2)^n \times G_0 \subseteq (\mathbb{Z}_2)^n \times S_n \cong \text{Im}(n,2),\]
define $s: G_0 \rightarrow (\mathbb{Z}_2)^n$ by picking an arbitrary lift $(s(\sigma), \sigma) \in G$, for each $\sigma \in G_0$; and observe that the subset of $(\mathbb{Z}_2)^n \times G_0$ determined by $(\mathbb{Z}_2)^n \subseteq (\mathbb{Z}_2)^n$ and $s$ is closed under multiplication if and only if $f \circ s$ is a crossed homomorphism. □

In view of the identifications made in the Imprimitivity Theorem, the exact sequence of the proposition will be referred to as an imprimitivity sequence for $\text{Gal}(K^c/\mathbb{Q})$. For any (transitive) $G \subseteq \text{Im}(n,2)$, the projection $G \rightarrow G_0$ will be denoted by $\text{Proj}_{\text{Sets}}$, or by $\text{Proj}_{G_0}$, and the exact sequence will be referred to as an imprimitivity sequence for $G$, regardless of the existence of a CM-field $K$ and an isomorphism $G \cong \text{Gal}(K^c/\mathbb{Q})$ inducing $G_0 \cong \text{Gal}(K_0^c/\mathbb{Q})$.

1.2. Let $\mathbb{C}$ denote the field of complex numbers, and let $t_j: K \rightarrow \mathbb{C}$, $j = 1, \ldots, n$, be field embeddings so that every embedding $\tau: K \rightarrow \mathbb{C}$ is among the collection \(\{t_1, t_2, \ldots, t_n, \bar{t}_1, \bar{t}_2, \ldots, \bar{t}_n\}\), $t_j$ being the embedding given by complex conjugation. Then $K$ has $2^n$ CM-types $(K, \Phi)$, where each type $\Phi$ on $K$ may be viewed as giving $n$ choices, picking one embedding from each of the sets $\{t_j, \bar{t}_j\}$. Recall that $\text{Gal}(K^c/\mathbb{Q})$ acts on the set of types on $K$ by sending $\Phi = \{\phi_1, \ldots, \phi_n\}$ to the type $\Phi^g$ with entries $\phi_j^g$ given by applying $g \in \text{Gal}(K^c/\mathbb{Q})$ to the image of $\phi_j$. Let $1^{st}$ denote the projection of $(\mathbb{Z}_2)^n$ onto the first coordinate.

**Proposition.** Let $G \cong \text{Gal}(K^c/\mathbb{Q})$ be given by an imprimitive permutation representation as in the Imprimitivity Theorem. Then a CM-type $\Phi$ may be specified by giving $f \in (\mathbb{Z}_2)^n$ in such a way that the $G$-set structure on the set of types is given by writing $g \in G$ as $g = (es(\sigma), \sigma)$, and then sending $\Phi = \Phi^f$ to $\Phi^g = \Phi^h$, with $h = \sigma^{-1} \ast (fes(\sigma))$, the product $fes(\sigma)$ being taken formally in $(\mathbb{Z}_2)^n$, with $G_0$ acting by permutation of coordinates.

**Proof.** Let $H_0 \subseteq G_0$ be the stabilizer of a letter under the inclusion $G_0 \subseteq S_n$. Give coset representatives $\tau_j$, $j = 1, \ldots, n$, for $H_0$ in $G_0$, and let $H$ be the subgroup of $G$ fixing the letters in the set of imprimitivity corresponding to the letter fixed by $H_0$. Observe that taking $g_j = (s(\tau_j), \tau_j), \rho g_j = (\rho s(\tau_j), \tau_j)$ gives $(g_1, \rho g_1, \ldots, g_n, \rho g_n)$ as coset representatives for $H$ in $G$, where $\rho = ((1, \ldots, 1), (1)) \in (\mathbb{Z}_2)^n \times \langle (1) \rangle \subset G$ is the element of $G$ corresponding to the automorphism $\rho$ of $K^c$ over $\mathbb{Q}$ induced by the restriction of complex conjugation. Then use $f \in (\mathbb{Z}_2)^n$ to specify the type given by the embeddings corresponding to the cosets $(Hg_1, \ldots, Hg_n)$ for $f = (f_1, \ldots, f_n), f_j \in \mathbb{Z}_2$ being written as 0 or 1.

To verify the $G$-action, let $H_0$ stabilize the letter 1, $H$ stabilize the letters in the set \((\pm 1)\), and observe that $\rho \in G$ may be used to alter the map $s: G_0 \rightarrow (\mathbb{Z}_2)^n$ so that $s(\sigma)$ has first coordinate 0 for all $\sigma \in G_0$. Consider the $j$th entry $Hg_j$ of $f^j$, and the translated coset $Hg_jg$. Write $g = (e', \sigma)$, with $e' = es(\sigma)$. Then compute $\rho^{f_j} g = (\rho^{f_j}s(\tau_j)g \ast e', \tau_j \sigma)$. The coset of $H_0$ in $G_0$ determines which coordinate of $h$ is being given, and $\tau_j \sigma$ takes $l$ to $\sigma(j)$ (permutation multiplication being read left-to-right), so $\tau_j \sigma$ belongs to the coset $H_0 \tau_{\sigma(j)}$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
The entry $h_{a(j)}$ of $h = (h_1, \ldots, h_n)$ is then determined by deciding whether $\rho^{f_j}g_jg$ belongs to $Hg_{a(j)}$ or to $Hpg_{a(j)}$. Noting that $1^{st}(s(\sigma)) = 0$ for all $\sigma \in G_0$, the calculation

$$1^{st}(\rho^{f_j}s(\tau_j) \tau_j * e') = f_j1^{st}(\tau_j * e') = f_j e'_j,$$

for $e' = (e'_1, \ldots, e'_n)$, gives $h_{a(j)} = f_j e'_j$, where the addition in $\mathbb{Z}_2$ is written multiplicatively. But then the $G_0$-action allows the entries to be given by $\sigma * h = fe'$, so $h = \sigma^{-1} * (fe)\sigma$, recalling $e' = es(\sigma)$.

1.3. The action of the proposition may be temporarily extended to give an action $f \to \sigma^{-1} * (fe)$ for all $(e, \sigma) \in (\mathbb{Z}_2)^n \times G_0$. For the extended action, observe that requiring $(e, \sigma)$ to fix $f$ determines $e = e(\sigma, f)$ uniquely, since $f = \sigma^{-1} * (fe)$ implies $e = fs(\sigma)$. Restricting the action back to $G \subset (\mathbb{Z}_2)^n \times G_0$ provides the following:

**Definition.** The splitting subgroup of $G \subset (\mathbb{Z}_2)^n \times G_0$ and $f \in (\mathbb{Z}_2)^n$ is the subgroup $S_0 = S_0(f)$ of $G_0$ defined by $S_0(f) = \{\sigma \in G_0 / fs(f) * f \in (\mathbb{Z}_2)^n s(\sigma)\}$, where $G$ is given by $(\mathbb{Z}_2)^n$ and $s$ as in the Imprimitivity Theorem.

**The Reflex Degree Theorem.** Let $K/\mathbb{Q}$ be a CM-field with maximal totally real subfield $K_0$. Let $0 \to (\mathbb{Z}_2)^n \to G \to G_0 \to 1$ be the imprimitivity sequence of $G = \text{Gal}(K^c/\mathbb{Q})$ and represent $G$ as in the Imprimitivity Theorem. Let $(K, \Phi)$ be a CM-type and $K' = K'(\Phi)$ the reflex field of $(K, \Phi)$. Then, when $\Phi$ is written in the form $\Phi = \Phi^f$,

$$[K' : \mathbb{Q}] = 2^e(G_0 : S_0),$$

where $2^e = [K^c : K_0^c]$, and $(G_0 : S_0)$ is the index in $G_0$ of the splitting subgroup $S_0 = S_0(f)$.

**Proof.** Recall that $K'(\Phi)$ is the subfield of $K^c$ fixed by the stabilizer of $\Phi$ under the Gal$(K'/\mathbb{Q})$-action, so that $[K' : \mathbb{Q}] = (G : H'(\Phi))$, with $H'(\Phi)$ the corresponding subgroup of $G$. Observe that $H'(\Phi) = \{(fs * f, \sigma) / \sigma \in S_0(f)\}$, since $(fs * f, \sigma)$ must belong to $G$. Then $|G| = 2^e|G_0|$ gives

$$(G : H'(\Phi)) = |G| / |H'(\Phi)| = 2^e |G_0| / |S_0| = 2^e (G_0 : S_0),$$

since $\text{Proj}_{G_0}$ gives an isomorphism of $H'(\Phi)$ onto $S_0$.

**Remark.** Note that $[K' : \mathbb{Q}]$ is also the order of the orbit of $\Phi$ under the $G$-action. Also observe that $H'(\Phi)$ is explicitly given, at least when $s(\sigma)$ is explicitly given.

2. $\rho$-structures.

2.1.1. To study the $G$-set structure on the collection of CM-types, a refinement of permutation structure on $G$ is introduced by the following:

**Definitions.** Let $G$ and $G_1$ be abstract groups with central involutions. Let $\rho \in G$ and $\rho_1 \in G_1$ be central involutions, and let $H$ be a subgroup of $G$ and $H_1$ a subgroup of $G_1$, with $(G : H) = (G_1 : H_1) = 2n$, so $G$ and $G_1$ act effectively on the coset spaces $H \setminus G$ and $H_1 \setminus G_1$. Then the triple $(G, H, \rho)$ will be said to be $\rho$-equivalent to the triple $(G_1, H_1, \rho_1)$ if there is an isomorphism $\psi : G \to G_1$, so that $\psi(H) = H_1$, and $\psi(\rho) = \rho_1$. A $\rho$-structure of degree $2n$ will refer to an equivalence class of triples $(G, H, \rho)$ under $\rho$-equivalence.
Remark 1. Shimura [17] observed that the automorphism $\rho$ of $K^c$ over $\mathbb{Q}$ induced by complex conjugation is central in $\text{Gal}(K^c/\mathbb{Q})$. A verification in the present context may be obtained by noting that $\rho$ is identified with the central element $((1, \ldots, 1), (1))$ of $\text{Im}(n, 2)$ in which $\text{Gal}(K^c/\mathbb{Q})$ has been effectively represented.

Remark 2. The above definition is a special case of an "imprimitivity equivalence" defined on triples $(G, H, S)$, with $(G : S) = n$, $(S : H) = k$, and $G$ effective on $H \setminus G$. Note the special circumstances $k = 2$ and $S = H \times \langle \rho \rangle$, a direct product with $\rho$ central in $G$, in the present study. The general case of these "imprimitivity structures" may also be of some Galois theoretic interest.

The present interest in $\rho$-structures is established by the following:

**Proposition.** Let $K$ and $K_1$ be CM-fields of degree $2n$, and suppose $G$ is an abstract group with $G \cong \text{Gal}(K^c/\mathbb{Q}) \cong \text{Gal}(K_1^c/\mathbb{Q})$. Let $\rho$ and $\rho_1$ be the central involutions of $G$ corresponding to the restriction of complex conjugation to $K^c$ and $K_1^c$, respectively, and let $H$ and $H_1$ be the subgroups of $G$ corresponding to $\text{Gal}(K^c/K)$ and $\text{Gal}(K_1^c/\mathbb{Q})$. Then if $(G, H, \rho)$ is $\rho$-equivalent to $(G, H_1, \rho_1)$, the collection of CM-types for $K$ and $K_1$ are equivalent $G$-sets.

**Proof.** Observe that a $\rho$-equivalence $\psi$ takes the pairing of cosets of $H$ in $G$ under $\rho$ to the pairing of cosets of $H_1$ in $G$ under $\rho_1$, so that the action of $G$ on types commutes with $\psi$.

Remark 3. In the case $K^c = K_1^c$, a $\rho$-equivalence is an automorphism of $\text{Gal}(K^c/\mathbb{Q})$ preserving the distinguished central element $\rho$. The subgroup of $\text{Aut}(G)$ preserving $\rho$ will be denoted by $\text{Aut}(G, \rho)$. Note that $n = 2$, $G = D_4$ dihedral of order 8, gives an example with $K$ and $K_1$ nonconjugate over $\mathbb{Q}$. An identification of the types for all such $K$ and $K_1$ may be observed in the treatment of $n = 2$ in Shimura and Taniyama [23, §8.4(2)].

2.1.2. The technique of imprimitive permutation representations may be introduced into the study of $\rho$-structures by the following:

**Proposition.** Let $G_0 \subset S_\rho$ be a transitive group of degree $n$ and let $(\mathbb{Z}_2)^v$ be a sub-$G_0$-module of $(\mathbb{Z}_2)^n$, with permutation action, so that $\rho \in (\mathbb{Z}_2)^v$ for $\rho = (1, \ldots, 1)$. Then $\bar{s} \in \mathbb{Z}^1(G_0, (\mathbb{Z}_2)^v/(\mathbb{Z}_2)^v)$ specifies a unique $\rho$-structure.

**Proof.** The $\rho$-structure will be defined on the abstract group $G$ given as a group extension by $c^1([\bar{s}])$, $c^1$ being the connecting homomorphism

$$c^1 : H^1(G_0, (\mathbb{Z}_2)^n/(\mathbb{Z}_2)^v) \to H^2(G_0, (\mathbb{Z}_2)^v).$$

Note that $G_0 \subset S_\rho$ specifies a subgroup $H_0$ up to conjugacy, and then a subgroup $S$ of $G$ as the inverse image of $H_0$ under $G \to G_0$. Note that by hypothesis $\rho \in (\mathbb{Z}_2)^v \subset S$, and $\rho$ is uniquely determined in $S$. A $\rho$-structure on $G$ is then determined by using $\bar{s}$ to specify $H$ of index 2 in $S$ as the stabilizer of the two letters in the set fixed by $H_0$ in the imprimitive permutation representation of $G$ defined by $\bar{s}$.
As a first indication of the relation between group extension equivalence and \( \rho \)-equivalence, consider the following:

**Corollary of the Reflex Degree Theorem.** Let \( K \) be a CM-field. Then the \( \rho \)-structure determined by an imprimitive permutation representation of \( G = \text{Gal}(K^c/Q) \) is given by the trivial class \([0] \in H^1(G_0, (\mathbb{Z}_2)^n/(\mathbb{Z}_2)^n)\) if and only if \( K \) has a reflex field \( K' \) with \([K':Q] = [K^c:K_0] = 2^r\), in which case \( \text{Gal}(K^c/K') \equiv \text{Gal}(K_0^c/Q) \) gives a splitting of the imprimitivity sequence of \( \text{Gal}(K^c/Q) \) (respectively, \( H' \equiv G_0 \) for \( G \)).

**Proof.** If \((G, H, \rho)\) is given by \( \bar{s} \in [0] \), then there is \( b \in (\mathbb{Z}_2)^n \), so \( \bar{s}(\sigma) = b\sigma \ast b(\mathbb{Z}_2)^n \). Take \( s(\sigma) = b\sigma \ast b \) and note that \( G \) is given as

\[
G = \bigcup_{\sigma \in G_0} (\mathbb{Z}_2)^n (b\sigma \ast b, \sigma).
\]

But then the type defined by \( \Phi = \Phi^f \), with \( f = b \), has \( H'(\Phi) = ((b\sigma \ast b, \sigma) / \sigma \in G_0) \equiv G_0 \) giving a splitting and \([K':Q] = [G]/[H'] = 2^n|G_0|/|G_0| = 2^r\). Conversely, if \( K \) has a type \( \Phi \) with \([K'(\Phi):Q] = 2^n\), represent \( \text{Gal}(K^c/Q) \) as in the Imprimitivity Theorem and write the type as \( \Phi = \Phi^f, f \in (\mathbb{Z}_2)^n \). Then observe \( \sigma \rightarrow (fo \ast f, \sigma) \) splits the imprimitivity sequence of \( \text{Gal}(K^c/Q) \), and \( \bar{s} = j \circ s \), for \( s(\sigma) = fo \ast f, \) is a coboundary.

**Remark.** In the Classification Theorem of §2.3, \([0]\) is shown to define a unique \( \rho \)-structure of degree \( 2n \) on \( G = (\mathbb{Z}_2)^n \times G_0 \). The condition on the degree of the reflex field in the corollary will therefore uniquely determine a \( \rho \)-structure for each \( G_0 \subset S_n \) and \((\mathbb{Z}_2)^n \subset (\mathbb{Z}_2)^n\). This method of specifying the \( G \)-set structure on the collection of CM-types is featured in §§3 and 4.

