Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Journal of Algebra 317 (2007) 306–323
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

Small linearly equivalent G-sets and a construction of Beaulieu ☆

Ben Webster [1]

Department of Mathematics, University of California, Berkeley, Berkeley, CA 94720, USA

Received 1 November 2006

Available online 9 August 2007

Communicated by Vera Serganova

Abstract

Two G-sets (G a finite group) are called linearly equivalent over a commutative ring k if the permutation representations $k[X]$ and $k[Y]$ are isomorphic as modules over the group algebra kG. Pairs of linearly equivalent non-isomorphic G-sets have applications in number theory and geometry. We characterize the groups G for which such pairs exist for any field, and give a simple construction of these pairs. If k is $\mathbb{Q}$, these are precisely the non-cyclic groups. For any non-cyclic group, we prove that there exist G-sets which are non-isomorphic and linearly equivalent over $\mathbb{Q}$, of cardinality $\leqslant 3(\#G)/2$. Also, we investigate a construction of P. Beaulieu which allows us to construct pairs of transitive linearly equivalent S_n-sets from arbitrary G-sets for an arbitrary group G. We show that this construction works over all fields and use it construct, for each finite set $\mathcal{P}$ of primes, S_n-sets linearly equivalent over a field k if and only if the characteristic of k lies in $\mathcal{P}$.

Keywords: Linearly equivalent G-sets; Arithmetically equivalent fields

Let G be a finite group, X a G-set and k a commutative ring. The set of maps from X to k, denoted $k[X]$, has a natural structure of a k-module, and a natural action of G given by precom-

☆ This material is based upon work supported under a National Science Foundation Graduate Research Fellowship and partially supported by the RTG grant DMS-0354321. The LSU Research Experience Program is supported by the Louisiana Board of Regents Enhancement grant, LEQSF (1999–2001)-ENH-TR-17 and National Science Foundation grant, DMS-0097530.

E-mail address: bwebste@math.berkeley.edu.

URL: http://math.berkeley.edu/~bwebste/.

[1] School of Mathematics, Institute for Advanced Study, 1 Einstein Drive, Princeton, NJ 08540, USA.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2007.07.007

position. That is, $k[X]$ is a module over the group algebra kG. We call $k[X]$ the *permutation representation of G on X*.

Two G-sets X and Y are called *linearly equivalent* over k if $k[X] \cong k[Y]$ as kG-modules. Linear equivalence is an equivalence relation, and will be denoted $X \overset{\text{lin}}{=}_k Y$. If no base ring is written, then it will be assumed to be $\mathbb{Q}$.

The definition of linear equivalence was originally motivated by the following theorems from number theory.

Theorem. *(See Perlis [Per1].) Two number fields $E = \mathbb{Q}[\alpha]$ and $E' = \mathbb{Q}[\alpha']$ have identical Dedekind zeta functions if and only if there is a Galois extension $L/\mathbb{Q}$ containing E, E' with Galois group $G = Gal(L/\mathbb{Q})$, such that $G \cdot \alpha \overset{\text{lin}}{=}_{\mathbb{C}} G \cdot \alpha'$.*

Theorem. *(See Perlis, Boltje [Per2,Bol].) Moreover, if $G \cdot \alpha \overset{\text{lin}}{=}_{\mathbb{F}_p} G \cdot \alpha'$, then the p-torsion subgroups of the class groups of E and E' are isomorphic.*

Ideas along these lines have been further developed in [dS,BB]. Similarly, pairs of linearly equivalent G-sets have been used, first by Sunada in [Sun], in the construction of pairs of manifolds with identical Laplacian and length spectra. By the same yoga, they can be used to produce pairs of isospectral graphs (see, for example, the work of Stark and Terras in [ST] on zeta functions of graphs).

In order for two G-sets X and Y to be linearly equivalent, it is necessary that $\#X = \#Y$, since $\#X = \dim k[X]$. Thus, a new invariant of the group G and ring k is the set

$$\deg_k(G) = \{n \mid \exists X, Y,\ X \overset{\text{lin}}{=}_k Y,\ X \ncong Y,\ \#X = \#Y = n\}.$$

If $X \overset{\text{lin}}{=}_k Y$, then $X \sqcup \{*\} \overset{\text{lin}}{=}_k Y \sqcup \{*\}$ for any singleton set $\{*\}$ so

$$\deg_k(G) = \{n \in \mathbb{Z} \mid n \geqslant \ell\}$$

for some integer ℓ, which is the degree of the smallest pair of linearly equivalent and non-isomorphic G-sets. We call this integer $\mathfrak{md}_k(G)$. If $\deg_k(G)$ is empty, we say $\mathfrak{md}_k(G) = \infty$. In this paper we use a variety of group theoretic techniques to obtain bounds on $\mathfrak{md}_{\mathbb{Q}}(G)$.

In Section 1, we recall the basic operations of restriction and induction of G-sets, and explore their interplay with linear equivalence. The relationship between linear equivalence on different groups will a primary tool in this paper.

In Section 2, we characterize those groups for which there are pairs of non-isomorphic G-sets which are linearly equivalent over a fixed field k. In the case where $k = \mathbb{Q}$, this is exactly the groups which are not cyclic. While the question of finding such G-sets which are transitive is quite difficult and subtle (see [dSL,Fei,Gur,GW] for some partial results), finding non-transitive examples is surprisingly easy. We then apply this construction to a number of special cases where particularly simple pairs of linearly equivalent G-sets can be found.

In Section 3, we show, by an analysis of cases, that

Theorem. *If G is not cyclic, $\mathfrak{md}_{\mathbb{Q}}(G)/\#G \leqslant 3/2$.*

We give sharper bounds for some smaller classes of groups, including the class of all non-solvable groups.

In Section 4, we discuss Beaulieu's construction [Bea] of pairs of transitive linearly equivalent S_n-sets starting from arbitrary pairs of linearly equivalent G-sets. We show that this construction is independent of the field used, and obtain some criteria for when the constructed sets are not isomorphic.

In Section 5, we apply this construction to find pairs of G-sets linearly equivalent over any field whose characteristic lies outside a given finite set of prime numbers.

1. Basic operations on G-sets

The symbols G, H and K will denote finite groups throughout. By convention, all G-actions are on the left. We let set_G be the category of finite G-sets, with morphisms given by equivariant maps. As usual, $\mathbb{F}_q$ denotes the finite field with q elements, considered as a field, or as an abelian group.

Throughout the rest of the paper, k will always denote a field and p will always denote the characteristic of this field, which may 0 or a prime number.

If X is a G-set, and A any set, we define a new G-set $A \cdot X$ to be the set $A \times X$ with G acting on the right factor only (we use $\cdot$ to distinguish this operation from the Cartesian product of two G-sets, which has the diagonal action by definition). We will denote $\{1, \dots, n\} \cdot X$ by $n \cdot X$.

If $\psi : H \to G$ is a homomorphism, then there is a functor

$$\mathrm{res}_\psi : \mathsf{set}_G \to \mathsf{set}_H$$

called *restriction along* ψ, defined by composition of action homomorphisms: if X is a G-set with action homomorphism $\rho_X : G \to \mathrm{Sym}\, X$, then H acts by $\rho_X \circ \psi$. If the map ψ is injective, we think of H as a subgroup of G, and denote the restriction by res_H^G.

We let $\mathrm{res}_\psi : kG\text{-mod} \to kH\text{-mod}$ denote the corresponding functor for representations.

