ACTA ARITHMETICA
LXXXIX.1 (1999)

Linear relations between roots of polynomials

by

Kurt Girstmair (Innsbruck)

Introduction. Let K be a field of characteristic 0 and $f = Z^n + c_1 Z^{n-1} + \ldots + c_n$ an irreducible polynomial with roots $x_1, \ldots, x_n$ in some splitting field $L = K(x_1, \ldots, x_n)$ of f. This article deals with additive relations

$$a_1 x_1 + \ldots + a_n x_n = 0, \quad a_j \in K, \tag{1}$$

between these roots and multiplicative ones

$$x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n} = 1, \quad a_j \in \mathbb{Z}. \tag{2}$$

Both types are comprised under the name of "linear relations".

One of our objectives consists in convincing the reader that the representation theory of finite groups, applied to the Galois group $G = \mathrm{Gal}(L/K)$ of f, is the appropriate framework for questions of this kind. More than 15 years ago we already pointed out this role of representation theory in our paper [11]—it seems, however, that the proper value of this tool has not been recognized by several later researchers (cf. [19], [9], [10], [1], [17]). As an effect, some minor observations of [11] appear as main results in later articles (cf., e.g., [11], Proposition 4, Assertion 3 and [9], Theorem 3). An exception to this tendency is the recent paper [7]. But although it uses representation theory, its viewpoint differs from that of our previous work: The results of [7] are mainly *necessary* conditions saying that a given relation (such as $x_1 = x_2 + x_3$) can occur for a certain class of polynomials only. Our paper [11], in contrast, contains a criterion that allows one to *decide* whether a given relation (1) is possible or not in a *specific* case (cf. Theorem 1 below). This criterion yields a classification of all possible relations (1) for polynomials f over $K = \mathbb{Q}$ of degree $n \leq 15$ with G acting primitively on its roots ([11], Theorem 1, and Section 2, ibid.). For example, the relation

1991 *Mathematics Subject Classification*: 12F10, 12E05.

$$4x_1 + x_2 + x_3 + x_4 + x_5 - 2(x_6 + x_7 + x_8 + x_9) = 0$$

actually occurs for $n = 9$ and a certain primitive group G of order $|G| = 72$.

In Section 1 we give a unified approach to *both* the additive and the multiplicative case. In particular, we show that both cases lead to the same basic concept: the concept of a *K-admissible set*. Roughly speaking, a K-admissible set consists of relations (1) that may occur for some specific polynomial f; multiplicative relations (2) are covered by the case $K = \mathbb{Q}$. The property of being K-admissible does not, however, depend on f or its splitting field L, but only on the Galois group G and the stabilizer

$$H = G_x = \{s \in G : s(x) = x\} \tag{3}$$

of a root $x \in \{x_1, \dots, x_n\}$ (clearly the groups H are conjugate for different choices of x). Hence it is quite natural to define the fundamental notions (such as "relation", "K-admissibility") in a completely abstract way in terms of *pairs of groups* (G, H), $H \subseteq G$. To each pair (G, H) we attach a canonical module $K[G/H]$ (over the group ring $K[G]$ of G). "Relations" are elements of this $K[G]$-module and "K-admissible sets" are subsets of $K[G/H]$ that can be characterized in terms of certain submodules (Theorem 1). In [11], the theory was developed more or less thus far but without regard to the multiplicative case.

It suffices, in fact, to consider only those K-admissible sets that are $K[G]$-modules themselves, so-called *K-admissible modules*. In Section 2 we work out the role which *character theory* plays in the description of these modules. The main result is a complete description (not of all but) of all *isotypically closed* K-admissible modules in terms of certain sets of characters (Theorem 2). As an illustration, we give an example that goes beyond hand-calculations, namely, nontrivial relations for a polynomial f of degree 55 whose Galois group is isomorphic to $\mathrm{PSL}(2, 11)$ and acts primitively on $x_1, \dots, x_{55}$ (Example 6). Moreover, the main result says that *all* K-admissible modules (and, thus, essentially all K-admissible sets) are under control if the canonical module $K[G/H]$ is multiplicity-free as a $K[G]$-module. In this case we say that the pair (G, H) is *K-multiplicity-free*. Pairs of this kind are quite important, as Examples 1–5 show.

Section 3 is devoted to polynomials f with *abelian* Galois groups, or, in our terminology, pairs $(G, 1)$ with G abelian. Here the module $K[G/H]$ is the group ring $K[G]$ itself. Since $(G, 1)$ is K-multiplicity-free, the foregoing results yield a nice criterion for K-admissibility: A subset of $K[G]$ is K-admissible if, and only if, it is annihilated by a set of *generators* of the character group of G (Theorem 3). As an application, we compute the greatest possible dimension of a $\mathbb{Q}$-admissible module (Proposition 11). Furthermore, we treat an interesting type of relations that was investigated in [10] and [7]: The authors of these papers asked under which conditions a root of

f may be the sum or product of two other roots, say

$$x_1 = x_2 + x_3 \quad \text{or} \quad x_1 = x_2 x_3. \tag{4}$$

Whereas [10] gives the complete answer in the abelian case, [7] yields a necessary condition in a more general situation. We show that the main result of [10] is a rather immediate consequence of Theorem 3 (cf. proof of Proposition 9). Moreover, we extend the positive answer that holds for abelian pairs $(G, 1)$, $|G|$ divisible by 6, to a class of "metabelian" pairs (G, H). This extension is a consequence of Proposition 10, which says that $\mathbb{Q}$-admissible sets belonging to a "cyclic" pair $(F, 1)$ remain $\mathbb{Q}$-admissible for pairs (FH, H), where FH is a certain type of semidirect product.

Section 4 deals with another class of K-multiplicity-free pairs, so-called *K-trivial* pairs. They correspond to polynomials f which admit no (additive) relations except

$$c(x_1 + \ldots + x_n) = 0, \qquad c \in K \setminus \{0\}.$$

In [11] we observed that f has this property only if G acts primitively on $x_1, \ldots, x_n$, whereas double transitivity is sufficient for K-triviality. Consequently, the really interesting K-trivial pairs are those corresponding to the primitive but not doubly transitive case. We display two types of examples of this kind: Proposition 13 concerns polynomials f of prime power degree q whose Galois group G is an affine group $\mathrm{AGL}(1, q)$. This type generalizes the class of all irreducible solvable polynomials f of prime degree, whose "triviality" has been known for a long time. The second type comprises certain groups $G = \mathrm{PSL}(2, 2^p)$ (p a prime number; Proposition 14). Both types can be extended to *automorphism groups* of the groups G in question (Proposition 15).

If the pair (G, H) is K-multiplicity-free, the mere use of group characters leads to a satisfactory theory of K-admissible sets (or modules). In the main, this statement remains true for the class of *K-tame* pairs, which contains all K-multiplicity-free pairs. It is no longer true, however, for the remaining pairs (G, H), which we call *K-wild*. The wild case is at least as important as the tame one, since it is likely to occur even more frequently. For instance, the symmetric group S_3 (of order 6) appears in the wild pair $(S_3, 1)$ (which corresponds to an irreducible polynomial f of degree $n = 6$ with Galois group S_3). Therefore, finding a simple criterion for wildness appears as a matter of priority. Although we cannot present a completely satisfactory solution of this task, the main result of Section 5 (Theorem 4) is not far from it. In particular, it yields some quite simple sufficient conditions for wildness (cf. Corollary 1 to Proposition 17 and Proposition 18).

At this point we should say that not all K-admissible modules deserve the same interest: Only the *maximal* ones are really important. A complete

description of all maximal K-admissible modules seems to be possible for the class of K-wild pairs which we study in Section 6. This description is based on Theorem 5, which gives, roughly speaking, a bijective parametrization of a certain infinite series of modules by points of a projective space. The main application of this theorem concerns the wild pairs $(D_{2p}, 1)$, where D_{2p} means the dihedral group of order $2p$, p a prime number (Example 8). However, the desired survey of all maximal K-admissible modules can be made completely explicit only if one knows the relevant *representation* of G, not only its character. We attain this degree of explicitness in the case of the pairs $(D_{2p}, 1)$, $p = 3, 5$. As a by-product, we show that the above-mentioned relations (4) are possible for $p = 3$ but impossible for $p = 5$. This fact deserves some interest with regard to Theorem 5 of [7], which gives restrictions for pairs (G, H) permitting relations (4): The pairs $(D_6, 1)$ and $(D_{10}, 1)$ are among the simplest covered by this theorem.

In order to make the present paper reasonably self-contained, we have to repeat some concepts and results of [11]—so there is a small overlap between our papers. We need quite a number of definitions that are specific to the topic. The most important ones have been highlighted and numbered consecutively, in order to facilitate recovering them where necessary. In these definitions we use the simple conjunction "if" instead of unwieldy "if, and only if". Our notation of finite groups is fairly standard (cf. [5]).

The basic structure of the theory of linear relations can be understood without reading each line of this rather long paper. We hope, for example, that the sense of our hierarchy of notions becomes clear from Sections 1, 2, and 5. The remaining sections concern (important) special cases which illustrate this hierarchy.

1. A common framework for both kinds of relations. Throughout this section we need not assume $\mathrm{char}(K) = 0$. We rephrase our main problem in a slightly different way. Let L be a finite Galois extension of K with Galois group $G = \mathrm{Gal}(L/K)$ and F an intermediate field whose pointwise stabilizer is $H = \mathrm{Gal}(L/F)$. Let f run through all irreducible polynomials having a root (say x_f) that generates F over K (so $F = K(x_f)$). The question to be considered is what kind of linear (i.e., additive or multiplicative) relations can exist between the roots of such an f. In general, some of these polynomials f may have nontrivial linear relations between their roots whilst others do not. For this reason it seems desirable to work with a concept of "possible relations" that does not depend on the choice of f. We shall describe this concept now.

We start with the *group ring* $R[G]$ of the Galois group G over some commutative ring R (usually one of $\mathbb{Z}$, $\mathbb{Q}$, or K). Since $(s : s \in G)$ is an R-basis of $R[G]$, the elements of $R[G]$ take the shape

$$\lambda = \sum_{s \in G} l_s s, \qquad l_s \in R. \tag{5}$$

The *additive group* of L is a left $K[G]$-module in the usual way, whereas the multiplicative group $L^\times = L \setminus \{0\}$ is a left $\mathbb{Z}[G]$-module. In both cases a group element $s \in G$ acts on $y \in L$ (or $L^\times$, respectively), by $sy = s(y)$. We consider the *additive* case first.

Let $G/H = \{\bar{s} : s \in G\}$ be the set of left cosets $\bar{s} = \{st : t \in H\} = sH$ of the subgroup H in G. By $K[G/H]$ we denote a K-vector space whose "canonical" basis is the system $(\bar{s} : \bar{s} \in G/H)$ of cosets—so the construction of $K[G/H]$ is quite similar to that of the group ring. Therefore, the elements of $K[G/H]$ can be written

$$\alpha = \sum_{\bar{s} \in G/H} a_{\bar{s}}\, \bar{s}, \qquad a_{\bar{s}} \in K, \tag{6}$$

in a unique way. Further, $K[G/H]$ becomes a left $K[G]$-module by virtue of the scalar multiplication

$$\lambda \bar{t} = \sum_{s \in G} l_s \overline{st},$$

where λ is as in (5) and $\bar{t} \in G/H$.

The $K[G]$-module $K[G/H]$ is a familiar object in the theory of permutation groups: If one considers G as a permutation group on G/H (acting via $s\bar{t} = \overline{st}$), one usually attaches $K[G/H]$ to this permutation representation of G (cf. [12], p. 597).

Let x be an element of L whose stabilizer $G_x = \{s \in G : sx = x\}$ equals H (thus, x generates the intermediate field F over K, or, in other words, $x = x_f$ for one of the polynomials f in question). Consider the $K[G]$-module generated by x, i.e., $K[G]x = \{\lambda x : \lambda \in K[G]\}$. Since $G_x = H$, the $K[G]$-linear map

$$K[G/H] \to K[G]x : \alpha \mapsto \alpha x = \sum_{\bar{s} \in G/H} a_{\bar{s}}\, sx \tag{7}$$

(α as in (6), $sx = s(x)$) is well defined and surjective. We say that an element $\alpha \in K[G/H]$ is an *additive relation* of x if, and only if, $\alpha x = 0$.

It is obvious that this concept of additive relations is consistent with that of (1): If $x = x_f$, then $(\bar{s}x : \bar{s} \in G/H)$ is a certain arrangement of the roots of f and $\alpha x = 0$ means that the respective linear equation (with coefficients in K) holds between these roots.

Definition 1. Let L be a finite Galois extension of K with Galois group G and H a subgroup of G. A subset M of $K[G/H]$ is called *admissible* (*in the additive sense*, to be precise) if there is an element $x \in L$ with $G_x = H$

such that all $\alpha \in M$ are additive relations of x. An element α of $K[G/H]$ is called admissible in this sense if the set $\{\alpha\}$ is admissible.

REMARKS. 1. Let $x \in L$ be as above. In general, the Galois extension L of K that contains $F = K(x)$ is not uniquely determined. However, it is natural (and sufficient for most purposes) to choose the smallest possible L, namely, the *normal closure* of F. This is equivalent to saying that $G = \mathrm{Gal}(L/K)$ acts *faithfully* on G/H.

2. A set M is admissible if, and only if, the $K[G]$-module ${}_{K[G]}\langle M\rangle$ generated by M is admissible. Suppose, for the moment, that the group ring $K[G]$ is semisimple (in other words, $\mathrm{char}(K)$ does not divide the order $|G|$ of the group G). Then all $K[G]$-submodules of $K[G/H]$ are cyclic, i.e., of the shape $K[G]\alpha$ for some $\alpha \in K[G/H]$. Consequently, the theoretical behaviour of admissible sets is not different from the behaviour of admissible elements: One can always replace the set M by a single generator α of the module ${}_{K[G]}\langle M\rangle$. In practice, however, it may be toilsome to find such a generator. For this reason it is sometimes advisable to work with admissible *sets*, not only elements.

Note that the concept of additive admissibility depends on the field L so far. The next proposition shows that it can be enounced in terms of the group ring $K[G]$ and the $K[G]$-module $K[G/H]$ only. We consider an element $\mu \in K[G]$ whose stabilizer $G_\mu = \{s \in G : s\mu = \mu\}$ equals H. If μ has this property, the definition $\bar{s}\mu = s\mu$ makes sense for each coset $\bar{s} = sH$. This is even true if only $G_\mu \supseteq H$. Hence we obtain an obvious analogue of the mapping (7), namely, a $K[G]$-linear map

$$K[G/H] \to K[G]\mu : \alpha \mapsto \alpha\mu = \sum_{\bar{s}\in G/H} a_{\bar{s}} s\mu$$

(α as in (6)). For a subset M of $K[G/H]$ and μ as above, let $M\mu$ denote the set $\{\alpha\mu : \alpha \in M\}$. Instead of $M\mu \subseteq \{0\}$ we simply write $M\mu = 0$ (so we disregard the case $M = \emptyset$). The notations Mx and $Mx = 0$ have the analogous meaning for an element $x \in L$ with $G_x \supseteq H$.

PROPOSITION 1. *Let G be the Galois group of a finite Galois extension L of K and H a subgroup of G. A subset M of $K[G/H]$ is admissible in the additive sense if, and only if, there is an element $\mu \in K[G]$ with $G_\mu = H$ such that $M\mu = 0$.*

Proof. Let $x \in L$ be such that $G_x = H$ and $Mx = 0$. Since $K[G]$ is a semisimple ring and $K[G]x$ a cyclic $K[G]$-module, there is a left ideal $\mathfrak{a}$ in $K[G]$ that is $K[G]$-isomorphic to $K[G]x$. Consider a $K[G]$-linear isomorphism $\mathfrak{a} \to K[G]x$ and take the element $\mu \in \mathfrak{a}$ that is mapped onto x. Then $G_\mu = H$ and $M\mu = 0$. Conversely, let $\mu \in K[G]$ be such that $G_\mu = H$ and $M\mu = 0$. By the normal basis theorem, there exists an element $y \in L$

such that the $K[G]$-linear map $K[G] \to K[G]y : \lambda \mapsto \lambda y$ is an isomorphism (in view of the requirements of the multiplicative case, we note that we make no use of the fact that $K[G]y = L$). Put $x = \mu y$. Then x has the desired property. ∎

The proof of Proposition 1 becomes a bit simpler if one uses the normal basis theorem to show *both* directions. The advantage of the above version consists in the fact that it can be adapted to the *multiplicative* situation, where we have only a weak form of the normal basis theorem at hand. The proposition shows that the concept of additive admissibility is of a purely group-theoretical nature and, thus, can be rephrased in terms of pairs of abstract groups (G, H), H being a subgroup of G. Our next aim is a similar result for the *multiplicative* case.

For this purpose we write the multiplicative group $L^\times$ *additively*. In order to free ourselves from torsion elements, we go over to the tensor product $L^\times \otimes_{\mathbb{Z}} \mathbb{Q}$, for which we simply write $L^\times \otimes \mathbb{Q}$. This kind of tensoring is quite common in the Galois module theory of unit groups (cf. also [7]). The "typical" elements of $L^\times \otimes \mathbb{Q}$ have the shape $x \otimes c$, $x \in L^\times$, $c \in \mathbb{Q}$. We consider $L^\times$ as a left $\mathbb{Z}[G]$-module in the usual way and obtain a canonical $\mathbb{Z}[G]$-linear map

$$L^\times \to L^\times \otimes \mathbb{Q} : x \mapsto x \otimes 1.$$

The kernel of this map is the torsion group of $L^\times$, i.e., the group of roots of unity in L. Obviously, $L^\times \otimes \mathbb{Q}$ is a $\mathbb{Q}[G]$-module now. For any element $u \in L^\times \otimes \mathbb{Q}$ with $G_u = H$, the analogue of (7), i.e., the $\mathbb{Q}[G]$-linear map

$$\mathbb{Q}[G/H] \to \mathbb{Q}[G]u : \alpha \mapsto \alpha u$$

is well defined.