2.2.0. A phenomenon that occurs for permutation groups, and may be observed in the analysis of Miller [11] for \( n = 6, 7 \), forces a distinction between \( \rho \)-equivalence and group extension equivalence. The existence of CM-fields whose imprimitivity sequences require this distinction will be established before proceeding with the algebraic definitions. One method for establishing the existence of a CM-field \( K \) so that \( \text{Gal}(K^c/Q) \) has a given \( \rho \)-structure is to give a subgroup analysis of the group \( \text{Gal}(L/Q) \), where \( L \) is a (non-Abelian) CM-field that is known to exist. Since interesting fields \( K \) with \( K^c \) proper in \( L \) occur, the triple \((G, H, \rho)\) will be said to define a \( \rho \)-structure with kernel when the action of \( G \) on \( H \setminus G \) is not effective.

2.2.1 In §5 it will be shown that there are exactly four \( \rho \)-structures for \( n = 3 \).

**Theorem.** There exist CM-fields \( K_1 \) such that each of the 4 \( \rho \)-structures of degree \( 2n \) with \( n = 3 \) occurs as \( \text{Gal}(K_1^c/Q) \). The field with structure having \( v = 1 \) occur as subfields of the fields with structures having \( v = 3 \). The groups for \( v = 3 \) are \( \mathbb{Z}_2 \times A_4 \) and \( \mathbb{Z}_2 \times S_4 \), and the CM-subfields of \( L \) are classified by 5 \( \rho \)-structures for \( \mathbb{Z}_2 \times A_4 \) and 10 \( \rho \)-structures for \( \mathbb{Z}_2 \times S_4 \).

**Proof.** See §5 for the fact that the structures and the groups are as specified. The existence of the fields with \( v = 3 \) is provided by Shimura [18, §1] as an application of results from class field theory, with the general case giving the existence of a field \( L \) with \( G = (\mathbb{Z}_2)^n \times G_0 \) whenever there exists a totally real field \( K_0^c \) having group
and the present case resulting for every $K_0$ totally real cubic. An explicit example may be found in Pohlman [12] for $G = \mathbb{Z}_2 \times S_4$. The existence of fields with $v = 1$, if in doubt, will follow from the assertions below on $\rho$-structures with kernel.

Consider $G = G_0^* \times \mathbb{Z}_2$ for $G_0^* = A_4, S_4$. The splitting here is the splitting of $0 \rightarrow \langle \rho \rangle \rightarrow G \rightarrow G_0 \rightarrow 1$, $G_0 \equiv \text{Gal}(L^{\langle \rho \rangle}/\mathbb{Q})$, given by a type $\Phi$ of $L$ as in the corollary of §2.1.2. Thus, $G_0^* = H'(\Phi) \equiv \text{Gal}(L/\mathbb{Q}(\sqrt{-d}))$, with $\mathbb{Q}(\sqrt{-d})$ imaginary quadratic, as may always be arranged whenever $(G, \rho)$ has a $\rho$-structure with $(G : H \times \langle \rho \rangle) = 2n$ for $n$ odd.

First obtain the permutation structures $(G, H \times \langle \rho \rangle)$ which classify the totally real fields of $L$ admitting CM-subfields of $L$ as quadratic extensions. These may be written as $H \times \langle \rho \rangle = H^* \times \langle \rho \rangle$ with $H^* \subset G_0^*$. Then for $G_0^* = A_4$, $H^*_0 = 1, \mathbb{Z}_2, \mathbb{Z}_3, (\mathbb{Z}_2)^2, or A_4$, and for $G_0^* = S_4$, $H^*_0 = 1, \langle (12) \rangle, \langle (12)(34) \rangle, \mathbb{Z}_3, (\mathbb{Z}_2)^2, (\mathbb{Z}_2)^2, \mathbb{Z}_4, S_3, D_4, A_4 or S_4$, where $(\mathbb{Z}_2)^2$ is transitive and $(\mathbb{Z}_2)^2$ is intransitive. Then observe that since $\rho$ is unique, the permutation structures $(G, H)$, with $H$ of index two in these $\langle \rho \rangle \times H^*_0$, determine the $\rho$-structures (as in Proposition 1 of §5.1). Immediate conclusions are that $H = H^* \times \langle \rho \rangle$ gives $\rho$-structures for $n = 4, 6$, and 12 for $G_0^* = A_4$, and for $n = 4, 6, 6, 8, 12, 12$, and 24 for $G_0^* = S_4$. For the omitted cases, $H^*_0$ gives $\rho$-structures with kernel, the kernel $(\mathbb{Z}_2)^2$, for each $G_0^*$, giving the required Galois cases with $n = 3, v = 1$.

The remaining $\rho$-structures have $H$ of index 2 in $\langle \rho \rangle \times H^*_0$, $H \neq H^*_0$. For $n = 3$, take

$$H = \langle (\rho, (12)(34)), (0, (13)(24)) \rangle$$

for $G_0^* = A_4$, and

$$H = \langle (\rho, (12)(34)), (0, (1234)) \rangle$$

for $G_0^* = S_4$. Note that the present notation is not in conflict with the previous notation used for $\mathbb{Z}_2 \times G_0 = G$, provided that $G$ is given its $n = 4$ structure with $G_0^*$ identified with $G_0$. The first nontrivial structures are obtained, one for each group, by observing that $\langle (0, (12)(34)) \rangle$ is inequivalent to $\langle (\rho, (12)(34)) \rangle$, since only $(0, (12)(34))$ is a commutator. The final $\rho$-structure has $n = 6, G_0^* = S_4$ and $S = \langle \rho \rangle \times (\mathbb{Z}_2)^2$, and is specified by the index two subgroup $H^{nt} \subset S$ given as $H^{nt} = \langle (\rho, (34)), (0, (12)) \rangle$. The inequivalence of this $\rho$-structure from the above structure with the same $S$ will be established below, while the other $\rho$-structure with $n = 6$ has the distinct permutation structure of degree 6 on $G_0 = S_4$ (cf. §5.3). To check that no further $\rho$-structures are allowed, either compute $H^1$ as suggested in §6, or use generators and relations directly, to produce an outer automorphism taking, e.g., $(0, (34))$ to $(\rho, (34))$ for $S_4$. The remaining index two $H$ are either conjugate to one of the above or to the image of such a conjugate under this automorphism.

2.2.2. Definitions. Let $G_0 \subset S_n$ and $(\mathbb{Z}_2)^v \subset (\mathbb{Z}_2)^n$ be as usual. The trivial $\rho$-structure will refer to the $\rho$-structure defined on the split group $G = (\mathbb{Z}_2)^v \times S_0$ defined by the 1-cocycle $\bar{s} = 0 \in Z^1(G_0, (\mathbb{Z}_2)^v)/(\mathbb{Z}_2)^v$ as in the Proposition of §2.1.2. A $\rho$-structure will be said to be nonsplit if it is defined by $\bar{s} \in Z^1(G_0, (\mathbb{Z}_2)^v)/(\mathbb{Z}_2)^v$, so that $c^1([\bar{s}]) \neq [0]$ in $H^2(G_0, (\mathbb{Z}_2)^v)$, $c^1$ being the map $c^1: H^1(G_0, (\mathbb{Z}_2)^v)/(\mathbb{Z}_2)^v \rightarrow H^2(G_0, (\mathbb{Z}_2)^v)$. For $\bar{s} \in Z^1(G_0, (\mathbb{Z}_2)^v)/(\mathbb{Z}_2)^v$, a nontrivial
\( \rho \)-structure relative to \( \bar{s} \) will refer to a \( \rho \)-structure defined by \( \bar{s}_1 \in \mathbb{Z}^1(G_0, (\mathbb{Z}_2)^n/(\mathbb{Z}_2)^{\rho}) \) with \( c^1([\bar{s}_1]) = c^1([\bar{s}]) \), but inequivalent to the \( \rho \)-structure defined by \( \bar{s} \). A nontrivial split \( \rho \)-structure will refer to a nontrivial \( \rho \)-structure relative to the initial structure given by \( \bar{0} \).

**Proposition.** Let \( L \) be a CM-field with \( \text{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}_2 \times S_4 \), and let \( K \) and \( K_{nt} \) be the two CM-fields having \( K_0 \) given as the fixed field of \( S = \langle \rho \rangle \times (\mathbb{Z}_2)^2 \) as a common maximal totally real subfield, \( K \) and \( K_{nt} \) being given by the subgroups \( H \) and \( H_{nt} \), of index 2 in \( S \), as specified in the proof of the above theorem. Then \( K_{nt} \) defines a nontrivial split \( \rho \)-structure inequivalent to the \( \rho \)-structure defined by \( K \).

**Proof.** Observe that both fields have \( v = 1 \), and \( K \) has an imaginary quadratic subfield, which therefore occurs as a reflex field \( K' \) for a type on \( K \). By contrast, \( K_{nt} \) may be seen to have no imaginary quadratic subfield and, therefore, no \( G \)-orbit of types containing just two elements. In fact, \( L \) has only two imaginary quadratic subfields, the second being the fixed field of the image of \( 1 \times G_0^* \) under the outer automorphism used in the proof of the theorem. But \( (\rho, (12(34))) \in H_{nt} \), so \( H_{nt} \) is not a subgroup of either \( 1 \times G_0^* \) or its image. Thus \( K \) and \( K_{nt} \) are inequivalent, but may be observed to have identical imprimitivity sequences.

2.3.1. The material of this subsection is not used until §5, and, in particular, is not required for the arithmetic results of §§3 and 4. Representatives for the distinct \( \rho \)-structures are provided by the following:

**Classification Theorem.** The \( \rho \)-structures of degree \( 2n \) are classified by:

(A) picking representatives \( G_0 \subset S_n \) for the distinct permutation structures of degree \( n \);

(B) picking representatives for the class of \( G_0 \)-submodules \( (\mathbb{Z}_2)^{\rho} \subset (\mathbb{Z}_2)^n \) with \( \rho \in (\mathbb{Z}_2)^{\rho} \) under identifications by the normalizer \( N_{S_n}(G_0) \) of \( G_0 \) in \( S_n \); and then,

(C) finding the \( N_{S_n}(G_0) \)-orbits of \( H^1(G_0, (\mathbb{Z}_2)^{\rho})/(\mathbb{Z}_2)^{\rho} \) for \( G_0 \) and \( (\mathbb{Z}_2)^{\rho} \) ranging over the choices in (A) and (B), where \( N_{S_n}(G_0) \) is the subgroup of \( N_{S_n}(G_0) \) preserving \( (\mathbb{Z}_2)^{\rho} \).

**Proof.** Let \( \psi: G \to G_1 \) be a \( \rho \)-equivalence. First observe that \( \psi \) induces an equivalence on the group actions of the groups obtained from \( \text{ProjSets} \), so that \( G_0 = \text{ProjSets}(G) \) and \( G_1 = \text{ProjSets}(G_1) \) may be regarded as equivalent permutation groups. Then the two \( \rho \)-structures may be given by imprimitive permutation representations in a common subgroup \( (\mathbb{Z}_2)^n \times_s G_0 \subset \text{Im}(n, 2) \), with a single \( G_0 \subset S_n \) for each permutation structure of degree \( n \). Next observe that \( (\mathbb{Z}_2)^n \times_s N_{S_n}(G_0) \subset \text{Im}(n, 2) \) acts on \( (\mathbb{Z}_2)^n \times_s G_0 \) by conjugation and is the maximal group having an action that corresponds to a reindexing of the elements \( \{\pm 1, \ldots, \pm n\} \) preserving the given sets of imprimitivity \( \{\pm 1\}, \ldots, \{\pm n\} \) specified in the choice of \( \text{Im}(n, 2) \) and preserving the choice \( G_0 \subset S_n \). Note that the action of \( 0 \times_s N_{S_n}(G_0) \) gives the identifications of (B). Finally, the action of \( (\mathbb{Z}_2)^n \times_s 1 \) gives \( B^1(G_0, -) \)-equivalence on the 1-cocycle defining the image of the permutation representation of \( G \), and then only the above \( N_{S_n}(G_0) \)-equivalence is allowed on \( H^1(G_0, (\mathbb{Z}_2)^n/(\mathbb{Z}_2)^{\rho}) \).
Proposition. The abstract groups $G$ in the above classification are given as group extensions by fixing the choices in (A) and (B) and computing

$$H^1(G_0, (\mathbb{Z}_2)^n/(\mathbb{Z}_2)^v) / j^1(H^1(G_0, (\mathbb{Z}_2)^n)),$$

which is isomorphic to

$$Z^1(G_0, (\mathbb{Z}_2)^n/(\mathbb{Z}_2)^v) / j^1(Z^1(G_0, (\mathbb{Z}_2)^n)),$$

where $j^1$ is used for the cocycle mapping induced by the projection $j: (\mathbb{Z}_2)^n \to (\mathbb{Z}_2)^n/(\mathbb{Z}_2)^v$, and also for the induced mapping on cohomology classes.

Proof. In fact, the condition $G \subset (\mathbb{Z}_2)^n \times G_0$ assures that $i^2(f) = 0$, for $f$ the 2-cocycle defining the extension, and the inclusion map $i^2: H^2(G_0, (\mathbb{Z}_2)^n) \to H^2(G_0, (\mathbb{Z}_2)^n)$. The assertion follows by exactness of the long exact cohomology sequence. The cocycle formulation, $Z^1/j^1(Z^1)$, is obtained by observing that $j^1: B^1(G_0, (\mathbb{Z}_2)^n) \to B^1(G_0, (\mathbb{Z}_2)^n/(\mathbb{Z}_2)^v)$ is surjective.

2.3.2. A choice of representatives for (A), (B) and (C) in the Classification Theorem will be referred to as a normalization, or “normal form”, for the elements of a $\rho$-structure. Some examples will be given here, with further cohomological considerations being postponed to §6.

Example 1. For $n = p$, $p$ a prime, any $G_0$ may be normalized to contain the $p$-cycle $(1 \, 2 \, \cdots \, p)$. Note that recent results on 2-transitivity supply a complete list of these $G_0$, as in [4].

Example 2. For $n = 4$, the transitive permutation groups with $G_0 \equiv \mathbb{Z}_4$, $G_0 \equiv D_4$ may be normalized as $\langle(1234)\rangle$, and $\langle(1234), (12)(34)\rangle$. By contrast $G_0 = (\mathbb{Z}_2)^2$, $G_0$ transitive, is uniquely determined as a subgroup of $S_4$, and allows arbitrary reindexing: $N_{S_4}((\mathbb{Z}_2)^2) = S_4$.

$G_0 = (\mathbb{Z}_2)^2$ also has three submodules of the form $(\mathbb{Z}_2)^v \subset (\mathbb{Z}_2)^n$ for $n = 4$, $v = 2$. A 3-cycle may be used to establish an equivalence between these three submodules, and also among the permutation groups $G$ with $G_0 = (\mathbb{Z}_2)^2$ and $v = 2$. The choice $(\mathbb{Z}_2)^v = \langle \rho, \xi \rangle$, for $v = 2$, with $\xi = (0101) \in (\mathbb{Z}_2)^4$, is preferred, since that choice fits the nesting $(\mathbb{Z}_2)^2 \subset D_4$, for $D_4$ normalized as above.

Example 3. Consider $G = \mathbb{Z}_2 \times \mathbb{Z}_4$. First observe that $G$ has 3 central order two elements in two $\text{Aut}(G)$ orbits. The imprimitivity sequence of $\text{Gal}(K^c/Q)$ may be observed to depend upon the isomorphism $G \equiv \text{Gal}(K^c/Q)$, since these two classes correspond to $K_0$ having group $(\mathbb{Z}_2)^2$ or $\mathbb{Z}_4$. The two noncharacteristic central order two elements define a single $\rho$-structure, although the imprimitivity sequences are inequivalent. The characteristic central order two element gives a $\rho$-structure that is supplied by a single cocycle group, $Z^1((\mathbb{Z}_2)^2, (\mathbb{Z}_2)^4/\langle \rho \rangle)$. Observe that $|Z^1/j^1(Z^1)| = 8$, while only four abstract groups are obtained. A reindexing of the form $(0, \sigma_4)$, with $\sigma_4$ a 3-cycle, gives a $\rho$-equivalence on the three group extensions with $G \equiv \mathbb{Z}_2 \times \mathbb{Z}_4$, and on the three group extensions with $G \equiv D_4$, so that the identifications made in (C) of the Classification Theorem are nontrivial. Note that $Z^1/j^1(Z^1)$ classifies subgroups of $(\mathbb{Z}_2)^n \times G_0$ up to extension equivalence, which is therefore too strong, in addition to being too weak, as shown in §2.2.