Proposition 1.1. *For all $\varphi : H \to G$,*

(1) *The diagram*

$$\begin{tikzcd}
\mathsf{set}_G \arrow[r, "\mathrm{res}_\psi"] \arrow[d, "k[\text{-}]"] & \mathsf{set}_H \arrow[d, "k[\text{-}]"] \\
kG\text{-mod} \arrow[r, "\mathrm{res}_\psi"] & kH\text{-mod}
\end{tikzcd}$$

commutes.

(2) *If $X \overset{\mathrm{lin}}{=}_k Y$, then $\mathrm{res}_\psi X \overset{\mathrm{lin}}{=}_k \mathrm{res}_\psi Y$.*

(3) *For X any G-set, we have $\#X = \#\mathrm{res}_\psi X$.*

Part (1) of the above allows us to bound $\mathfrak{md}_k(G)$ by $\mathfrak{md}_k()$ of all its quotients.

Lemma 1.2. *If $\psi : H \to G$ is a surjective homomorphism, then $\mathfrak{md}_k(H) \leqslant \mathfrak{md}_k(G)$.*

Proof. Let X and Y be non-isomorphic G-sets linearly equivalentover k with $\#X = \mathfrak{md}_k(G)$. We know that $\operatorname{res}_\psi X \overset{\text{lin}}{=}_H \operatorname{res}_\psi Y$. Thus, we need only confirm that $\operatorname{res}_\psi X \ncong_H \operatorname{res}_\psi Y$.

Since X and $\operatorname{res}_\psi X$ have the same underlying set, any H-set isomorphism $\operatorname{res}_\psi X \to \operatorname{res}_\psi Y$ also defines an isomorphism $X \to Y$ (a priori this is only a set map). Obviously, this map commutes with the action of any group element in the image of ψ. Since ψ is surjective, this is in fact a G-set isomorphism. More elegantly, one could apply the functor ind_ψ and use part (7) of Proposition 1.3 below.

Thus $\operatorname{res}_\psi X \ncong_H \operatorname{res}_\psi Y$, and $\mathfrak{md}_k(H) \leqslant \#X = \mathfrak{md}_k(G)$. $\square$

Unfortunately, restriction is not useful for understanding $\mathfrak{md}_k(G)$ in terms of the subgroups of G. Since most groups are richer in subgroups than quotients, we will need an operation that can transfer linearly equivalent G-sets to overgroups.

This is provided by the natural adjoint to the functor res_ψ, which is called *induction along* ψ. For any H-set X, we let $\operatorname{ind}_\psi X = (G \times X)/H$, where H acts on the Cartesian product $G \times X$ by

$$^h(g, x) = \bigl(g\psi\bigl(h^{-1}\bigr), {}^h x\bigr).$$

This defines a functor $\operatorname{ind}_\psi : \mathsf{set}_H \to \mathsf{set}_G$.

We will also use ind_ψ to denote the analogue of this functor from representation theory: for a kH-module V, we define $\operatorname{ind}_\psi V = kG \otimes_{kH} V$, using the fact that kG is a right kH-algebra.

Proposition 1.3. *For all $\varphi : H \to G$,*

(1) *The functor* ind_ψ *is left adjoint to* res_ψ.
(2) *The diagram*

$$\begin{tikzcd} \mathsf{set}_H \arrow[r, "\operatorname{ind}_\psi"] \arrow[d, "k[\text{-}]"] & \mathsf{set}_G \arrow[d, "k[\text{-}]"] \\ kH\text{-mod} \arrow[r, "\operatorname{ind}_\psi"] & kG\text{-mod} \end{tikzcd}$$

commutes.
(3) *If* $X \overset{\text{lin}}{=}_k Y$, *then* $\operatorname{ind}_\psi X \overset{\text{lin}}{=}_k \operatorname{ind}_\psi Y$.
(4) *For any subgroup* $K \subset H$, $\operatorname{ind}_\psi(H/K) \cong G/\psi(K)$. *In particular,*

$$\#\operatorname{ind}_\psi(H/K) = \frac{(G : \operatorname{im}\psi)}{(\ker\psi : K \cap \ker\psi)} \#(H/K).$$

(5) *If* ψ *is injective, then* $\#\operatorname{ind}_H^G X = (G : H)\#X$ *for any* H*-set* X.
(6) *If* ψ *is injective, then the stabilizer of any element of* $\operatorname{ind}_\psi X$ *is isomorphic to the stabilizer of some element of* X.
(7) *If* ψ *is surjective, then* $\operatorname{ind}_\psi X \cong \ker\psi \backslash X$, *the orbit space for the action of* $\ker\psi$. *In particular,* $\operatorname{ind}_\psi(\operatorname{res}_\psi(X)) \cong_G X$ *for any* G*-set* X.

Proof. Part (4). Under the action specified above $G \times H/K$ is an $G \times H$-set. The stabilizer of the coset $(1, K)$ is $K' = \{(\psi(x), x) \mid x \in K\}$, and this action is transitive, so $G \times H/K \cong (G \times H)/K'$. Thus $\mathrm{ind}_\psi H/K$ is transitive as a G-set, and the stabilizer of $H(1, K)$ is $\psi(K)$.

The stabilizer of H acting on the coset $(1, K)$ is $K \cap \ker\psi$. Furthermore, G-acts transitively on all H-orbits, so they are all of cardinality $(H : \ker\psi \cap K)$. Thus, we calculate that

$$\#\mathrm{ind}_\psi(H/K) = \frac{\#G}{(H : \ker\psi \cap K)}\#(H/K) = \frac{\#G}{\#\mathrm{im}\,\psi(\ker\psi : \ker\psi \cap K)}\#(H/K).$$

Part (5). Apply the formula of part (4) to each component.

Part (6). This only needs to be checked for X a transitive G-set. In this case, $X \cong H/K$ for some subgroup $K \subset H$, and $\mathrm{ind}_\psi X \cong G/\psi(K)$. Thus the stabilizer of any element of X is conjugate in H to K, and thus isomorphic to K. Similarly, the stabilizer of any element of $\mathrm{ind}_\psi X$ is conjugate in G, and thus isomorphic to $\psi(K)$. Since ψ is injective, the two stabilizers just be isomorphic.

Part (7). For each transitive G-set G/K,

$$\mathrm{ind}_\psi\big(\mathrm{res}_\psi(G/K)\big) \cong_G \mathrm{ind}_\psi\big(H/\psi^{-1}(K)\big) \cong_G G/K.$$

Since res_ψ and ind_ψ respect disjoint union, this implies the result for all X. □

Corollary 1.4. *If $X \overset{\mathrm{lin}}{=}_k Y$, then X and Y have the same number of orbits.*

Proof. Let $\tau : G \to 1$ be the trivial homomorphism. Then by part (7) of Proposition 1.3, $\mathrm{ind}_\tau X \cong G\backslash X$, the orbit space of X. By part (2) of the same proposition, $G\backslash X$ and $G\backslash Y$ are isomorphic as sets with an action of the trivial group, i.e. they are sets with the same cardinality. □

Unfortunately, one must be more careful when using induction than when using restriction, since if we have non-isomorphic H-sets X and Y, it may still be that $\mathrm{ind}_H^G X \cong_G \mathrm{ind}_H^G Y$ (unlike restriction along a surjective map, induction is not full).