Definition 2. In the above setting, a subset M of $\mathbb{Q}[G/H]$ is said to be *admissible in the multiplicative sense* if there is an element $u \in L^\times \otimes \mathbb{Q}$ with $G_u = H$ such that $Mu = 0$.

Of course, the reader may ask whether this definition is suitable for the multiplicative case. We answer this question by the following proposition, where we use, for the last time in this paper, the multiplicative notation for $L^\times$.

Proposition 2. *Suppose that K contains only finitely many roots of unity. A subset M of $\mathbb{Z}[G/H]$ is admissible in the multiplicative sense if, and only if, there exists an element $x \in L^\times$ with the following properties*:

(a) $G_x = H$.

(b) *Each element of M is a multiplicative relation between the conjugates*

of x; more precisely, if

$$\alpha = \sum_{\bar{s}\in G/H} a_{\bar{s}}\,\bar{s}, \qquad a_{\bar{s}} \in \mathbb{Z},$$

is in M, then

$$\prod_{\bar{s}\in G/H} s(x)^{a_{\bar{s}}} = 1.$$

(c) *If sx/x is a root of unity for some $s \in G$, then $sx = x$.*

Proof. We return to the additive notation of $L^\times$. First suppose there is an element $x \in L^\times$ with properties (a)–(c). Put $u = x \otimes 1$. Let $s \in G$ be such that $su = u$. This means that $(s-1)x$ is a torsion element of $L^\times$, hence $sx = x$, by (c), and $s \in H$, by (a). On the other hand, each $s \in H$ fixes x and thus u. Moreover, (b) yields $Mu = 0$.

Conversely, let $u \in L^\times \otimes \mathbb{Q}$ be such that $G_u = H$ and $\alpha u = 0$ for all $\alpha \in M$. The element u is a finite sum of "typical" elements $x_k \otimes r_k$, $x_k \in L^\times$, $r_k \in \mathbb{Q}$. Take an integer $m > 0$ such that mr_k is in $\mathbb{Z}$ for all indices k. Since L is a finite extension of K, it contains only finitely many roots of unity, so there is an integer $n > 0$ such that $nw = 0$ for each torsion element w of $L^\times$. Put $y = \sum (mr_k)x_k \in L^\times$ and $x = ny$. Then $y \otimes 1 = mu$ and $x \otimes 1 = nmu$. If $s \in G$ stabilizes x, it stabilizes nmu and hence u itself, because $L^\times \otimes \mathbb{Q}$ is torsion-free. On the other hand, each $s \in H$ stabilizes u, hence mu, so $(s-1)y$ is a torsion element of $L^\times$; this implies $0 = n(s-1)y = (s-1)x$ and $s \in G_x$. The remaining properties can be checked in a similar way: for instance, αy is a torsion element for each $\alpha \in M$, and so $n\alpha y = \alpha x = 0$. ∎

Proposition 2 shows that the concept of multiplicative admissibility comprises almost all possible multiplicative relations—the only exceptions are those occurring, exclusively, between conjugates that differ by a mere root of unity (such as $n(s-1)$, $s \in G \smallsetminus G_x$, $n \in \mathbb{Z}$, $n \neq 0$). This type of relations has been investigated in [7] (e.g., Lemma 3, ibid.). In the remainder of this section we prove a multiplicative analogue of Proposition 1 under certain assumptions about K and L. We start with

Proposition 3. *Let L be a finite Galois extension of the field K with Galois group G, H a subgroup of G, and M a subset of $\mathbb{Q}[G/H]$. If M is admissible in the multiplicative sense, then there is an element $\mu \in \mathbb{Q}[G]$ with stabilizer $G_\mu = H$ such that $M\mu = 0$.*

Proof. One imitates the first part of the proof of Proposition 1: each element $u \in L^\times \otimes \mathbb{Q}$ with $G_u = H$ and $Mu = 0$ produces an appropriate element $\mu \in \mathbb{Q}[G]$ via a $\mathbb{Q}[G]$-linear isomorphism $\mathfrak{a} \to \mathbb{Q}[G]u$ of a left ideal $\mathfrak{a}$ of $\mathbb{Q}[G]$ onto $\mathbb{Q}[G]u$. ∎

The next proposition is a sort of converse of Proposition 3. It is based on the validity of a weak multiplicative analogue of the normal basis theorem, which guarantees the existence of a $\mathbb{Q}[G]$-submodule of $L^\times \otimes \mathbb{Q}$ that is isomorphic to $\mathbb{Q}[G]$. Note, however, that $L^\times \otimes \mathbb{Q}$ *itself* cannot be isomorphic to $\mathbb{Q}[G]$ in general; for instance, if L is an algebraic number field, then $L^\times \otimes \mathbb{Q}$ is not even finite-dimensional as a $\mathbb{Q}$-vector space.

PROPOSITION 4. *In the situation of Proposition* 3, *suppose there is an element $v \in L^\times \otimes \mathbb{Q}$ such that*

$$\mathbb{Q}[G] \to \mathbb{Q}[G]v : \lambda \mapsto \lambda v$$

is a $\mathbb{Q}[G]$-linear isomorphism. Let M be a subset of $\mathbb{Q}[G/H]$ and $\mu \in \mathbb{Q}[G]$ be such that $G_\mu = H$ and $M\mu = 0$. Then M is admissible in the multiplicative sense.

Proof. Put $u = \mu v$. Then $G_u = G_\mu = H$ and $Mu = 0$. ∎

In [10] it was shown that an element v with the above property exists in the case of the ground field $K = \mathbb{Q}$. We think that the existence of such elements is known for much more general fields but have no suitable reference at hand. Therefore, we include the following proposition.

PROPOSITION 5. *Let L be a finite Galois extension of the field K with Galois group G. Suppose there is a place $\mathfrak{p}$ of K that splits completely in L. Then there is an element $x \in L^\times$ such that $v = x \otimes 1$ defines a $\mathbb{Q}[G]$-linear isomorphism*

$$\mathbb{Q}[G] \to \mathbb{Q}[G]v : \lambda \mapsto \lambda v.$$

Proof. Let $\mathfrak{p}$ be a place of K that splits completely in L. For any place $\mathfrak{P}$ of L lying above $\mathfrak{p}$ let $v_\mathfrak{P}$ denote the corresponding valuation of $L^\times$. Now choose one particular $\mathfrak{P}$ of this kind. Since $\mathfrak{p}$ splits completely, all places $s(\mathfrak{P})$, $s \in G$, are different. By the approximation theorem, there is an element $x \in L^\times$ such that $v_\mathfrak{P}(x) \neq 0$, whereas $v_{s(\mathfrak{P})}(x) = 0$ for all $s \in G$, $s \neq 1$. Thus x has the desired property: Let $\lambda = \sum_s l_s s$ be in $\mathbb{Z}[G]$ and $t \in G$ arbitrary. Then

$$v_{t(\mathfrak{P})}(\lambda x) = \sum_{s \in G} l_s v_{t(\mathfrak{P})}(s(x)) = \sum_s l_s v_{s^{-1}t(\mathfrak{P})}(x) = l_t v_\mathfrak{P}(x).$$

Hence λx is a root of unity only if $l_t = 0$ for all $t \in G$. ∎

The existence of a place $\mathfrak{p}$ with the above property is known, e.g., for global fields K, in particular, for algebraic number fields (by the Chebotarev density theorem, cf. [4], p. 165). Of course, global fields contain only finitely many roots of unity (as was required in Proposition 2). Accordingly, we may say that multiplicative admissibility is, for these ground fields K, an adequate characterization of sets of multiplicative relations. Furthermore,

the concepts of additive and of multiplicative admissibility are very similar. The only difference lies in the scalars: Whereas an admissible set in the multiplicative sense belongs to $\mathbb{Q}[G/H]$, the additive analogue is in $K[G/H]$. Their formal properties, however, are the same and do not depend on the specific Galois extension L of K but only on the respective module structure of $\mathbb{Q}[G/H]$ and $K[G/H]$. On adopting the necessary notations for *arbitrary* pairs (G, H) of finite groups G and subgroups H, we arrive at

DEFINITION 3. Let G be a finite group, H a subgroup of G, and K a field. A subset M of $K[G/H]$ is said to be *K-admissible* if there is an element $\mu \in K[G]$ with $G_\mu = H$ such that $M\mu = 0$. An element α of $K[G/H]$ is said to be K-admissible if $\{\alpha\}$ is K-admissible.

REMARK. Some authors use the notion *relation* in a slightly more general sense, inasmuch as they only require that the right sides of (1), (2) are in K (not necessarily $= 0$, e.g., [1], [7]). One may say that this type of relations is covered by the concept of K-admissibility, too. Indeed, let $\mathrm{char}(K)$ be prime to $|G|$ and M a subset of $K[G/H]$. Suppose that $\mu \in K[G]$ is such that $G_\mu = H$ and that the elements $\alpha\mu$, $\alpha \in M$, remain fixed under all $s \in G$. Put $\varepsilon = |G|^{-1} \sum_{s\in G} s$ and $\mu' = \mu - \varepsilon\mu$. Then $G_{\mu'} = H$ and, since $\varepsilon\alpha\mu = \alpha\mu = \alpha\varepsilon\mu$, we have $\alpha\mu' = 0$ for all $\alpha \in M$.

2. The role of character theory. For the sake of simplicity we assume $\mathrm{char}(K) = 0$ in what follows, though several results remain valid if only the group ring $K[G]$ is semisimple (i.e., $\mathrm{char}(K)$ is prime to $|G|$). Our main concern will be the study of K-admissible subsets of $K[G/H]$. We have seen above that it suffices to consider K-admissible *modules*, i.e., $K[G]$-submodules of $K[G/H]$ that are themselves K-admissible subsets of $K[G/H]$ (cf. Remark 2 on Definition 1). In what follows "module" or "submodule" means "$K[G]$-module" or "$K[G]$-submodule", respectively. The notation ${}_{K[G]}\langle \ldots \rangle$ denotes the $K[G]$-module generated by the bracketed entries.

Throughout this section we fix a pair of groups (G, H), H being a subgroup of G (instead, one might say that we fix a certain transitive permutation representation of the group G, cf. [8], p. 17). Such a pair is called *faithful*, *primitive*, *imprimitive*, *doubly transitive*, etc., when the permutation representation of G on G/H has the respective property. We write $H' > H$ or $H < H'$ if H' is a subgroup of G, $H' \supseteq H$, and $H' \neq H$. Note that one need not distinguish *permutation isomorphic* pairs: Any group isomorphism $G \to \widetilde{G}$ that carries the subgroup H to $\widetilde{H}$ transports the whole theory from (G, H) to $(\widetilde{G}, \widetilde{H})$.

We start with a fundamental type of module (introduced in [11] already). Let H' be a subgroup of G containing H. Consider the canonical $K[G]$-linear

surjection

$$\varrho : K[G/H] \to K[G/H'] : \overline{s} \mapsto \overline{s}, \tag{8}$$

and in particular, its kernel

$$U(H') = \{\alpha \in K[G/H] : \varrho(\alpha) = 0\}.$$

It is not hard to see that

$$U(H') = {}_{K[G]}\langle \overline{s} - \overline{1} : s \in H' \rangle. \tag{9}$$

The following theorem is the cornerstone of our further investigation. In the main it is identical with Proposition 1 of [11]. We think, however, that the proof given in [11] is too short, so we include a full-length version of this proof here.

THEOREM 1. *A $K[G]$-submodule V of $K[G/H]$ is K-admissible if, and only if, V does not contain $U(H')$ for any group $H' > H$.*

REMARK. The right-hand condition of Theorem 1 can also be enounced in the following way: *For every $s \in G \setminus H$, $\overline{s} - \overline{1}$ is not in V.* In order to see the equivalence of these conditions, one shows that $\overline{s} - \overline{1} \in V$ implies $\overline{s'} - \overline{1} \in V$ for all $s' \in \langle \{s\} \cup H \rangle$; the proof of the last mentioned fact is based on relations like $\overline{s^k} - \overline{1} = \lambda(\overline{s} - \overline{1})$, $k \geq 1$, $\lambda \in K[G]$, and $\overline{s^j t s^k} - \overline{1} = s^j t(\overline{s^k} - \overline{1}) + (\overline{s^j} - \overline{1})$, $t \in H$. Although the condition of the theorem looks more complicated, it fits better to the character-theoretical approach we are going to describe.

Proof (of Theorem 1). Let $\mu \in K[G]$ be such that $G_\mu = H$ and $V\mu = 0$. Let H' be a subgroup of G with $H' > H$ and $U(H') \subseteq V$. Take an element $s \in H', s \notin H$. Then $\overline{s} - \overline{1}$ is in $U(H')$. Since $U(H') \subseteq V$, we have $(s-1)\mu = 0$, which contradicts $G_\mu = H$.

Conversely, suppose that, for all $H' > H$, $U(H')$ is not contained in V. The canonical map $\varrho : K[G] \to K[G/H] : s \mapsto \overline{s}$ is of the type considered in (8). Let $\mathfrak{a} = \varrho^{-1}(V)$ be the inverse image of V. By semisimplicity, the left ideal $\mathfrak{a}$ is generated by an idempotent element ε. Put $\mu = 1 - \varepsilon$. If s is in H, then $s - 1$ is in the kernel of ϱ and hence in $\mathfrak{a} = K[G]\varepsilon$. Therefore, $s - 1 = (s-1)\varepsilon$ and $(s-1)\mu = 0$. This shows $H \subseteq G_\mu$. Next take an arbitrary element $s \in G_\mu$. Then $(s-1)\mu = 0$, i.e., $s - 1 = (s-1)\varepsilon$ and $s - 1 \in \mathfrak{a}$. In particular, V contains ${}_{K[G]}\langle \overline{s} - \overline{1} : s \in G_\mu \rangle = U(G_\mu)$. It follows that $G_\mu = H$. Finally, for an element $\alpha \in V$, let $\lambda \in \mathfrak{a}$ be such that $\varrho(\lambda) = \alpha$. Then $\alpha\mu = \lambda\mu = 0$. ∎

A subgroup H' of G with $H' > H$ is called *minimal* with this property if there is no relation like $H' > H'' > H$. Of course, there are only finitely many distinct minimal subgroups $H' > H$, which we denote by $H_1, \ldots, H_m$ in the remainder of this section (observe that "distinct" means "distinct in the set-theoretical sense" but possibly isomorphic or even conjugate). For

instance, if (G,H) is primitive, then $m=1$ and $H_1=G$. On observing that $U(H')$ is contained in $U(H'')$ whenever $H'\subseteq H''$, we obtain the important

Corollary. *A submodule V of $K[G/H]$ is K-admissible if, and only if, V contains none of the modules $U(H_1),\dots,U(H_m)$.*

Theorem 1 also yields the less trivial direction of the following proposition. Consider an extension field K' of K, so $K[G]\subseteq K'[G]$, $K[G/H]\subseteq K'[G/H]$.

Proposition 6. *A subset M of $K[G/H]$ is K'-admissible if, and only if, it is K-admissible.*

P r o o f. If M is K-admissible, there is an element $\mu\in K[G]$ with $G_\mu=H$ and $M\mu=0$. Since μ also lies in $K'[G]$, M is K'-admissible. Conversely, if M is not K-admissible, then there is an $s\in G\setminus H$ such that $\overline{s}-\overline{1}$ is in ${}_{K[G]}\langle M\rangle$ (cf. (9) and the above remark). But then $\overline{s}-\overline{1}$ is also in ${}_{K'[G]}\langle M\rangle$. ∎

We start using *characters* now, in particular, absolutely irreducible (i.e., irreducible complex) characters of G. They are known for many finite groups (cf., e.g., [5]). Let $\overline{K}$ be a character-theoretic splitting field of G over K, for instance, $\overline{K}=K(\zeta)$, ζ a primitive root of unity of order $|G|$. We consider each absolutely irreducible character χ as a character over $\overline{K}$. There is a uniquely determined central idempotent of the group ring $\overline{K}[G]$ connected with χ, namely,

$$\varepsilon_\chi=\chi(1)|G|^{-1}\sum_{s\in G}\chi(s^{-1})s.$$

Moreover, there is exactly one K-irreducible character $\widehat{\chi}$ containing χ, which is obtained as follows (cf. [12], p. 546): Let $\chi_1=\chi,\chi_2,\dots,\chi_c$ be the distinct K-conjugate characters of χ (so these characters form the set $\{\sigma\circ\chi:\sigma\in\mathrm{Gal}(\overline{K}/K)\}$). Then

$$\widehat{\chi}=\kappa(\chi_1+\ldots+\chi_c), \tag{10}$$

the natural number κ being the Schur index of χ. Whereas the computation of κ is, in general, not a trivial task, one easily finds the central idempotent $\varepsilon_{\widehat{\chi}}\in K[G]$ belonging to $\widehat{\chi}$: Simply put $\widetilde{\chi}=\chi_1+\ldots+\chi_c$. Then $\widetilde{\chi}$ is a character with values in K (however, not a character *defined* over K unless $\kappa=1$) and

$$\varepsilon_{\widehat{\chi}}=\chi(1)|G|^{-1}\sum_{s\in G}\widetilde{\chi}(s^{-1})s.$$

This is the same as saying $\varepsilon_{\widehat{\chi}}=\varepsilon_{\chi_1}+\ldots+\varepsilon_{\chi_c}$ (cf. [6], p. 734, Theorem 74.4). For the time being, we write $\psi=\widehat{\chi}$, in particular, $\varepsilon_\psi=\varepsilon_{\widehat{\chi}}$. Consider

$$I_\psi=\varepsilon_\psi K[G/H]=\{\varepsilon_\psi\alpha:\alpha\in K[G/H]\}. \tag{11}$$

Since ε_ψ is central, I_ψ is a $K[G]$-module, namely, the cyclic module

$$I_\psi = {}_{K[G]}\langle \varepsilon_\psi \overline{1} \rangle = K[G]\varepsilon_\psi \overline{1}. \tag{12}$$

In fact, I_ψ is the *isotypical component* of ψ, i.e., the sum of all (necessarily simple) submodules of $K[G/H]$ whose character is ψ. We obtain

$$K[G/H] = \bigoplus_\psi I_\psi, \tag{13}$$

with ψ running through *all* K-irreducible characters of G.