Example 4. Nonsplit extensions are supplied by the group

$$G^+ = \{ (e, \sigma) \in (\mathbb{Z}_2)^n \times G_0 = G / \text{sgn}(e) \text{sgn}(\sigma) = +1 \},$$
with $\text{sgn}(e)$ from $e \in (\mathbb{Z}_2)^w \subset (\mathbb{Z}_2)^n \subset S_{2^n}$ and $\text{sgn}(\sigma)$ from $\sigma \in G_0 \subset S_n$ (cf. Coxeter and Moser [3]). Whenever $G_0$ and $(\mathbb{Z}_2)^w$ have odd elements, $G^+$ will be a nonsplit extension over $G_0$, with $v = w - 1$, and therefore distinct from the trivial structure on the split group $[(\mathbb{Z}_2)^n]^+ \times G_0$, where $[(\mathbb{Z}_2)^n]^+$ is the even subgroup of $(\mathbb{Z}_2)^n$, common to both groups. When $n$ is even both groups contain $\rho$, while when $n$ is odd, extra structures for $G_0^1$ of degree $n_1 = 2n$ are obtained.

Note especially the case $n$ even, $w = n$, $v = n - 1$. By the Reflex Degree Theorem, $v = n - 1$ implies that either there are two $G$-orbits of types, each of order $2^{n-1}$, in which case the $\rho$-structure is trivial, or else all types form a single $G$-orbit. Further examples with a single $G$-orbit of types are found for $n = 4$, one with $v = 1$, two with $v = 2$ and several cases with $v = 3$ that are nonsplit but not of the form $G^+$. For complete results when $n = 4$, see §5.2.

3. Degeneracy in composite dimensions.

3.1.0. Recall that for a CM-type $(K, \Phi)$, an Abelian variety $A$ with complex multiplication of type $(K, \Phi)$ is obtained by the analytic construction of Shimura and Taniyama [23]. The existence of a CM-field with a given type therefore assures the existence of Abelian varieties of that type. The rank of $A$, $t(A) = t(\Phi)$, is the rank of the free $\mathbb{Z}$-module $M$ spanned by the $\text{Gal}(K^{c}/\mathbb{Q})$ orbit of $\Phi$ inside the $\mathbb{Z}$-module spanned by the $2w$ embeddings of $K$ into $\mathbb{C}$. Observe that the sum of the coefficients of the embeddings $\tau$ and $\bar{\tau}$ is a constant for each element of $M$, so that the maximal rank is obtained when coefficients for $n$ embeddings, pairwise nonconjugate, and the common value of the sum of the coefficients are given independently. Then the rank of $A$ is $n + 1$ and $A$ is said to be nondegenerate. The variety $A$ is said to be degenerate when $\text{rank}(A) = \text{rank}(K, \Phi) < n + 1$.

Let $(K', \Phi')$ be the reflex type of $(K, \Phi)$. Recall that $\text{rank}(K, \Phi) = \text{rank}(K', \Phi')$ (Kubota [8] or Shimura [22]), so $[K' : \mathbb{Q}] \geq [K : \mathbb{Q}]$ is a necessary condition for $(K, \Phi)$ to be nondegenerate. Also, $(K, \Phi)$ is said to be primitive, and $A$ is simple, when $(K', \Phi)' = (K, \Phi)$ (Shimura [19]); and $(K')' \subseteq K$, with $(K')' = K$ if and only if $(K, \Phi)$ is primitive. Observe that if $A$ is reducible,

$$\text{rank}(K, \Phi) = \text{rank}(K', \Phi') = \text{rank}((K', \Phi')') < \frac{1}{2}[K : \mathbb{Q}] + 1,$$

so that the distinction between degeneracy and nondegeneracy is meaningful only when $(K, \Phi)$ is primitive.

The proposition of §1.2 provides a method for computing the $G$-orbit, and therefore, the rank $t(\Phi)$ of $(K, \Phi)$, subject to explicit information on $G_0 \subset S_n$, $(\mathbb{Z}_2)^w \subset (\mathbb{Z}_2)^n$, and $s \colon G_0 \to (\mathbb{Z}_2)^n$. Also, the Classification Theorem of §2.3 provides a reduction to the distinct cases. In the following, the weight of $f \in (\mathbb{Z}_2)^n$, $f = (f_1, \ldots, f_n)$ will refer to the sum $f_1 + \cdots + f_n$, where each $f_j$ is regarded as being given by an integer, $f_j = 0$ or 1, $j = 1, \ldots, n$.

3.1.1. The following Theorem will be referred to as the “constant weight criterion” for degeneracy.

**Theorem.** Suppose the CM-field $K$ has an imaginary quadratic subfield, and let $G_0 \cong \text{Gal}(K_0^{c}/\mathbb{Q})$ be given by $G_0 \subset S_n$. Then $G \cong \text{Gal}(K^{c}/\mathbb{Q})$ has the trivial $\rho$-structure with $v = 1$ on $\langle \rho \rangle \times G_0$. Let $\Phi = \Phi^f$, $f \in (\mathbb{Z}_2)^n$, be a CM-type on $K$ and let $r$ be
the rank of the $\mathbb{Z}$-span of the orbit $G_0*(f)$, regarded as a subset of $\mathbb{Z}^n$. Then $\tau(\Phi) = r + 1$, unless the weight of $f$ is $n/2$, in which case $\tau(\Phi) = r$ may also occur.

**Proof.** Let $D$ be an imaginary quadratic subfield of $K$. Then $K^c$ is the composite $K^c = DK^c_0$, so that $[K^c : K^c_0] = 2$, i.e., $v = 1$. But then $K$ has two types having $D$ as a reflex field of degree $2 = 2^v$, so that $K$ determines the trivial $p$-structure by the corollary of the Reflex Degree Theorem and the fact that $B^1(G_0, -)$ gives $p$-equivalences (cf. the Classification Theorem). The $p$-structure is then given by $s(\sigma)$ identically $0$, so that the $G$-orbit of $f$ is $G_0*(f) \cup G_0*(pf)$.

Let $v_1, \ldots, v_r \in G_0*(f)$ span $G_0*(f) \subset \mathbb{Z}^n$, still identifying the elements of $\mathbb{Z}_2$ with $0, 1 \in \mathbb{Z}$. Observe that $\tau(\Phi)$ is the rank of the $\mathbb{Z}$-module spanned by $W = \langle (v, pv) \in \mathbb{Z}^{2\cdot n} : v \in G_0*(f) \subset \mathbb{Z}^n \rangle$, where $pv$ denotes the multiplication in $(\mathbb{Z}_2)^n$, the result regarded as an element of $\mathbb{Z}^n$. Next, note that the weight $w = \text{weight}(v)$ is constant for $v \in G_0*(f)$, and, in particular, weight $(v) = w$, for $j = 1, \ldots, r$. The assertion of the Theorem will follow from the lemma below, which will be used to show that $(v_1, p v_1), \ldots, (v_r, p v_r), (\rho, \rho)$ is a spanning set for $W$.

**Lemma.** Let $v_1, \ldots, v_r \in (\mathbb{Z}_2)^n$ have constant weight $w$. Suppose every entry of $w \in \mathbb{Z}^n$ is a $0$ or a $1$, and that $\text{weight}(w) = w$. Then $w = \sum n_j v_j$ implies $\rho w = \sum n_j (\rho v_j)$.

**Proof.** Consider the $k$th entry, $w_k$, in $w$. Then $w_k = \sum n_j v_{jk}$, for $v_{jk}$ the $k$th entry of $v_j$. But observe that the $k$th entry, $\rho v_{jk}$, of $\rho v_j$ is defined by $v_{jk} + \rho v_{jk} = 1$, with $v_{jk}, \rho v_{jk} \in \{0, 1\}$. Then

$$w = \text{weight}(w) = \sum n_j \text{weight}(v_j) = w \left( \sum n_j \right)$$

$$= w \left( \sum n_j (v_{jk} + \rho v_{jk}) \right) = w \left( w_k + \left( \sum n_j \rho v_{jk} \right) \right),$$

so the $k$th entry $\sum n_j \rho v_{jk}$ and $w_k$ satisfy the same defining condition.

Returning to the proof of the Theorem, the lemma gives that $\langle (v, pv) : v \in G_0*(f) \rangle$ is contained in the $\mathbb{Z}$-span of the $(v_j, \rho v_j)$, while $(\rho v, v) = (\rho, \rho) - (v, pv)$ accounts for $G_0*(\rho f)$. Finally, the rank of $\Phi = \Phi^f$ can be $r$ if and only if $(\rho, \rho)$ belongs to the $\mathbb{Z}$-span of the $(v_j, \rho v_j)$, in which case weight$(\rho v_j) = n - w$ gives that $(\sum n_j) w = (\sum n_j)(n - w)$, so $2w = n$.

3.1.2. The following Theorem, which suffices for the present applications, will be referred to as the “minimal weight criterion” for nondegeneracy.

**Theorem.** Let $G \subset (\mathbb{Z}_2)^n \times G_0 \subset \text{Im}(n, 2)$ be an imprimitive permutation representation of $\text{Gal}(K^c/\mathbb{Q})$, with $[K : \mathbb{Q}] = 2n$, and let the $G$-orbit of the type $\Phi = \Phi^f$ be given by $G_0*(f) = \langle w_1, \ldots, w_n, \rho w_1, \ldots, \rho w_n \rangle$. Then $(K, \Phi)$ is nondegenerate provided there are indices $i_1, \ldots, i_n$ so that when $v_j \in (w_i, \rho w_i)$, for $j = 1, \ldots, n$, is selected to be of minimal weight, the collection $v_1, \ldots, v_n$ is linearly independent (in $\mathbb{Q}^n$) and for at least one index $j_0$, weight$(v_{j_0}) < n/2$.

**Proof.** The weight condition assures that there is no nonzero relation $\sum m_j (v_j, \rho v_j) + m_{n+1}(\rho, \rho) = 0$, since weight$(v_j) \leq n/2$, weight$(v_{j_0}) < n/2$, gives

$$\sum m_j \text{weight}(v_j) < \sum m_j \text{weight}(\rho v_j).$$
Remark. When \( \mathbf{0} = (0, \ldots, 0) \in (\mathbb{Z}_2)^n \) belongs to the orbit \( G_\mathbf{0}(f) \), \( v_j \) of maximal weight may be preferred. As only a single \( G \)-orbit is affected, the choice of \( v_j \) of minimal weight is suggested by the natural determinate calculations in low degrees. Note that \( n' > n \) is necessary, as observed above in §3.1.0, and that in the applications \( n' = n \), in which case the \( \binom{n}{n'} \) possible choices of indices may be avoided.

3.2.1. Theorem (A Converse of Ribet's Theorem [15]). Let \( n > 4 \) be composite and factor \( n \) as \( n = kl \), with \( k > 2 \), \( l \geq 2 \). Then there exist simple degenerate Abelian varieties of dimension \( n \) and rank \( n - l + 2 \).

Proof. Observe that there exist cyclic totally real fields for every \( n \), so there exist CM-fields \( K \) with \( K/\mathbb{Q} \) Abelian and \( \text{Gal}(K/\mathbb{Q}) \cong \langle \rho \rangle \times \mathbb{Z}_n = G \). Normalize the \( \rho \)-structure so that \( G_0 = \mathbb{Z}_n \) is given by \( G_0 = \langle \sigma \rangle \), \( \sigma = (1 \ 2 \ \cdots \ n) \), and consider the type defined by \( f = ((1, \ldots, 1), 0, \ldots, 0) \), written in \( k \) blocks, each with \( l \) entries. Let \( M \) be the \( n \times n \) matrix with rows given by successive cyclic shifts under \( \sigma \), to obtain the successive images of \( f \) under \( g = (0, \sigma^{-1}) \in G \). The first \((k - 1)l + 1 = n - l + 1 \) rows of \( M \) are linearly independent, while the last \( l \) rows may be written in \( l \times l \) blocks as \((I_1, 0, \ldots, 0, I_2)\), with

\[
I_1 = \begin{pmatrix}
0 & 0 & \ldots & 0 & 0 \\
1 & 0 & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
1 & 1 & \ldots & 1 & 0
\end{pmatrix},
\]

and

\[
I_2 = \begin{pmatrix}
1 & 1 & \ldots & 1 \\
0 & 1 & \ldots & 1 \\
\vdots & \vdots & \ddots & \vdots \\
0 & \ldots & 0 & 1
\end{pmatrix}.
\]

Subtract the first row of \( M \) from the last \( l - 1 \) rows and then add the \( j \)th row to the \(((k - 1)l + j)\)th, for \( j = 2, \ldots, l \) to obtain the last rows \((0, I_1, 0, \ldots, 0, I_2)\). Repeating the procedure with the next \( l \) rows will shift \( I_1 \) again, until the rows \((0, \ldots, 0, I_1 + I_2)\) are obtained. Then \( r = (k - 1)l + 1 \) in the constant weight criterion, so \( \text{rank}(K, \Phi^I) = n - l + 2 \), with \( \Phi^I \) the type defined by \( f \). Finally, note that \( \Phi \) is primitive since the orbit of \( f \) under \( G \) has order \( 2n \), with \( K/\mathbb{Q} \) Abelian.

3.2.2. Existence of simple Abelian varieties of smaller rank, in special dimensions, is provided by the following:

Theorem. Suppose the prime ideal \((2)\) decomposes in the cyclotomic field \( \mathbb{Q}((\zeta_p^p)) \), \( p \) a prime, into \( g > 1 \) factors of degree \( f \), and note that \( p \equiv \pm 1 \pmod{8} \) is sufficient but not necessary to insure \( g > 1 \). Then there exist Abelian varieties with complex multiplication having dimension \( 2^{l/p} \), \( l = 0, 1, \ldots, g - 1 \), and rank \( p + 1 \). In particular, for \( l > 0 \), these Abelian varieties are simple, degenerate, and in fact are of CM-type \((K, \Phi)\), with \( \Phi \) primitive, but with reflex field \( K' \), of degree \( 2p \), a proper subfield of \( K \).
Proof. First observe that the condition \( p \equiv \pm 1 \pmod{8} \) is necessary and sufficient for (2) to decompose in the quadratic subfield of \( \mathbb{Q}(\xi_p) \), so \( g > 1 \). Note the case \( p = 43 \), where \( f = 14 \). Next observe that there exist cyclic totally real fields of degree \( p \), e.g., as subfields of \( \mathbb{Q}(\xi_q) \), for \( q \) an auxiliary prime with \( p/(q - 1) \). Therefore by Shimura \([18, \S 1]\), there exist CM-fields with Galois groups \((\mathbb{Z}_2)^p \times_\pi \mathbb{Z}_p \).

Viewing the decomposition of (2) in \( \mathbb{Q}(\xi_p) \) as corresponding to a factorization of \((x^p - 1)/(x - 1)\) into \( g \) irreducible polynomials of degree \( f \) (mod 2), use the coefficients of these irreducible polynomials to construct irreducible representations \( V_j \) of \( \mathbb{Z}_p \) with \( \dim_{\mathbb{F}_2}(V_j) = f \), and \( V_j \subset \mathbb{F}_2[\mathbb{Z}_p] \), \( \mathbb{F}_2 \) being the field with two elements and \( \mathbb{F}_2[\mathbb{Z}_p] \) being the regular representation. The corresponding decomposition of \((\mathbb{Z}_2)^p\) is then \((\mathbb{Z}_2)^p = \langle p \rangle \oplus V_1 \oplus \cdots \oplus V_g\), with \( V_j \equiv (\mathbb{Z}_2)^f \). Note that \( V_j \) and each sum \( V_{j_1} \oplus \cdots \oplus V_{j_k} \) is normal in \((\mathbb{Z}_2)^p \times_\pi \mathbb{Z}_p\), and, since no such subgroup contains \( p \), will fix a Galois CM-subfield of the CM-field with group \((\mathbb{Z}_2)^p \times_\pi \mathbb{Z}_p \).