For instance, let $K_1, K_2 \subset H$ are subgroups which are not conjugate in H, but which are conjugate in G. Of course, $H/K_1 \ncong_H H/K_2$, but using part (4) of Proposition 1.3, we see that

$$\mathrm{ind}_H^G(H/K_1) \cong_G G/K_1 \cong_G G/K_2 \cong_G \mathrm{ind}_H^G(H/K_2),$$

since in G, the subgroups K_1 and K_2 are conjugate.

For example, if A_4 is the alternating group on 4 elements, and K_4 the Klein four-group generated by the permutations $\{(12)(34), (13)(24), (14)(23)\}$, then all elements of order two are conjugate to each other in A_4, even though they are not in K_4.

However, if there is an element $x \in X$ such that for all $y \in Y$ the stabilizers $\mathrm{Stab}_H(x)$ and $\mathrm{Stab}_H(y)$ are not isomorphic as abstract groups, then $\mathrm{ind}_\psi X \ncong_G \mathrm{ind}_\psi Y$, since induction along an injective map preserves the isomorphism class of stabilizers, by Proposition 1.3.

Lemma 1.5. *If $\psi : H \to G$ is injective, if X and Y are non-isomorphic linearly equivalent G-sets, and if there is $x \in X$ such that for all $y \in Y$ the stabilizers $\mathrm{Stab}_H(x)$ and $\mathrm{Stab}_G(y)$ are not isomorphic, then $\mathfrak{md}_k(G) \leqslant (G : H)\#X$.*

2. An existence theorem

As is well known, the representations $\mathbb{Q}[X] \cong \mathbb{Q}[Y]$ are isomorphic if and only if they have the same character. We denote this character π_X. This character is know to be given by $\pi_X(g) = \#\mathrm{Fix}_g X$, the number of fixed points for the action of g.

Since we will be interested in equivalence over all characteristics, we will need an analogue of character over fields of positive characteristic. In the case of permutation representations, there is a very nice solution to this problem, in which needs only to consider the fixed points of a more general class of groups than cyclic ones.

We call a group cyclic mod p if it is an extension of a cyclic group by a p-group. By convention, a 0-group is trivial, so "cyclic mod 0" simply means "cyclic."

Lemma 2.1. *For two G-sets, X and Y, the following are equivalent*:

(1) $X \overset{\mathrm{lin}}{=}_k Y$.
(2) $\mathrm{res}^G_H X \cong_H \mathrm{res}^G_H Y$ *for all cyclic mod p subgroups $H \subset G$.*
(3) $\#\mathrm{Fix}_X(H) = \#\mathrm{Fix}_Y(H)$ *for all cyclic mod p subgroups $H \subset G$.*

In the case where $p = 0$, this obviously reduces to the statement that representations are determined by their characters.

Proof. (1) $\Rightarrow$ (2). Restriction is a functor, so it sends isomorphisms to isomorphisms.

(2) $\Rightarrow$ (3). Consider $g \in G$ of order d. For each $k \in \mathbb{Z}$, let $\zeta_k = \dim k[X]^{g^k}$ be the dimension of the subspace of $k[X]$ fixed by g^k. This is the same as the number of $\langle g^k\rangle$-orbits on X (as we have previously calculated). Now let ξ_m denote the number of g-orbits of size m on X. These quantities are related by

$$\zeta_k = \sum_{m|d} (k, m)\xi_m.$$

Thus, by Möbius inversion,

$$\xi_m = \frac{1}{(k, m)} \sum_{k|d} \mu(d/k)\zeta_k,$$

where, as usual, μ denotes the Möbius function. In particular,

$$\#\mathrm{Fix}_X(g) = \xi_1 = \sum_{k|d} \mu(d/k)\zeta_k.$$

Thus, the number of fixed points of a cyclic group is determined by the permutation representation.

Now, fix a cyclic mod p subgroup $H \subset G$ and let P be a p-group such that H/P is cyclic, and let $F = \mathrm{Fix}_X(P)$. Note that F is naturally an H/P-set, and the H/P action on $k[F]$ is induced from its embedding into $k[\mathrm{res}^G_H X]$.

In this case, $k[F]$ is the maximal trivial *summand* of $\mathrm{res}^G_P k[X]$, because over characteristic p, no nontrivial transitive permutation representation of a p-group has any trivial summands. This subspace is not unique, since Krull–Schmidt decomposition is not unique, but its isomorphism class as a H/P representation is well defined. Applying the Möbius inversion argument above, we can find the quantity $\#\mathrm{Fix}_F(H/P)$ just from the representation $k[F]$ (and thus just from the representation $k[\mathrm{res}^G_H X]$). Of course,

$$\mathrm{Fix}_F(H/P) = \mathrm{Fix}_X(H),$$

so the number of fixed points of H is determined by $k[\mathrm{res}^G_H X]$.

(3) ⇒ (1). This is the hardest implication, and we will not present a proof here. See [CR, 81.25 and 81.28]. □

We will need a simple computation of $\#\mathrm{Fix}_{G/H}(K)$ for a subgroup $K \subset G$. First, we let

$$L_K(H) = \{g \in G \mid K \subset gHg^{-1}\}.$$

Note that $L_K(H_1) \cap L_K(H_2) = L_K(H_1 \cap H_2)$ and that $L_K(H)H = L_K(H)$. That is, $L_K(H)$ is equipped with a free right H-action by multiplication.

Lemma 2.2.

$$\#\mathrm{Fix}_{G/H}(K) = \#\big(L_K(H)/H\big) = \frac{\#L_K(H)}{\#H}. \tag{1}$$

Proof. The natural map $L_K(H)/H \to G/H$ is an injection, and its image is $\mathrm{Fix}_{G/H}(K)$. □

Let $\mathcal{M} = \{M_1, \ldots, M_\ell\}$ be a set of distinct subgroups of G such that:

(1) The union $H = \bigcup_i M_i$ is a subgroup of G.
(2) For all i, M_i is a proper subgroup of H.
(3) Each cyclic mod p subgroup $C \subset H$ is also contained in M_i for some i.

Note that in the case where $p = 0$, the condition (3) is implied by condition (1).

If G is not cyclic mod p, then all the proper maximal subgroups of G, or all the cyclic mod p subgroups of G will serve as such a set.

On the other hand, the subgroup H must be non-cyclic mod p, since otherwise, condition (3) implies $H = M_i$ for some i, which condition (2) explicitly forbids. In particular, if G is cyclic mod p, then no such subsets of the subgroups of G exist.

We let $\mathcal{J}_e$ be the set of non-empty subsets of $\{1, \ldots, \ell\}$ which have even cardinality, and $\mathcal{J}_o$ be those of odd cardinality. Define G-sets $X_\mathcal{M}$ and $Y_\mathcal{M}$

$$X_\mathcal{M} = \#H \cdot \frac{G}{H} \sqcup \left[\bigsqcup_{S \in \mathcal{J}_e} \#\left(\bigcap_{i \in S} M_i \right) \cdot \frac{G}{\bigcap_{i \in S} M_i} \right], \tag{2}$$

$$Y_\mathcal{M} = \bigsqcup_{S \in \mathcal{J}_o} \#\left(\bigcap_{i \in S} M_i \right) \cdot \frac{G}{\bigcap_{i \in S} M_i}. \tag{3}$$

Note that $X_\mathcal{M} \ncong Y_\mathcal{M}$, since $\mathrm{Fix}_{X_\mathcal{M}}(H)$ is not empty, and, by condition (2) $\mathrm{Fix}_{Y_\mathcal{M}}(H)$ is.