Definition 4. A submodule V of $K[G/H]$ is called *isotypically closed* (or simply *closed*) if it contains the whole isotypical component I_ψ as soon as $V \cap I_\psi \neq 0$.

We shall show that the above data suffices to describe *all isotypically closed K-admissible* modules. To this end we consider the character of the $K[G]$-module $K[G/H]$. This character is induced on G by the trivial character 1 of the subgroup H and, consequently, denoted by 1_H^G. We need the absolutely irreducible characters χ occurring in 1_H^G, namely, the set

$$\mathcal{X} = \{\chi : \langle \chi, 1_H^G \rangle \neq 0\},$$

where $\langle\ ,\ \rangle$ means the usual scalar product of characters. It is fairly easy to check whether some χ belongs to $\mathcal{X}$. In fact, by Frobenius reciprocity,

$$\langle \chi, 1_H^G \rangle = |H|^{-1} \sum_{s \in H} \chi(s); \tag{14}$$

and so $\langle \chi, 1_H^G \rangle = 0$ if, and only if, $\sum_{s\in H} \chi(s) = 0$. The knowledge of $\mathcal{X}$ is equivalent to the knowledge of the *nonzero* components I_ψ occurring in the decomposition (13) of $K[G/H]$. More precisely, if $\widehat{\chi}$ is attached to χ in the sense of (10), its component $I_{\widehat{\chi}}$ is nonzero if, and only if, $\chi \in \mathcal{X}$.

If χ is in $\mathcal{X}$, all of its K-conjugate characters $\chi_1 = \chi, \ldots, \chi_c$ also belong to $\mathcal{X}$. For this reason we go over to a *reduced set* $\mathcal{X}_K$, which contains exactly one member of each class of K-conjugate characters contained in $\mathcal{X}$. Then

$$K[G/H] = \bigoplus_{\chi \in \mathcal{X}_K} I_{\widehat{\chi}}.$$

In this direct sum all summands are nonzero, i.e., they contain at least one simple $K[G]$-module. For a subset $\mathcal{Y}$ of $\mathcal{X}_K$ we define

$$\varepsilon_{\mathcal{Y}} = \sum_{\chi \in \mathcal{Y}} \varepsilon_{\widehat{\chi}} \quad \text{and} \quad I_{\mathcal{Y}} = \bigoplus_{\chi \in \mathcal{Y}} I_{\widehat{\chi}}.$$

Then $I_{\mathcal{Y}}$ is isotypically closed and

$$I_{\mathcal{Y}} = \varepsilon_{\mathcal{Y}} K[G/H] = K[G]\varepsilon_{\mathcal{Y}} \overline{1}$$

(this is the exact analogue of (11) and (12)). In this way we obtain *all* closed submodules of $K[G/H]$:

PROPOSITION 7. *The map $\mathcal{Y} \mapsto I_{\mathcal{Y}}$ defines a bijection*

$$\{\mathcal{Y} : \mathcal{Y} \subseteq \mathcal{X}_K\} \to \{V : V \text{ a closed submodule of } K[G/H]\}.$$

This bijection preserves the inclusion, i.e., $\mathcal{Y} \subseteq \mathcal{Z}$ is equivalent to $I_{\mathcal{Y}} \subseteq I_{\mathcal{Z}}$.

In the sequel it will sometimes be advantageous to consider the *complementary* module $J_{\mathcal{Y}} = I_{\mathcal{X}_K \setminus \mathcal{Y}}$ of $I_{\mathcal{Y}}$ instead of $I_{\mathcal{Y}}$ itself. On the one hand, we have $J_{\mathcal{Y}} = K[G]\beta_{\mathcal{Y}}$, where

$$\beta_{\mathcal{Y}} = \varepsilon_{\mathcal{X}_K \setminus \mathcal{Y}} \overline{1} \tag{15}$$

arises from $\overline{1} \in K[G/H]$ by application of the "complementary" idempotent of $\varepsilon_{\mathcal{Y}}$. On the other hand,

$$J_{\mathcal{Y}} = \{\alpha \in K[G/H] : \varepsilon_{\mathcal{Y}} \alpha = 0\}. \tag{16}$$

This means that one can *test* whether a given element α belongs to $J_{\mathcal{Y}}$ by checking whether $\varepsilon_{\mathcal{Y}} \alpha = 0$.

Next we look at the character of the module $U(H')$ for a subgroup H' of G, $H' > H$. Since $U(H')$ is the kernel of the surjection (8), its character must be $1_H^G - 1_{H'}^G$. An absolutely irreducible character χ occurs in $1_H^G - 1_{H'}^G$ if, and only if,

$$\langle \chi, 1_{H'}^G \rangle < \langle \chi, 1_H^G \rangle. \tag{17}$$

Combined with (14), this criterion works well in practice. Put

$$\mathcal{X}_K(H') = \{\chi \in \mathcal{X}_K : \chi \text{ satisfies (17)}\}.$$

Let χ be in $\mathcal{X}_K$. Then $I_{\widehat{\chi}} \cap U(H') \neq 0$ if, and only if, $\chi \in \mathcal{X}_K(H')$. In other words, the module $I_{\mathcal{X}_K(H')}$ is the smallest *closed* module that contains $U(H')$.

DEFINITION 5. As above, let $H_1, \ldots, H_m$ be the minimal groups $> H$. A subset $\mathcal{Z}$ of $\mathcal{X}_K$ is called *generic* if

$$\mathcal{Z} \cap \mathcal{X}_K(H_j) \neq \emptyset$$

for all $j = 1, \ldots, m$. If $\mathcal{Z}$ is *minimal* with this property, we call $\mathcal{Z}$ a *selection* of $\mathcal{X}_K$ (more precisely, of $\mathcal{X}_K(H_1), \ldots, \mathcal{X}_K(H_m)$).

The name "generic" comes from the special case of an abelian group G (cf. Proposition 8). The importance of generic sets becomes clear from the next theorem; the meaning of "selections" will be discussed later.

THEOREM 2. *The map $\mathcal{Z} \mapsto J_{\mathcal{Z}}$ defines a bijection between the set of generic subsets $\mathcal{Z}$ of $\mathcal{X}_K$ and the set of isotypically closed K-admissible submodules $V = J_{\mathcal{Z}}$ of $K[G/H]$. This bijection inverts the inclusion.*

P r o o f. In view of Proposition 7 we have to show that the closed K-admissible submodules V of $K[G/H]$ are exactly those of the shape $J_{\mathcal{Z}}$, $\mathcal{Z}$ generic. Let $V = I_{\mathcal{Y}}$, $\mathcal{Y} \subseteq \mathcal{X}_K$, be closed. Put $\mathcal{Z} = \mathcal{X}_K \setminus \mathcal{Y}$, so $V = J_{\mathcal{Z}}$. Let χ be in $\mathcal{Z} \cap \mathcal{X}_K(H_j)$ for some $j \in \{1, \ldots, m\}$. Then $I_{\widehat{\chi}} \cap U(H_j) \neq 0$. On the other hand, $I_{\widehat{\chi}} \cap I_{\mathcal{Y}} = I_{\widehat{\chi}} \cap V = 0$, since $\chi \notin \mathcal{Y}$. So $U(H_j) \subseteq V$ is impossible. Accordingly, V is K-admissible if only $\mathcal{Z}$ is generic. Conversely, if $\mathcal{Z} \cap \mathcal{X}_K(H_j) = \emptyset$ for some j, then $\mathcal{X}_K(H_j) \subseteq \mathcal{Y}$ and

$$U(H_j) \subseteq I_{\mathcal{X}_K(H_j)} \subseteq I_{\mathcal{Y}} = V,$$

so V is not K-admissible. ∎

The character-theoretic equivalent of the decomposition (13) can be written

$$1_H^G = \sum_{\psi} n_\psi \psi. \tag{18}$$

Here ψ runs through all K-irreducible characters of G. Further, $n_\psi \geq 1$ if $\psi = \widehat{\chi}$ for some $\chi \in \mathcal{X}_K$ and $n_\psi = 0$, otherwise. For the trivial character $\psi = 1$ we always have $n_\psi = 1$. The following definition fits into the commonly used terminology:

Definition 6. The pair (G, H) is called *K-multiplicity-free* if the numbers n_ψ of (18) take the values 0 or 1 only.

In other words, (G, H) is K-multiplicity-free if each of the nonzero isotypical components I_ψ of $K[G/H]$ is *simple* as a $K[G]$-module. In this case *all* submodules V of $K[G/H]$ are isotypically closed, so Theorem 2 gives a complete survey of *all* possible K-admissible modules. The following list of examples may convince the reader of the import of the multiplicity-free case. If no other specification is given, K may be an arbitrary field with $\mathrm{char}(K) = 0$. Note that "K'-multiplicity-free", holding for an extension field K' of K, implies "K-multiplicity-free", but not conversely. Since *faithful* pairs are the most interesting ones (cf. Remark 1 on Definition 1), we eventually say some words about the faithfulness of the respective pair.

Example 1. Let G be an *abelian* group. Then each possible pair (G, H) is K-multiplicity-free. This can be seen as follows: The set of absolutely irreducible characters of G is just the *character group*

$$\widehat{G} = \{\chi : G \to \overline{K}^\times : \chi \text{ a group homomorphism}\}$$

of G; moreover, $\mathcal{X} = \{\chi \in \widehat{G} : \ker \chi \supseteq H\}$ and $1_H^G = \sum_{\chi \in \mathcal{X}} \chi$. Note, however, that (G, H) is faithful only if $H = 1$.

Example 2. Let G be a *solvable* group and (G, H) primitive. Then G is K-multiplicity-free. This is an easy consequence of the fact that G has a transitive abelian subgroup (cf. [11], Proposition 3).

EXAMPLE 3. If G is a *simple* group, then (G, H) is faithful for every subgroup H. There is a good chance that (G, H) is K-multiplicity-free as long as the index $[G : H]$ is not too large. The following list of—mainly primitive—examples has been taken from [5] and [2].

(a) *Alternating groups* A_n. Almost all primitive pairs are K-multiplicity-free for $n \le 13$. Possible exceptions occur only for $n = 9$, $[G : H] = 840$, $n = 10$, $[G : H] = 2520$, $n = 12$, $[G : H] \ge 5775$, $n = 13$, $[G : H] \ge 1716$. For $n = 13$ there exists a pair of index 1716 that is not $\mathbb{Q}$-multiplicity-free. For $n = 11$ there is a K-multiplicity-free pair of index 2520 such that $|\mathcal{X}_K| = 5$. Thus, 1_H^G consists of five characters ψ (whose degrees may be as large as 1100) in this case.

(b) *Classical groups*. All possible primitive pairs (G, H) are K-multiplicity-free if G is one of the following groups: $\mathrm{PSL}(2, 7)$, $\mathrm{PSL}(2, 8)$, $\mathrm{PSL}(2, 16)$, $\mathrm{PSL}(2, 32)$, $\mathrm{PSL}(3, 4)$, $\mathrm{PSU}(3, 3)$, $\mathrm{PSU}(4, 2)$, $\mathrm{PSp}(6, 2)$. For instance, the group $G = \mathrm{PSp}(6, 2)$ (of order 1451520) admits, up to permutation isomorphy, 8 primitive pairs (G, H); the largest index $[G : H]$ equals 960, and 1_H^G consists of six characters ψ of degrees up to 420.

(c) *Sporadic groups*. The paper [2] contains the complete (and rather long) list of all K-multiplicity-free pairs (G, H), where G is a sporadic simple group. We just pick out two cases: For $G = M_{12}$ (the Mathieu group) there are, up to isomorphy, seven primitive K-multiplicity-free pairs with indices ≤ 220. For the sporadic Fischer group $G = \mathrm{Fi}_{23}$ there are four primitive and two imprimitive K-multiplicity-free pairs. The largest index of a primitive pair is 195747435; here $K[G/H]$ consists of 16 simple modules.

EXAMPLE 4. Let G be the symmetric group S_6 and $H < G$ a transitive subgroup. There are, up to permutation isomorphy, 13 faithful pairs (G, H) of this kind (only $H = A_6$ does not yield a faithful pair); of these, eight pairs are K-multiplicity-free (among them four primitive ones) but the remaining five not.

EXAMPLE 5. Let G be the quaternion group of order 8 and $H = 1$. Then (G, H) is $\mathbb{Q}$-multiplicity-free. This pair, however, is not K-multiplicity-free if there are elements a, b in K such that $a^2 + b^2 = -1$ (as in $K = \mathbb{Q}(\sqrt{-d})$, $d = 1, 2, 3, 5$).

We continue the discussion of Theorem 2. This theorem provides a complete survey of all closed K-admissible submodules of $K[G/H]$ in terms of generic subsets of $\mathcal{X}_K$. In general, the number of these subsets is close to $2^{|\mathcal{X}_K|}$, so it is often very large. In this case working with all closed K-admissible modules becomes an unmanageable task. Fortunately, however, not all of these modules are equally interesting. The notion of a *selection* $\mathcal{Z}$ has been introduced with special regard to this fact (cf. Definition 5):

By Theorem 2, the modules $J_{\mathcal{Z}}$ which belong to selections $\mathcal{Z}$ are *maximal* among all closed K-admissible submodules of $K[G/H]$. For most purposes it suffices to control these maximal modules. Suppose, for instance, we would like to know whether some finite set $M \subseteq K[G/H]$ is K-admissible. If we know that ${}_{K[G]}\langle M\rangle$ is closed (as is the case whenever (G,H) is K-multiplicity-free), then there is a simple test: One looks for a selection $\mathcal{Z}$ of $\mathcal{X}_K$ such that $M \subseteq J_{\mathcal{Z}}$; by (16), this is true if, and only if,

$$\varepsilon_{\mathcal{Z}}\alpha = 0 \tag{19}$$

holds for all $\alpha \in M$. If such a selection exists, then M is K-admissible, otherwise it is not. Conversely, for any selection $\mathcal{Z}$, the relevant generating element of the "large" module $J_{\mathcal{Z}}$ is given by (15), namely,

$$\beta_{\mathcal{Z}} = \varepsilon_{\mathcal{X}_K \setminus \mathcal{Z}}\overline{1} \in K[G/H]. \tag{20}$$

As a rule, it is easy to read $\varepsilon_{\mathcal{Z}}$ from a character table and, thereby, to obtain $\beta_{\mathcal{Z}}$. But the shape (20) of the "relation" $\beta_{\mathcal{Z}}$ is usually not what one desires. Rather one would like to know the coefficients $b_{\bar{s}} \in K$ occurring in

$$\beta_{\mathcal{Z}} = \sum_{\bar{s}\in G/H} b_{\bar{s}}\,\bar{s},$$

since this is, in view of Section 1, the *canonical* form of a K-admissible element (i.e., of a relation, cf. (6)). The actual computation of the coefficients $b_{\bar{s}}$, however, soon goes beyond human computing capacities—as in the following example, which is based on computer calculations.

Example 6. Let $K = \mathbb{Q}$ and $G = \mathrm{PSL}(2,11)$, which we consider (in the most natural way) as a subgroup of S_{12} (cf. [5], p. 7). This simple group has a primitive permutation representation of degree 55, defined by the subgroup $H = D_{12}$, a dihedral group of order 12. Moreover, let $F = \mathrm{ASL}(1,11)$ be the affine subgroup of order 55 in G (i.e., the stabilizer of a point under the action of G on $\{1,\dots,12\}$). The map

$$F \to G/H : s \mapsto \bar{s}$$

is bijective; therefore,

$$\mathbb{Q}[G/H] = \bigoplus_{s\in F} \mathbb{Q}\bar{s}. \tag{21}$$

The groups $F = \langle s_1, s_2\rangle$ and $H = \langle s_3, s_4\rangle$ are generated by permutations $s_1,\dots,s_4 \in S_{12}$, whose decompositions into disjoint cycles look as follows:

$$\begin{aligned}
s_1 &= (1,2,3,4,5,6,7,8,9,10,11),\\
s_2 &= (1,4,5,9,3)(2,8,10,7,6),\\
s_3 &= (1,8,9,2,3,10)(4,12,7,6,11,5),\\
s_4 &= (1,6)(2,4)(3,5)(7,8)(9,12)(10,11).
\end{aligned}$$