The fixed field \( K \) then has group

\[
(\mathbb{Z}_2)^p \times_\pi \mathbb{Z}_p / (\mathbb{Z}_2)^{f(g - 1)} \cong (\mathbb{Z}_2)^{f/g + 1} \times_\pi \mathbb{Z}_p,
\]

with \((\mathbb{Z}_2)^{f/g + 1}\) being identifiable with the complementary summands of \( V_{j_1} \oplus \cdots \oplus V_{j_k} \) in \((\mathbb{Z}_2)^p\). Next take \( H' = \text{Ker}(1^{(f!)}(\mathbb{Z}_2)^{f/g + 1}) \) and note that \( p \not\in H' \) so \( H' \) fixes a CM-field \( K' \) of degree \( (G : H') = (2^{f+1}p)/2^f = 2\rho \), \( G \) being the group \((\mathbb{Z}_2)^{f+1} \times_\pi \mathbb{Z}_p\). The properties asserted above will be shown to hold for this choice of \( K \) and \( K' \).

Now observe that \( K' \) has a single class of types, which maybe represented by a type written as \( \Phi^0 \), with an orbit of order \( 2^{f+1} < 2\rho \), and that all other types have orbits of order \( 2^{f+1}p \), so have reflex field \((K')' = K\), the Galois closure of \( K' \). In fact, let such a type be given as \( \Phi^f, (G, H', \rho) \) having structure by \( s(\sigma) = 0 \), for all \( \sigma \in \mathbb{Z}_p \). Then \( \mathbb{Z}_p \) fixes \( f \in (\mathbb{Z}_2)^p \pmod{(\mathbb{Z}_2)^{f+1}} \), \( v = f + 1 \), if and only if \( f \in (\mathbb{Z}_2)^v \), so \([K' : \mathbb{Q}] = 2^v(\mathbb{Z}_p : (1)) = 2^{f+1}p \). Since \( K' \) has no CM-subfields, \( K' \) will be the reflex field of \((K, (\Phi^f))\), for such an \( f \), \( f \in (\mathbb{Z}_2)^v \), so the notation \( K' \) is not misleading, and the primity of the type on \( K \), with corresponding simplicity of Abelian varieties of type \((K, (\Phi^f))\), is assured, since the reflex type is always primitive. Finally, observe that rank \( r((\Phi^f)) = r(\mathbb{F}_2) \leq p + 1 \), with the exact value \( p + 1 \) being the result of Ribet’s Theorem in \([15]\).

Remark 1. The lowest-dimensional cases have dimension 56, from \( n' = 7 \), \( v = 4 \), and \( 2^5 \cdot 31 = 992 \), from \( n' = 31 \), \( v = 6 \). The method described for obtaining \( V_j \subset (\mathbb{Z}_2)^p \) is standard in algebraic coding theory, and a proof for the assertions required in the above proof may be found in \([9, p. 277]\), a reference kindly supplied by E. F. Assmus, Jr. Professor Assmus also emphasized that the cases \( p = 7 \), \( v = 4 \), and \( p = 23 \), \( v = 12 \) are extremely exceptional among the cases \( p \equiv \pm 1 \pmod{8} \), \( v = (p + 1)/2 \), where \((\mathbb{Z}_2)^v \subset (\mathbb{Z}_2)^p \) is one of the two choices given as quadratic reciprocity codes. The automorphism groups of these linear codes, which correspond to a maximal \( G_0 \) in the present terminology, are \( \mathbb{Z}_p \times_\pi \mathbb{Z}_{(p - 1)/2} \) except in the above two cases, \( p = 23 \) admitting the Mathiew group \( M_{23} \). As a consequence, the other codes for this \( v \) presumably having smaller automorphism groups, CM-fields of degree \( 2p \) having reflex fields \( K' \) of degree \( 2n' \) in the range \( 2^{(p + 1)/2}p(p - 1)/2 < 2n' < 2^p \) may be expected to give Abelian varieties with interesting properties.
Remark 2. The first example of $G$ with a type for which $K$ could have a reflex field with $K \subseteq K'$ was obtained by Shimura in [20] for $G = D_{14}$. Such types predominate for $D_{2n}$, $n$ odd, as will follow from the formula of the proposition of §4.1. Other examples provided by the present investigation include a case with $n = 4$ and $|G| = 16$ (minimal), and examples with $n = 7$, $\nu = 4$, the cases with $G_0 = \mathbb{Z}_7 \times \mathbb{Z}_3$ and $\text{PSL}(2, 7)$ having $K \subseteq K' \subseteq K^c$.

Remark 3. Yoshida has brought to the author’s attention an elementary proof that there exist totally real fields with group $S_n$ for every $n$. The existence of simple degenerate Abelian varieties in the dimensions

$$\frac{1}{2} \binom{n}{n/2} \quad \text{and} \quad \binom{n}{k}, \quad k = \frac{n}{2},$$

with $\frac{k}{2} \leq n + 1$ follows from Yoshida’s comment and the present methods.

3.3.1. While the $K/\mathbb{Q}$ Abelian case avoids existence problems, the special properties that result from the existence of various non-Abelian groups as the Galois groups of totally real fields may be formulated as the following:

Theorem. (A) Suppose there exists a totally real field $K_0$ with Galois group $\text{Gal}(K_0/\mathbb{Q}) = \mathbb{Z}_k \ltimes \mathbb{Z}_l$, $k > 2$, $l \neq 1$, the wreath product. Then there exist simple degenerate Abelian varieties with complex multiplication by a non-Galois CM-field such that the varieties have dimension $n = kl$ and rank $n - l + 2$.

(B) Under the same hypothesis, except that $k = 2$ is allowed, there exist simple Abelian varieties with dimension $n' = k_1l$ having rank $\leq k_1l + 1$.

(C) Further, in the even case, the existence of totally real fields with Galois groups $[(\mathbb{Z}_2)^m] \times \mathbb{Z}_m$ ($m \geq 3$) and $D_m$ for $m$ odd ($m > 5$) supplies simple Abelian varieties of CM-type $(K, \Phi)$, and reflex field $K'$, with dimension $n = 4m$, and with dimension $n = 2m$ ($m$ odd, $m > 5$), respectively, in each case with $K' \subset K$, $[K : K'] = 2$, so that $\text{rank}(\Phi) \leq \frac{1}{2}n + 1$.

Proof. (A) Write

$$\mathbb{Z}_k \ltimes \mathbb{Z}_l = \langle \sigma_1, \sigma_2, \ldots, \sigma_l, \sigma_{l+1} \rangle,$$

with

$$\sigma_1 = (12 \cdots k), \quad \sigma_2 = (k + 1 \cdots 2k), \ldots, \quad \sigma_l = (k(l - 1) + 1 \cdots kl),$$

and

$$\sigma_{l+1} = (1k + 1 \cdots k(l - 1) + 1)(2 \cdots ) \cdots (k \cdots kl).$$

Then take $K_0$ to be the subfield fixed by $H_0 = \langle \sigma_2, \ldots, \sigma_l \rangle$. Note that a transitive degree $n = kl$ structure, $G_0 = \mathbb{Z}_k \ltimes \mathbb{Z}_l \subset \text{Im}(l, k)$, has been given, with $H_0 = \text{Stab}_{G_0}(1)$. Take $K$ to be the composite of $K_0$ with an imaginary quadratic field, and then observe that $K^c/\mathbb{Q}$ has group $G = \mathbb{Z}_2 \times G_0$, with $K$ determining the $\rho$-structure that may be given by $s(\sigma) = 0$ for all $\sigma \in G_0$. Taking any $\tau_j$ with $\tau_j(1) = j$, let $\Phi^f$ be the CM-type with $f = ((1, 0, \ldots, 0)_k, \ldots, (1, 0, \ldots, 0)_k)$, with $f$ being written in $l$ blocks, $(1, 0, \ldots, 0)_k$ having $k$ entries, with $\sigma_r = 1, \ldots, l$, transitive on the $r$th block. Then since $\sigma_1, \ldots, \sigma_l$ act independently and $\sigma_{l+1}$ stabilizes, $f$ has a $G$-orbit of order $2k^l$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
To check that \((K, \Phi')\) is primitive, and establish that the Abelian varieties of type \((K, \Phi')\) are simple, apply the method of Shimura and Taniyama \[23, \text{Proposition 26}\]. Observe that explicit coset representatives \(T_j\) can be given as \(\sigma_1^{u_1}, \ldots, \sigma_{l-1}^{u_{l-1}}\), taking \(l = uk + 1 + w\). Then write \(S = \bigcup_{j=1}^{n} H \rho^j T_j\), with the notation there. Since \(k > 2\), observe that \((\rho, \sigma) \not\in H_1 = \{g \in G/gS = S\}\), the number of elements with first entry \(\rho\) being changed. Next observe that \(\sigma_1^{u_1} \cdots \sigma_{l-1}^{u_{l-1}} \in H_1\) implies \(a_1 = 0\), and, finally, that \(\sigma_1^{u_1} \cdots \sigma_k^{u_k} \in H_1\) implies \(f_{k+1} = \cdots = f_{2k}\), which is also false for the present \(f\).

To determine the rank, use the constant weight criterion and observe that \(f\) and the elements \(((\sigma_a^b)^f f, a = 1, \ldots, l; b = 1, \ldots, (k - 1))\), supply \(1 + l(k - 1)\) independent elements of \(G_{0*}(f)\) that span \(G_{0*}(f)\). Then

\[
\text{rank } t(\Phi') = 1 + l(k - 1) + 1 = lk - l + 2 = n - l + 2 < n + 1,
\]
as asserted.

(\(B\)) With the same subgroups as above, consider the type with \(f = ((10 \cdots 0)_k, (10 \cdots 0)_k, \ldots, (10 \cdots 0)_k)\). Then \(\sigma_3, \ldots, \sigma_l\) stabilize this type, and no element of the form \(\sigma_1^{u_1} \cdots \sigma_{l-1}^{u_{l-1}}\), with any one of \(a_1, a_2, \text{ or } a_{l+1}\) nonzero, can fix this type, so an orbit of order \(k^2l\) is obtained. Then the reflex type of this type may be fixed to construct Abelian varieties with the required properties.

(\(C\)) The case of \(D_{2n}, n\) odd, is deferred until §4.1. For \(G_0 = [(\mathbb{Z}_2)^m]^{\times}, \mathbb{Z}_m\), take \(H_0 = \text{Ker}(1^{st}|_{[(\mathbb{Z}_2)^m]})\). \(G = \mathbb{Z}_2 \times G_0\) and \(H = 0 \times H_0\), \(G\) corresponding to the composite with an imaginary quadratic field. Then \((G : H \times \langle \rho \rangle) = 2m\). Using \(G_0 = ((1m+1)(2m+2), \ldots, (m - 12m - 1)(m2m)) = \langle \sigma_1, \ldots, \sigma_m \rangle\), and \(s(\sigma)\) identically zero, let \(\Phi'\) be given by \(f = (110 \cdots 0)\). Then \(H'(\Phi') = \langle (0, \sigma_3), \ldots, (0, \sigma_{m-1}) \rangle\) with \(H' \subset H\). \((G : H') = 2\), so we take \(K\) to be the fixed field of \(H'\).

Remarks. In case (\(C\)) observe that \(m = 3\) gives \(G_0 = A_4\) in degree \(2m = 6\), so the degenerate reflex type gives an Abelian variety of dimension \(4m = 12\) with rank 7, which exists by the theorem of §2.2.1. Under the hypothesis on the existence of the totally real fields, (\(B\)) combined with (\(C\)) gives the existence of pairs \((K, \Phi), (K', \Phi')\) with \([K' : \mathbb{Q}] > [K : \mathbb{Q}]\), except when \([K : \mathbb{Q}] = 2n'\) with \(n'\) odd and square free. Note the exceptional case \(n' = 6\), which is even, but does not allow this strong form of degeneracy. Likewise, case (\(B\)) and the proof of case (\(A\)) give much smaller ranks than those obtained in the Abelian case of §3.2.1 for dimensions divisible by a large square, or of the form \(k^4\).

3.3.2. As a final result on degeneracy, the results of §5.2 clarify the number of cases involved and provide a method of proof for a result stated without proof in Ribet’s paper \[14\]. One formulation of the result is the following:

**Theorem.** Let \(A\) be a simple Abelian variety of CM-type \((K, \Phi), \text{ with } \dim_{\mathbb{C}}(A) = 4\). Then \(A\) is degenerate if and only if \(\text{Gal}(K^c/\mathbb{Q}) \cong \mathbb{Z}_2 \times A_4, \text{ or } \mathbb{Z}_2 \times S_4\) and \((K, \Phi)\) is the reflex of a type on a CM-field of degree 6.
Proof. The essential observation will be made in the proposition of §5.2.2, where the cocycle analysis establishes that there are only six orbits in question, the case \([\mathbb{Z}_2)^4 - \langle \rho \rangle\) being the degenerate type known to occur. The minimal weight criterion establishes nondegeneracy for the other five cases.

4. A relative class number formula.

4.0. For cases of the form \(G = (\mathbb{Z}_2)^v \times \mathbb{Z}_p\), as in the theorem of §3.2.2, the general partition formula for the degrees of the reflex fields,

\[
2^p = 2^v + (2^p - 1) \left( \sum_c 1 \right),
\]

where \(\sum_c\), the sum of \(c = (1/p)(2^p - 1)\) ones, has been established in the proof. Other cases with \(K \subseteq K'\) have been remarked upon, but the dihedral group \(G = D_{2n}, n\) odd, and \(\langle \rho \rangle \times S_n\) are the cases for which a general partition formula has been obtained. More information is available for the case \(G = D_{2n}, n\) odd, where the elementary character theory of \(G\) may be used to give explicit relations among certain characters \(\chi_{K'/K_0}\) and \(\chi_{K/K_0}\), where \(K'\) is a reflex field of \(K\) and \(K_0 = (K')^{(\rho)}\). The previously obtained example of Shimura is of the form \(\chi_{K/K_0} = \chi_{K'/K_0}\) and gives the relative class number relation of Proposition A.7 in [20, p. 84].

4.1. In the case of \(G = D_{2n}, n\) odd, \(G\) determines a unique \(\rho\)-structure \((G, H, \rho)\) with \((G : H) = 2n\) \((D_{2n}\) of order \(4n\)). Giving \(G\) the usual split structure \(s(\sigma) = 0\) for all \(\sigma \in G_0 = D_n\), the partition is given by the following:

Proposition. For \(G = D_{2n}, n\) odd, the partition giving the degrees of the reflex fields is given as

\[
2^n = 2 + \sum \left( 2ls_{l,1} + 4ls_{l,2} \right),
\]

where \(s_{l,1}, s_{l,2}\) are summations of \(s_{l,1}\) and \(s_{l,2}\) ones, with \(s_{l,1}\) defined recursively by

\[
s_{l,1} = 2^{(l-1)/2} - \sum_{l'/l} s_{l'/1},
\]

and \(s_{l,2}\) defined recursively as

\[
s_{l,2} = \frac{1}{4l} \left[ 2l' - 2 - \sum_{l'/l} \left( 2l's_{l'/1} + 4l's_{l'/2} \right) - 2ls_{l,1} \right],
\]

both summations being over divisors \(l' < l\). For the particular case of primes,

\[
s_{p,1} = 2^{(p-1)/2} - 1 \quad \text{and} \quad s_{p,2} = (1/4p) \left[ 2p - 2 - p(2^{(p+1)/2} - 2) \right].
\]

\(s_{l,1} \neq 0\) for all \(l\), and \(s_{l,2} \neq 0\), except for \(l = 3, 5\).

