Linearly equivalent actions of solvable groups

B. de Smit and H. W. Lenstra, Jr.

Mathematisch Instituut
Universiteit Leiden
Postbus 9512, 2300 RA Leiden
Netherlands

Department of Mathematics # 3840
University of California
Berkeley CA 94720–3840
USA

Abstract. We determine the positive integers n for which there exist a solvable group G and two non-conjugate subgroups of index n in G that induce the same permutation character.

Key words: permutation character, Gassmann equivalence, arithmetical equivalence.

1991 Mathematics subject classification: 20C15, 20F16.

Acknowledgements. The authors thank R. M. Guralnick, I. M. Isaacs, and C. Pomerance for their advice. The first author was supported by a fellowship from the Koninklijke Nederlandse Akademie van Wetenschappen. The second author was supported by the National Science Foundation under Grant No. DMS 9224205.

1. Introduction

Let G be a group. A G-set is a finite set provided with a left action of G. For a G-set X and $g \in G$ we write $X^g = \{x \in X : gx = x\}$. The permutation character of a G-set X is the function π_X from G to the ring $\mathbb{Z}$ of integers that sends g to the cardinality $\#X^g$ of X^g. We say that two G-sets X and Y are *linearly equivalent* if $\pi_X = \pi_Y$. By representation theory of finite groups, two G-sets X and Y are linearly equivalent if and only if the permutation modules $\mathbb{C}^X$ and $\mathbb{C}^Y$ are isomorphic as modules over the group ring $\mathbb{C}[G]$; here $\mathbb{C}$ denotes the field of complex numbers.

Theorem 1. *For every positive integer n the following are equivalent:*

(1) *there exist a finite solvable group G and two non-isomorphic transitive G-sets of cardinality n that are linearly equivalent;*

(2) *there are prime numbers p, q, r with $pqr \mid n$ and $p \mid q(q-1)$.*

If X is a transitive G-set and H is the stabilizer of a point in X then we have $\pi_X = 1_H^G$, i. e., the permutation character is the character of G induced by the trivial character 1_H of H. Thus condition (1) is equivalent to the existence of a solvable group G with two non-conjugate subgroups H and K of index n for which $1_H^G = 1_K^G$.

Our interest in condition (1) stems from a number theoretic context. Let L and M be two algebraic numbers fields, and denote by X and Y the sets of field embeddings of L and

M, respectively, in some algebraic closure $\bar{\mathbb{Q}}$ of the field $\mathbb{Q}$ of rational numbers. Then X and Y are transitive G-sets, where G is the Galois group of $\bar{\mathbb{Q}}$ over $\mathbb{Q}$. By Galois theory, X and Y are isomorphic as G-sets if and only if L and M are isomorphic as fields. Moreover, X and Y are linearly equivalent if and only if L and M have the same zeta function; see [2, Exercise 6]. Number fields with the same zeta function are often called "arithmetically equivalent" [11].

By Theorem 1 a number field whose degree n does not satisfy (2) and that is solvable by radicals, is determined up to isomorphism by its zeta-function. To show that, conversely, every integer n that does satisfy (2) is the degree of two non-isomorphic solvable number fields with the same zeta-function, it suffices to combine Theorem 1 with Shafarevich's claim that every finite solvable group can be realized as a Galois group over $\mathbb{Q}$; see [10]. Alternatively, one may try to realize the groups constructed in Section 2 as Galois groups over $\mathbb{Q}$.

In Section 2 we shall prove that (2) implies (1). In our construction we can choose G to be 3-step abelian. The G-sets we give are imprimitive. For the case that n is divisible by p^3 for some prime p one can also use a 2-step abelian construction of Guralnick [5]. One may ask for which n condition (1) holds for a 2-step abelian group. The construction in Section 2 has benefited from [1], where it is proved that one can take exactly five non-isomorphic solvable groups in (1) for $n = 12$, if the actions are assumed to be faithful. Two of these groups are 2-step abelian, and the other three are only 3-step abelian.

In Sections 3 and 4 we shall prove the following theorem. We denote by φ the Euler phi-function. By an n-element in a finite group we mean an element whose order is built up from primes dividing n.