Theorem 2.3. *Let $\mathcal{M}$ satisfy conditions* (1)–(3). *Then for any field k of characteristic p,*

$$X_{\mathcal{M}} \overset{\text{lin}}{=}_k Y_{\mathcal{M}}.$$

Proof. Using formula (1),

$$\mathrm{Fix}_{X_{\mathcal{M}}}(C) = \#L_C(H) + \sum_{S \in \mathcal{J}_e} \#L_C\left(\bigcap_{i \in S} M_i\right), \tag{4}$$

$$\mathrm{Fix}_{Y_{\mathcal{M}}}(C) = \sum_{S \in \mathcal{J}_o} \#L_C\left(\bigcap_{i \in S} M_i\right). \tag{5}$$

By condition (3), $C \leqslant M_i$ for some i. By inclusion–exclusion,

$$\#L_C(H) = \sum_{S \in \mathcal{J}_o} \#\bigcap_{i \in S} L_C(M_i) - \sum_{S \in \mathcal{J}_e} \#\bigcap_{i \in S} L_C(M_i). \tag{6}$$

Substituting this into (4), we find that

$$\mathrm{Fix}_{X_{\mathcal{M}}}(C) = \mathrm{Fix}_{Y_{\mathcal{M}}}(C) \tag{7}$$

for all $g \in G$, so $X_{\mathcal{M}}$ and $Y_{\mathcal{M}}$ are linearly equivalent over any field of characteristic p. □

Remark 1. If the set $\mathcal{M}$ contains all maximal subgroups of H, it leads to a new formula for the idempotents in the Burnside ring, which were described by Solomon in [Sol], and in this case our G-sets X and Y could also be defined using the formula given by Gluck in [Glu].

On the other hand, our formula is more general, since it allows to choose smaller sets of subgroups, which will result in smaller G-sets.

Combining Lemma 2.1 and Theorem 2.3, we see that

Corollary 2.4. *There exist non-isomorphic, linearly equivalent G-sets over k if and only if G is not cyclic* mod p.

2.1. Frobenius groups

In this subsection, we only consider the case where $p = 0$ (for example, $k = \mathbb{Q}$).

We call G a *Frobenius group* if there is a non-trivial proper subgroup $H \subset G$ such that $H \cap gHg^{-1} = \{1\}$ for all $g \in G \setminus H$. This is equivalent to the existence of a transitive, non-regular G-set X such that each non-trivial element fixes exactly 1 point, or none.

By Frobenius's theorem [Rob, 8.5.5], if G is a Frobenius group there is a normal subgroup $K \lhd G$ such that $K \cap gHg^{-1} = \{1\}$ for all $g \in G$ and $G = KH$. In fact, K is simply the elements G which are not conjugate to any nontrivial element of H.

Thus the set $\mathcal{F} = \{K, H, g_1 H g_1^{-1}, \ldots\}$, where $\{1, g_1, \ldots\}$ contains exactly one element from each coset of H, satisfies $F_1 \cap F_2 = \{1\}$ for $F_1, F_2 \in \mathcal{F}$, $F_1 \neq F_2$ and $\bigcup_{F \in \mathcal{F}} F = G$, i.e., $\mathcal{F}$ is a partition of G in the sense of [Acc]. Thus we may calculate

$$X_{\mathcal{F}} = \#G \cdot \frac{G}{G} \sqcup \left(2^{\#\mathcal{F}-1} - 1\right) \cdot \frac{G}{\{1\}},$$
$$Y_{\mathcal{F}} = \left(\bigsqcup_{F \in \mathcal{F}} \#F \cdot \frac{G}{F}\right) \sqcup \left(2^{\#\mathcal{F}-1} - (G:H) - 1\right) \cdot \frac{G}{\{1\}}.$$

Removing redundant copies of the regular action, we find the G-sets

$$\tilde{X}_{\mathcal{F}} = \#G \cdot \frac{G}{G} \sqcup (G:H) \cdot \frac{G}{\{1\}}, \tag{8}$$
$$\tilde{Y}_{\mathcal{F}} = \bigsqcup_{F \in \mathcal{F}} \#F \cdot \frac{G}{F} \cong_G \#K \cdot \frac{G}{K} \sqcup \#G \cdot \frac{G}{H} \tag{9}$$

are linearly equivalent.

Note that $\tilde{X}_{\mathcal{F}} \cong (G:H) \cdot X'_{\mathcal{F}}$ and $\tilde{Y}_{\mathcal{F}} \cong (G:H) \cdot Y'_{\mathcal{F}}$, where

$$X' = \#H \cdot \frac{G}{G} \sqcup \frac{G}{\{1\}}, \qquad Y' = \#H \cdot \frac{G}{H} \sqcup \frac{G}{K}.$$

This is, of course, considerably easier than the calculation we would have to do for the G-sets $X_{\mathcal{M}}$ and $Y_{\mathcal{M}}$ using all maximal subgroups or all cyclic subgroups, and gives us much smaller G-sets; $\#X' = \#Y' = \#G + \#H$.

Thus, if G is a non-regular Frobenius group, $\mathfrak{md}_{\mathbb{Q}}(G) \leqslant \#G + \#H$.

In fact, we have

Proposition 2.5. *If G is a non-regular Frobenius group,*

$$\frac{\mathfrak{md}_{\mathbb{Q}}(G)}{\#G} \leqslant \frac{4}{3}.$$

Proof. From the discussion above, we know that

$$\frac{\mathfrak{md}_{\mathbb{Q}}(G)}{\#G} \leqslant 1 + \frac{1}{\#K}.$$

Since $khk^{-1} \in H$ if and only if k or h is the identity, the natural map $H \to \operatorname{Aut} K$ is injective. Thus, $\#K \geqslant 3$. $\square$

A computer search conducted with the computer algebra system GAP shows that $\mathfrak{md}_{\mathbb{Q}}(S_3) = 8$, so this bound is strict.

Unfortunately, these G-sets will often not be equivalent over a field of characteristic which divides the order of the group.

2.2. q-Groups

In this subsection, k is of characteristic p which may be positive or 0.

We consider the case where G is a q-group, for q a prime different from p. Since q-groups have so many quotients, we can hope to find a quotient $\tilde{G}$ of any q-group G which is both complicated enough that $\mathfrak{md}_k(\tilde{G})$ is relatively low, but its computation is tractable. Luckily, such a quotient is already provided by classical group theory.

First, we define the *Frattini subgroup* of G, $\operatorname{Frat} G$, to be the intersection of all the maximal subgroups of G. This subgroup is normal, since any conjugate of a maximal subgroup is maximal. We define $\tilde{G} = G/\operatorname{Frat} G$.

Note that if $\{a_1, \dots, a_n\}$, with $a_i \in G$ is a generating set of G if and only if its image in $\tilde{G}$ is as well. Thus G is cyclic if and only if $\tilde{G}$ is.

For a general group, this quotient is rather hard to compute, but if G is a q-group, we can obtain important information about $\tilde{G}$ from the Burnside Basis Theorem.

Theorem 2.6. *(See Burnside [Rob, 5.3.2].) If G is a q-group, then $\tilde{G} = G/\operatorname{Frat} G$ is the largest elementary abelian quotient of G.*

Thus using this reduction, we obtain the

Proposition 2.7. *If G is any non-cyclic q-group with $q \neq p$,*

$$\frac{\mathfrak{md}_k(G)}{\#G} \leqslant \frac{q+1}{q}.$$

In particular, if $k = \mathbb{Q}$, this bound holds for all q.

Of course, $\mathfrak{md}_k(G) = \infty$ if G is a p-group (since G is cyclic mod p).