Proof. The term 2 corresponds to the type \(\Phi^0\). For \(l < n\), the term \(2ls_{l,1}\) counts the types \(\Phi^f\) for which \(f \in (\mathbb{Z}_2)^n\) is fixed by \(D_{n/l} \subset D_n\) but no larger subgroup, and the term \(4ls_{l,2}\) counts \(f\) fixed by \(\mathbb{Z}_{n/l}\) but no larger subgroup. The factors \(2l\) and \(4l\) give the orbit of such types under \(G\). Finally, \(2ns_{n,1}\) counts the types fixed only by a reflection (in \(G_0 = D_n\)), \(2n\) being the order of such orbits, and \(4ns_{n,2}\) counts the types fixed by no element of \(G\).
The cases \( n = 3, 5, 7, 15, \) and 45 give illustrations of the formula and its recursive nature. Note that all of the partition terms \( s_{n,2} \) correspond to types for which the reflex fields \( K' \) of \( K \) have \( K \subseteq K' = K^c \), the existence of such types supplying the remaining portion of the proof of part (C) of the theorem in §3.3.1. The case \( D_{2n}, n \) even, appears to present somewhat contrasting phenomena, which has not yet been fully developed. Note that \( D_{2n} \), like \( D_{2p} \), allows few CM-subfields. The partition \( 64 = 4 + 12 + 12 + 12 + 24 \) from \( n = 6, G = D_{12} \), shows that \( K \subseteq K' = K^c \) can also occur for \( n \) even.

4.2. A concern for the \( \rho \)-structure identifications made by Outer\( (G) \) will be supported by the introduction of character theory to the description of a more arithmetic structure. The relative class numbers below retain geometric significance, as is established, for example, in Shimura [17] (cf. also Weil’s review in Math. Reviews), [20], via the field of moduli.

**Definition.** Let \((G, H, \rho)\) be an element of a \( \rho \)-structure, possibly having kernel. Then \( \chi_{H \times \langle \rho \rangle} / H \) denotes the character of \( G \) induced from the character of \( H \times \langle \rho \rangle \) trivial on \( H \), but nontrivial on \( H \times \langle \rho \rangle \). The notation \( \chi_{K/K_0} \) will be used when the case \( G \cong \text{Gal}(K^c/Q) \), with \( H \) corresponding to \( \text{Gal}(K^c/K) \) and \( \rho \) to complex conjugation, is intended.

**Proposition.** Suppose \( G = D_{2n}, n \) odd, occurs for a CM-field \( L = K^c, [L : K] = 2 \). Let \( K^1 \) be a CM-subfield of \( L, [L : K^1] = 2, \) nonconjugate to \( K \) over \( Q \), and let \( L_0, K_0, K_0^1 \) denote the maximal totally real subfields. Then the character relation

\[
\chi_{L/L_0} = \chi_{K/K_0} + \chi_{K^1/K_0^1}
\]

holds.

**Proof.** Observe that \( \chi_{L/L_0} \) may be decomposed into irreducible characters, with the decomposition written in the notation of Serre [16] as

\[
\chi_{L/L_0} = \bigoplus_{h \text{ odd}} 2\chi^h \oplus \psi_3 \oplus \psi_4,
\]

the last two being characters of degree 1, the others of degree 2. The above relation then follows from the decompositions of \( \chi_{K/K_0} \) and \( \chi_{K^1/K_0^1} \), one giving \( \bigoplus_{h \text{ odd}} \chi^h \oplus \psi_3, \) the other \( \bigoplus_{h \text{ odd}} \chi^h \oplus \psi_4. \)

Note that which character has which decomposition will depend upon which Outer\( (G) \) class is represented by \( (G, H, \rho) \) in the \( \rho \)-structure defined by \( (G, H, \rho) \).

For an algebraic number field \( F \), let \( h_F \) be the class number of \( F \), \( d_F \) its discriminate, and \( E_F \) the group of units. Then applying the method of Shimura [20] provides the following:

**Theorem.** Suppose \( L/Q \) is a CM-field, \( \text{Gal}(L/Q) = D_{2n}, n \) odd, and let \( K, K^1, L_0, K_0, K_0^1 \) be as in the above proposition. Then the following relations hold.

(i) \( d_{L}/d_{L_0} = (d_{K}/d_{K_0})(d_{K^1}/d_{K_0^1}) \) and

(ii) \( 2[E_L \cdot E_{L_0}]^{-1}h_L/h_{L_0} = [E_K \cdot E_{K_0}]^{-1}h_K/h_{K_0}[E_{K^1} \cdot E_{K_0^1}]^{-1}h_{K^1}/h_{K_0^1}. \)

**Proof.** By the formula of Hecke [7], \( E/E_0 \) Abelian and quadratic gives \( \xi_E(s) = \zeta_{E_0}(s)L(s, \chi_0) \), \( \zeta \) being the Dedekind Zeta function and \( L(s, \chi_0) \) being the \( L \)-function for the character of the extension \( E/E_0 \). Apply the formula for the residue of
the Zeta function. Then the discriminant terms are isolated, and the regulator terms are absorbed as in Shimura [20, p. 84]. But the $L$-function terms are equal by standard properties of the Artin $L$-series and the above proposition.

5. Examples for $n < 8$. 

5.0. In this section $\rho$-structures are not allowed to have kernels. In §5.1 all cases for the values $n = 3, 5, \text{ and } 7$ will be obtained with some general properties of $n$ odd, and $n = p, p$ a prime, included. All of the $\rho$-structures for these values are split, with $n = 7$ giving two cases having nontrivial structure. The case $n = 4$ is treated in 5.2, with many nonsplit cases obtained. Preliminary results for $n = 6$, especially the examples generalized in §3, are presented in 5.3.

For all of the $\rho$-structures with $n = 3, 4, 5$ and 7, the $G$-orbit structure of the collection of types is given. Recall from §1 that the $G$-orbit structure is a partition of the set of types, i.e., of $\{f | f \in (\mathbb{Z}_2)^n\}$. Pick $\Phi_j, j = 1, \ldots, l$, to represent each $G$-orbit. Then, in the CM-field case, a numerical partition $2^n = \sum_{j=1}^{l} [J_j : \mathbb{Q}]$ results, $J_j$ being the reflex field of $(K, \Phi_j)$. Every other reflex type of $K$ is then given as $(J_j, \Phi_j)^g = (J_j^g, (\Phi_j)^g)$, for $g \in \text{Gal}(K^c/\mathbb{Q})$, so that the $(J_j, \Phi_j), j = 1, \ldots, l$, represent all of the reflex types of $K$. The partition $2^n = \sum_{j=1}^{l} (G : H'(\Phi_j))$ is then given for each $\rho$-structure.

5.1.1. First observe that when $G$ has a $\rho$-structure with $n$ odd the classifications of $\rho$-structures and permutation structures coincide. The result is the following:

**Proposition.** Suppose $G$ has a central order two element $\rho$. Then for a permutation structure $(G, H)$ to support distinct $\rho$-structures, every permutation structure $(G, H_x)$, $G$ effective on $H_x \setminus G$, for which $(G : H_x) = 2n_1$, must have $n_1$ even. Further, $(G, H_1, \rho)$ must have $\text{Proj}_{\text{Sets}}(G)$ with a central order two element.

**Proof.** For $(G, H)$ to support distinct $\rho$-structures, $G$ must have at least two central order two elements, else $\rho$ is characteristic, and $\text{Aut}(G, \rho) = \text{Aut}(G)$. Consider the imprimitivity sequence $0 \to (\mathbb{Z}_2)^{v_1} \to G \to G_0' \to 1$ for $(G, H_1, \rho)$. Since $G_0'$ is transitive, $\rho$ is the unique central order two element of $G$ in $(\mathbb{Z}_2)^{v_1}$, so a second central order two element, $\rho_1$, would be of the form $\rho_1 = (e', \sigma')$, $\sigma' \neq (1)$. But then $\rho_1$ of order two implies $\sigma'$ of order two, and $\rho_1$ central in $G$ implies $\sigma'$ central in $G_0'$. Finally, since $H_1$ is without normal subgroups of $G$, $\rho_1 \not\in H_1$, and $G$ has the subgroup lattice $G \supset H_1 \times \langle \rho \rangle \times \langle \rho_1 \rangle \supset H_1 \times \langle \rho \rangle \supset H_1$, with $2 = (H_1 \times \langle \rho \rangle \times \langle \rho_1 \rangle : H_1 \times \langle \rho_1 \rangle)$, so $2/n_1$, for $n_1 = (G : H_1 \times \langle \rho \rangle)$.

The $\rho$-structures for the values $n = 3, 5$ and 7 will then be obtained by determining which of the permutation structures of degree $2n = 6, 10$ and 14 have abstract groups containing a central order two element. The analysis is further simplified by the fact that $n = p$, $p$ a prime, strongly restricts the values of $v$, and therefore of $|G| = 2^v |G_0|$. In fact, observe the following:

**Proposition.** Let $n = p$ be an odd prime. Then for any $G_0$ of degree $p$, and any imprimitivity sequence $0 \to (\mathbb{Z}_2)^v \to G \to G_0 \to 1$ for a $\rho$-structure $(G, H, \rho)$ ($\rho \in (\mathbb{Z}_2)^v$), the divisibility condition $p/2^{v-1} - 1$ holds.
Proof. \(G_0\) must contain a \(p\)-cycle \(\sigma\), so \((\mathbb{Z}_2)^v\) may be decomposed into \(\mathbb{Z}_p\)-orbits for \(\mathbb{Z}_p = \langle \sigma \rangle\). Since \(p\) is odd, \(\rho\) gives a pairing of these orbits, so

\[
(\mathbb{Z}_2)^v = \{0 \cup \rho\} \cup \{O_1 \cup \rho O_1\} \cup \cdots \cup \{O_s \cup \rho O_s\},
\]

with each \(O_j\) of order \(p\).

Thus for \(p = 3\) and \(5\), \(v = 1\) or \(p\); while for \(p = 7\), \(v = 1, 4\) or 7. The general case of \(p \equiv \pm 1 \mod 8\) allows \((\mathbb{Z}_2)^v\) with \(1 < v < p\) by quadratic reciprocity and the construction in §3. Recall that \(p = 43 \equiv 3 \mod 8\), but \(v = 15\) occurs.

5.1.2. Now recall the transitive \(G_0\) for \(n = 3, 5\) and 7. For \(n = 3\), there are only \(G_0 = \mathbb{Z}_3\) and \(S_3\); for \(n = 5\), \(G_0 = \mathbb{Z}_5, D_5, \mathbb{Z}_5 \times \mathbb{Z}_4, A_5\) and \(S_5\); and, for \(n = 7\), \(G_0 = \mathbb{Z}_7, D_7, \mathbb{Z}_7 \times \mathbb{Z}_3, \mathbb{Z}_7 \times \mathbb{Z}_6,\) PSL(2,7), \(A_7\) and \(S_7\). The \(\rho\)-structures for these values are then described by the following:

Theorem. For \(n = 3, 5\) and 7 there are a total of 33 \(\rho\)-structures. Of these, 28 are the split structures \(\mathbb{Z}_2 \times G_0\) and \((\mathbb{Z}_2)^n \times G_0\) for the above 14 \(G_0\). Three more are the \(n = 7, v = 4\) split structures \((\mathbb{Z}_2)^4 \times G_0\), for \(G_0 = \mathbb{Z}_7, \mathbb{Z}_7 \times \mathbb{Z}_3,\) and PSL(2,7). All but two of these split groups have unique permutation structure, the two nontrivial split \(\rho\)-structures resulting from distinct permutation structures on \(\mathbb{Z}_2 \times \text{PSL}(2,7)\) and \((\mathbb{Z}_2)^4 \times \text{PSL}(2,7)\).

Proof. See the lists of Miller [10] or Zassenhaus [25] for \(n = 3\) (2\(n = 6\)), the list of Cole [2] for \(n = 5\) (2\(n = 10\)), and the list of Miller [11] for \(n = 7\) (2\(n = 14\)). Note that the corrections to Cole’s list in Miller [11] do not affect the present case.

Only the list for \(n = 7, 2n = 14\) presents any problem. Since \(n = 7\) is odd, observe that the only cases admitting 2 sets of order \(7\) are split and have \(v = 1\). The other cases listed above account for 12 of the 27 permutation groups that admit 7 sets of order 2 but not 2 sets of order 7. The remaining 15 such permutation groups fail to have a central order two element, since they occur as \([((\mathbb{Z}_2)^v)^+ \times G_0]^-\), as \([((\mathbb{Z}_2)^v \times G_0)]^+\), or as \(G_1\) with \((\mathbb{Z}_2)^v \times G_0 = \langle \rho \rangle \times G_1\), the \([\ ]^+\) cases failing to contain \(\rho\) since \(n = 7\) is odd.

5.1.3. Proposition 1. When \(n = 3, v = 1\), the partition \(2^3 = 2 + 6\) holds for both \(G = \mathbb{Z}_2 \times G_0\), and \(2^3 = 8\) holds for both \(G = (\mathbb{Z}_2)^3 \times G_0\). When \(n = 5\) there are two cases with \(v = 1\). For \(G = \mathbb{Z}_2 \times G_0\) with \(G_0 = \mathbb{Z}_5\) or \(D_5\), the partition is \(2^5 = 2 + 10 + 10 + 10 + 10\), while for \(G_0 = \mathbb{Z}_5 \times \mathbb{Z}_4, A_5\), or \(S_5\), \(2^5 = 2 + 10 + 20\). The case \(G = (\mathbb{Z}_2)^5 \times G_0\) gives a single orbit, \(2^5 = 32\).

Proof. Use \(\mathbb{Z}_p \subset G_0\) to give coset representatives \(\tau_i\), and take \(s(\sigma) = 0\) for all \(\sigma \in G_0\). Then the type \(\Phi^0, 0 \in (\mathbb{Z}_2)^v\), accounts for the term 2 when \(v = 1\). The first term of 2\(n\) is then represented by (001) or (00001). For \(n = 5\), the first two \(G_0\) have (11000) and (10100) in distinct orbits, while the other three \(G_0\), being 2-transitive, identify these to give a single orbit. That the case \(v = n\) gives a single orbit has been previously distinguished by Shimura [18, §1].
While the same principles apply to \( n = 7, v = 1, s(\sigma) \) identically 0, there are several more cases. The notation \([ \_ k, n - k \]) is used to denote the preliminary decomposition into orbits having \( f \) with \( k \) or \( n - k \) entries of 1. Also the notation \( \Sigma, 1 \), for the sum of \( r \)'s is used. Then the \( n = 7 \) partitions are given by the following:

**Proposition 2.** For \( n = 7, v = 1, s(\sigma) \) identically 0, the partitions are as follows:

1. \( 2^7 = 2 + 14(\Sigma, 1), \text{for } G_0 = \mathbb{Z}_7; \)
2. \( 2^7 = 2 + 14 + [14(\Sigma, 1)]_{2,5} + [14(\Sigma, 1) + 28]_{3,4}, \text{for } D_7; \)
3. \( 2^7 = 2 + 14 + [42]_{2,5} + [14 + 14 + 42]_{3,4}, \text{for } \mathbb{Z}_7 \times \mathbb{Z}_3 \text{ and } \text{PSL}(2, 7); \)
4. \( 2^7 = 2 + 14 + [42]_{2,5} + [28 + 42]_{3,4}, \text{for } \mathbb{Z}_7 \times \mathbb{Z}_6; \) and
5. \( 2^7 = 2 + 14 + [42]_{2,5} + [70]_{3,4} \text{ for } A_7 \text{ and } S_7. \)

Representatives for the orbits are as given below.

Further, the other cases have the partitions \( 2^7 = 16 + 112 \) for the three split cases with \( v = 4 \) and \( s = 0 \), and the nontrivial split case with \( v = 1 \), and a single orbit, \( 2^7 = 128 \), for the nontrivial split case with \( v = 4 \), in addition to the cases with \( v = 7 \).

**Proof.** For the cases with \( v = 1, s = 0 \) use \( \mathbb{Z}_7 \subset G_0 \) to specify \( \Phi^f \), and obtain the preliminary decomposition

\[
2^7 = 2 + [14]_{1,6} + \left[ 14 \left( \sum_3 1 \right) \right]_{2,5} + \left[ 14 \left( \sum_5 1 \right) \right]_{3,4}.
\]

The case \( G_0 = \mathbb{Z}_7 \) is completed by specifying the representatives

\[
(1100000), \quad (1010000) \quad \text{and} \quad (10001000)
\]

for \([ ]_{2,5} \); and

\[
(0000111), \quad (0001011), \quad (0001101), \quad (0010011), \quad \text{and} \quad (0010101)
\]

for \([ ]_{3,4} \). All other cases except for \( D_7 \) have \( G_0 = \mathbb{Z}_7 \times \mathbb{Z}_3 \) as a subgroup, which identifies the three orbits from \([ ]_{2,5} \) to give the \([42]_{2,5} \) terms. \( G_0 = D_7 \) has an element stabilizing each of the representatives, so the orbits remain distinct.