Theorem 2. *Let n be a positive integer. Suppose that n is coprime to $\varphi(n)$ or is of the form $n = pq$ for prime numbers p and q. Let G be a finite solvable group acting transitively on a set X of cardinality n. Then for any G-set Y the following are equivalent:*

(3) *for all n-elements $g \in G$ we have $\#X^g = \#Y^g$;*

(4) *X and Y are linearly equivalent as G-sets;*

(5) *X and Y are isomorphic as G-sets.*

Any positive integer n for which condition (2) fails, satisfies the hypothesis of Theorem 2. Therefore, the implication (1) $\Rightarrow$ (2) of Theorem 1 follows from the implication (4) $\Rightarrow$ (5) in Theorem 2.

The implications (5) $\Rightarrow$ (4) $\Rightarrow$ (3) of Theorem 2 are trivial. In Section 3 we prove the implication (3) $\Rightarrow$ (5) in the case that n is coprime to $\varphi(n)$, by induction on the number of prime factors of n. In Section 4 we prove (3) $\Rightarrow$ (5) in the case $n = pq$.

The condition (3) on G-sets of cardinality n is apparently new. It is forced upon us by the inductive argument of Section 3, since (3) is all we can verify when the inductive assumption is to be invoked. Thus, in the case $\gcd(n, \varphi(n)) = 1$, we do not know a proof of (4) $\Rightarrow$ (5) that avoids the detour over (3). This is not true in the case $n = pq$. In fact, our proof of (3) $\Rightarrow$ (5) for $n = pq$ is based on the proof of (4) $\Rightarrow$ (5) for $n = pq$, $p \neq q$ that was given by Guralnick and Wales [6].

We do not know whether (3) and (4) are equivalent when the condition on n is dropped, but G is still assumed to be solvable. As Guralnick pointed out to us, some condition on G is necessary: the group $G = \mathrm{PSL}(2, 11)$ has two subgroups of order 12 and index $n = 55$ whose permutation characters are distinct, while they both vanish on all non-trivial n-elements. There is also a positive result: if G is any finite group acting transitively on two sets X and Y so that $n = \#X$ is a prime power coprime to $\#G/\#X$, then (3) and (4) are equivalent; see Isaacs [9].

In Section 5 we consider the set of integers n satisfying condition (1) of Theorem 1 without the assumption that G be solvable. Combining our results with those of Feit, Guralnick, and Wales, which depend on the classification of finite simple groups, we investigate the asymptotics of this set and its complement, and we implicitly list all of its elements up to 2000.

The following notation will be used throughout this paper. The cardinality of a set S is denoted by $\#S$. For sets S and T we let S^T be the set of maps from T to S. For subsets S, T of a set we denote the set-theoretic difference $\{x \in S : x \notin T\}$ by $S - T$. Suppose that G is a group and that X is a G-set. The set of fix-points of X is denoted by $\mathrm{Fix}_G X$; so for $g \in G$ we have $\mathrm{Fix}_{\langle g \rangle} X = X^g$. The set of G-orbits of X is written as $G \backslash X$. Let N be a normal subgroup of G. The N-orbits of X form a block structure for the G-action, so $N \backslash X$ has a G-set structure for which the natural map $X \to N \backslash X$ respects the action of G. In addition, the induced map $\mathbb{C}^{N \backslash X} \to \mathbb{C}^X$ is injective with image $\mathrm{Fix}_N(\mathbb{C}^X)$, so it gives rise to an isomorphism $\mathbb{C}^{N \backslash X} \to \mathrm{Fix}_N(\mathbb{C}^X)$ of $\mathbb{C}[G]$-modules.

2. Constructing examples

Lemma. *Let G be a finite group and let A be an abelian normal subgroup of G of prime index. Suppose X and Y are two G-sets each of which is isomorphic to A as an A-set. Write $\bar{X} = G'\backslash X$ and $\bar{Y} = G'\backslash Y$, where G' is the commutator subgroup of G. Then we have an equality $\pi_X - \pi_Y = \pi_{\bar{X}} - \pi_{\bar{Y}}$ of maps from G to $\mathbb{Z}$.*

Proof. The permutation module $\mathbb{C}^X$ over G decomposes as a direct sum of 1-dimensional eigenspaces for A, and G permutes these eigenspaces. Such an eigenspace is G-stable if and only if it is fixed pointwise by $G' = [G, A]$. Thus, the sum of the G-stable eigenspaces has character $\pi_{\bar{X}}$, and the sum V_X of the other eigenspaces has character $\pi_X - \pi_{\bar{X}}$. Since $[G : A]$ is prime, every $g \in G$ with $g \notin A$ stabilizes only the G-stable eigenspaces. For such $g \in G$ the action of g on V_X is therefore given by a matrix with only zeros on the diagonal. It follows that the character $\pi_X - \pi_{\bar{X}}$ of G is zero on $G - A$. The same holds for $\pi_Y - \pi_{\bar{Y}}$, and since X and Y are A-isomorphic we deduce that $\pi_X - \pi_{\bar{X}} = \pi_Y - \pi_{\bar{Y}}$.