The absolutely irreducible characters occurring in 1_H^G can be found in [5]. We obtain

$$\mathcal{X} = \{1, \chi_1, \chi_1', \chi_2, \chi_3, \chi_3'\},$$

where χ_j, χ_j', $j \in \{1,3\}$, are pairs of $\mathbb{Q}$-conjugate characters, and $\chi_1(1) = 5$, $\chi_2(1) = 10$, $\chi_3(1) = 12$. Thus,

$$\mathcal{X}_{\mathbb{Q}} = \{1, \chi_1, \chi_2, \chi_3\}$$

is a possible choice. As (G, H) is primitive, $H_1 = G$ is the only group $> H$; so it is minimal, of course, and

$$\mathcal{X}_{\mathbb{Q}}(H_1) = \{\chi_1, \chi_2, \chi_3\}.$$

Hence there are exactly three selections of $\mathcal{X}_{\mathbb{Q}}(H_1)$, namely, $\mathcal{Z} = \{\chi_j\}$, $j = 1, 2, 3$. For reasons of comfort we have multiplied the corresponding generator $\beta_{\mathcal{Z}}$ of $J_{\mathcal{Z}}$, as defined in (20), by the group order $|G| = 660$. In view of (21) we may write

$$660\beta_{\mathcal{Z}} = \sum_{k=1}^{11} \sum_{l=1}^{5} b_{lk} \overline{s_1^k s_2^l},$$

where the coefficients b_{lk} are the entries of the following 5×11-matrices: For $\mathcal{Z} = \{\chi_1\}$,

$$\begin{pmatrix} 3 & -2 & -2 & -1 & 2 & 2 & -1 & -2 & -2 & 3 & 0 \\ 0 & 0 & -2 & 2 & -1 & -1 & 2 & -2 & 0 & 0 & 2 \\ -1 & 0 & 2 & 0 & -2 & -2 & 0 & 2 & 0 & -1 & 2 \\ -1 & -2 & 3 & 2 & -2 & -2 & 2 & 3 & -2 & -1 & 0 \\ 0 & 3 & 2 & -1 & -1 & -1 & -1 & 2 & 3 & 0 & 27 \end{pmatrix} \tag{22}$$

for $\mathcal{Z} = \{\chi_2\}$,

$$\begin{pmatrix} 0 & -1 & -1 & 4 & -2 & -2 & 4 & -1 & -1 & 0 & 0 \\ 0 & 0 & -1 & -2 & 4 & 4 & -2 & -1 & 0 & 0 & -2 \\ 4 & 0 & -2 & 0 & -1 & -1 & 0 & -2 & 0 & 4 & -2 \\ 4 & -1 & 0 & -2 & -1 & -1 & -2 & 0 & -1 & 4 & 0 \\ 0 & 0 & -2 & 4 & 4 & 4 & 4 & -2 & 0 & 0 & 21 \end{pmatrix},$$

and for $\mathcal{Z} = \{\chi_3\}$,

$$\begin{pmatrix} -4 & 6 & 6 & -4 & 1 & 1 & -4 & 6 & 6 & -4 & 1 \\ 1 & 1 & 6 & 1 & -4 & -4 & 1 & 6 & 1 & 1 & 1 \\ -4 & 1 & 1 & 1 & 6 & 6 & 1 & 1 & 1 & -4 & 1 \\ -4 & 6 & -4 & 1 & 6 & 6 & 1 & -4 & 6 & -4 & 1 \\ 1 & -4 & 1 & -4 & -4 & -4 & -4 & 1 & -4 & 1 & 31 \end{pmatrix}.$$

Observe the symmetry $b_{lk} = b_{l,11-k}$, which holds for all $l, k \in \{1, \ldots, 5\}$. The $\mathbb{Q}$-dimensions of the "large" $\mathbb{Q}$-admissible modules $J_{\mathcal{Z}}$ are 45, 35, and 31, respectively. Since G occurs as a Galois group over $\mathbb{Q}$ (cf. [16]), we obtain:

There is an irreducible polynomial $f \in \mathbb{Q}[Z]$ *of degree* 55 *with Galois group* $\mathrm{PSL}(2,11)$ *such that the entries of the matrix* (22) *are the coefficients of a relation* (*like* (1) *or* (2)) *between its roots. The same holds for the other two of the above matrices.*

The forementioned three relations exclude each other, i.e., they cannot occur with the same polynomial. This is due to the maximality of the closed modules they generate. We note, furthermore, that the pair (G,H) in question is *not* $\mathbb{Q}$-multiplicity-free, because of $\widehat{\chi}_2 = \chi_2$ and $\langle \chi_2, 1_H^G \rangle = 2$. Therefore, the isotypical component I_{χ_2} is the direct sum of two simple modules with character χ_2; and it contains infinitely many simple submodules W of this kind. For this reason the closed module $J_{\{\chi_2\}}$ can be extended to a larger $\mathbb{Q}$-admissible module $W \oplus J_{\{\chi_2\}}$ by choosing $W \subseteq I_{\chi_2}$ in infinitely many ways (cf. Example 7, Section 6). Each of these infinitely many larger modules is a *maximal* submodule of $\mathbb{Q}[G/H]$ in the usual sense. Therefore, it is impossible to check the $\mathbb{Q}$-admissibility of an element by a finite number of tests like (19). Here we are confronted, for the first time, with the phenomenon of "wildness", which will be discussed in Sections 5 and 6. On the other hand, the closed $\mathbb{Q}$-admissible submodules $J_{\{\chi_1\}}$, $J_{\{\chi_3\}}$ are maximal submodules of $\mathbb{Q}[G/H]$ themselves.

3. Abelian pairs. Let K be a field with $\mathrm{char}(K) = 0$, as above. For the time being, G denotes a finite *abelian* group. Then (G,H) is K-multiplicity-free for any subgroup H, but it is faithful if, and only if, $H = 1$ (cf. Example 1). We restrict ourselves to this case, so $K[G/H] = K[G]$ and the property of being K-admissible or not refers to subsets of $K[G]$ now. Moreover, $\mathcal{X} = \widehat{G}$. As above, let $\mathcal{X}_K$ be a complete set of representatives of all classes of K-conjugate characters in $\mathcal{X}$. The next proposition is a partial justification of the notion of "generic" introduced in Definition 5.

PROPOSITION 8. *Let* G *be abelian and* $H = 1$. *A subset* $\mathcal{Z}$ *of* $\mathcal{X}_K$ *is generic if, and only if,* $\mathcal{Z}$ *generates the character group* $\mathcal{X} = \widehat{G}$.

Proof. Let H' be a subgroup of G, $H' > 1$. From Example 1 we see that

$$\mathcal{X}_K(H') = \{\chi \in \mathcal{X}_K : \ker \chi \not\supseteq H'\}. \tag{23}$$

Let $\mathcal{Z} \subseteq \mathcal{X}_K$. We consider the kernel

$$\ker \mathcal{Z} = \{s \in G : \chi(s) = 1 \text{ for all } \chi \in \mathcal{Z}\}.$$

Then $\langle \mathcal{Z} \rangle = \widehat{G}$ if, and only if, $\ker \mathcal{Z} = 1$. If $\langle \mathcal{Z} \rangle \neq \widehat{G}$, there is an $s \in \ker \mathcal{Z}$ whose order $\mathrm{ord}(s)$ is a prime p. So $H' = \langle s \rangle$ is a minimal group > 1. Because of $\ker \chi \supseteq H'$ for all $\chi \in \mathcal{Z}$, (23) implies $\mathcal{X}_K(H') \cap \mathcal{Z} = \emptyset$, so $\mathcal{Z}$ is not generic. Conversely, if $\ker \mathcal{Z} = 1$, a group H' of the aforesaid kind is never contained

in $\ker \mathcal{Z}$, hence there is a character $\chi \in \mathcal{Z}$ such that $\ker \chi \not\supseteq H'$; so (23) yields $\mathcal{Z} \cap \mathcal{X}_K(H') \neq \emptyset$. ∎

In the above setting, Proposition 8 appears as a simple criterion for genericity. Our next aim is a description of the module $J_{\mathcal{Y}} \subseteq K[G]$ ($\mathcal{Y} \subseteq \mathcal{X}_K$ not necessarily generic) that is sometimes more suitable than that of (16). To this end we consider, once more, a character-theoretic splitting field $\overline{K}$ of G over K. We may assume that $\overline{K}$ is a finite abelian extension of K with Galois group Γ. Then the K-conjugates $\chi = \chi_1, \ldots, \chi_c$ of a character $\chi \in \mathcal{X} = \widehat{G}$ form an orbit under the canonical action of Γ, i.e.,

$$\{\chi_1, \ldots, \chi_c\} = \{\tau \circ \chi : \tau \in \Gamma\}. \tag{24}$$

Fix an element $\alpha = \sum_{s \in G} a_s s \in K[G]$. Since G is abelian, the central idempotent $\varepsilon_\chi \in \overline{K}[G]$ applies to α in the following simple way:

$$\varepsilon_\chi \alpha = \chi(\alpha)\varepsilon_\chi \in \overline{K}[G], \tag{25}$$

where $\chi(\alpha)$ has the usual meaning

$$\chi(\alpha) = \sum_{s \in G} a_s \chi(s). \tag{26}$$

Let $\widehat{\chi} = \chi_1 + \ldots + \chi_c$ be the K-irreducible character attached to χ and $\varepsilon_{\widehat{\chi}} = \varepsilon_{\chi_1} + \ldots + \varepsilon_{\chi_c}$ its central idempotent (observe that the Schur index κ equals 1 here). By (25),

$$\varepsilon_{\widehat{\chi}}\, \alpha = \sum_{j=1}^{c} \chi_j(\alpha)\varepsilon_{\chi_j}.$$

Thus, $\varepsilon_{\widehat{\chi}}\, \alpha$ vanishes if, and only if, all values $\chi_j(\alpha)$ vanish. But (24) and (26) show that these values are K-conjugate elements of $\overline{K}$. Hence we conclude that $\varepsilon_{\widehat{\chi}}\, \alpha = 0$ if, and only if, $\chi(\alpha) = 0$. Accordingly, every set $J_{\mathcal{Y}} \subseteq K[G]$, $\mathcal{Y} \subseteq \mathcal{X}_K$, is given by

$$J_{\mathcal{Y}} = \{\alpha \in K[G] : \chi(\alpha) = 0 \text{ for all } \chi \in \mathcal{Y}\}. \tag{27}$$

Further, we observe that two K-conjugate characters χ, χ' generate the *same* group of characters. This is due to the following fact: For each $\tau \in \Gamma$ there is an integer k, prime to the order $\operatorname{ord}(\chi)$, such that

$$\tau \circ \chi = \chi^k.$$

With this in mind, we are in a position to prove

THEOREM 3. *Let $(G, 1)$ be an abelian pair. A subset $M \subseteq K[G]$ is K-admissible if, and only if, there is a set $\mathcal{Z} \subseteq \widehat{G}$ of characters such that $\langle \mathcal{Z} \rangle = \widehat{G}$ and $\chi(\alpha) = 0$ for all $\chi \in \mathcal{Z}$ and $\alpha \in M$.*

Proof. If M is K-admissible, there is a generic set $\mathcal{Z} \subseteq \mathcal{X}_K$ such that $M \subseteq J_{\mathcal{Z}}$. By Proposition 8 and (27), $\mathcal{Z}$ has the property required in the

theorem. Conversely, suppose $\mathcal{Z} \subseteq \widehat{G}$ has this property. For each $\chi \in \mathcal{Z}$, $\mathcal{X}_K$ contains a uniquely determined character χ' that is K-conjugate to χ. Put $\mathcal{Z}' = \{\chi' : \chi \in \mathcal{Z}\}$. Because of $\langle\chi\rangle = \langle\chi'\rangle$, $\mathcal{Z}$ and $\mathcal{Z}'$ generate the same group of characters, namely, the group $\widehat{G}$. Moreover, $\chi'(\alpha) = \chi(\alpha) = 0$ for all $\alpha \in M$, hence $M \subseteq J_{\mathcal{Z}'}$ is K-admissible. ∎

Next we apply Theorem 3 to the following problem: Several people have asked whether relations like (4), i.e., $x_1 = x_2 + x_3$ or $x_1 = x_2 x_3$, are possible between the roots of an irreducible polynomial f as in the Introduction. In our terminology this problem reads as follows: Characterize those faithful pairs of groups (G, H) for which there exists a K-admissible element of the shape

$$\overline{1} - \overline{s} - \overline{t} \in K[G/H], \tag{28}$$

where $\overline{1}, \overline{s}, \overline{t}$ are three distinct cosets in G/H. The solution of this problem in the abelian case is one of the main results of [10]. Here we obtain this result as an almost immediate consequence of our theorem (strictly speaking, [10] enounces the following proposition only for $K = \mathbb{Q}$; by Proposition 6, however, this statement remains true for an arbitrary field of characteristic 0).

PROPOSITION 9. *Let $(G, 1)$ be an abelian pair. The group ring $K[G]$ contains a K-admissible element of the shape $1 - s - t$, $1 \neq s \neq t \neq 1$, if, and only if, the order $|G|$ of G is divisible by* 6.

Proof. If $\alpha = 1 - s - t$ is K-admissible, there is a character $\chi \in \widehat{G}$ such that $\chi(\alpha) = 0$, so $\chi(s) + \chi(t) = 1$. Hence $\chi(s)$ and $\chi(t)$ are complex-conjugate roots of unity, $\chi(s) = \zeta$ and $\chi(t) = \zeta^{-1}$, say. The equation $\zeta + \zeta^{-1} = 1$ shows that $\operatorname{ord}(\zeta) = 6$, which divides $|G|$. If, conversely, $|G|$ is divisible by 6, there is a character $\chi \in \widehat{G}$ of order 6 (since there are characters of orders 2 and 3). Choose $s \in G$ such that $\zeta = \chi(s)$ is a primitive sixth root of unity (s exists since $\widehat{G}/\ker\chi$ is a cyclic group of order 6). Let $\mathcal{Y} \subseteq \widehat{G}$ be a set of characters that generates $\ker\chi$. Then

$$\mathcal{Z} = \{\chi'\chi : \chi' \in \mathcal{Y}\} \cup \{\chi\}$$

generates $\widehat{G}$, and each character in $\mathcal{Z}$ vanishes on $\alpha = 1 - s - s^{-1}$. So α is K-admissible. ∎

Only little is known, in general, about K-admissible elements (28). The following case has been studied in [7]: G is a product $FH = \{st : s \in F, t \in H\}$, where F is an abelian group, which thus acts transitively on G/H. For this reason (G, H) is K-multiplicity-free by the argument used in Example 2. The cited paper [7] gives a necessary condition for the K-admissibility of (28): The order $|F|$ must be divisible by 6. According to Proposition 9, this condition is sufficient if $H = 1$, i.e., in the abelian case. We shall now

prove the sufficiency of this condition in the following situation: F is a cyclic normal subgroup of G and $F \cap H = 1$ (so G is a semidirect product). This result is an immediate consequence of the next proposition, which is of independent interest: It is a sort of "lifting theorem" for the $\mathbb{Q}[F]$-linear bijection

$$\mathbb{Q}[F] \to \mathbb{Q}[G/H] : \alpha = \sum_{s \in F} a_s s \mapsto \overline{\alpha} = \sum_{s \in F} a_s \overline{s}.$$

PROPOSITION 10. *Let (G, H) be a faithful pair of the following kind: There is a cyclic normal subgroup F of G such that $G = FH$ and $F \cap H = 1$. Let $M \subseteq \mathbb{Q}[F]$ be $\mathbb{Q}$-admissible for $(F, 1)$ and $\overline{M} = \{\overline{\alpha} : \alpha \in M\}$ $(\subseteq \mathbb{Q}[G/H])$. Then $\overline{M}$ is K-admissible for every field K of characteristic 0 (which contains $\mathbb{Q}$, of course).*

We give some explanations before we start the proof. The faithfulness condition excludes that G is abelian unless $H = 1$. Moreover, the groups $G = FH$ in question can be classified completely: H acts on F by automorphisms and this action is faithful, too. So we may assume that H is a subgroup of the automorphism group of F. In other words, if F is isomorphic to $\mathbb{Z}/k\mathbb{Z}$, then H is a subgroup of the multiplicative group $(\mathbb{Z}/k\mathbb{Z})^\times$, and G a subgroup of the usual semidirect product of these groups, which goes by the name of the "holomorph" of $\mathbb{Z}/k\mathbb{Z}$. For example, the dihedral group D_{2k} (with $F = \mathbb{Z}/k\mathbb{Z}$ and $H = \{\pm 1\}$, $k \geq 3$) is of this type. Note that the assumption "F cyclic" cannot easily be dispensed with. A counterexample is $G = A_4$, $F = \langle s, t \rangle$ being the (noncyclic) normal subgroup of order 4, and H a cyclic subgroup of order 3; here the $\mathbb{Q}$-admissible element $1 + s \in \mathbb{Q}[F]$ produces the element $\overline{1} + \overline{s} \in \mathbb{Q}[G/H]$, which is not $\mathbb{Q}$-admissible. Further, it seems necessary to assume that the coefficients of $\alpha \in M$ are *rational* numbers. Indeed, consider $G = S_3$, $F = A_3 = \langle s \rangle$, H of order 2, and $K = \mathbb{Q}(\zeta)$, ζ a primitive third root of unity; then $s - \zeta \cdot 1 \in K[F]$ is K-admissible, whereas $\overline{s} - \zeta \cdot \overline{1} \in K[G/H]$ is not K-admissible. On applying Proposition 10 to the situation of Proposition 9, we obtain

COROLLARY. *Let $G = FH$ be as in Proposition* 10. *Then $K[G/H]$ contains a K-admissible element of the shape* (28) *if the order of the cyclic normal subgroup F is divisible by* 6. (This condition is necessary by Theorem 5 of [7].)

Proof (of Proposition 10). First some basic observations. Let $F = \langle s \rangle$, $\mathrm{ord}(s) = k$, and $\chi \in \widehat{F}$ be a character of F. Then χ is a group homomorphism $F \to \langle \zeta \rangle$, ζ being a primitive kth root of unity. Because F is normal in G, each $t \in G$ defines a character $t * \chi \in \widehat{F}$ by $t * \chi(u) = \chi(t^{-1}ut)$. Since F is cyclic, $t * \chi$ coincides with a character χ^{k_t} for an integer k_t prime to k (observe that $t^{-1}st$ has order k, so this element equals s^{k_t} for such a number

k_t). On the other hand, $\zeta \mapsto \zeta^{k_t}$ defines an element σ_t of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, so we may write $t * \chi = \sigma_t \circ \chi$. In particular, χ and $t * \chi$ are $\mathbb{Q}$-conjugate characters.

By Proposition 6, it suffices to show that $\overline{M}$ is $\mathbb{Q}$-admissible. Let $\mathcal{X}$ be, as usual, the set of absolutely irreducible characters χ' of G satisfying $\langle \chi', 1_H^G \rangle \neq 0$. Let $\mathcal{X}_{\mathbb{Q}}$ be the above-chosen system of representatives of $\mathcal{X}$ with respect to $\mathbb{Q}$-conjugation. We start with a set $\mathcal{Z}$ of generators of $\widehat{F}$ such that $\chi(\alpha) = 0$ for all $\chi \in \mathcal{Z}$ and α in M. In part (a) we construct a subset $\widetilde{\mathcal{Z}}$ of $\mathcal{X}_{\mathbb{Q}}$; in (b) we show that this set is generic; and (c) contains the proof of $\overline{M} \subseteq J_{\widetilde{\mathcal{Z}}}$.