For \([ ]_{3,4} \), note that the second and third representatives give the exceptional orbits for \( \mathbb{Z}_7 \), and the representatives chosen give the coefficients in the factorization

\[
(x^7 - 1)/(x - 1) = (x^3 + x + 1)(x^3 + x^2 + 1) \pmod{2}.
\]

These exceptional orbits give terms of \( 14 + 14 \) for the \( G_0 \) admitting \( v = 4 \), and 28 for \( G_0 = D_7 \subset G_0 = \mathbb{Z}_7 \times \mathbb{Z}_6 \). Again \( D_7 \) has a reflection fixing the other three representatives, giving distinct orbits, while \( G_0 = \mathbb{Z}_7 \times \mathbb{Z}_3 \subset G_0 \) identifies these. Finally, \( G_0 = A_7 \) and \( S_7 \) are 3-transitive, so that \([ ]_{3,4} \) is a single orbit.

For the cases with \( v = 4 \) and \( s = 0 \), a term of 16 is required by the corollary of the Reflex Degree Theorem and can be represented by \( 0 \). Then \((\mathbb{Z}_2)^4 \times \mathbb{Z}_7 \) is a subgroup of the other two, and \((\mathbb{Z}_2)^4 \) gives identifications of the other orbits for \( \mathbb{Z}_2 \times \mathbb{Z}_7 \), the orbit used to construct \((\mathbb{Z}_2)^4 \) being excepted, and \( \text{odd} = (00000001) \) is a representative in any case. The nontrivial case with \( v = 4 \) and \( G_0 = \text{PSL}(2, 7) \) has a
trivial subgroup with $G_0 = \mathbb{Z}_7$, $v = 4$, but must not allow a term of 16 by the same corollary, so must identify the two $(\mathbb{Z}_2)^4 \times \mathbb{Z}_7$ orbits, giving a single orbit. Finally, the nontrivial structure with $v = 1$ may be written as $G = \mathbb{Z}_2 \times \operatorname{PSL}(2,7)^*$, $\operatorname{PSL}(2,7)^*$ being a “head = 1” subgroup. Explicitly,

$$(00000000), (1234567) \quad \text{and} \quad ((0011101), (12)(47))$$

satisfy Burnside’s relations for $\operatorname{PSL}(2,7)$, and make identifications on the orbits of the trivial $\mathbb{Z}_7 \times \mathbb{Z}_3$ subgroup given by the above 7-cycle and (253)(467).

5.2.1. For $n = 4$, $2n = 8$, several cases allow nonunique central order two elements, in distinct $\operatorname{Aut}(G)$-orbits, so permutation structures are not sufficient. The cocycle method, having been established in general, provides the following:

**THEOREM.** There are 38 $p$-structures for $n = 4$, which may be arranged according to $(G_0, (\mathbb{Z}_2)^v)$, and have partitions as on the table of $n = 4$ results below.

**PROOF.** Observe that for each of the five transitive $G_0$, $v = 1, 3$ and 4 determines $(\mathbb{Z}_2)^v$ uniquely, $v = 1$ giving $\langle \rho \rangle$ and $v = 3$ giving $[(\mathbb{Z}_2)^4]^+$. Neither $G_0 = A_4$, nor $G_0 = S_4$ allow $v = 2$, and recall that the three $G_0$-modules for $G_0 = (\mathbb{Z}_2)^2$ have been found to be equivalent in §2.3.2, where the normalizations for $G_0 = \mathbb{Z}_4$, $G_0 = D_4$ determine $(\mathbb{Z}_2)^v$, $v = 2$, uniquely.

Now compute $H^1(G_0, (\mathbb{Z}_2)^4)$ to get $\langle 0 \rangle$ for $G_0 = (\mathbb{Z}_2)^2$, $\mathbb{Z}_4$ and $A_4$; and $\langle \rho \rangle$ for $G_0 = D_4$ and $S_4$. In the latter case, note that $H^1(G_0, (\mathbb{Z}_2)^v) = \langle \rho \rangle$, so the inclusion $i^1$ is an isomorphism, giving $j^1 = 0$ in all cases. Note that $\operatorname{Outer}(G)$ makes nontrivial identifications if and only if $G_0 = D_4$ or $S_4$, as in the Structures Theorem of §6.

Since $j^1 = 0$ we have $H^1(G_0, (\mathbb{Z}_2)^4)/(\mathbb{Z}_2)^v) \cong Z^1/j^1(Z^1)$, so we compute the group $Z^1/j^1(Z^1)$ of extension classes. For the cases $G_0 = (\mathbb{Z}_2)^2$, $\mathbb{Z}_4$ and $D_4$, pick $s$: $G_0 \rightarrow (\mathbb{Z}_2)^4$ for each class and compute the order structure to see that nonisomorphic groups result from each extension class with $(G_0, (\mathbb{Z}_2)^v)$ held constant, except in the two cases $G_0 = (\mathbb{Z}_2)^2$, $v = 1$ and $v = 3$. The case with $v = 1$ has appeared in §2.3.2, and the case with $v = 3$ gives $|Z^1/j^1(Z^1)| = 4$, with two $N_4(\mathbb{Z}_2)^2 = S_4$ orbits. For $G_0 = A_4$ and $S_4$ note that the groups listed on the following table for $n = 4$ are nonisomorphic and belong to the appropriate cohomology spaces. Since nonisomorphic representatives have been obtained, and equivalence between distinct $(G_0, (\mathbb{Z}_2)^v)$ is not allowed, the number of structures is given by $|Z^1/j^1(Z^1)|$, with the above two exceptions.

The identifications of the abstract 2-groups, while not essential, may be easily obtained by comparing the structure $(\mathbb{Z}_2)^4 \times \mathbb{Z}_3$ $G_0$ with successive index two subgroups, as provided on the lattice diagrams of Hall and Senior [5]. The partition results follow from the methods of §§1 and 2, explicit calculation with $(s(o), o)$ being rarely required. The primitive cases will be described below.

Note that in each case the split structure is given first in the following:
### Table of \( n = 4 \) Results.

<table>
<thead>
<tr>
<th>Structures</th>
<th>Partition giving degrees of reflexes</th>
</tr>
</thead>
<tbody>
<tr>
<td>( G_0 = (\mathbb{Z}_2)^2 )</td>
<td></td>
</tr>
<tr>
<td>( v = 1 )</td>
<td>( (\mathbb{Z}_2)^3 ) 2 + 2 + 2 + 2 + 8</td>
</tr>
<tr>
<td></td>
<td>( (\mathbb{Z}_2) \times \mathbb{Z}_4 (\rho \in \mathbb{Z}_4) ) 4 + 4 + 8</td>
</tr>
<tr>
<td></td>
<td>( D_4 ) 4 + 4 + 4 + 4</td>
</tr>
<tr>
<td></td>
<td>( Q ) 8 + 8</td>
</tr>
<tr>
<td>( v = 2 )</td>
<td>( \mathbb{Z}_2 \times D_4 (\rho \in D_4) ) 4 + 4 + 8</td>
</tr>
<tr>
<td></td>
<td>( 16\Gamma_2 b ) 8 + 8</td>
</tr>
<tr>
<td>( v = 3 )</td>
<td>( 32\Gamma_7 a_1 ) 8 + 8</td>
</tr>
<tr>
<td></td>
<td>( 32\Gamma_7 a_1 ) 16</td>
</tr>
<tr>
<td>( v = 4 )</td>
<td>( 64\Gamma_{22} a_1 ) 16</td>
</tr>
<tr>
<td>( G_0 = \mathbb{Z}_4 )</td>
<td></td>
</tr>
<tr>
<td>( v = 1 )</td>
<td>( \mathbb{Z}_2 \times \mathbb{Z}_4 (\rho \notin \mathbb{Z}_4) ) 2 + 2 + 4 + 8</td>
</tr>
<tr>
<td></td>
<td>( \mathbb{Z}_8 ) 8 + 8</td>
</tr>
<tr>
<td>( v = 2 )</td>
<td>( 16\Gamma_2 c_1 ) 4 + 4 + 8</td>
</tr>
<tr>
<td></td>
<td>( 16\Gamma_2 d ) 16</td>
</tr>
<tr>
<td>( v = 3 )</td>
<td>( 32\Gamma_7 a_1 ) 8 + 8</td>
</tr>
<tr>
<td></td>
<td>( 32\Gamma_7 a_2 ) 16</td>
</tr>
<tr>
<td>( v = 4 )</td>
<td>( 64\Gamma_{22} a_1 ) 16</td>
</tr>
<tr>
<td>( G_0 = D_4 )</td>
<td></td>
</tr>
<tr>
<td>( v = 1 )</td>
<td>( \mathbb{Z}_2 \times D_4 (\rho \notin D_4) ) 2 + 2 + 4 + 8</td>
</tr>
<tr>
<td></td>
<td>( 16\Gamma_2 c_1 ) 4 + 4 + 8</td>
</tr>
<tr>
<td></td>
<td>( 16\Gamma_3 a_1 (= D_8) ) 8 + 8</td>
</tr>
<tr>
<td></td>
<td>( 16\Gamma_3 a_2 ) 8 + 8</td>
</tr>
<tr>
<td>( v = 2 )</td>
<td>( 32\Gamma_4 a_1 ) 4 + 4 + 8</td>
</tr>
<tr>
<td></td>
<td>( 32\Gamma_7 a_1 ) 8 + 8</td>
</tr>
<tr>
<td></td>
<td>( 32\Gamma_3 e ) 16</td>
</tr>
<tr>
<td></td>
<td>( 32\Gamma_6 a_1 ) 16</td>
</tr>
<tr>
<td>( v = 3 )</td>
<td>( 64\Gamma_{22} a_1 ) 8 + 8</td>
</tr>
<tr>
<td></td>
<td>( 64\Gamma_{23} a_1 ) 16</td>
</tr>
<tr>
<td></td>
<td>( 64\Gamma_{22} a_1 ) 16</td>
</tr>
<tr>
<td></td>
<td>( 64\Gamma_{28} a_1 (\cong 2\text{-Sylow of } W(D_4)) ) 16</td>
</tr>
<tr>
<td>( v = 4 )</td>
<td>( (\mathbb{Z}_2)^4 \times D_4 (\cong 2\text{-Sylow of } W(C_4)) ) 16</td>
</tr>
<tr>
<td>( G_0 = A_4 )</td>
<td></td>
</tr>
<tr>
<td>( v = 1 )</td>
<td>( \mathbb{Z}_2 \times A_4 ) 2 + 6 + 8</td>
</tr>
<tr>
<td></td>
<td>( SL(2,3) ) 8 + 8</td>
</tr>
<tr>
<td>( v = 3 )</td>
<td>( [(\mathbb{Z}_2)^4]^{\ast} \times A_4 ) 8 + 8</td>
</tr>
<tr>
<td>( v = 4 )</td>
<td>( (\mathbb{Z}_2)^4 \times A_4 ) 16</td>
</tr>
<tr>
<td>( G_0 = S_4 )</td>
<td></td>
</tr>
<tr>
<td>( v = 1 )</td>
<td>( \mathbb{Z}_2 \times S_4 ) 2 + 6 + 8</td>
</tr>
<tr>
<td></td>
<td>( GL(2,3) ) 16</td>
</tr>
<tr>
<td>( v = 3 )</td>
<td>( [(\mathbb{Z}_2)^4]^{\ast} \times S_4 ) 8 + 8</td>
</tr>
<tr>
<td></td>
<td>( [(\mathbb{Z}_2)^4 \times S_4]^{\ast} (\cong W(D_4)) ) 16</td>
</tr>
<tr>
<td>( v = 4 )</td>
<td>( (\mathbb{Z}_2)^4 \times S_4 (\cong W(C_4)) ) 16</td>
</tr>
</tbody>
</table>
Remark 1. For 2-groups, the notation is that of Hall and Senior [5], in which the first number is the order of the group, the symbol \( \Gamma \) denotes the family to which the group belongs in the sense of P. Hall [6], and the remaining portion of the notation specifies the group within that family. The symbol \( Q \) denotes the quaternion group. The \([ \cdot ]^+\) notation is from Coxeter and Moser [3], as recalled in §2.3.2; likewise, \( W(-) \) denotes the Weyl group of the reduced root system of the simple Lie algebra of that type. Note that \( \text{Im}(\mathfrak{u}, 2) \cong W(B_n) = W(C_n) \) is the “hyperoctahedral group”.

Remark 2. Twenty of these structures are nonsplit, some of which belong to more general cases. The three cases with two distinct \( \rho \)-structures on a single permutation group are \( G = \mathbb{Z}_2 \times \mathbb{Z}_4 \), \( G = \mathbb{Z}_2 \times D_4 \), and \( G = 16 \mathbb{Z}_2 \). In particular, 35 degree 8 permutation groups admit 4 sets of order 2 and the central order two element \( \rho \). The groups 64 \( \Gamma_2 \mathcal{A}_1 \) and 64 \( \Gamma_3 \mathcal{A}_1 \) which occur twice have distinct permutation structures in each appearance, while 32 \( \Gamma_5 \mathcal{A}_1 \) occurs three times, each time with distinct permutation structure. Thus 31 nonisomorphic groups occur, 22 of which are 2-groups.

5.2.2. Proposition. Up to normalization there are just six subsets of \((\mathbb{Z}_2)^4\) that occur as the \( G \)-orbits of primitive types. Four of these arise from the split structures, and are given as \((\mathbb{Z}_2)^4\), \([\mathbb{Z}_2]^4]^+, [(\mathbb{Z}_2)^4]^+ (\text{odd})\), and \([\mathbb{Z}_2]^4]^+ - \langle \rho \rangle\). The other two are associated with the cyclic case \( G = \mathbb{Z}_8 \), and are both of order 8, containing even and odd elements.

Proof. First observe that normalization by \( B^1 \) does not disturb \( s(\sigma) \) odd or even, so that specific \( \Phi^\ell \) need not be given. Checking cocycle calculations, observe that, for \( v < 3 \), there is \( s \in G_0 \) so that \( s(\sigma) \) is odd if and only if \( G_0 \) has a 4-cycle \( \tau \) with \( s(\tau) \) odd. But then \( G \) has a subgroup \( Z_8 = \langle (s(\sigma), \tau) \rangle \), which may easily be observed to have the partition \( 2^4 = 8 + 8 \), each orbit being primitive. For primitivity, observe that \( H = \langle 1 \rangle \) with every \( H \subset H_1 \) having \( \rho \in H_1 \), so no proper containment is allowed. For explicit representatives, take \( Z_8 = \langle (0100), (1324) \rangle \), and observe the elements \((0001), (1000), (1100), (1110)\) in one orbit, \((0010), (1001), (0100), (1010)\) in the other. As to the orbits of \( G \), either \( G \) must preserve these orbits, or else \( G \) has \((\mathbb{Z}_2)^4\) as a single \( G \)-orbit with partition \( 2^4 = 16 \).

Next observe that the cases with \( v = 3 \) give \((\mathbb{Z}_2)^4\), \([\mathbb{Z}_2]^4]^+\) and \([\mathbb{Z}_2]^4]^+ (\text{odd})\), the latter two if and only if \( G \) is split, as analyzed in §2.3.2, Example 4. The remaining cases all have \( s(\sigma) \) even for all \( \sigma \in G_0 \), and also have \( v \leq 2 \). But when \( s(\sigma) \) is always even, \([\mathbb{Z}_2]^4]^+\) and \([\mathbb{Z}_2]^4]^+ (\text{odd})\) must be preserved by the \( G \)-action. Now if \( 3 \not| G_0 \), no orbit of order 6 occurs. As the reflex of a type with an orbit of order 4 is of degree 2 or 4, no orbit of order 4 contains primitive types, and no further primitive types are obtained. For \( 3/|G_0| \), the two split cases may be easily computed and give
\[
(\mathbb{Z}_2)^4 = \langle \rho \rangle \cup \left[ [([\mathbb{Z}_2]^4]^+ - \langle \rho \rangle) \cup ([\mathbb{Z}_2]^4]^+ (\text{odd}) \right].
\]

Otherwise there is no term of order two, so no term of order 6 occurs, and only the two “split” orbits of order 8 occur for \( s(\sigma) \) even. As the required cocycle calculations may be easily supplied, the present description is complete.