Proposition. *Let p be a prime number, let $k > 1$ be an integer, and let $m > 1$ be a product of prime powers q that are 0 or 1 modulo p. Then there exist a 3-step abelian group G of order $(pm)^k k$ and two non-isomorphic transitive G-sets of cardinality pmk that are linearly equivalent.*

Proof. Let $\mu = \mu_p$ be the group of pth roots of unity in $\mathbb{C}$. The subring of $\mathbb{C}$ generated by μ is denoted by $\mathbb{Z}[\mu]$. If $\zeta \in \mu$ and $\zeta \neq 1$, then $1 - \zeta$ generates the unique ideal $\mathfrak{p}$ of $\mathbb{Z}[\mu]$ of index p. By the assumption on the integer m there exists an ideal $\mathfrak{a} \subset \mathfrak{p}^2$ of $\mathbb{Z}[\mu]$ with $m = [\mathfrak{p}^2 : \mathfrak{a}]$.

The ideal $A = \mathfrak{p}/\mathfrak{a}$ of the finite ring $R = \mathbb{Z}[\mu]/\mathfrak{a}$ acts by translation on the subsets A and $1 + A$ of R. The group μ acts on R by multiplication, and this action stabilizes the sets A and $1 + A$. Thus, we obtain an induced action of the semidirect product $B = A \rtimes \mu$ of order $p^2 m$ on the sets $X = A$ and $Y = 1 + A$ of cardinality pm. The commutator subgroup B' of B is given by $B' = \mathfrak{p}^2/\mathfrak{a}$, and it has order m. The quotient B-sets $\bar{X} = B'\backslash X$ and $\bar{Y} = B'\backslash Y$ have cardinality p. Note that $\pi_{\bar{X}} \neq \pi_{\bar{Y}}$ because μ acts trivially on $\bar{X}$ but not on $\bar{Y}$. By the lemma we also have $\pi_X \neq \pi_Y$.

Let Z be a finite group of order k. For any Z-set S the group operation on B makes B^S into a group. Moreover, Z acts on this group by group automorphisms: for $z \in Z$ and $f \in B^S$ we let $(zf)(s) = f(z^{-1}s)$ whenever $s \in S$. Identifying B^S with $\prod_{s \in S} B$ we see that multiplication in B^S is coordinate-wise, and that Z acts on B^S by permuting coordinates. We thus obtain actions of the wreath product $B^S \rtimes Z$ on $X \times S$ and $Y \times S$. We now take the Z-set S to be Z itself, on which Z acts by left multiplication. Since $k > 1$ we can choose an element $z \in Z$ with $z \neq 1$. We let $\alpha\colon S \to S$ be the fix-point free Z-set automorphism given by right multiplication by z.

Let us fix an A-set isomorphism $\varphi\colon \bar{X} \to \bar{Y}$. We define H to be the largest subgroup of B^S for which the bijection $\bar{X} \times S \to \bar{Y} \times S$ given by $\varphi \times \alpha$ respects the action of H. Now let $G = H \rtimes Z$. If we choose Z to be abelian we obtain a 3-step abelian group G. We claim that $\#G = (pm)^k k$ and that the G-sets $X \times S$ and $Y \times S$ satisfy our conditions, i. e., they are transitive, non-isomorphic, and linearly equivalent.

For each $s \in S$ the actions of H on $X \times \{s\}$ and $Y \times \{s\}$ factor through the map $H \to B$ sending h to $h(s)$. Applying, for each $s \in S$, the lemma to the group B with its normal subgroup A, we find that there is an equality

$$\pi_{X \times S} - \pi_{Y \times S} = \pi_{\bar{X} \times S} - \pi_{\bar{Y} \times S}$$

of functions on H. We know that $\bar{X} \times S$ and $\bar{Y} \times S$ are isomorphic as H-sets, so it follows that $\pi_{X \times S} = \pi_{Y \times S}$ on H. But on $G - H$ these two permutation characters vanish because all elements of $G - H$ act fix-point free on S. Therefore $X \times S$ and $Y \times S$ are linearly equivalent over G.