(a) For a character χ in $\mathcal{Z}$, let χ_F^G be the character induced by χ on G. Since F is a normal subgroup of G,

$$\chi_F^G(u) = \begin{cases} 0 & \text{if } u \notin F, \\ \sum_{t \in H} t * \chi(u) & \text{otherwise.} \end{cases} \tag{29}$$

Accordingly,

$$\sum_{u \in H} \chi_F^G(u) = \sum_{u \in H \cap F} \sum_{t \in H} t * \chi(u) = |H|,$$

because $H \cap F = 1$. This means $\langle \chi_F^G, 1_H^G \rangle = 1$ (cf. (14)), so there is a uniquely determined absolutely irreducible character χ' of G which occurs both in χ_F^G and 1_H^G. Since χ' is in $\mathcal{X}$, there is a unique character $\widetilde{\chi} \in \mathcal{X}_{\mathbb{Q}}$ that is $\mathbb{Q}$-conjugate to χ'. We put

$$\widetilde{\mathcal{Z}} = \{\widetilde{\chi} : \chi \in \mathcal{Z}\}.$$

(b) If H' is a subgroup $> H$, then $H' \cap F$ is a nontrivial subgroup of F. For this reason there is a character $\chi \in \mathcal{Z}$ with $\ker \chi \not\supseteq H' \cap F$, which means

$$\sum_{u \in H' \cap F} \chi(u) = 0. \tag{30}$$

By the above, each character $t * \chi = \sigma_t \circ \chi$, $t \in H$, has the same kernel, so (30) also holds for $t * \chi$ instead of χ. But then (29) gives $\langle \chi_F^G, 1_{H'}^G \rangle = 0$. Consequently, $\langle \chi', 1_{H'}^G \rangle = \langle \widetilde{\chi}, 1_{H'}^G \rangle = 0$ for the characters χ' and $\widetilde{\chi}$ introduced in (a) (recall that 1_H^G is a $\mathbb{Q}$-character, so it contains $\mathbb{Q}$-conjugates with the same multiplicity). This implies $\widetilde{\chi} \in \widetilde{\mathcal{Z}} \cap \mathcal{X}_{\mathbb{Q}}(H')$, so $\widetilde{\mathcal{Z}}$ is generic.

(c) Consider, for a character $\chi \in \mathcal{Z}$, the central idempotent $\varepsilon = \varepsilon_{\chi_F^G} \in \mathbb{Q}(\zeta)[G]$ that belongs to χ_F^G. From (29) one sees that

$$\varepsilon = \sum_{t \in H} \varepsilon_{t * \chi} \in \mathbb{Q}(\zeta)[F] \subseteq \mathbb{Q}(\zeta)[G].$$

Then (25) yields

$$\varepsilon \alpha = \sum_{t \in H} t * \chi(\alpha) \varepsilon_{t * \chi} = 0$$

for any element $\alpha \in M$—this is due to $\chi(\alpha) = 0$, on the one hand, and the $\mathbb{Q}$-conjugacy of the characters $t * \chi$, on the other hand. Because χ' occurs in χ_F^G, we get $\varepsilon_{\chi'}\alpha = 0$. But α has coefficients in $\mathbb{Q}$, so this identity also holds for all $\mathbb{Q}$-conjugate characters of χ' (such as $\widetilde{\chi}$). Thus, $\varepsilon_{\widetilde{\mathcal{Z}}}\alpha = 0$ and, obviously, $\varepsilon_{\widetilde{\mathcal{Z}}}\overline{\alpha} = 0$. ∎

As a further application of Theorem 2, we compute the maximal dimension of a $\mathbb{Q}$-admissible module in $\mathbb{Q}[G]$ for an *abelian* pair $(G, 1)$. Let $\mathcal{Z}$ denote a minimal subset of $\mathcal{X} = \widehat{G}$ that generates $\widehat{G}$. Since $\mathbb{Q}$-conjugate characters generate the same group, $\mathcal{Z}$ does not contain any two different but $\mathbb{Q}$-conjugate characters. Hence we may assume $\mathcal{Z} \subseteq \mathcal{X}_{\mathbb{Q}}$ ($\mathcal{Z}$ is a selection of $\mathcal{X}_{\mathbb{Q}}$, indeed). Let φ denote Euler's function. Then $\varphi(\mathrm{ord}(\chi))$ is the number of $\mathbb{Q}$-conjugates of a character $\chi \in \mathcal{Z}$. Therefore,

$$\dim_{\mathbb{Q}} J_{\mathcal{Z}} = |G| - \sum_{\chi \in \mathcal{Z}} \varphi(\mathrm{ord}(\chi)).$$

This fact and the isomorphy of G and $\widehat{G}$ show that maximizing the $\mathbb{Q}$-dimension of a $\mathbb{Q}$-admissible module is the same as computing the minimum of

$$\varphi(\mathcal{U}) = \sum_{s \in \mathcal{U}} \varphi(\mathrm{ord}(s))$$

when $\mathcal{U}$ runs through all minimal sets of generators of G. We need the following notations: For a natural number d and a prime p let $d^{(p)}$ denote the *p-part* of d, i.e., the greatest power of p that divides d (which is 1 if $p \nmid d$). We put

$$\Phi(d) = \sum_{\substack{p \mid d \\ p > 2}} \varphi(d^{(p)}) + \begin{cases} \varphi(d^{(2)}) & \text{if } d^{(2)} > 2 \text{ or } d = 2, \\ 0 & \text{otherwise.} \end{cases}$$

We denote by $C(d)$ a (multiplicative) cyclic group of order d.

Proposition 11. *Let G be a finite abelian group whose elementary divisors are $d_1, \ldots, d_k$ (so G is isomorphic to $C(d_1) \times \ldots \times C(d_k)$ with $d_1 \mid d_2 \mid \ldots \mid d_k$). The greatest possible $\mathbb{Q}$-dimension of a $\mathbb{Q}$-admissible module in $\mathbb{Q}[G]$ equals*

$$|G| - \sum_{j=1}^{k} \Phi(d_j).$$

We restrict ourselves to a sketch of the proof. Let $\mathcal{U}$ be a set of generators of G such that $\varphi(\mathcal{U})$ is *minimal*. One may assume, without loss of generality, that the order of each $s \in \mathcal{U}$ is either p^e or $2p^e$ for a prime p. If not, the element $s \in \mathcal{U}$ can be replaced by two elements t, u for which $\langle t, u \rangle = \langle s \rangle$,

$$\varphi(\mathrm{ord}(t)) + \varphi(\mathrm{ord}(u)) \le \varphi(\mathrm{ord}(s)),$$

and whose orders are divisible by fewer primes than $|\{p : p \mid \operatorname{ord}(s)\}|$. Because of this special shape of the elements of $\mathcal{U}$, it is possible to reduce the proof to the case of a direct product

$$G = C(2)^{r_0} \times C(p^{e_1})^{r_1} \times \ldots \times C(p^{e_h})^{r_h},$$

with $p \geq 3$, $1 \leq e_1 < \ldots < e_h$, $r_0 \geq 0$, and $r_j \geq 1$ for all $j \geq 1$. Put $\mathcal{U}_2 = \{s \in \mathcal{U} : \operatorname{ord}(s) = 2\}$ and $\mathcal{U}_p = \{s \in \mathcal{U} : p \mid \operatorname{ord}(s) \mid 2p^e\}$. First one shows

$$\varphi(\mathcal{U}_p) \geq \sum_{j=1}^{h} r_j \varphi(p^{e_j}). \tag{31}$$

For this purpose consider

$$l_j = |\{s \in \mathcal{U}_p : p^{e_j} \mid \operatorname{ord}(s)\}|, \quad j = 1, \ldots, h.$$

The invariance of the p-rank requires $l_j \geq r_j + r_{j+1} + \ldots + r_h$ for all $j = 1, \ldots, h$; and this gives, after some calculations, the inequality (31). Moreover, it is easy to write down a set $\mathcal{U}_p$ generating the p-part of G such that equality holds in (31). Put $r = r_1 + \ldots + r_h$. Because of $l_1 \geq r$, we have $|\mathcal{U}_p| \geq r + l$ for some $l \geq 0$. If $r \geq r_0$, a suitable exchange of elements in $\mathcal{U}_p$ shows that $\mathcal{U}_2$ must be empty. If $r_0 > r$, one could diminish $\mathcal{U}_2$ by choosing $l \geq 1$, but this would *increase* $\varphi(\mathcal{U})$, since $\varphi(p) > \varphi(2) = 1$. So $l = 0$ is the optimal choice, but then $|\mathcal{U}_2| \geq r_0 - r$. Altogether, we see that

$$\varphi(\mathcal{U}_2) \geq \max\{r_0 - r, 0\} \tag{32}$$

is necessary. On the other hand, one can choose $\mathcal{U}_2$ and $\mathcal{U}_p$ such that $\varphi(\mathcal{U})$ equals the sum of the right sides of (31) and (32), so we have computed the desired minimum.

4. "Trivial" pairs. We study a further class of K-multiplicity-free pairs (G, H). Let H' be a subgroup of G that contains H. Consider the element

$$\eta_{H'} = \sum_{\bar{s} \in H'/H} \bar{s} \in K[G/H]$$

attached to H' and the module

$$V(H') = {}_{K[G]}\langle \eta_{H'} \rangle$$

generated by this element. The canonical surjection ϱ of (8) induces a $K[G]$-linear isomorphism $V(H') \to K[G/H']$. In this way we obtain the decomposition

$$K[G/H] = U(H') \oplus V(H'), \tag{33}$$

which we note here for later use. It is not hard to see that $\eta_{H'}$ (and, thus, $V(H')$) is K-admissible: The elements of $V(H')$ are exactly those

$\alpha = \sum_{\bar{s}\in G/H} a_{\bar{s}}\,\bar{s} \in K[G/H]$ for which $a_{\bar{s}} = a_{\bar{t}}$ whenever $t^{-1}s \in H'$. Since this type of identity is impossible for any element $\bar{s}-\bar{1}$, $s \in G\setminus H$, Theorem 1 says that $V(H')$ is K-admissible. In particular, the element

$$\eta_G = \sum_{\bar{s}\in G/H} \bar{s} \tag{34}$$

and the one-dimensional module $V(G) = K\eta_G$ are always K-admissible.

Definition 7. The pair (G, H) of groups is called *K-trivial* if 0 and $V(G)$ are the only K-admissible modules in $K[G/H]$.

We look at an *imprimitive* pair (G, H) first. Imprimitivity means that there exists a group H' with $G > H' > H$. Since $V(H')$ is isomorphic to $K[G/H']$, its K-dimension is the group index $[G : H'] \geq 2$, so the K-admissible module $V(H')$ is certainly different from 0 and $V(G)$. Consequently, (G, H) is *not* K-trivial. Suppose now that (G, H) is *primitive*, i.e., $H_1 = G$ is the only minimal group $> H$. Then the pair (G, H) is K-trivial if, and only if, $U(G)$ is simple as a $K[G]$-module. Indeed, if $U(G)$ is not simple, then there is a submodule V of $U(G)$ different from 0 and $U(G)$. But V is K-admissible, by Theorem 1, and not contained in $V(G)$, hence (G, H) is not K-trivial. Conversely, if $U(G)$ is simple, then $K[G/H]$ is the direct sum of two simple isotypical components, namely, $V(G)$ and $U(G)$ (cf. (33)). So it has only four submodules: 0, $V(G)$, $U(G)$, and $K[G/H]$; of these, only 0 and $V(G)$ are K-admissible.

For the time being, let $\psi = 1_H^G - 1$ denote the character belonging to $U(G)$. Our considerations result in the following proposition (which is essentially contained in Proposition 4 of [11]):

Proposition 12. *An imprimitive pair (G, H) is never K-trivial. A primitive pair (G, H) is K-trivial if, and only if, the character $\psi = 1_H^G - 1$ is K-irreducible.*

It is well known that ψ is *absolutely* irreducible if, and only if, (G, H) is doubly transitive (cf. [12], p. 597, Satz 20.2). In this case (G, H) is clearly K-trivial for an arbitrary field K with $\mathrm{char}(K) = 0$. This was observed in [11] (for the additive case, to be precise) and by later authors (cf. [1], Theorem 3, [7], Theorem 1). Since there exists a complete classification of all doubly transitive pairs (cf., e.g., [3]), they are not of interest here. In the remainder of this section we study *faithful* pairs (G, H) for which ψ is $\mathbb{Q}$-irreducible but not absolutely irreducible. To our knowledge only the most obvious class of pairs (G, H) of this kind has been considered so far: pairs whose index $[G : H]$ is a prime number p—so they belong to polynomials $f \in \mathbb{Q}[Z]$ of prime degree (cf. [14], [11], and [9]). The assumptions "$[G : H] = p$" and "(G, H) not doubly transitive" imply that the group G is solvable. But then

(G, H) is of a well known type: G is a proper subgroup of the affine group $\mathrm{AGL}(1, p)$ and H is the stabilizer of an element under the usual action of G on $\mathbb{Z}/p\mathbb{Z}$. We are going to generalize this class of $\mathbb{Q}$-trivial pairs now.

To this end let $q = p^e$ be a prime power, $e \geq 1$, and $\mathbb{F}_q$ the finite field with q elements. For any $a \in \mathbb{F}_q^\times$ and $b \in \mathbb{F}_q$, let

$$aX + b : \mathbb{F}_q \to \mathbb{F}_q$$

be the affine mapping defined by $x \mapsto ax + b$. The group

$$\mathrm{AGL}(1, q) = \{aX + b : a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q\}$$

acts as a permutation group on $\mathbb{F}_q$. The stabilizer of $0 \in \mathbb{F}_q$ under this action is $F = \{aX : a \in \mathbb{F}_q^\times\}$, which is obviously isomorphic to $\mathbb{F}_q^\times$. The group $\mathrm{AGL}(1, q)$ is a semidirect product $\mathrm{AGL}(1, q) = TF$, where $T = \{X + b : b \in \mathbb{F}_q\}$ is a normal subgroup of $\mathrm{AGL}(1, q)$. More precisely, $\mathrm{AGL}(1, q)$ is a Frobenius group of order $|T| \cdot |F| = q(q-1)$ with Frobenius kernel T and complement F. Let G be a transitive subgroup of $\mathrm{AGL}(1, q)$ of index d. Then T is the p-Sylow group of G; and G has the shape $G = TH$, H being a subgroup of F of the same index $[F : H] = d$. The pair (G, H) defines the usual permutation representation of G on the set $\mathbb{F}_q$.

We show

Proposition 13. *As above, let $q = p^e$ be a prime power and $G = TH$ a transitive subgroup of $\mathrm{AGL}(1, q)$ of index $d = [\mathrm{AGL}(1, q) : G]$. The pair (G, H) is $\mathbb{Q}$-trivial if, and only if, the index d divides $p - 1$ and is relatively prime to the exponent e.*

Proof. Let $T^* = \widehat{T} \setminus \{1\}$ be the set of nontrivial, absolutely irreducible characters of the elementary abelian p-group T. The group F acts on T^* by conjugation since T is a normal subgroup of G. This action looks as follows: For an element $aX \in F$ and a character $\chi \in T^*$, the character $aX * \chi$ is defined by

$$aX * \chi\,(X + b) = \chi(X + ab).$$

Moreover, this action is *regular*, which means, first, that $aX * \chi = \chi$ holds only if $a = 1$ and, second, that it is transitive (observe $|T^*| = |F|$). Each $\chi \in T^*$ is a (surjective) group homomorphism $\chi : T \to \langle\zeta\rangle$ onto the multiplicative group generated by a primitive pth root of unity ζ. The Galois group $\Gamma = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is isomorphic to $\mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times$; it is embedded in F by

$$\sigma \mapsto \overline{k}_\sigma X,$$

where $k_\sigma \in \mathbb{Z}$ is such that $\sigma(\zeta) = \zeta^{k_\sigma}$ and $\overline{k}_\sigma$ is the residue class of k_σ mod p. The ($\mathbb{Q}$-conjugate) character $\sigma \circ \chi$ coincides with $\overline{k}_\sigma X * \chi$ because

$$\sigma \circ \chi\,(X + b) = (\chi(X + b))^{k_\sigma} = \chi(X + \overline{k}_\sigma b) = \overline{k}_\sigma X * \chi\,(X + b).$$

In the remainder of the proof we identify $\sigma \in \Gamma$ with $\overline{k}_\sigma X \in F$, so we consider Γ as a subgroup of F and, consistently, denote its action on T^* by "$*$" instead of "$\circ$". It turns out that the decomposition of $\psi = 1_H^G - 1$ into $\mathbb{Q}$-irreducible components can be completely described in terms of the actions of the subgroups $\Gamma, H \subseteq F$ on T^*. Indeed, the induced characters χ_T^G, $\chi \in T^*$, are absolutely irreducible characters of G; further, if $H\backslash T^* = \{H * \chi : \chi \in T^*\}$ denotes the set of H-orbits on T^*, then there is a bijection

$$H\backslash T^* \to \{\chi_T^G : \chi \in T^*\}, \tag{35}$$

defined by $H * \chi \mapsto \chi_T^G$ (cf. [12], p. 561, Satz 16.13). By the forementioned regularity, $|H * \chi| = |H|$ and, thus, $|H\backslash T^*| = (q-1)/|H| = d$ (recall that $[F : H] = d$). So (35) says that there are exactly d distinct characters of G of the shape χ_T^G, $\chi \in T^*$. We denote them by $\chi_1, \ldots, \chi_d$. The computation of $\langle 1_H^G, \chi_j \rangle$ now follows the same pattern as an analogous computation in the proof of Proposition 10 (cf. (29), (14); observe $H \cap T = 1$). It shows that $\sum_{j=1}^d \chi_j$ is contained in the character ψ. On comparing the degrees of both characters, one obtains

$$\psi = \sum_{j=1}^{d} \chi_j. \tag{36}$$

Clearly ψ is $\mathbb{Q}$-irreducible if, and only if, all characters χ_j are $\mathbb{Q}$-conjugate. The field $\mathbb{Q}(\zeta)$ is a splitting field of each character χ_j since all values of χ_j lie in $\mathbb{Q}(\zeta)$, on the one hand, and since (36) requires that the Schur index of χ_j equals 1, on the other hand—for ψ is defined over $\mathbb{Q}$. Moreover, the action of $\Gamma \subseteq F$ on T^* respects H-orbits, i.e., $\sigma * (H * \chi) = H * (\sigma * \chi)$, since F is abelian. Because

$$\sigma \circ \chi_T^G = (\sigma * \chi)_T^G,$$

we obtain: Two characters $\chi_j = \chi_T^G$ and $\chi_k = \chi_T'^G$ are $\mathbb{Q}$-conjugate if, and only if, there exists an automorphism $\sigma \in \Gamma$ such that $\sigma * (H * \chi) = H * \chi'$. In particular, *all* characters $\chi_1, \ldots, \chi_d$ are $\mathbb{Q}$-conjugate if, and only if, Γ acts transitively on $H\backslash T^*$. But F acts regularly on T^*, so this is the same as saying $\Gamma H = F$. Hence the proof comes down to an exercise about two subgroups of the cyclic group F, whose indices are $[F : H] = d$, $[F : \Gamma] = (q-1)/(p-1)$. One finds: $\Gamma H = F$ if, and only if, $d \mid p-1$ and d is prime to $(q-1)/(p-1)$. However, if $d \mid p-1$, then $p \equiv 1 \bmod d$ and so $(q-1)/(p-1) \equiv e \bmod d$. This concludes the proof. ∎

Whenever the index d of Proposition 13 is > 1, the pair (G, H) is not doubly transitive. If, in addition, $d \mid p-1$ and the greatest common divisor (d, e) equals 1, the pair (G, H) is of the desired type, i.e., $\mathbb{Q}$-trivial but not doubly transitive. This class of examples clearly covers the above-mentioned

faithful pairs of prime index $[G : H] = p$. We go over to another class of examples.