Proof. Since G is non-cyclic, Theorem 2.6 shows that $\tilde{G} \cong \mathbb{F}_q^n$, with $n \geqslant 2$. Fix a subspace $K \subset \tilde{G}$ of codimension 2 (that is $K \cong (\mathbb{F}_q)^{n-2}$). For any $g \in \tilde{G}$, $\langle g, K\rangle$ is a proper subspace, so every element of $\tilde{G}$ is in a proper subgroup containing K. We let $\mathcal{A}$ be the set of maximal subgroups of $\tilde{G}$ containing K.

This satisfies the first two hypotheses of Theorem 2.3. Since p does not divide the order of G, any cyclic mod p subgroup of G is actually cyclic. Thus, the sets $X_{\mathcal{A}}$ and $Y_{\mathcal{A}}$ described in Theorem 2.3 are linearly equivalent over k.

Now, if $A_1, A_2 \in \mathcal{A}$, $A_1 \neq A_2$, then $A_1 + A_2 = \tilde{G}$, by maximality, so $\dim(A_1 \cap A_2) = n - 2$, and since it contains K, $K = A_1 \cap A_2$. Thus, removing isomorphic orbits from $X_{\mathcal{A}}$ and $Y_{\mathcal{A}}$, and dividing out by q^{n-2}, we find that

$$X'_{\mathcal{A}} = \frac{\tilde{G}}{K} \sqcup q^2 \cdot \frac{\tilde{G}}{\tilde{G}}, \tag{10}$$

$$Y'_{\mathcal{A}} = \bigsqcup_{A \in \mathcal{A}} q \cdot \frac{\tilde{G}}{A} \tag{11}$$

are linearly equivalent over k.

Thus, $\frac{\mathfrak{md}_k(\tilde{G})}{\#\tilde{G}} \leqslant \frac{q+1}{q}$. Applying Lemma 1.2, we obtain the desired result. $\square$

3. Bounding degrees

In this section, we will only consider the case where k is characteristic 0. While it would be very interesting to see analogues of these results over other characteristics, the group theory involved would be much more difficult.

Theorem 3.1. *For all non-cyclic groups G,*

$$\frac{\mathfrak{md}_{\mathbb{Q}}(G)}{\#G} \leqslant \frac{3}{2}.$$

Proof. We split into 2 cases, depending on whether G has a non-cyclic Sylow subgroup or not.

Case 1. Assume $S \subset G$ is a non-cyclic Sylow q-subgroup. By Theorem 2.7, $\mathfrak{md}_{\mathbb{Q}}(S) \leqslant q(q+1)$. Since $|S| \geqslant q^2$,

$$\frac{\mathfrak{md}_{\mathbb{Q}}(S)}{\#S} \leqslant 1 + \frac{1}{q} \leqslant \frac{3}{2}.$$

Furthermore, if X_S and Y_S are the sets we constructed in Proposition 2.7 which realize this bound, X_S has a fixed point and Y_S does not, so we may apply Lemma 1.5 to see that $\mathfrak{md}_{\mathbb{Q}}(G) \leqslant (G:S)q(q+1)$ so

$$\frac{\mathfrak{md}_{\mathbb{Q}}(G)}{\#G} \leqslant \frac{q(q+1)(G:S)}{\#G} \leqslant \frac{3}{2}.$$

Case 2. Now, assume that all Sylow subgroups of G are cyclic. Such groups have been classified by Hölder, Burnside, and Zassenhaus [Rob]. They are exactly groups of the form

$$G = \langle a, b\colon\ a^m = b^n = 1,\ bab^{-1} = a^r \rangle \tag{12}$$

for some $m, n, r \in \mathbb{Z}$, where $r^n \equiv 1 \pmod{m}$ and m and $n(r-1)$ are coprime.

Let p be a prime dividing m, and let G act on $\mathbb{F}_p$ by ${}^{a^\ell b^k}d = r^k d + \ell$. The number of fixed points of any element $a^\ell b^k \in G$ is simply the number of solutions to the equation

$$(r^k - 1)d = -\ell \pmod{p}.$$

Every element fixes an affine subspace of $\mathbb{F}_p$, that is, a set with 0,1 or p points. If g fixes p points, then it is in the kernel K of the action on $\mathbb{F}_p$.

Consider the action of $G' = G/K$ on $\mathbb{F}_p$. Each nontrivial element of G' fixes 0 or 1 elements of $\mathbb{F}_p$. Note that $b \in G$ fixes $0 \in \mathbb{F}_p$, but no other element since p and $r-1$ are coprime. Therefore, G' is a non-regular Frobenius group (by our second definition). Thus

$$\frac{\mathfrak{md}_{\mathbb{Q}}(G)}{\#G} \leqslant \frac{\mathfrak{md}_{\mathbb{Q}}(G')}{\#G'} \leqslant \frac{4}{3}. \qquad \square$$

Remark 2. As we mentioned before, we cannot hope for such a strong bound if our field k has positive characteristic. The first reduction step will imply that the bound is true for all groups except those with a non-cyclic Sylow p-subgroup, and all other Sylow subgroups cyclic, a much more complicated class of groups than those with all Sylow subgroups cyclic.

Since $\mathfrak{md}_{\mathbb{Q}}(\mathbb{F}_2 \times \mathbb{F}_2) = 6$, this bound is sharp. However for most groups, it is actually quite bad.

For example, consider A_4, the alternating group of degree 4. As before, we let $K_4 \lhd A_4$ denote the subgroup $K_4 = \langle (12)(34), (13)(24) \rangle$. One can check that the actions

$$X \cong \frac{A_4}{A_4} \sqcup \frac{A_4}{\langle (12)(34) \rangle}, \qquad Y \cong \frac{A_4}{K} \sqcup \frac{A_4}{\langle (123) \rangle}$$

are linearly equivalent over $\mathbb{Q}$ and of degree 7. A computer search shows, in fact, $\mathfrak{md}_{\mathbb{Q}}(A_4) = 7$, when our theorem implies it is $\leqslant 18$.

Here are a few results that give better bounds for certain classes of groups.

Theorem 3.2. *If G is non-cyclic and*

$$\frac{\mathfrak{md}_{\mathbb{Q}}(G)}{\#G} > \frac{3}{4},$$

G is solvable.

Proof. Every non-abelian simple group has a 2-Sylow of order at least 8 or subgroup isomorphic to A_4. Thus $\frac{\mathfrak{md}_{\mathbb{Q}}(G)}{\#G} \leqslant \frac{3}{4}$. If G is not solvable, it has a non-abelian simple subquotient, so $\frac{\mathfrak{md}_{\mathbb{Q}}(G)}{\#G} \leqslant \frac{3}{4}$. $\square$

Theorem 3.3.

$$\frac{\mathfrak{md}_{\mathbb{Q}}(G)}{\#G} > \frac{4}{3}$$

if and only if $G \cong \mathbb{F}_2 \times \mathbb{F}_2$.

Proof. The "if" direction is known. For the "only if," let G be such a group. If G has only cyclic Sylow subgroups, or a non-cyclic Sylow q-subgroup for $q > 2$, then $\frac{\mathfrak{md}_{\mathbb{Q}}(G)}{\#G} \leqslant \frac{4}{3}$, and if the Sylow 2-subgroup of G has order > 4, $\frac{\mathfrak{md}_{\mathbb{Q}}(G)}{\#G} \leqslant \frac{3}{4}$. Thus, G must have a Sylow 2-subgroup $S \cong \mathbb{F}_2 \times \mathbb{F}_2$.