5.3.1. For \( n = 6 \) and larger composite values such as \( n = 8, 9 \) or 15, a nesting of the \( G_0 \) as with \( Z_2 \subset G_0 \) for \( p \) prime and with \((\mathbb{Z}_2)^2 \cdot Z_4 = D_4 \subset S_4, (\mathbb{Z}_2)^2 \subset A_4 \) for
n = 4 is not so readily apparent. For the general case certain G₀ with corresponding properties are distinguished by the following:

**Definition.** A transitive group G₀ of degree n is called a minimal group of degree n, and written as G₀^{min} (when n is understood), provided that no proper subgroup of G₀ is transitive.

For n = 6, the minimal groups are provided by the following:

**Proposition.** The imprimitive transitive permutation groups of degree 6 may be normalized to have the inclusion relations indicated on the lattice diagram for n = 6 below, with the notations introduced in the proof. The primitive G₀ of degree 6 are never minimal, so there are four minimal groups G₀^{min} for n = 6; these are the groups Z₆, S₃, A₄ and Im(2, 3)^{+} indicated in the lattice diagram by boxes.

**Proof.** To fix the notation, the relevant structure of these well-known groups is recalled. The group Im(2, 3) has the structure S₃ \ltimes Z₂, the wreath product, and is also given as (S₃ × S₃) \ltimes Z₂, semidirect. Im(2, 3)^{+} is the subgroup by

$$\text{Im}(2, 3)^{+} = \left\{ ((\sigma_1, \sigma_2), \rho) \in (S_3 \times S_3) \ltimes Z_2 / \text{sgn}(\sigma_1) \text{sgn}(\sigma_2)(-1)^{\rho} = 1 \right\}.$$  

The group G₃₆, also of order 36, is G₃₆ = (S₃ × S₃)^{+} \ltimes Z₂. Note that ρ is the usual product of 3 disjoint two cycles, but with nontrivial action in Im(2, 3). Since (123) and (456) are even, the Z₆ subgroup given by (((123), (456)), ρ) does not belong to Im(2, 3)^{+}, but does to G₃₆ as well as the wreath product Z₃ \ltimes Z₂. Further inclusions are obtained by observing that G₃₆ is the holomorph of S₃, that is, G₃₆ ≅ S₃ \rtimes Aut(S₃) ≡ S₃ \rtimes S₃. A subgroup analysis may be used to establish that Im(2, 3)^{+} is a minimal group.

For Im(3, 2) = (Z₂)^{3} \rtimes Z₃ as usual, observe that Im(3, 2) \cap Im(2, 3) = D₆, with D₆ also given as D₆ = S₃ \cdot Z₆. A₄ is the subgroup [(Z₂)^{3}]^{+} \rtimes Z₃ of Im(3, 2), and contains no subgroups of order 6. Observe that A₄ \cdot D₆ = A₄ \cdot S₃ \cdot Z₆ = Im(3, 2). The permutation groups S₄ and Im(3, 2)^{+} are both abstractly isomorphic to S₄, the notation “S₄” being reserved for [(Z₂)^{3}]^{+} \rtimes Z₃, which contains A₄ as given. A₄ \times Z₂ = (Z₂)^{3} \rtimes Z₃ and is given as A₄ \cdot Z₆. Likewise Im(3, 2)^{+} = A₄ \cdot S₃, completing the description of the 12 imprimitive G₀.

The four primitive groups of degree 6 are given as A₅ ≅ PSL(2, 5), S₅ ≅ PGL(2, 5), A₆ and S₆. To see that none of these are minimal, observe A₄ \subset A₅ \subset A₆ \subset S₆ and A₅ \subset S₅.

**Lattice Diagram for n = 6**

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
The steps (A) and (B) of the Classification Theorem are given for \( n = 6 \) by the following:

**Theorem.** For \( n = 6 \) there are 66 inequivalent pairs \( (G_0, (\mathbb{Z}_2)^v) \), with \( v \in (\mathbb{Z}_2)^v \), and therefore 66 inequivalent \( p \)-structures with trivial cochain \( s(\sigma) = 0 \) for all \( \sigma \in G_0 \). All 16 \( G_0 \) admit \( \langle \rho \rangle \) with \( v = 1 \), \( [(\mathbb{Z}_2)^6]^+ \) with \( v = 5 \), and \( (\mathbb{Z}_2)^6 \), accounting for 48 cases. \( G_0 \) admits \( v = 2 \) if and only if \( G_0 \subset \text{Im}(2, 3) \), supplying 7 cases; \( G_0 \) admits \( v = 3 \) if and only if \( G \subset \text{Im}(3, 2) \), supplying 8 cases; and, \( G_0 \) admits \( v = 4 \) if and only if \( G_0 \subset D_6 = \text{Im}(2, 3) \cap \text{Im}(3, 2) \), for 3 cases.

**Proof.** Consider the 4 \( G_0^{\text{min}} \) cases, and decompose \( (\mathbb{Z}_2)^6 \) into \( G_0^{\text{min}} \) orbits, taking account of the pairing given by \( \rho \). The action of \( G_0 \) preserves the number of 1’s, allowing a preliminary decomposition \( (\mathbb{Z}_2)^6 = \langle \rho \rangle \cup [1_{1,5}] \cup [1_{2,4}] \cup [1]_3 \), subscripts denoting the number of 1’s. Since \( G_0 \) is transitive, the pairing by \( \rho \) gives \( [1]_1 \) as a single orbit of order 12.

The remaining terms decompose as follows:

(1) \( |[1]_{2,4}| = 12 + 12 + 6 \), \( |[1]_3| = 12 + 6 + 2 \), for \( G_0 = \mathbb{Z}_6 \);

(2) \( |[1]_{2,4}| = 6 + 6 + 6 + 12 \), \( |[1]_3| = 2 + 6 + 6 + 6 \), for \( G_0 = S_3 \);

(3) \( |[1]_{2,4}| = 24 + 6 \), \( |[1]_3| = 8 + 12 \), for \( G_0 = A_4 \);

and

(4) \( |[1]_{2,4}| = 12 + 18 \), \( |[1]_3| = 2 + 18 \), for \( G_0 = \text{Im}(2, 3)^+ \).

The cases for \( (G_0^{\text{min}}, (\mathbb{Z}_2)^v) \) are then obtained by examining unions of orbits to see when sub-\( G_0 \)-modules are obtained. First results are that \( v = 3 \) and \( v = 4 \) do not occur for \( G_0^{\text{min}} = \text{Im}(2, 3)^+ \), nor does \( v = 4 \) for \( G_0^{\text{min}} = A_4 \).

To obtain some of the pairs \( (G_0^{\text{min}}, (\mathbb{Z}_2)^v) \), aside from the cases with \( v = 1, 5 \) and 6, observe that \( (\mathbb{Z}_2)^v = \langle (e, e) e (\mathbb{Z}_2)^6/e \in (\mathbb{Z}_2)^3 \rangle \), gives a case with \( v = 3 \) for \( G_0 \subset \text{Im}(3, 2) \), and \( (\mathbb{Z}_2)^v = \langle (\rho, 0, \rho_0) \rangle \) with \( \rho_0 = (111) \in (\mathbb{Z}_2)^3 \), gives a case with \( v = 2 \) for \( G_0 \subset \text{Im}(2, 3) \). Observe that \( D_6 \) admits \( (\mathbb{Z}_2)^v = \langle (e, \rho_a^6 e) e (\mathbb{Z}_2)^6/e \in (\mathbb{Z}_2)^3, a = 0, 1 \rangle \) since both \( S_3 \) and \( \mathbb{Z}_6 \) do, and \( D_6 = S_3 \cdot \mathbb{Z}_6 \). Note that for \( G_0 \) containing either \( A_4 \) or \( \text{Im}(2, 3)^+ \), \( [(\mathbb{Z}_2)^6]^+ \) is unique for \( v = 5 \), since otherwise \( [(\mathbb{Z}_2)^6]^+ \) would give \( v = 4 \).

Next observe that each value \( v = 1, 2, \ldots, 6 \) occurs for \( G_0 = \mathbb{Z}_6 \), with \( (\mathbb{Z}_2)^v \) uniquely determined for each value. For example, \( v = 2 \) gives odd elements, so \( v = 3 \) must have only even elements, else a second \( v = 2 \) would result. But then \( (\mathbb{Z}_2)^v = \langle (\rho) \cup \emptyset \rangle \), for \( \emptyset \) the orbit from \([1]_{2,4}\) with order 6. The remaining case \( G_0^{\text{min}} = S_3 \) has 3 submodules \( (\mathbb{Z}_2)^v \) for each of \( v = 3 \) and \( v = 4 \). The equivalence of these under \( N_{S_3}(S_3) = G_{36} \) may be observed by noting that \( G_{36} \) gives the same decomposition of \( (\mathbb{Z}_2)^6 \) as \( \text{Im}(2, 3)^+ \), so that \( G_{36} \) does not preserve any \( (\mathbb{Z}_2)^v \) for \( v = 3 \) or 4, as would be required for \( S_3 \) to have inequivalent submodules as in (B) of the Classification Theorem. No other nonunique \( (\mathbb{Z}_2)^v \)'s occur for \( S_3 \), as in the previous cases.

All 20 \( (G_0^{\text{min}}, (\mathbb{Z}_2)^v) \) cases having been obtained, most of the general cases follow from the inclusion relations in the above proposition. For example, in the case...
$\mathbb{Z}_6 S_3 = \mathbb{Z}_3 \setminus \mathbb{Z}_2$, here with subgroups $\mathbb{Z}_6$ and $S_3$ so $\mathbb{Z}_6 \cap S_3 = \mathbb{Z}_2$, observe that $S_3$ does not preserve the unique submodule with $v = 3$ for $\mathbb{Z}_6$, and therefore does not preserve the submodule with $v = 4$ either. Finally, consider the primitive cases, all of which have been observed to contain $A_4$. The inclusion rules out 2 and 4, and gives uniqueness for $v = 5$. The remaining case, $v = 3$, may be eliminated since each of these $G_0$ is at least 2-transitive, so that $[\ ]_{2,4}$ is a single orbit or order 30.

**Corollary of proof.** Let $G = \mathbb{Z}_2 \times G_0^{\min}$ be the split $v = 1$ group with structure by $s(\sigma) = 0$ for all $\sigma \in G_0$. Then the types of $G$, i.e., of $(G, \text{Stab}_G(\pm 1), \rho)$, have $G$-orbit structure giving the following partitions:

1. $2^6 = 2 + 12 + [12 + 12 + 6]_{2,4} + [12 + 6 + 2]_3$, for $G_0 = \mathbb{Z}_6$;
2. $2^6 = 2 + 12 + [6 + 6 + 6 + 12]_{2,4} + [2 + 6 + 6 + 6]_3$, for $G_0 = S_3$;
3. $2^6 = 2 + 12 + [24 + 6]_{2,4} + [8 + 12]_3$, for $G_0 = A_4$; and
4. $2^6 = 2 + 12 + [12 + 18]_{2,4} + [2 + 18]_3$, for $G_0 = \text{Im}(2, 3)^+.$

**Proof.** The split structure $\mathbb{Z}_2 \times G_0$ with $s(\sigma) = 0$ for all $\sigma \in G_0$ exactly gives the $G_0$-orbits with pairing by multiplication by $\rho$, so the computations are the same.

The examples generalized in §3 occur for the cases $G_0 = \mathbb{Z}_6, A_4,$ and $\text{Im}(2, 3)^+.$ The group $G_0 = \mathbb{Z}_3 \setminus \mathbb{Z}_2$ is adopted in place of $\text{Im}(2, 3)^+$ as an orbit with similar properties is obtained.

6. The relation to group extensions.

6.0. The present section does not depend upon the material of §§3, 4 or 5. For the remainder of §6 the requirement $\rho \in (\mathbb{Z}_2)^{v}$ will be dropped, unless otherwise noted, to allow a general “imprimitivity structure”, $(G, H, S)$, with $n$ sets of order 2, as in Remark 2 of §2.1. The imprimitivity sequence still has the form $0 \to (\mathbb{Z}_2)^{v} \to G \to G_0 \to 1$ and $G$ is given by an imprimitive permutation representation as in the Imprimitivity Theorem of §1. While the case $v = 0$, where the action of $G$ on $S \setminus G$ is effective, still allows such a representation, $v > 0$ will be supposed.

Let $H$ be the subgroup fixing the elements of the set $(\pm k)$, and let $k^{th}$ denote the projection of $(\mathbb{Z}_2)^{v}$ on the $k^{th}$ coordinate. Then since $(S : H) = 2$, and the action of $G$ on $S \setminus G$ has a nontrivial kernel, there exists $e_0 \in (\mathbb{Z}_2)^{v}$ such that $k^{th}(e_0) \neq 0$, else $(\mathbb{Z}_2)^{v} \subset H$, contradicting the requirement that $G$ be effective on $H \setminus G$. Then $e_0$ may be used to arrange $k^{th}(s(\sigma)) = 0$, for all $\sigma \in G_0$, so $H$ may still be given as $H\{((es(\sigma), \sigma) \in G/\sigma \in H_0(k), k^{th}(e) = 0), for H_0 = H_0(k) the subgroup of G_0 fixing the set (\pm k).

Fix $s \in Z^1(G_0, (\mathbb{Z}_2)^{v}/(\mathbb{Z}_2)^{v})$ and consider, in the case $\rho \in (\mathbb{Z}_2)^{v}$, the following:

**Proposition.** Let $S = \text{Proj}^{-1}_{\text{Sets}}(H_0)$, for $\text{Proj}_{\text{Sets}}$ defined by $s$; and, for $t \in Z^1(G_0, (\mathbb{Z}_2)^{v})$, let $H_t = \{(es(\sigma), \sigma) \in S/k^{th}(e) = k^{th}(t(\sigma))\}$. Then representatives for the nontrivial $\rho$-structures relative to $s$ are among the $\rho$-structures $(G, H_t, S)$.

**Proof.** Consider the factor $j^1(Z^1)$ in the proposition following the Classification Theorem in §2.3. Observe that $H_t$ is the inverse image of the stabilizer of a letter in the image of $G$ under the automorphism $(e, \sigma) \to (et(\sigma), \sigma)$ of $(\mathbb{Z}_2)^{v} \times G_0 \subset S_{2n}$ defined by $t$. Then $(H_t, S)$ represents (under $\rho$-equivalence) the $\rho$-structure defined by $\bar{s}j^1(t)$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
6.1. To account for the structures \((H_t, S)\) on \(G\), the essential features are abstracted by the following:

**Definitions.** Let \((G, H, S)\) define an imprimitivity structure with \(n\) sets of order 2, so that \(G\) acts effectively on \(H \setminus G\), and suppose the action of \(G\) on \(S \setminus G\) has nonzero kernel. Then \((G, H, S)\) is said to have \(H_0 = \text{Proj}^{\text{sets}}(H)\) as its initial structural subgroup. Let \(N\) be a subgroup of \(H_0\), normal in \(H_0\). Then a pair \((H_N, S)\), where \(H_N\) is a subgroup of \(S\) is said to define an imprimitivity structure with structural subgroup \(N\) provided that \(H_N\) is without normal subgroups (aside from \((1)\)) of \(G\), that the index \((S : H_N) = 2\), and that \(N\) is the largest among the normal subgroups \(K\) of \(H_0\) for which \(\text{Proj}^{\text{sets}}(K) \cap H = \text{Proj}^{\text{sets}}(K) \cap H_N\). The pair \((H_N, S)\) is said to define a nontrivial structure, relative to the initial structure \((H, S)\), provided that \((H_N, S)\) defines an imprimitivity structure inequivalent to that defined by the initial structure \((H, S)\). In the case \(S = H \times \langle \rho \rangle\), where the imprimitivity structures are referred to as \(\rho\)-structures, the notation \((H_N, \rho)\) is used.