Let $q = 2^p > 4$ be a power of 2 such that $l = q - 1$ is a prime. This demands that p is a prime ≥ 3, so l is one of the *Mersenne primes* $7, 31, 127, 8191, \ldots$ We consider the simple group $G = \mathrm{PSL}(2, q)$ as a permutation group on $\mathbb{F}_q \cup \{\infty\}$ in the usual way. The group G contains a cyclic subgroup of (odd) order $q + 1$, whose normalizer in G is a dihedral group $H = D_{2(q+1)}$; its index $[G : H]$ equals $q(q - 1)/2$.

PROPOSITION 14. *Let the above notations hold*; *in particular*, $G = \mathrm{PSL}(2, q)$, $H = D_{2(q+1)}$, $q = 2^p$, *and* $2^p - 1$ *is a prime number* ≥ 7. *Then* (G, H) *is* $\mathbb{Q}$*-trivial but not doubly transitive.*

P r o o f. Let $G_\infty = \mathrm{ASL}(1, q)$ denote the stabilizer of ∞ under the said action of G. Then $G_\infty = TF$, where the normal subgroup T is elementary abelian of order $q = 2^p$ and F a cyclic group of prime order $q - 1 = l$. The nontrivial (absolutely irreducible) characters χ of F can be identified with those characters of G_∞ whose kernel contains T. According to [13], p. 207, Lemma 5.3, these characters produce, by induction from G_∞ to G, $(l - 1)/2$ distinct absolutely irreducible characters $\chi_1, \ldots, \chi_{(l-1)/2}$ of G. These induced characters are $\mathbb{Q}$-conjugate and have $\mathbb{Q}(\zeta + \zeta^{-1})$ as their common field of values, where ζ is a primitive lth root of unity. One readily checks that the characters $\psi = 1_H^G - 1$ and $\chi_1 + \ldots + \chi_{(l-1)/2}$ have the same degree, namely, $(q + 1)(q - 2)/2$. Thus, these characters are equal provided that $\langle \chi_j, 1_H^G \rangle \neq 0$ for all $j = 1, \ldots, (l - 1)/2$ (an argument which was also used in the proof of Proposition 13). The quoted lemma, however, allows us to verify this: For an element $s \in H \setminus \{1\}$ it gives

$$\chi_j(s) = \begin{cases} 0 & \text{if } \mathrm{ord}(s) \mid q + 1, \\ 1 & \text{if } \mathrm{ord}(s) = 2, \end{cases}$$

whence $\sum_{s \in H} \chi_j(s) = 2(q + 1) = |H|$ and $\langle \chi_j, 1_H^G \rangle = 1$ follow. ∎

REMARK. If $l = q - 1$ is not a prime, not all of the said characters $\chi \neq 1$ of F are $\mathbb{Q}$-conjugate, so they do not produce $\mathbb{Q}$-conjugate characters of G. For this reason the proposition is wrong in this case. The (excluded) case $l = 3$ gives a doubly transitive pair (G, H) (in fact, $G = A_5$ and $H = D_{10}$).

The last two propositions can be extended to *groups of automorphisms* of G: For the group $\mathrm{AGL}(1, q)$ of Proposition 13, the (full) automorphism group consists of all semiaffine mappings

$$a\lambda + b : \mathbb{F}_q \to \mathbb{F}_q : x \mapsto a\lambda(x) + b,$$

with $\lambda \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, $a \in \mathbb{F}_q^\times$, $b \in \mathbb{F}_q$. Let Λ be a subgroup of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ and $G = TH$ as in Proposition 13. Then Λ normalizes the groups T and H (in the latter case this is due to the fact that the elements $a \in \mathbb{F}_q^\times$ and $\lambda(a)$

have the same order), hence it also normalizes G. We put

$$G' = G\Lambda = \{a\lambda + b : aX + b \in G, \lambda \in \Lambda\}.$$

The stabilizer of 0 under the action of G' on $\mathbb{F}_q$ is $H' = H\Lambda = \{a\lambda : aX \in H, \lambda \in \Lambda\}$. Now the restriction $1_{H'}^{G'}|_G$ equals 1_H^G: Indeed, $1_{H'}^{G'}(s)$ is the number of fixed points in $\mathbb{F}_q$ of an element $s \in G'$; and this number equals $1_H^G(s)$ whenever $s \in G$. Consequently, the character $\psi' = 1_{H'}^{G'} - 1$, when restricted to G, coincides with $\psi = 1_H^G - 1$. If ψ is $\mathbb{Q}$-irreducible (which is true under the premisses of Proposition 13), then clearly so is ψ'. On the other hand, the order $|G'|$ divides $q(q-1)e/d$ since $|\Lambda|$ divides e. Because $(d, e) = 1$, G' cannot be doubly transitive unless $d = 1$.

A similar argument works for the groups $\mathrm{PSL}(2, q)$ of Proposition 14: As p is a prime, the only nontrivial subgroup Λ of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_2)$, $q = 2^p$, is the whole group, whose order equals p. However, it is not quite obvious that Λ normalizes the dihedral group $D_{2(q+1)}$. As a matter of fact, this holds only for a *suitably chosen* dihedral group but not for an arbitrary conjugate of it. In order to obtain an appropriate group $D_{2(q+1)}$, we start with a primitive $(q+1)$th root of unity ξ in the field $\mathbb{F}_{q^2}$ (observe that $|\mathbb{F}_{q^2}^\times|$ is divisible by $q+1$). The transformation $x \mapsto \xi x$ of $\mathbb{F}_{q^2}$ can be considered as an element of $\mathrm{GL}(2, q)$ and thus defines a fractional linear transformation $s \in \mathrm{PGL}(2, q) = \mathrm{PSL}(2, q)$ of order $q+1$: More precisely, let $Z^2 - aZ - b \in \mathbb{F}_q[Z]$ be the minimal polynomial of ξ over $\mathbb{F}_q$; then $s = b/(X + a) \in \mathrm{PSL}(2, q)$. For any $\lambda \in \Lambda$,

$$\lambda \circ \frac{b}{X + a} \circ \lambda^{-1} = \frac{\lambda(b)}{X + \lambda(a)}.$$

But $Z^2 - \lambda(a)Z - \lambda(b)$ is the minimal polynomial of another element ξ' of order $q+1$; and since $\xi' \in \langle\xi\rangle$ one obtains $\lambda(b)/(X + \lambda(a)) \in \langle s\rangle$. Therefore Λ normalizes $\langle s\rangle$. The dihedral group $D_{2(q+1)}$ we are looking for is the *normalizer* of $\langle s\rangle$ in G (cf. [12], p. 192, Satz 8.4). This group is also normalized by Λ. The remainder runs along the above lines: Put $H = D_{2(q+1)}$, $G' = G\Lambda$, $H' = H\Lambda$. By means of the bijection $G/H \to G'/H'$ one shows, for the respective characters, $1_{H'}^{G'}|_G = 1_H^G$ and $\psi' = \psi$. Since ψ is $\mathbb{Q}$-irreducible, this is true for ψ'. It should be noted, however, that (G', H') may be doubly transitive. On comparing $|G'| = |G|p$ with $[G : H]([G : H] - 1)$, one sees that this may happen only for $p = 3$, $q = 8$—where it actually happens (cf. [12], p. 214, exercise 17). Altogether, we obtain:

Proposition 15. *In the situation of Proposition* 13 *or Proposition* 14, *let Λ be a subgroup of* $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ *or* $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_2)$, *respectively*, *and suppose that (G, H) is $\mathbb{Q}$-trivial. Then $(G\Lambda, H\Lambda)$ is $\mathbb{Q}$-trivial and*, *up to the exception just mentioned*, *not doubly transitive.*

Our final observations in this section result from

PROPOSITION 16. *Let* (G, H) *be* $\mathbb{Q}$*-trivial. If* $[G : H]$ *is even, then* (G, H) *is* K*-multiplicity-free for every field* K *of characteristic* 0.

P r o o f. As in (10) we have

$$\psi = 1_H^G - 1 = \kappa(\chi_1 + \ldots + \chi_c),$$

where the χ_j's are $\mathbb{Q}$-conjugate, absolutely irreducible characters of G and the Schur index κ is a natural number. Since $\psi(1) = \kappa c \chi_1(1)$ is odd, the numbers c and $\chi_1(1)$ are also odd. Consequently, χ_1 is a real-valued character of odd degree. Now a theorem of Brauer and Speiser ([6], p. 750) says that $\kappa = 1$. ∎

In the case of the groups $G = \mathrm{PSL}(2, q)$, $H = D_{2(q+1)}$ of Proposition 14, the index $[G : H]$ is, in fact, even. This is not true for most pairs (G, H) of Proposition 13. Nevertheless, these pairs are K-multiplicity-free for any K, since G is solvable and (G, H) primitive (cf. Example 2).

Possibly the contemporary knowledge about permutation groups suffices for a complete classification of all $\mathbb{Q}$-trivial pairs that are not doubly transitive. All *primitive* pairs (G, H) of *odd* index are known (cf., e.g., [15]); so one could try to figure out the relevant ones from the (long and involved) list. On the other hand, if $[G : H]$ is even, we know that (G, H) is K-multiplicity-free for any K. But this means that Theorem 30.2 of [20], p. 92, can be applied: We find that, apart from the case $|G| = 2$, $H = 1$, the pair (G, H) is 3/2-fold transitive. Therefore, the classification of all primitive, 3/2-fold transitive permutation groups of even degree would be the basis for the same kind of search as in the odd case.

5. "Tame" and "wild" pairs. As above, let K be a field of characteristic 0 and (G, H) a pair of groups with $H \subseteq G$. The notions of "module" and "submodule" always refer to $K[G]$-modules. Furthermore, $V \cong V'$ means that the $K[G]$-modules V and V' are isomorphic. In Section 2 we have seen (cf. the discussion concentrated around (19)) that the complete list of all K-admissible submodules of $K[G/H]$ is, in general, too complicated to be written down—even for K-multiplicity-free pairs. Consequently, we restrict ourselves to the following important type of K-admissible modules:

DEFINITION 8. Let V be a K-admissible submodule of $K[G/H]$. We say V is a *maximal* K*-admissible module* (or simply: V is *maximally* K*-admissible*) if no larger module $V' \supseteq V$, $V' \neq V$, is K-admissible.

The notion of maximal K-admissibility leads to the following generalization of the class of K-multiplicity-free pairs:

DEFINITION 9. The pair (G, H) is called *K-tame* if there are only finitely many maximal K-admissible modules in $K[G/H]$. Otherwise, (G, H) is called *K-wild*.

If (G, H) is K-multiplicity-free, then $K[G/H]$ contains only a finite number of submodules, so (G, H) is clearly K-tame. We conjecture that the converse ("K-tame" implies "K-multiplicity-free") is also true, which means that the class of K-tame pairs is not really larger than the class of K-multiplicity-free pairs. We cannot prove this, but our characterization of K-tame pairs (Theorem 4) comes close to the property of being K-multiplicity-free. For instance, it turns out that in the K-tame case the maximal K-admissible modules are just those of the shape $J_{\mathcal{Z}}$, where $\mathcal{Z}$ is a selection of the set of characters $\mathcal{X}_K$ (cf. Proposition 20). In view of Section 2 (context of (19)) we may say that K-tame pairs do *not* behave different from K-multiplicity-free pairs with respect to *maximal K-admissible modules.* In particular, the simple *test* of K-admissibility described there also works for K-tame pairs. The said characterization also yields some simple criteria for the K-wildness of a pair (e.g., Propositions 18, 19).

A good case can be made out in favour of our forementioned conjecture. However, in order to avoid a lengthy (and, in the end, not conclusive) discussion, not all possible arguments are rendered here—we only draw the reader's attention to the corollaries to Proposition 17.

We adopt the notations of Section 2. Thus, $\mathcal{X}_K$ denotes the reduced set of absolutely irreducible characters attached to (G, H); and for any $\chi \in \mathcal{X}_K$, $I_{\widehat{\chi}} = K[G]\varepsilon_{\widehat{\chi}}$ is the corresponding isotypical component of $K[G/H]$ (cf. (11)). Recall that, for any subgroup $H' \subseteq G$ containing H, $\mathcal{X}_K(H')$ is the set of all $\chi \in \mathcal{X}_K$ which occur in $U(H')$, i.e., $\langle \chi, 1_H^G - 1_{H'}^G \rangle \neq 0$. Moreover,

$$I_{\mathcal{X}_K(H')} = \bigoplus_{\chi \in \mathcal{X}_K(H')} I_{\widehat{\chi}} \tag{37}$$

is the smallest *closed* submodule of $K[G/H]$ that contains $U(H')$. Finally, let $H_1, \ldots, H_m$ denote the (distinct) minimal subgroups of G which are $> H$. The main result of this section shows that the property of being K-tame requires $U(H_j) = I_{\mathcal{X}_K(H_j)}$ for all $j = 1, \ldots, m$; this is the same as

$$\langle 1_{H_j}^G, 1_H^G - 1_{H_j}^G \rangle = 0, \quad j = 1, \ldots, m. \tag{38}$$

However, the validity of (38) is not sufficient for tameness:

THEOREM 4. *In the above setting, the following statements are equivalent*:

(a) *The pair (G, H) is K-tame.*

(b) *Each module $U(H_j)$, $j = 1, \ldots, m$, is closed and all of its isotypical components $I_{\widehat{\chi}}$, $\chi \in \mathcal{X}_K(H_j)$, are simple.*

We postpone the proof of Theorem 4 and note some of its implications instead. Consider, first, the special case of a *primitive* pair (G, H), so $m = 1$ and $H_1 = G$. Then K-tameness means that $U(G)$ consists of simple isotypical components of $K[G/H]$ only. Since *every* isotypical component of $K[G/H]$ except the trivial one, i.e. $V(G) = K\eta_G$ (cf. (33), (34)), occurs in $U(G)$, we obtain

COROLLARY. *If the pair (G, H) is primitive but not K-multiplicity-free, it is K-wild.*

Next we need a simple but useful lemma. Here it seems appropriate to recall that $\langle S\rangle$ denotes the subgroup generated by the set S.

LEMMA 1. *Let H' and H'' be subgroups of G that contain H.*

(a) $U(H') \subseteq U(H'')$ *if, and only if,* $H' \subseteq H''$.
(b) $U(H') + U(H'') = U(\langle H' \cup H''\rangle)$.