By Theorem 3.2, G is solvable. Let A be a minimal normal abelian subgroup (which is thus elementary abelian). If A is a p-group for $p > 2$, then G/A is not cyclic, and $\frac{\mathfrak{md}_{\mathbb{Q}}(G)}{\#G} \leqslant \frac{3}{2\#A} < \frac{4}{3}$.

Thus, A is a 2-group, and the quotient by it is cyclic. Since G/A has a unique normal Sylow 2-subgroup, G does as well. By Schur–Zassenhaus, G is a semi-direct product of A and a subgroup A' which acts faithfully on A (since the kernel of such an action would be an abelian normal subgroup which is not a 2-group).

Since $\mathrm{Aut}(\mathbb{F}_2 \times \mathbb{F}_2) \cong \mathbb{F}_3$, either $\#A' = 3$ and $G \cong A_4$, a case we have already ruled out, or $\#A = 1$. $\square$

For "most" groups, $\frac{\mathfrak{md}_{\mathbb{Q}}(G)}{\#G}$ is smaller still. While there are no consistent results along these lines, we have found a number of first steps.

Theorem 3.4. *If $\frac{\mathfrak{md}_{\mathbb{Q}}(G)}{\#G} \geqslant 1$, then G is of the form $C \ltimes \mathbb{F}_q^{\epsilon}$ where C is cyclic, $\epsilon \in \{1, 2\}$, and q is a prime number. Furthermore, C acts faithfully on $\mathbb{F}_q^{\epsilon}$.*

Proof. Note that if G has a non-cyclic quotient, then $\frac{\mathfrak{md}_{\mathbb{Q}}(G)}{\#G} \leqslant 3/4$. Thus all quotients of G must be cyclic. Similarly, by Theorem 3.2, G is solvable.

First, assume G has non-cyclic Sylow ℓ- and q-subgroups for distinct primes $\ell \neq q$. We may assume G is solvable, so let $A \lhd G$ be a normal abelian subgroup, and let S be a Sylow subgroup of A. The subgroup S is characteristic in A, and hence normal in G, and G/S must have a non-cyclic ℓ- or q-Sylow. Thus, we may exclude this case.

Now assume G has a non-cyclic Sylow q-subgroup for exactly one prime q. Let A and S be as above. If $(\#S, q) = 1$, then G/S has a non-cyclic Sylow subgroup. Thus S is a Sylow q-subgroup of A. Thus G/S is cyclic. In particular, G has a unique, normal Sylow q-subgroup R. Applying Schur–Zassenhaus again, $G \cong C \ltimes R$, where $C \cong G/R$.

If G has only cyclic Sylow subgroups, then G is of the form described in Eq. (12). As we have already seen, if m is not prime, this group has a non-cyclic quotient. Thus $\langle a\rangle \cong \mathbb{F}_q$, and obviously $G \cong \langle b\rangle \ltimes \langle a\rangle$.

In either case, the map $C \to \operatorname{Aut} R$ must be injective, since if $C' \subset C_G(R)$, $C' \lhd G$ and the quotient G/C' is not cyclic. $\square$

Theorem 3.5. *For all $\epsilon > 0$, there are only finitely many groups such that $\frac{\mathfrak{md}_{\mathbb{Q}}(G)}{\#G} \geqslant 1 + \epsilon$, but infinitely many such that $\frac{\mathfrak{md}_{\mathbb{Q}}(G)}{\#G} > 1$.*

Proof. We need only prove the theorem for $\epsilon = 1/n$ for $n \in \mathbb{Z}$. By the characterization above, if $\frac{\mathfrak{md}_{\mathbb{Q}}(G)}{\#G} \geqslant \frac{n+1}{n}$, then G corresponds to an element of $\operatorname{Aut}(\mathbb{F}_q^{\epsilon})$ for some prime $q \leqslant n$ and $\epsilon \in \{1, 2\}$. These groups are finite, so there are only finitely many choices for G.

We note that when n is prime,

$$\frac{\mathfrak{md}_{\mathbb{Q}}(D_n)}{\#D_n} = \frac{n+1}{n}$$

since in this case all proper subgroups of D_n are cyclic, so the pair constructed in Section 2.1 is the unique "irreducible" pair of non-isomorphic linearly equivalent G-sets, in the sense that all others must this pair as a subset. This exhibits infinitely many groups such that $\frac{\mathfrak{md}_{\mathbb{Q}}(G)}{\#G} > 1$. $\square$

4. Beaulieu's construction

In this section, we will describe the most fruitful known construction of transitive G-sets, and how it allows to transfer some of our results obtained in a highly non-transitive context to the transitive case.

We let X and Y be G-sets, linearly equivalent over k. By fixing bijections $X \to \{1, \dots, n\}$ and $Y \to \{1, \dots, n\}$, where $n = |X| = |Y|$, we obtain natural homomorphisms $\varphi_X : G \to S_n$ and $\varphi_Y : G \to S_n$, where as usual, $S_n = \mathrm{Sym}(\{1, \dots, n\})$. The homomorphisms φ_X and φ_Y are not unique, but any two choices of φ_X will differ by an inner automorphism of S_n. Fix bijections $\sigma_X : X \to \{1, \dots, n\}$ and $\sigma_Y : Y \to \{1, \dots, n\}$.

Let X' be the S_n-set $S_n/\varphi_X(G)$ (and similarly for Y'). Note that isomorphism class of X' is not changed by replacing $\varphi_X(G)$ with a conjugate, and thus will not depend on the choice of φ_X.

For simplicity, we will assume that the G-sets X and Y are faithful (i.e., the homomorphisms φ_X and φ_Y are injective).

Theorem 4.1. *If G-sets X and Y of degree n are linearly equivalentover k, then the S_n-sets X' and Y' are linearly equivalentover k as well.*

This theorem was originally proved for characteristic 0 by P. Beaulieu in her PhD thesis [Bea]. When $p = 0$, our proof essentially reduces to a restatement of hers.

Proof. We will apply Lemma 2.1 to S_n. Let C be a cyclic mod p subgroup of S_n. If C is not conjugate to a subgroup of $\varphi_{\mathrm{res}_C^G X}(G) = H_X$ or $\varphi_{\mathrm{res}_C^G Y}(G) = H_Y$, then $\mathrm{Fix}_{X'}(C) = \mathrm{Fix}_{Y'}(C) = \emptyset$.

Thus, we need only consider cyclic mod p subgroups contained in H_X or H_Y. If $C \subset H_X$, then there is a subgroup $K \subset G$ such that $C = \varphi_X(K)$. Let $C' = \varphi_Y(K)$. Now, consider the actions $\mathrm{res}_K^G X$ and $\mathrm{res}_K^G Y$. Since $X \overset{\mathrm{lin}}{=}_k Y$, and K is cyclic mod p, there is an isomorphism of K-sets $\tau : \mathrm{res}_K^G X \to \mathrm{res}_K^G Y$ by Lemma 2.1.

Thus, the permutation $s_K = \sigma_Y \circ \tau \circ \sigma_X^{-1}$ intertwines the action of C and C' on $\{1, \dots, n\}$, that is, $s_K C s_K^{-1} = C'$.