**Proposition.** The subgroup \(H_N\) of \(S\) is uniquely determined by the normal subgroup \(N \subset H_0\).

**Proof.** Let \((\mathbb{Z}_2)^{v-1}\) denote the subgroup \((\mathbb{Z}_2)^{v-1} = (\mathbb{Z}_2)^v \cap H = \ker(k^\text{th}|(\mathbb{Z}_2)^v)\). Since \(1 \in N\), the subgroup \((\mathbb{Z}_2)^{v-1}\) is common to both \(H\) and \(H_N\). Write \(H = \bigcup_{\sigma \in H_0} (\mathbb{Z}_2)^{v-1}(s(\sigma), \sigma)\), recalling that \(s(\sigma)\) has been chosen so that \(k^\text{th}(s(\sigma)) = 0\) for all \(\sigma \in G_0\). Then observe that

\[
H_N = \bigcup_{\sigma \in H_0} (\mathbb{Z}_2)^{v-1}(e_0^\text{sgn}(\sigma)s(\sigma), \sigma),
\]

where \(e_0\) has been fixed with \(k^\text{th}(e_0) \neq 0\), and \(\text{sgn}(\sigma) = \chi^N(\sigma)\) is the characteristic function of \(\overline{N} = H_0 - N\). To check, note that the above collection must be contained in \(H_N\), but then equality holds by the requirement \((S : H_N) = 2\) in the definition of \((H_N, S)\).

**Examples.** For the case \(G = \mathbb{Z}_2 \times S_4, H = H_0 = S_3,\) with \(n = 4, (\mathbb{Z}_2)^v = \langle \rho \rangle,\) and \(e_0 = \rho,\) observe that the subgroup \(N = 1\) is not allowed as a structural subgroup. Let \(\sigma \in H_0\) be a 3-cycle. Then \((\rho, \sigma) \in H_N\) gives \((\rho, \sigma)^3 = (\rho, 1) \in H_N,\) contradicting \((S : H_N) = 2.\)

For the general subgroup \(H_t,\) observe that \(H_t = H_N\) is the subgroup of \(S\) corresponding to the normal subgroup \(N = \ker(k^\text{th}),\) for \(k^\text{th}: H_0 \to \mathbb{Z}_2\) defined by \(k^\text{th}(\sigma) = k^\text{th}(t(\sigma)).\)

6.2. With the above preliminaries established, the nature of the \(\rho\)-structures classified by the Classification Theorem may be clarified by the following:

**Structures Theorem.** Let \((G, H, S)\) define an imprimitivity structure, and suppose the imprimitivity sequence \(0 \to (\mathbb{Z}_2)^v \to G \to G_0 \to 1\) has \(v > 0\). Then the collection of structural subgroups \(N\) depends only on \((G_0, (\mathbb{Z}_2)^v)\). There is a collection \(\mathcal{C}\) of structural subgroups with the following properties:

1. the structures \((H_N, S)\), with \(N \in \mathcal{C}\), are equivalent to \((H, S)\), independent of \(G\);
2. \((H_N, S)\) is a nontrivial split structure for all \(N \in \mathcal{C}\), when \(G\) is split; and
3. for \(G\) to have a smaller number of nontrivial structures than the split group, \(\text{Aut}(G)\) must contain elements as specified precisely below.
Further, the collection $C$ is computable from $H^1(G_0, (\mathbb{Z}_2)^\nu)$, with the structural subgroups corresponding to nonzero classes requiring identifications by $\text{Outer}(G)$, the group of outer automorphisms.

Before beginning the proof, some technical results describing the effect of $\text{Aut}(G)$ on the structures $(H_N, S)$, will be given. In order that $\alpha \in \text{Aut}(G)$ give an equivalence of the initial structure $(H, S)$ with some structure $(H_N, S)$, $\alpha$ must satisfy $\alpha(S) = S$ and $\alpha(H) = H_N$, by definition. Then $\alpha((\mathbb{Z}_2)^\nu) = (\mathbb{Z}_2)^\nu$ so $\alpha$ defines an automorphism $\alpha_v: (\mathbb{Z}_2)^\nu \to (\mathbb{Z}_2)^\nu$ by $(\alpha_v(e), (1)) = (\alpha(e), (1))$ and induces an automorphism $\bar{\alpha}: G_0 \to G_0$. The automorphism $\alpha$ is then determined by these two maps and a third map $\alpha_s: G_0 \to (\mathbb{Z}_2)^\nu$, with $\alpha_s(\sigma)$ defined by $\alpha(s(\sigma), \sigma) = (\alpha_s(\sigma) s(\bar{\alpha}(\sigma)), \bar{\alpha}(\sigma))$. Write $\alpha \in \text{Aut}(G)$, under the assumption $\alpha(S) = S$, as $\alpha = (\alpha_v, \alpha_s, \bar{\alpha})$.

Next, $S$ and $H$ have $\text{Proj}_G(H_0) = \text{Proj}_G(H_0)$, since $\nu > 0$, so $\bar{\alpha}(H_0) = H_0$. Recall that the subgroup $(\mathbb{Z}_2)^{\nu-1} = (\mathbb{Z}_2)^\nu \cap H = \ker(k^{th}((\mathbb{Z}_2)^\nu))$, for $H = H(k)$, $H_0 = H_0(k)$, is common to all of the subgroups $H_N$ so $\alpha_v$ is restricted by $\alpha_v((\mathbb{Z}_2)^{\nu-1}) = (\mathbb{Z}_2)^{\nu-1}$. Apply the requirement that $\alpha$ be multiplicative to the product $(e's(\sigma), \sigma)(e, (1)) = (e's(\sigma) \star e, \sigma)$ to obtain the compatibility condition $\alpha_v(\sigma \star e) = \bar{\alpha}(\sigma) \star \alpha_v(e)$, for all $e \in (\mathbb{Z}_2)^\nu$, $\sigma \in G_0$.

The remaining condition for $\alpha = (\alpha_v, \alpha_s, \bar{\alpha})$ to define an element of $\text{Aut}(G)$ taking $(H, S)$ to some $(H_N, S)$ is given by the following:

**Lemma 1.** Suppose $\alpha_v \in \text{Aut}(\mathbb{Z}_2)^\nu$, $\alpha_s \in \text{Aut}(G_0, H_0)$, and the above compatibility condition relating $\alpha_v$ and $\bar{\alpha}$ holds. Then $\alpha = (\alpha_v, \alpha_s, \bar{\alpha})$ defines an automorphism if and only if the map $\alpha_s: G_0 \to (\mathbb{Z}_2)^\nu$ satisfies the condition

$$
(\delta_s)(\sigma, \sigma_1) = s(\sigma) \sigma_1 \star s(\sigma_1),
$$

where $\delta$ is the coboundary map

$$
(\delta s)(\sigma, \sigma_1) = s(\sigma) \sigma_1 \star s(\sigma_1),
$$

and $\delta_s$ is the coboundary

$$
(\delta_s)(\tau, \tau_1) = \tau(\sigma) \tau_1 \star \tau(\tau_1).
$$

**Proof.** The condition holds if and only if the map

$$
\alpha(es(\sigma), \sigma) = (\alpha_v(e) \alpha_s(\sigma) s(\bar{\alpha}(\sigma)), \bar{\alpha}(\sigma))
$$

is multiplicative, noting that the cochain map $s$ has $(\delta s)(\sigma, \sigma_1) \in (\mathbb{Z}_2)^\nu$, since $(j \circ s) \in Z^1(G_0, (\mathbb{Z}_2)^\nu/((\mathbb{Z}_2)^\nu)^\nu)$.

The above condition is also sufficient to insure that $\alpha(S) = S$ and $\alpha(H) = H_N$, so any such triple will produce a structural subgroup $N$, determining which $H_N$ arise as $\alpha(H) = H_N$. Recall that $\nu > 0$ allows normalizing the $k^{th}$ coordinate of $s(\sigma)$ to be 0, for all $\sigma \in G_0$, $k$ depending upon $H = H(k)$. Then observe that $N$ may be obtained by the following:

**Lemma 2.** The structural subgroup $N$ determining $\alpha(H) = H_N$ is given as $N = \ker(k^{th}(\alpha_s(\bar{\alpha}^{-1}(\sigma))]|H_0)$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Proof. Recall $H = \bigcup_{\sigma \in H_0}(\mathbb{Z}_2)^{v-1}(s(\sigma), \sigma)$, and then observe that for $\alpha = (\alpha_v, \alpha_s, \bar{\alpha})$ as above,

$$\alpha(H) = \bigcup_{\sigma \in H_0}(\mathbb{Z}_2)^{v-1}(\alpha_s(\sigma)s(\bar{\alpha}(\sigma)), \bar{\alpha}(\sigma)).$$

Then

$$k^\text{th}(\alpha_s(\sigma)s(\bar{\alpha}(\sigma))) = k^\text{th}(\alpha_s(\sigma))$$

since $k^\text{th}(s(\sigma)) = 0$ for all $\sigma \in G_0$. But the map $\text{sgn}_N(\sigma)$ used to describe $H_N$ gives the lift of $\sigma$, so $\sigma = \bar{\alpha}^{-1}(\sigma_1)$ gives $k^\text{th}(\alpha_s(\bar{\alpha}^{-1}(\sigma_1)))$ as $\text{sgn}_N(\sigma_1)$.

A complete account of the effect of $\text{Aut}(G)$ on the structures $(H_N, S)$ has been reduced to understanding the maps $\alpha_s: G_0 \to (\mathbb{Z}_2)^v$ allowed by $\text{Aut}(G)$. If the right-hand side, $\alpha_v(\delta s)\delta_\sigma s$, of equation (\star) of Lemma 1 is nonzero, then the map $\alpha_s$ strictly depends on $G$, since the split extension with trivial structure $s(\sigma) = 0$ for all $\sigma \in G_0$ forces the right-hand side to be zero. Then the existence of such an automorphism of $G$ supplies the promised precise specification in (3), as may be observed in the analysis of the case $\delta_\sigma(\alpha_s) = 0$ in the following:

Proof of the Structures Theorem. For the collection of structural subgroups, observe that $H_N$, a subgroup of index two in $S$, is not normal if $H_N$ is without normal subgroups of $G$. Only $(\mathbb{Z}_2)^k \subset (\mathbb{Z}_2)^{v-1}$ is possible, but if $e \in (\mathbb{Z}_2)^k$ has a nonzero entry, the transitive $G_0$-action will conjugate that entry to the $k^\text{th}$ component, taking $e$ outside $H_N$. To insure that $H_N = \bigcup_{\sigma \in H_0}(\mathbb{Z}_2)^{v-1}(e_0\text{sgn}_N(\sigma)s(\sigma), \sigma)$ is closed under products, consider a relation $\sigma_1\sigma_2 \cdots \sigma_r = 1$ among elements of $H_0$. Lifting the relation to $H_N$ gives

$$(\epsilon^{\text{sgn}_N(\sigma_1)s(\sigma_1)}, \sigma_1)(\epsilon^{\text{sgn}_N(\sigma_2)s(\sigma_2)}, \sigma_2) \cdots (\epsilon^{\text{sgn}_N(\sigma_r)s(\sigma_r)}, \sigma_r)$$

$$= (\epsilon^{\text{sgn}_N(\sigma_1)s(\sigma_1)}\sigma_1 \star \epsilon^{\text{sgn}_N(\sigma_2)s(\sigma_2)}\sigma_1 \star s(\sigma_2)$$

$$\cdots (\sigma_1 \cdots \sigma_{r-1}) \star \epsilon^{\text{sgn}_N(\sigma_r)}(\sigma_1 \cdots \sigma_{r-1}) \star s(\sigma_r), (1)).$$

Then closure requires the first entry to be in $(\mathbb{Z}_2)^{v-1} = \ker(k^\text{th}|(\mathbb{Z}_2)^v)$. But $k^\text{th}(s(\sigma)) = 0$ and $\text{sgn}_N$ is only required on $H_0 = H_0(k)$, so that

$$k^\text{th}(-) = k^\text{th}(\epsilon^{\text{sgn}_N(\sigma_1)s(\sigma_1)}\star \epsilon^{\text{sgn}_N(\sigma_2)} \cdots (\sigma_1 \cdots \sigma_{r-1}) \star \epsilon^{\text{sgn}_N(\sigma_r)}(\sigma_1 \cdots \sigma_{r-1}))$$

is independent of $s$. But lifting generators and relations for $H_0$ to $H_N$ and taking account of the subgroup $(\mathbb{Z}_2)^{v-1}$, with action determined by $H_0$, suffices to determine $H_N$, regardless of $s$.

For $t_0 \in Z^1(G_0, (\mathbb{Z}_2)^v)$ the map $\alpha = (0, t_0, 1)$ is always an automorphism, as may be seen, in particular, from Lemma 1. But for $t_0 \in B^1(G_0, (\mathbb{Z}_2)^v)$, $k^\text{th}(t_0|H_0) = 0$ since $H_N$ fixes $k^\text{th}$ components, so $k^\text{th}(t_0|H_0)$ is well defined for $[t_0] \in H^1(G_0, (\mathbb{Z}_2)^v)$. Then $H^1(G_0, (\mathbb{Z}_2)^v)$ gives a collection of structural subgroups, independent of $G$. But $\alpha(H) = H_N$ for $N \neq H_0$ is never achieved by $\alpha \in \text{Inn}(G)$, since $H_N$ is not one of the $n$ conjugates $H(j), j = 1, \ldots, n$, of $H = H(k)$. Therefore $H^1(G_0, (\mathbb{Z}_2)^v) \neq 0, t_0 \in Z^1(G_0, (\mathbb{Z}_2)^v)$ nonprincipal with $\ker(k^\text{th}(t_0|H_0)) = N \neq H_0$ always corresponds to an equivalence requiring $\text{Outer}(G)$.

Only the assertions on $G = \bigcup_{\sigma \in G_0}(\mathbb{Z}_2)^v(0, \sigma)$, by an argument depending only upon the right-hand side of the equation of Lemma 1 being zero for all $\alpha \in \text{Aut}(G)$,
remains. But under this assumption, $\alpha_j \in Z^1_{G_0}(G_0, (\mathbb{Z}_2)^2)$, the group of cocyles with action twisted by $\alpha$, i.e., $\sigma \mapsto (e) = \alpha(e) \cdot e$. Finally, observe that $t_0(\sigma) = \alpha_j(\sigma^{-1}(e))$, for $\alpha_j \in Z^1_{G_0}$, gives $t_0 \in Z^1$, untwisted, so that $k^{th}(\alpha_j(\sigma^{-1}(e))) = k^{th}(t_0(\sigma))$ adds no new structural subgroups.

**Remarks.** In the low degree examples considered in the present investigation, nontrivial structures have been obtained only when the imprimitivity sequence of $G$ is split. Observe that a nontrivial split imprimitivity structure, $\rho \in (\mathbb{Z}_2)^n$, occurs for $n = 3$ and accounts for the fact that $G_0 = S_4$ has two distinct permutation structures of degree 6. Recall that the nontrivial structure on $\text{Gal}(K^c/\mathbb{Q})$ in §2.2 uses one of these.

The nontrivial structures obtained are only asserted to be distinct from the initial structure and might therefore allow further equivalences among themselves. A generalization of Miller’s examples is the case $G = \mathbb{Z}_2 \times \text{PSL}(2, p)$, the direct product $G_0 = \text{PSL}(2, p)$ being allowed to range over all transitive permutation structures. For $(H_N, \rho)$ with $H_N = H_1$, $t \in Z^1(G_0, (\mathbb{Z}_2)^{\deg(G_0)})$, a calculation establishes that the trivial cochain structure admits $l$ such nontrivial structures for $l = 0, 1$ or $3$, with $l = 3$ implying $H_0 \cong D_{2q_1}$, dihedral of order $4q_1$, $q_1 \geq 1$. Since $\rho$ is characteristic, the $\rho$-structures $(\mathbb{Z}_2 \times \text{PSL}(2, p), \langle 0 \rangle \times D_{2q_1}, \rho)$ are in one-to-one correspondence with the permutation structures $(\mathbb{Z}_2 \times \text{PSL}(2, p), \langle 0 \rangle \times D_{2q_1})$. The permutation structures do not determine the $\rho$-structures for each $\rho$ only when $\rho$ is noncharacteristic. The case where $\rho$ is the unique element of order 2 strongly restricts the structure of $G$, as in [13].

**References**


22. ______, The arithmetic of certain zeta functions and automorphic forms on orthogonal groups, Ann. of Math. (2) 111 (1980), 313–375.

DEPARTMENT OF MATHEMATICS, LEHIGH UNIVERSITY, BETHLEHEM, PENNSYLVANIA 18015