P r o o f. Assertion (a) is easy to check if one observes that $U(H') = {}_{K[G]}\langle \overline{s} - \overline{1} : s \in H'\rangle$ (cf. (9)) and that $U(H'')$ is the kernel of the canonical map $\varrho : K[G/H] \to K[G/H'']$ (cf. (8)). From (a) it is clear that $U(H') + U(H'') \subseteq U(\langle H' \cup H''\rangle)$. The converse inclusion follows from

$$\overline{st} - \overline{1} = (\overline{s} - \overline{1}) + s(\overline{t} - \overline{1}) \in U(H') + U(H''),$$

where $s \in H'$ and $t \in H''$. This assertion can be extended to arbitrary elements of the shape $s_1t_1 \dots s_ht_h$, $s_j \in H'$, $t_j \in H''$. ∎

By the lemma, $U(H_1) + \dots + U(H_m) = U(\langle H_1 \cup \dots \cup H_m\rangle)$. If each $U(H_j)$ consists of simple isotypical components of $K[G/H]$ only, this is also true for $U(H_1) + \dots + U(H_m)$. Consequently, we obtain

PROPOSITION 17. *The pair (G, H) is K-tame if, and only if, $U(\langle H_1 \cup \dots \cup H_m\rangle)$ consists of simple isotypical components of $K[G/H]$ exclusively.*

We note, in addition, that any $K[G]$-linear complement of the module $U(\langle H_1 \cup \dots \cup H_m\rangle)$ (such as $V(\langle H_1 \cup \dots \cup H_m\rangle)$) is isomorphic to $K[G/\langle H_1 \cup \dots \cup H_m\rangle]$. This observation yields

COROLLARY 1. *Suppose that the pair $(G, \langle H_1 \cup \dots \cup H_m\rangle)$ is K-multiplicity-free (this is true, for instance, if $\langle H_1 \cup \dots \cup H_m\rangle = G$). Then (G, H) is K-tame if, and only if, (G, H) is K-multiplicity-free.*

Corollary 1 supports our opinion that, in reality, the notions of "K-multiplicity-free" and "K-tame" are equivalent. One can also read this corollary in the following way: If (G, H) is K-tame but not K-multiplicity-free, then there is a group $H' > H$ such that (G, H') is *not* K-multiplicity-free. As every tower of subgroups $H < H' < H'' < \dots$ ends with the group G, and (G, G) is K-multiplicity-free, we obtain another argument in favour of our opinion:

Corollary 2. *Suppose that (G,H) is K-tame but not K-multiplicity-free. Then there is a subgroup H' of G, $H' > H$, such that (G,H') is K-wild.*

Proposition 18. *Suppose that there are minimal groups $H_1, H_2 > H$, $H_1 \neq H_2$, which are conjugate. Then (G,H) is K-wild.*

Proof. Since H_1 and H_2 are conjugate groups, the characters $1_{H_1}^G$ and $1_{H_2}^G$ are identical. Accordingly, the character of $U(H_1)$, namely, $1_H^G - 1_{H_1}^G$, coincides with the character of $U(H_2)$. This means that $U(H_1)$ and $U(H_2)$ are *isomorphic* modules. If (G,H) is K-tame, these modules are *closed*, so they must be equal in the set-theoretic sense. By Lemma 1, $H_1 = H_2$. ∎

Corollary. *Let $(G,1)$ be K-tame. Then each subgroup of G of prime order is normal in G.*

The corollary shows that pairs $(G,1)$ are, as a rule, K-wild unless G is abelian. An exception is the quaternion group G of order 8, for which $(G,1)$ is $\mathbb{Q}$-multiplicity-free.

Let H' and H'' be subgroups of G. Consider

$$H'H'' = \{st : s \in H',\ t \in H''\}.$$

We say *H' commutes with H''* whenever $H'H'' = H''H'$ (which is the same as saying $H'H''$ is a subgroup of G).

Proposition 19. *Let (G,H) be K-tame and H_1 a minimal subgroup $> H$ of G. Then H_1 commutes with every group H' that contains H.*

Proof. By Frobenius reciprocity,

$$\langle 1_H^G, 1_{H_1}^G \rangle = |H|^{-1} \sum_{s \in H} 1_{H_1}^G(s).$$

According to [12], p. 597, Satz 20.2, this is the number of orbits of the group H acting on G/H_1. On the other hand, (G,H) is K-tame, so (38) gives

$$\langle 1_H^G, 1_{H_1}^G \rangle = \langle 1_{H_1}^G, 1_{H_1}^G \rangle,$$

which is the number of orbits of H_1 on the same set. Since $H \subseteq H_1$, this means that every H-orbit on G/H_1 is an H_1-orbit, and conversely. In other words, $H_1 t \subseteq HtH_1$ for each $t \in G$. In particular, if H' is a subgroup of G with $H \subseteq H'$, we obtain

$$H_1 H' \subseteq HH'H_1 = H'H_1.$$

But $|H'H_1| = |H_1H'|$, so H_1 commutes with H'. ∎

Proof of Theorem 4. Suppose, first, that (b) holds, so each $U(H_j)$ is closed and all of its isotypical components are simple. Let $V \subseteq K[G/H]$ be a K-admissible module. We show that there is a generic set $\mathcal{Z} \subseteq \mathcal{X}_K$ such that $V \subseteq J_{\mathcal{Z}}$. Then each maximal K-admissible module has the shape

$J_{\mathcal{Z}}$—there are, however, only finitely many modules of this shape, so (G,H) is K-tame. In fact, since V is K-admissible, it does not contain any of the modules

$$U(H_j) = \bigoplus_{\chi \in \mathcal{X}_K(H_j)} I_{\widehat{\chi}},$$

$j = 1, \dots, m$ (cf. (37)). Thus we can select, for each j, a character $\chi \in \mathcal{X}_K(H_j)$ such that $I_{\widehat{\chi}}$ is not contained in V. Since $I_{\widehat{\chi}}$ is simple, this means $I_{\widehat{\chi}} \cap V = 0$. In view of

$$\varepsilon_{\widehat{\chi}} V \subseteq \varepsilon_{\widehat{\chi}} K[G/H] = I_{\widehat{\chi}}$$

(cf. (11)), we obtain $\varepsilon_{\widehat{\chi}} V \subseteq V \cap I_{\widehat{\chi}} = 0$. If, therefore, $\mathcal{Z}$ denotes the set of all selected characters, one has $\varepsilon_{\mathcal{Z}} V = 0$ and $V \subseteq J_{\mathcal{Z}}$.

Before we prove the considerably more complicated direction (a)⇒(b), we note the following by-product of what we have shown so far:

PROPOSITION 20. *Suppose (G,H) satisfies condition* (b) *of Theorem* 4 (*which is true if (G,H) is K-tame, as we shall show*). *Then the map $\mathcal{Z} \mapsto J_{\mathcal{Z}}$ defines a bijection between the set of selections $\mathcal{Z}$ of $\mathcal{X}_K$ and the set of maximal K-admissible modules of $K[G/H]$.*

The remainder of the proof of Theorem 4 is based on the following

LEMMA 2. *Let V be a simple $K[G]$-module, I a module $\cong V^r$ for some $r \geq 2$, and $V_1, \dots, V_k$ submodules of I that are all $\cong V$. Then there are infinitely many distinct submodules W_i of I, $i = 1, 2, \dots$, such that each W_i is $\cong V^{r-1}$ and $W_i \not\supseteq V_j$ for all $j = 1, \dots, k$.*

We postpone the proof of this lemma and start the (indirect) proof of (a)⇒(b): Suppose $U(H_1)$ does not fulfil condition (b). Then there is an isotypical component I of $K[G/H]$ such that $I \cap U(H_1) \neq 0$, I nonsimple; so $I \cong V^r$ for some simple module V and some $r \geq 2$. Without loss of generality we may assume that $I \cap U(H_j) \neq 0$ if $j \in \{1, \dots, k\}$ and $I \cap U(H_j) = 0$ if $j \in \{k+1, \dots, m\}$, for some k, $1 \leq k \leq m$. For each $j \leq k$ let V_j be a simple submodule of $I \cap U(H_j)$ (so $V_j \cong V$). By Lemma 2, there are infinitely many distinct maximal submodules W_i, $i = 1, 2, \dots$, of I such that $W_i \not\supseteq V_j$ for all $j \leq k$. Let J denote the (uniquely determined) $K[G]$-linear complement of I in $K[G/H]$. The definition of k requires $U(H_j) \subseteq J$ for all $j > k$. We put $M = U(H_1) \cap J$. Then M contains none of the modules $U(H_j)$, $j > k$; otherwise, $U(H_j) \subseteq U(H_1)$ would imply $H_j \subseteq H_1$ (cf. Lemma 1), which contradicts the minimality of the groups $H_1, \dots, H_m$. Suppose now that $\widetilde{M}$ is a submodule of J which is *maximal* with respect to the following properties:

$$\widetilde{M} \supseteq M \quad \text{and} \quad \widetilde{M} \not\supseteq U(H_j) \quad \text{for all } j > k.$$

Such a module $\widetilde{M}$ exists since M has these properties and J is finite-dimensional. We put

$$U_i = W_i + \widetilde{M} = W_i \oplus \widetilde{M}, \quad i = 1, 2, \dots$$

Because $W_i \subseteq I$ and $\widetilde{M} \subseteq J$, these modules are all distinct. They are K-admissible. Indeed, for all $j \le k$ we know $V_j \not\subseteq W_i$ and hence $U(H_j) \cap I \not\subseteq W_i$. This implies $U(H_j) \not\subseteq W_i \oplus J$ and, in particular, $U(H_j) \not\subseteq U_i$. For all $j > k$ we have $U(H_j) \not\subseteq \widetilde{M}$ and, as $U(H_j) \subseteq J$, we have $U(H_j) \not\subseteq I \oplus \widetilde{M}$, which implies $U(H_j) \not\subseteq U_i$. Finally, our modules U_i are *maximally* K-admissible. Let the module U be strictly larger than some U_i. Since W_i is a maximal submodule of I, U either contains I or $U \cap J$ contains $\widetilde{M}$ as a proper submodule. In the first case U contains $I \oplus M = I \oplus (U(H_1) \cap J)$ and thus $U(H_1)$. In the second case there is a $j > k$ such that $U(H_j) \subseteq U \cap J$ (by the maximality property of $\widetilde{M}$) and hence $U(H_j) \subseteq U$. Consequently, U is not K-admissible. Altogether, we have constructed an infinite series U_i of maximal K-admissible modules. ∎

Proof of Lemma 2. The proof goes by induction on $r \ge 2$. First let $r = 2$, so $I = U_1 \oplus U_2$ with $U_1 \cong U_2 \cong V$. Let $\lambda : U_1 \to U_2$ be a $K[G]$-linear isomorphism. For an element $a \in K$ define

$$W^{(a)} = \{u + a\lambda(u) : u \in U_1\}.$$

Then $W^{(a)}$ is a submodule of I, $W^{(a)} \cong U_1 \cong V$, and $W^{(a)} \cap W^{(b)} = 0$ whenever $a \ne b \in K$. Therefore, I contains infinitely many submodules $\cong V$, as K is an infinite field. Among these, one can choose infinitely many modules W_i, $i = 1, 2, \dots$, different from $V_1, \dots, V_k$. Since both W_i and V_j are simple, this means $W_i \cap V_j = 0$ for all i, j.

Suppose the lemma holds for $r \ge 2$. Let $I \cong V^{r+1}$ and $V_1, \dots, V_k \subseteq I$ be $\cong V$. Of course, I also contains infinitely many submodules $\cong V$. We choose one of these, say V_0, different from $V_1, \dots, V_k$. Let I' be a $K[G]$-linear complement of V_0 and $\pi : I = V_0 \oplus I' \to I'$ the corresponding $K[G]$-linear projection (whose kernel is V_0). Then $\pi(V_j) \ne 0$ for all $j = 1, \dots, k$; otherwise $V_j \subseteq V_0$ and, since both modules are simple, $V_j = V_0$. In particular, $\pi(V_j) \cong V_j \cong V$ for all $j = 1, \dots, k$. Because $I' \cong V^r$, there are infinitely many distinct modules $W_i' \subseteq I'$, $i = 1, 2, \dots$, none of which contains $\pi(V_j)$, $j = 1, \dots, k$. Put $W_i = V_0 \oplus W_i'$. The modules W_i are all distinct since $\pi(W_i) = W_i'$. Further, $V_j \not\subseteq W_i$, for otherwise $\pi(V_j) \subseteq \pi(W_i) = W_i'$—which we have excluded. ∎

6. Wild pairs with Schur index 1. Let V be a simple $K[G]$-module and $I \cong V^r$ its isotypical component in $K[G/H]$. In the sequel we assume $r \ge 2$ and that $U_1, \dots, U_k$ are nonzero submodules of I. The description of all maximal K-admissible modules in $K[G/H]$ often relies on the knowledge of

all maximal submodules W of I with $W \not\supseteq U_j$ for $j = 1, \dots, k$. For instance, suppose that $U(H_j) \cap I \neq 0$ for all minimal groups $H_j > H$, $j = 1, \dots, m$. Let J be the (uniquely determined) $K[G]$-linear complement of I in $K[G/H]$. If W runs through all maximal submodules of I not containing $U(H_j) \cap I$, $j = 1, \dots, m$, then each module $W \oplus J$ is a maximal K-admissible submodule of $K[G/H]$.

The purpose of this section is a one-to-one parametrization of the said modules W under the additional assumption that the Schur index κ of V equals 1. In this way we obtain a description of all maximal K-admissible modules in the case of the wild pairs $(D_{2p}, 1)$, where D_{2p} means the dihedral group of order $2p$, p a prime (our main example). Special attention will be paid to the cases $p = 3$, 5.

For the time being we simply assume that $I = V^r$. Let $\varepsilon \in K[G]$ denote the central idempotent belonging to V, so $\varepsilon = \varepsilon_{\widehat{\chi}}$ for some absolutely irreducible character χ that occurs in the K-irreducible character $\widehat{\chi}$ of V. The field $L = K(\chi(s) : s \in G)$ plays an important role now. It is known that this field is isomorphic to the center $C(K[G]\varepsilon) = C(K[G])\varepsilon$ of the simple K-algebra $K[G]\varepsilon$ (cf. [12], p. 544, Hilfssatz 14.7, b)). In other words, if $L' = C(K[G])\varepsilon$ is considered as a K-algebra with unit element ε, then there is an isomorphism

$$\lambda : L \to L' : 1 \mapsto \varepsilon \tag{39}$$

of K-algebras. By means of (39), any L'-vector space can be considered as an L-vector space, and conversely. In particular, the L'-algebra $K[G]$ is an L-algebra. For this reason we shall feel free to identify elements $a \in L'$ with their preimages $\lambda^{-1}(a) \in L$.

We assume that L (or L', respectively) is a splitting field of V, which is the same as $\kappa = 1$. Under this assumption each $K[G]$-linear endomorphism ϱ of V has the shape

$$\varrho = a \cdot \mathrm{id}_V, \qquad a \in L;$$

conversely, since L' lies in the center of $K[G]$, it is clear that mappings of this type are $K[G]$-linear.

In what follows we fix an arbitrary element $v \in V$, $v \neq 0$. Then we form the element $v_i = (0, \dots, v, \dots, 0) \in V^r$ whose ith entry is v whereas all other entries are zero, $i = 1, \dots, r$. These elements form an L-basis of the vector space

$$V_L^r = {}_L\langle v_1, \dots, v_r \rangle.$$

Every submodule U of V^r is isomorphic to V^q for some $q \leq r$. This number q is called the *rank* of U and denoted by $\operatorname{rank} U$. We put

$$U_L = U \cap V_L^r.$$

The following fundamental proposition is probably implicit in the literature but we do not know an appropriate quotation. So we include the proof here.

PROPOSITION 21. *The map $U \mapsto U_L$ defines an inclusion-preserving bijection between the set of $K[G]$-submodules of V^r and the set of L-subspaces of V_L^r. Moreover*, $\operatorname{rank} U$ *equals the L-dimension* $\dim U_L$, *and* $U = {}_{K[G]}\langle U_L\rangle$.

Proof. Let U be a submodule of V^r and $\varrho : V^q \to U$ a $K[G]$-linear isomorphism. We define the elements $v_j \in V^q$, $j = 1, \dots, q$, just in the same way as the above elements $v_i \in V^r$: So the jth entry of v_j equals v and the others are zero. Note that the family $(\varrho(v_j) : j = 1, \dots, q)$ is L-linearly independent because

$$\varrho(V^q) = \bigoplus_{j=1}^{q} K[G]\varrho(v_j).$$

In the following parts (a) and (b) of the proof we show

$$U_L = {}_L\langle \varrho(v_j) : j = 1, \dots, q\rangle.$$

This yields, in particular, $\operatorname{rank} U = \dim U_L$; the other assertions will follow quickly.

(a) First we show $\varrho(v_j) \in U_L$ for each j. To this end we consider the $K[G]$-linear injection

$$\theta_j : V \to V^q : v \mapsto v_j$$

and the $K[G]$-linear projection

$$\pi_i : V^r \to V$$

that maps v_i onto v and the remaining v_l's onto 0. Then $\pi_i \circ \varrho \circ \theta_j$ is a $K[G]$-linear endomorphism of V. By our assumption, this endomorphism can be written $a_{ij} \cdot \mathrm{id}_V$ for some element $a_{ij} \in L$. Therefore, $\pi_i(\varrho(v_j)) = a_{ij} v$ and, consequently,

$$\varrho(v_j) = \sum_{i=1}^{r} a_{ij} v_i \in V_L^r \cap U = U_L. \tag{40}$$

(b) Since the vectors $\varrho(v_j)$ are L-linearly independent, the $r \times q$ matrix $A = (a_{ij})$ has rank q. Thus, there is a $q \times r$ matrix $B = (b_{ji})$ such that BA is the $q \times q$ unit matrix. Now suppose that w is in U_L; this means, on the one hand,

$$w = \sum_{i=1}^{r} c_i v_i, \qquad c_i \in L, \tag{41}$$

on the other hand,

$$w = \sum_{j=1}^{q} \mu_j \varrho(v_j), \qquad \mu_j \in K[G]. \tag{42}$$

We show that there are elements $m_j \in L$ such that $\mu_j v = m_j v$ for all $j = 1, \dots, q$. Then the $K[G]$-linearity of ϱ implies

$$w = \sum_{j=1}^{q} m_j \varrho(v_j) \in {}_L\langle \varrho(v_j) : j = 1, \dots, q \rangle,$$

as desired. But (40)–(42) give

$$\sum_{i=1}^{r} c_i v_i = \sum_{i=1}^{r} \Big(\sum_{j=1}^{q} a_{ij} \mu_j \Big) v_i,$$

whence, because $V^r = \bigoplus_{i=1}^{r} K[G] v_i$,

$$c_i v_i = \sum_{j=1}^{q} a_{ij} \mu_j v_i$$

follows for each $i = 1, \dots, r$. This equation remains valid if v_i is replaced by v on both sides. On applying the matrix B, we obtain

$$\sum_{i=1}^{r} b_{ji} c_i v = \mu_j v$$

for all $j = 1, \dots, q$. So the left side of each of these equations yields an appropriate element $m_j \in L$.