Now, consider the set $L_C(H_X)$. This set can be partitioned as

$$L_C(H_X) = \bigsqcup L_C^{C_1}(H_X)$$

as C_1 ranges over conjugates of C contained in H, and

$$L_C^{C_1}(H_X) = \{ g \in L_C(H_X) \mid g^{-1} C g = C_1 \}.$$

Now, note that $L_C^{C_1}(H_X) s_{K_1} = L_C^{C_1'}(H_Y)$, where $\varphi_X(K_1) = C_1$, $\varphi_Y(K_1) = C_1'$. This gives a bijection between $L_C(H_X)$ and $L_C(H_Y)$.

By Lemma 2.2, this implies that $\#\mathrm{Fix}_{X'}(C) = \#\mathrm{Fix}_{Y'}(C)$, and by Lemma 2.1, we see that $X' \overset{\mathrm{lin}}{=}_k Y'$. □

The above theorem contains no information about whether X' and Y' are isomorphic as S_n-sets. This, of course, occurs exactly when H_X and H_Y are conjugate in S_n.

This is true if and only if the actions X and Y are similar, that is, when there is a map $\mu : X \to Y$ and an automorphism ψ of G such that $\mu({}^g x) = {}^{\psi(g)}\mu(x)$. This is a weaker condition than requiring $X \cong_G Y$, though these conditions are closely related.

This shows that the converse of Theorem 4.1 is obviously false, since we could take the actions X and Y to be similar but not linearly equivalent over k. In this case, $\varphi_X(G) \sim \varphi_Y(G)$ so X' and Y' are isomorphic and thus linearly equivalent over k.

Question. Are X' and Y' are linearly equivalent if and only if X is linearly equivalent to a G-set similar to Y?

This seems unlikely, since examples have been constructed by Perlis [Per1] of pairs of permutation groups (G, X) and (G', Y) such that G and G' are not isomorphic but X' and Y' are linearly equivalent for a field of characteristic 0.

Since at present, we cannot answer the question above in general, let us address a weaker form: When we can be sure that $k[X'] \ncong k[Y']$?

Lemma 4.2. *If $k[X'] \cong k[Y']$ then for any cyclic* mod p *subgroup $H_1 \subset G$, there exists a subgroup $H_2 \subset G$ such that $\operatorname{res}^G_{H_1} X$ and $\operatorname{res}^G_{H_2} Y$ are similar. In particular,*

$$\#\mathrm{Fix}_X(H_1) = \#\mathrm{Fix}_Y(H_2).$$

While somewhat crude, this simple criterion allows us to construct many pairs of G-sets for which we can be sure that $k[X'] \ncong k[Y']$.

Proof. Assume that X' and Y' are linearly equivalentover k. If H_1 is a cyclic mod p subgroup of G, then $\varphi_X(H_1)$ must be conjugate to some cyclic mod p subgroup of $\varphi_Y(G)$ by Lemma 2.1, which must be of the form $\varphi_Y(H_2)$, for some $H_2 \subset G$. Translating back into G-sets, this means that $\operatorname{res}^G_{H_1} X$ and $\operatorname{res}^G_{H_2} Y$ are similar.

Since any similarity of G-sets must preserve fixed points,

$$\#\mathrm{Fix}_X(H_1) = \#\mathrm{Fix}_Y(H_2). \qquad \square$$

5. An application

In general, it is quite difficult to find transitive G-sets which are linearly equivalent but not isomorphic. A number of examples for small degrees have been studied by Perlis [Per1], Feit [Fei], Guralnick and Wales [Gur,GW], and DeSmit and Lenstra have recently given a more general construction for G solvable [dSL], but for the most part, this field remains wide open.

Beaulieu's construction gives us a method of constructing a wide variety of G-sets. For example, it implies that the stabilizers of linearly equivalent G-sets have no special properties other than not being cyclic mod p:

Theorem 5.1. *If G is a group which is not cyclic* mod p*, then for some n there exist subgroups $G_1, G_2 \subset S_n$ such that $G_1 \cong G_2 \cong G$ and S_n/G_1 and S_n/G_2 are linearly equivalent over k but not isomorphic.*

Proof. The G-sets $X_{\mathcal{M}}$ and $Y_{\mathcal{M}}$ defined in (2) and (3) where $\mathcal{M}$ contains the set of all maximal subgroups of G and satisfies $\bigcap_{M_i \in \mathcal{M}} M_i = \{1\}$ are linearly equivalent by Theorem 2.3. Now, $G_1 = \varphi_{X_G}(G)$ and $G_2 = \varphi_{Y_G}(G)$ are precisely the subgroups we were looking for. Since the G-sets are faithful, the maps are injective and thus isomorphisms onto their respective images. By Theorem 4.1, $S_n/G_1 \overset{\mathrm{lin}}{=}_k S_n/G_2$. Lemma 4.2 shows that these are not isomorphic. $\square$

Beaulieu's construction also allows us to show that $\mathfrak{md}_k(S_n)$ is much smaller than the bounds shown in Section 3, and that there is no lower bound over all groups of $\frac{\mathfrak{md}_k(G)}{\#G}$. In fact, the examples constructed by de Smit and Lenstra in [dSL] show that no such lower bound can be applied to the class of solvable groups, nilpotent groups or q-groups for any q.

Theorem 5.2. *For any field k, and any $\epsilon > 0$, there exists an N such that for all $n > N$,*

$$\frac{\mathfrak{md}_k(S_n)}{\#S_n} < \epsilon.$$

That is

$$\lim_{n\to\infty} \frac{\mathfrak{md}_k(S_n)}{\#S_n} = 0.$$

Proof. Fix a group G which is not cyclic mod q for any q. Using Theorem 5.1, for some N, there are subgroups $H, H' \subset S_N$, which we can think of as subgroups of S_n for any $n \geqslant N$ by the standard inclusion maps, such that $H \cong H' \cong G$, $S_n/H \ncong_{S_n} S_n/H'$, and $S_n/H \overset{\text{lin}}{=}_k S_n/H'$. Thus

$$\frac{\mathfrak{md}_k(S_n)}{\#S_n} \leqslant \frac{1}{\#G}$$

for all $n \geqslant N$. Since there exist groups not cyclic mod any prime q of arbitrary order (for example S_m as $m \geqslant 4$), the limit is proved. $\square$

In general, Beaulieu's construction helps us to turn non-transitive constructions into transitive ones. For example, I am not aware of any previous example of a pair of transitive actions which are linearly equivalent over all fields but not isomorphic. But since we can easily construct non-transitive examples, Beaulieu's construction will now allow us to construct as many of these as we would like.

For example, we can use the smallest group not cyclic mod any prime, $G = D_6 = \langle a, b : a^6 = b^2 = (ab)^2\rangle$. Consider the following G-sets:

$$X_{D_6} = \frac{G}{\langle a^2\rangle} \sqcup \frac{G}{\langle b\rangle} \sqcup \frac{G}{\langle ab\rangle} \sqcup \frac{G}{\langle a^3\rangle} \sqcup 2\cdot\left(\frac{G}{G}\right), \tag{13}$$

$$Y_{D_6} = \frac{G}{\langle a^2, b\rangle} \sqcup \frac{G}{\langle a^2, ab\rangle} \sqcup \frac{G}{\langle a\rangle} \sqcup \frac{G}{\{1\}} \sqcup 2\cdot\left(\frac{G}{\langle b, a^3\rangle}\right). \tag{14}$$

One can check that these G-sets are linearly equivalent over any field, since their restrictions to any proper subgroup are isomorphic. Since $|X_{D_6}| = |Y_{D_6}| = 24$, we see that S_{24} has transitive G-sets linearly equivalent over any field.

In fact, this can be expanded further. For any pair of G-sets, there is a set of primes $\mathcal{P}_{X,Y}$, which is exactly the primes p such that $k[X] \ncong k[Y]$ for fields of characteristic p. This set is either all primes, or a finite set dividing the order of G (in fact, dividing the order of the stabilizer of at least one point in X or Y).

Theorem 5.3. *Given an arbitrary finite set of primes $\mathcal{P} = \{p_1, \ldots, p_n\}$, there exists a group G, and a pair of transitive G-sets X and Y such that $k[X] \cong k[Y]$ if and only if $p = \operatorname{char} k \notin \mathcal{P}$, i.e. $\mathcal{P} = \mathcal{P}_{X,Y}$.*

Proof. We have already done the case where $\mathcal{P} = \{\}$.

Next we tackle singletons. Let $\mathcal{P} = \{p\}$. If G is a p-group, then for any X and Y linearly equivalent over any field of characteristic different from p, $\mathcal{P}_{X,Y} = \{p\}$ (since all subgroups are cyclic mod p). By a construction of de Smit and Lenstra given in [dSL], there exists a p-group G_p with transitive G_p-sets X_p, Y_p linearly equivalent over a field of characteristic 0 (and, in fact, with degree p^3).

Now, for $\mathcal{P}$ general, the exterior Cartesian products

$$X = \prod_{p\in\mathcal{P}} X_p, \qquad Y = \prod_{p\in\mathcal{P}} Y_p$$

are obviously linearly equivalent as $G = \prod_{p\in\mathcal{P}} G_p$-sets for fields of characteristic $q \notin \mathcal{P}$. If $p_i \in \mathcal{P}$, the p-subgroup

$$H_{p_i} = \mathrm{Stab}_{G_{p_i}}(x_{p_i}) \subset G$$

for $x_{p_i} \in X_{p_i}$ fixes points of X but not of Y, and so by Lemma 2.1, X and Y are not linearly equivalent for any field of characteristic p_i. Thus $\mathcal{P}_{X,Y} = \mathcal{P}$. □

This proof only realized examples for groups which are nilpotent. The question of which sets appear for groups which not nilpotent (or more generally, for groups which are indecomposable) appears more subtle, but, in fact, the answer is the same.

A fairly limited number of sets (for the most part, singletons) have thus forth come to light as $\mathcal{P}_{X,Y}$ for transitive G-sets X and Y, with G indecomposable, but in fact, any finite set of primes can appear.

Theorem 5.4. *Theorem* 5.3 *holds, with the additional assumption that $G \cong S_n$ for some integer n.*

Proof. Let G be as in the proof of Theorem 5.3, let $\mathcal{M}$ be the set of cyclic subgroups of G, and let $X_{\mathcal{M}}$ and $Y_{\mathcal{M}}$ be as defined in (2) and (3). These G sets are linearly equivalent over $\mathbb{Q}$ and thus over all fields of characteristic $q \notin \mathcal{P}$, since $q \nmid \#G$. Thus, $\mathcal{P}_{X_{\mathcal{M}},Y_{\mathcal{M}}} \subset \mathcal{P}$.

Now, we apply Beaulieu's construction to $X_{\mathcal{M}}$ and $Y_{\mathcal{M}}$, and denote the corresponding S_n-sets by X' and Y' as before. By Theorem 4.1, $\mathcal{P}_{X',Y'} \subset \mathcal{P}$.

On the other hand, assume $p \in \mathcal{P}$, and let K be any non-cyclic, cyclic mod p subgroup of G. Let $\mathrm{Fix}_X(K)$ is the unique trivial orbit, while $\mathrm{Fix}_Y(K)$ is empty. Thus, by Lemma 4.2, X' and Y' are not linearly equivalent over any field of characteristic p. So, $\mathcal{P}_{X',Y'} = \mathcal{P}$. □

The reader may wonder why we did not use the G-sets constructed in the proof of Theorem 5.3. In this case, it becomes unclear whether one can apply Lemma 4.2 at the end of the proof of Theorem 5.4 to ensure that $\mathcal{P}_{X',Y'} \subset \mathcal{P}_{X,Y}$.

These constructions unfortunately tend to lead to S_n-sets of quite enormous degrees. For example, the example (13) has degree $24!/12$. It would be very interesting to find other constructions of G-sets isomorphic over a fixed set of fields, or over other rings, which would better live up to the title of this paper.

Acknowledgments

I would like to thank Robert Perlis, Bill Dunbar, Neal Stoltzfus and Robert Snyder for their generous support and advice, and the Louisiana State REU for a great opportunity to do mathematics as well as for their warm hospitality.

References

[Acc] Robert D.M. Accola, Two theorems on Riemann surfaces with noncyclic automorphism groups, Proc. Amer. Math. Soc. 25 (1970) 598–602, MR41 #3747.

[Bea] Patricia Beaulieu, On a new construction of subgroups inducing isomorphic representations, PhD thesis, Louisiana State University, 1991.

[BB] Werner Bley, Robert Boltje, Cohomological Mackey functors in number theory, J. Number Theory 105 (1) (2004) 1–37, MR2032439 (2004k:11169).

[Bol] Robert Boltje, Class group relations from Burnside ring idempotents, J. Number Theory 66 (2) (1997) 291–305, MR98i:20006.

[CR] Charles W. Curtis, Irving Reiner, Methods of Representation Theory: With Applications to Finite Groups and Orders, vol. 2, Wiley, New York, 1987, MR88f:20002.

[dS] B. de Smit, On arithmetically equivalent fields with distinct p-class numbers, J. Algebra 272 (2) (2004) 417–424, MR2028064 (2005f:11252).

[dSL] B. de Smit, H.W. Lenstra Jr., Linearly equivalent actions of solvable groups, J. Algebra 228 (1) (2000) 270–285, MR2001f:20069.

[Fei] Walter Feit, Some consequences of the classification of finite simple groups, in: The Santa Cruz Conference on Finite Groups, Univ. California, Santa Cruz, CA, 1979, Amer. Math. Soc., Providence, RI, 1980, pp. 175–181, MR82c:20019.

[Glu] David Gluck, Idempotent formula for the Burnside algebra with applications to the p-subgroup simplicial complex, Illinois J. Math. 25 (1) (1981) 63–67, MR82c:20005.

[Gur] Robert M. Guralnick, Subgroups inducing the same permutation representation, J. Algebra 81 (2) (1983) 312–319, MR84j:20010.

[GW] Robert M. Guralnick, David B. Wales, Subgroups inducing the same permutation representation. II, J. Algebra 96 (1) (1985) 94–113, MR86m:20006.

[Per1] Robert Perlis, On the equation $\zeta_K(s) = \zeta_{K'}(s)$, J. Number Theory 9 (3) (1977) 342–360, MR56 #5503.

[Per2] Robert Perlis, On the class numbers of arithmetically equivalent fields, J. Number Theory 10 (4) (1978) 489–509, MR80c:12014.

[Rob] Derek J.S. Robinson, A Course in the Theory of Groups, second ed., Springer-Verlag, New York, 1996, MR96f:20001.

[Sol] Louis Solomon, The Burnside algebra of a finite group, J. Combin. Theory 2 (1967) 603–615, MR35 #5528.

[ST] H.M. Stark, A.A. Terras, Zeta functions of finite graphs and coverings. II, Adv. Math. 154 (1) (2000) 132–195, MR2002f:11123.

[Sun] Toshikazu Sunada, Riemannian coverings and isospectral manifolds, Ann. of Math. (2) 121 (1) (1985) 169–186, MR86h:58141.