(c) According to (a) and (b), $U_L = {}_L\langle \varrho(v_j) : j = 1, \dots, q \rangle$. This implies $U = {}_{K[G]}\langle U_L \rangle$. Consequently, the map $U \mapsto U_L$ is injective. It preserves the inclusion, for $U \subseteq U'$ implies $U \cap V_L^r \subseteq U' \cap V_L^r$. So there remains only one fact to be shown, namely, that every L-subspace W of V_L^r has the form U_L. Let $(w_1, \dots, w_q)$ be an L-basis of W. Since each w_j can be written $w_j = \sum_{i=1}^{r} a_{ij} v_i$, $a_{ij} \in L$, it is easy to see that $v_j \mapsto w_j$ defines a $K[G]$-linear map $\widetilde{\varrho} : V^q \to V^r$. The module $U = \widetilde{\varrho}(V^q)$ has a rank $\leq q$; so we know already that $\dim U_L \leq q$. On the other hand, $w_1, \dots, w_q$ are in U_L, so $\dim U_L = q$ and $U_L = W$. ∎

In reality, $I \subseteq K[G/H]$ is not *identical* with V^r but only isomorphic. Hence we assume that

$$I = \bigoplus_{i=1}^{r} K[G] v_i,$$

where $K[G]v_i$ is a submodule of I isomorphic to the simple module V. Then Proposition 21 remains true word by word, provided that the elements v_i have been chosen in a *symmetry-adapted manner:* This means that for all

$i, j \in \{1, \ldots, r\}$ there is a $K[G]$-linear isomorphism $K[G]v_i \to K[G]v_j$ mapping v_i to v_j. On putting $I_L = {}_L\langle v_1, \ldots, v_r\rangle$, we obtain the corresponding bijection $U \mapsto U_L = U \cap I_L$ between the submodules of I and the L-subspaces of I_L.

Let $a = (a_1, \ldots, a_r) \in L^r$. For a vector $w = b_1v_1 + \ldots + b_rv_r \in I_L$, put

$$[a, w] = a_1b_1 + \ldots + a_rb_r \in L.$$

If a is different from $0 \in L^r$, the set $\{w \in I_L : [a, w] = 0\}$ forms an $(r-1)$-dimensional subspace of I_L, and all $(r-1)$-dimensional subspaces are obtained in this way. By Proposition 21, the corresponding $K[G]$-modules

$$W_a = {}_{K[G]}\langle w \in I_L : [a, w] = 0\rangle, \qquad a \in L^r \smallsetminus \{0\},$$

run through all maximal (i.e., rank $r-1$) submodules of I. This fact allows parametrizing the maximal submodules by the points of the projective space

$$\mathbb{P}_L^{r-1} = \{a \cdot L^\times : a \in L^r \smallsetminus \{0\}\}.$$

Indeed, it is now easy to see that

$$\mathbb{P}_L^{r-1} \to \{W : W \text{ a maximal submodule of } I\} : a \cdot L^\times \mapsto W_a \tag{43}$$

defines a bijection. Further, we note the following system of $K[G]$-generators of the module W_a: If $a = (a_1, \ldots, a_r)$ and $a_i \neq 0$, say, then

$$W_a = \bigoplus_{\substack{j=1 \\ j \neq i}}^{r} K[G](a_iv_j - a_jv_i).$$

This follows from the fact that these generators form an L-basis of $\{w \in I_L : [a, w] = 0\}$.

Let U be an arbitrary submodule of I of rank q ($\leq r$). Then U_L has an L-basis $(w_1, \ldots, w_q)$. Consequently, the system of linear equations $([a, w_j] = 0 : j = 1, \ldots, q)$ has rank q. Therefore,

$$\mathbb{P}(U) = \{a \cdot L^\times : [a, w_j] = 0,\ j = 1, \ldots, q\}$$

is an $(r - 1 - q)$-dimensional projective subspace of $\mathbb{P}_L^{r-1}$. Proposition 21 shows that $a \cdot L^\times$ is in $\mathbb{P}(U)$ if, and only if, W_a contains U. Altogether, we have

THEOREM 5. *In the above setting let $U_1, \ldots, U_k$ be submodules of the isotypical component I. Then the map* (43) *induces a bijection between*

$$\mathbb{P}_L^{r-1} \smallsetminus (\mathbb{P}(U_1) \cup \ldots \cup \mathbb{P}(U_k))$$

and the set of maximal submodules W of I that do not contain any of $U_1, \ldots, U_k$.

EXAMPLE 7. Let (G, H) be a primitive but not K-multiplicity-free pair, so there is an isotypical component $I \cong V^r$ of $K[G/H]$ with $r \geq 2$. Then

$G = H_1$ is the only minimal group $> H$ and $U(G) \cap I = I$. As we pointed out at the beginning of this section, all modules of the shape $W \oplus J$, where J denotes the complement of I and W a maximal submodule of I, are K-admissible. Whenever the Schur index of V equals 1, our theorem gives a parametrization of this infinite series of maximal K-admissible modules: The points $a \cdot L^\times$ of $\mathbb{P}_L^{r-1}$ correspond to the modules $W_a \oplus J$. We inspect the case of Example 6 (Section 2) more closely: So $K = \mathbb{Q}$, $G = \mathrm{PSL}(2, 11)$, $H = D_{12}$. On adopting suitable notations we have the decomposition

$$\mathbb{Q}[G/H] = I_1 \oplus I_{\widehat{\chi}_1} \oplus I_{\chi_2} \oplus I_{\widehat{\chi}_3},$$

where $I_1, I_{\widehat{\chi}_1}, I_{\widehat{\chi}_3}$ are simple but $I = I_{\chi_2} \cong V^2$ for some simple $\mathbb{Q}[G]$-module V of $\mathbb{Q}$-dimension 10. Hence the projective line $\mathbb{P}^1_{\mathbb{Q}}$ parametrizes the family $W_a \oplus J_{\{\chi_2\}}$, $W_a \cong V$, $a = (a_1, a_2) \in \mathbb{Q}^2 \setminus \{0\}$, of maximal $\mathbb{Q}$-admissible modules of $\mathbb{Q}$-dimension 45. Apart from these, there are only two other maximal $\mathbb{Q}$-admissible modules, namely, the closed modules $J_{\{\chi_1\}}$ and $J_{\{\chi_3\}}$ described in Section 2, of respective dimensions 45 and 31.

Example 8. Let $p \geq 3$ be a prime number and $G = D_{2p}$ the dihedral group of order $2p$, generated by the elements s, t with $\mathrm{ord}(s) = p$, $\mathrm{ord}(t) = 2$, $ts = s^{-1}t$. We take $K = \mathbb{Q}$ and $H = 1$, so $K[G/H] = \mathbb{Q}[G]$. There are exactly three $\mathbb{Q}$-irreducible characters of G: the trivial character 1, the nontrivial group homomorphism $\chi_1 : G \to \{\pm 1\}$, and a character ψ of degree $\psi(1) = p - 1$. This character is given by $\psi(u) = -1$ for each $u \in \langle s \rangle \setminus \{1\}$ and $\psi(u) = 0$ for each $u \in G \setminus \langle s \rangle$ (cf. also the proof of Proposition 13). The corresponding central idempotent is

$$\varepsilon = \varepsilon_\psi = (p-1)/p \cdot 1 - 1/p \cdot \sum_{j=1}^{p-1} s^j. \tag{44}$$

Let ζ denote a primitive pth root of unity. Any absolutely irreducible character χ occurring in ψ has the field of values $L = \mathbb{Q}(\xi)$, with $\xi = \zeta + \zeta^{-1}$. The isomorphic field $L' = C(\mathbb{Q}[G])\varepsilon$ is generated by $\xi' = (s + s^{-1})\varepsilon$, and an isomorphism λ as in (39) can be defined by $\xi \mapsto \xi'$. The simple module V belonging to $I_\psi = \mathbb{Q}[G]\varepsilon$ has $\mathbb{Q}$-dimension $\psi(1) = p - 1$ and, therefore, L-dimension 2. Moreover, $I_\psi \cong V^2$ as $\mathbb{Q}[G]$-modules. This implies, in particular, that the Schur index of V equals 1. Because of (43), the projective line $\mathbb{P}^1_L$ parametrizes a family of maximal submodules of $\mathbb{Q}[G/H]$ bijectively. The members of this family can be written

$$W_a \oplus I_1 \oplus I_{\chi_1}, \qquad a = (a_1, a_2) \in L^2 \setminus \{0\},$$

with $W_a \subseteq I_\psi$, $W_a \cong V$. *Which of these modules are $\mathbb{Q}$-admissible?* The answer requires the knowledge of the minimal subgroups of G. There are exactly $p+1$ groups of this kind: namely, the groups $H_j = \langle s^j t \rangle$, $j = 1, \ldots, p$, of order 2, and $H_{p+1} = \langle s \rangle$ of order p. It is easy to check that $U(H_{p+1}) = I_\psi$.

However, for every $j \in \{1, \dots, p\}$ there is a simple submodule $W^{(j)}$ of I_ψ such that $U(H_j) = W^{(j)} \oplus I_{\chi_1}$. Suppose, therefore, that the projective points $a^{(j)} \cdot L^\times$ of $\mathbb{P}^1_L$ are such that $W^{(j)} = W_{a^{(j)}}$. Then the above parametrization maps the set

$$\mathbb{P}^1_L \smallsetminus \{a^{(j)} \cdot L^\times : j = 1, \dots, p\}$$

onto an infinite series of maximal $\mathbb{Q}$-admissible modules. The reader may convince himself that the only maximal $\mathbb{Q}$-admissible modules different from these have the shape

$$W_{a^{(j)}} \oplus I_1, \quad j = 1, \dots, p.$$

It should be remarked that there is no *closed* maximal $\mathbb{Q}$-admissible module.

The above examples suffer from one defect so far: It would be desirable to explicitly know the symmetry-adapted generators $v_1, \dots, v_r$ of the isotypical component $I \cong V^r$ in question. This defect can be remedied if one has the simple module V at hand. Taking this for granted, we extend the isomorphism λ of (39) to a homomorphism of K-algebras

$$L[G] \to K[G]\varepsilon,$$

by mapping $s \in G$ to $s\varepsilon$. Thereby $K[G]\varepsilon$ becomes a simple L-algebra (in fact, a subalgebra of $L[G]$) and the $K[G]\varepsilon$-modules V and $I = \varepsilon K[G/H]$ become $L[G]$-modules. Since V is a simple $L[G]$-module with splitting field L, one can adapt the procedure described in [18], p. 23 ff., to the present context: Let $(x_1, \dots, x_d)$ be an L-basis of V. Suppose we know the coefficients $c_{lj} \in L$ occurring in the relations

$$sx_j = \sum_{l=1}^{d} c_{lj}(s) x_l, \quad j = 1, \dots, d,$$

for all $s \in G$. Then we put

$$\pi = \sum_{s \in G} c_{11}(s^{-1}) s \in L[G] \quad \text{and} \quad I_L = \pi I.$$

In fact, I_L also equals $\pi K[G/H] = \{\pi\alpha : \alpha \in K[G/H]\}$, and $\dim I_L = r$. Now let $(v_1, \dots, v_r)$ be an arbitrary L-basis of I_L. Then

$$I = \bigoplus_{i=1}^{r} L[G]v_i = \bigoplus_{i=1}^{r} K[G]v_i,$$

and $v_i \mapsto v_j$ defines a $K[G]$-linear isomorphism between any two of the summands. Finally, for any submodule U of $K[G/H]$, $U_L = \pi U$, so it is easy to check relations like $W_a \supseteq U$.

Example 9. We consider $K = \mathbb{Q}$ and the above pair $(G, H) = (D_{2p}, 1)$ in the special case $p = 5$. Put $I = I_\psi$. Here $\xi = \zeta + \zeta^{-1}$ equals $(-1 + \sqrt{5})/2$

for one of the two possible choices of $\sqrt{5}$. Recall that λ maps ξ onto $\xi' = (s + s^{-1})\varepsilon$ with ε as in (44). We give an *ad hoc* description of the module V: $V = Lx_1 \oplus Lx_2$, and the generators s and t of D_{10} act on these basis elements by

$$\begin{aligned} sx_1 &= -x_1 + x_2, & sx_2 &= -(2+\xi)x_1 + (1+\xi)x_2, \\ tx_1 &= -(1+\xi)x_1 + x_2, & tx_2 &= -(1+\xi)x_1 + (1+\xi)x_2. \end{aligned}$$

This data suffices to compute the element $\pi \in L[G]$. Then $I_L = \pi I$ has the L-basis

$$v_1 = 1 - s^4 - st + s^2t, \quad v_2 = v_1t = -s + s^2 + t - s^4t.$$

We obtain $I = \mathbb{Q}[G]v_1 \oplus \mathbb{Q}[G]v_2$, with the symmetry-adapted generators v_1, v_2. The simple submodules W_a of I, $a = (a_1, a_2) \in L^2 \setminus \{0\}$, have the shape $\mathbb{Q}[G](a_2v_1 - a_1v_2)$. In particular,

$$U(H_j) = W_{a^{(j)}} \oplus I_{\chi_1}, \quad j = 1, \dots, 5,$$

with $a^{(1)} = (2 + \xi, -1)$, $a^{(2)} = (2\xi, -1)$, $a^{(3)} = (1 + \xi, -2)$, $a^{(4)} = (\xi - 1, 1)$, $a^{(5)} = (1, 1)$.

We conclude this paper by returning to the relations (4) of the Introduction. So far, the possibility of these relations has been studied in some tame cases (cf. Corollary to Proposition 10). We look at our main examples of wild pairs now. In other words: *Is there a $\mathbb{Q}$-admissible element of the shape $\alpha = 1 - u - v$, $u \neq v \in G \setminus \{1\}$, in the case $(G, H) = (D_{2p}, 1)$?* By Theorem 5 of [7], the answer can be affirmative only for $p \in \{3, 5\}$. As above, put $\varepsilon = \varepsilon_\psi$. In the case $p = 5$ one can check that the $\mathbb{Q}[G]$-module $\mathbb{Q}[G]\varepsilon\alpha$ always has $\mathbb{Q}$-dimension 8, so $\mathbb{Q}[G]\alpha$ contains $I = I_\psi = U(H_{p+1})$. Accordingly, the answer is *negative*. In the case $p = 3$ the group $D_6 = \langle s, t\rangle$ is the symmetric group S_3. We collect the relevant data in the sense of our above results: $L = \mathbb{Q}$ and $I = I_\psi$ has the symmetry-adapted generators

$$v_1 = 1 - s^2 - st + s^2t, \quad v_2 = v_1t = -s + s^2 + t - s^2t,$$

$W_a = \mathbb{Q}[G](a_2v_1 - a_1v_2)$ for $a = (a_1, a_2) \in \mathbb{Q}^2$, $a \neq 0$. Further, $U(H_j) \cap I = W_{a^{(j)}}$, $j = 1, 2, 3$, with $a^{(1)} = (1, -2)$, $a^{(2)} = (-2, 1)$, $a^{(3)} = (1, 1)$. On the other hand, when α runs through $1 - t - st$, $1 - t - s^2t$, and $1 - st - s^2t$, the module $\mathbb{Q}[G]\alpha$ equals $W_b \oplus I_1 \oplus I_{\chi_1}$, where b runs through $(0, 1)$, $(1, 0)$, $(1, -1)$, respectively. Therefore, each of these three elements α is $\mathbb{Q}$-admissible.

The above pairs $(D_{2p}, 1)$, $p = 3, 5$, belong to the simplest examples covered by the cited theorem of [7]. The result in either case sheds some light on the question to which extent this theorem describes the reality.

References

[1] G. Baron, M. Drmota and M. Skałba, *Polynomial relations between polynomial roots*, J. Algebra 177 (1995), 827–846.

[2] T. Breuer and K. Lux, *The multiplicity-free permutation characters of the sporadic simple groups and their automorphism groups*, Comm. Algebra 24 (1996), 2293–2316.

[3] P. J. Cameron, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. 13 (1981), 1–22.

[4] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic Number Theory*, Academic Press, London, 1967.

[5] J. H. Conway *et al.*, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[6] C. W. Curtis and I. Reiner, *Methods of Representation Theory*, Vol. II, Wiley, New York, 1987.

[7] J. D. Dixon, *Polynomials with nontrivial relations between their roots*, Acta Arith. 82 (1997), 293–302.

[8] J. D. Dixon and B. Mortimer, *Permutation Groups*, Springer, New York, 1996.

[9] M. Drmota and M. Skałba, *On multiplicative and linear independence of polynomial roots*, in: Contributions to General Algebra 7, D. Dorninger *et al.* (eds.), Hölder-Pichler-Tempsky, Wien, and Teubner, Stuttgart, 1991, 127–135.

[10] —, —, *Relations between polynomial roots*, Acta Arith. 71 (1995), 65–77.

[11] K. Girstmair, *Linear dependence of zeros of polynomials and construction of primitive elements*, Manuscripta Math. 39 (1982), 81–97.

[12] B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967; reprint 1979.

[13] B. Huppert and N. Blackburn, *Finite Groups III*, Springer, Berlin, 1982.

[14] V. A. Kurbatov, *Galois extensions of prime degree and their primitive elements*, Soviet Math. (Iz. VUZ) 21 (1977), 49–53.

[15] M. W. Liebeck and J. Saxl, *The primitive permutation groups of odd degree*, J. London Math. Soc. (2) 31 (1985), 250–264.

[16] G. Malle und B. H. Matzat, *Realisierung von Gruppen* $\mathrm{PSL}_2(\mathbb{F}_p)$ *als Galoisgruppen über* $\mathbb{Q}$, Math. Ann. 272 (1985), 549–565.

[17] H. P. Schlickewei and S. A. Stepanov, *Algorithms to construct normal bases of cyclic number fields*, J. Number Theory 44 (1993), 30–40.

[18] J. P. Serre, *Linear Representations of Finite Groups*, Springer, New York, 1977.

[19] C. J. Smyth, *Additive and multiplicative relations connecting conjugate algebraic numbers*, J. Number Theory 23 (1986), 243–254.

[20] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.

Institut für Mathematik
Universität Innsbruck
Technikerstr. 25/7
A-6020 Innsbruck, Austria
E-mail: Kurt.Girstmair@uibk.ac.at

Received on 18.9.1998
and in revised form on 7.12.1998 (3465)