In order to compute $\#H$ we now give a more explicit description of H. Let $C_{\bar{X}}$ and $C_{\bar{Y}}$ be the images of B in the permutation groups of $\bar{X}$ and $\bar{Y}$. Then $C_{\bar{X}}$ and $C_{\bar{Y}}$ are both of order p, and the map $B \to C_{\bar{X}} \times C_{\bar{Y}}$ is surjective with kernel B'. The actions of A on $\bar{X}$ and $\bar{Y}$ provide isomorphisms $A/B' \cong C_{\bar{X}}$ and $A/B' \cong C_{\bar{Y}}$, which give an isomorphism $\sigma\colon C_{\bar{X}} \to C_{\bar{Y}}$. This isomorphism σ respects φ in the sense that for all $c \in C_{\bar{X}}$ we have an equality $\varphi \circ c = \sigma(c) \circ \varphi$ of maps from $\bar{X}$ to $\bar{Y}$. The condition for an element $h \in B^S$ to lie in H is that for all $s \in S$ the isomorphism σ sends the image of $h(s)$ in $C_{\bar{X}}$ to the image of $h(\alpha(s))$ in $C_{\bar{Y}}$. It follows that the natural map $\psi\colon H \to C_{\bar{Y}}^S$ is surjective with kernel B'^S, so that $\#H = (pm)^k$.

We now claim that for every $s \in S$ the map $H \to B$ sending h to $h(s)$ is surjective. To see this, suppose we are given $b \in B$, with image (b_X, b_Y) in $C_{\bar{X}} \times C_{\bar{Y}}$. Define $c \in C_{\bar{Y}}^S$ by

$$c(s) = b_Y, \qquad c(\alpha(s)) = \sigma(b_X), \qquad c(t) = 1 \quad \text{for } t \in S - \{s, \alpha(s)\}.$$

Let $h \in H$ be any element with $\psi(h) = c$. Then $h(s) \in B$ maps to (b_X, b_Y) in $C_{\bar{X}} \times C_{\bar{Y}}$. Multiplying h by a suitable element of B'^S we obtain an element $h' \in H$ with $h'(s) = b$. This proves the claim.

It follows that H acts transitively on $X \times \{s\}$ for each $s \in S$. Since Z acts transitively on S we conclude that $X \times S$ is a transitive G-set. The same holds for $Y \times S$.

Let us now show that $X \times S$ and $Y \times S$ are not G-isomorphic. Since $\#B' = m > 1$ there is an element $h \in B'^S$ so that $h(s) = 1$ for a *unique* $s \in S$. We then have $(X \times S)^h = X \times \{s\}$. Using that $\pi_X \neq \pi_Y$, we choose an element $b \in B$ that does not fix the same number of points in X and Y. By the claim above there is an element $h' \in H$ with $h'(s) = b$. Then the subgroup of H generated by h and h' does not fix the same number of points in $X \times S$ and $Y \times S$. In particular, $X \times S$ and $Y \times S$ are not even isomorphic as H-sets. This proves the proposition.

We now prove (2) $\Rightarrow$ (1) in Theorem 1. Suppose that n, p, q, and r are as in (2). Put $m = q$ and $k = n/(pq)$. Then m is a prime that is 0 or 1 modulo p, and k is at least 2 because $r \mid k$. The proposition now provides us with a solvable group G and two non-isomorphic linearly equivalent transitive G-sets of cardinality $pmk = n$.

3. The case that n and $\varphi(n)$ are coprime

In this section we prove the implication (3) $\Rightarrow$ (5) of Theorem 2 for all positive integers n for which $\varphi(n)$ is coprime to n. We start with some general remarks.

Let G be a finite group. If N is a normal subgroup of G, and X and Y are linearly equivalent G-sets, then the $\mathbb{C}[G]$-isomorphisms $\mathbb{C}^{N\backslash X} \cong \mathrm{Fix}_N(\mathbb{C}^X) \cong \mathrm{Fix}_N(\mathbb{C}^Y) \cong \mathbb{C}^{N\backslash Y}$ imply that $N\backslash X$ and $N\backslash Y$ are also linearly equivalent as G-sets. In particular, with $N = G$, we see that the number of G-orbits of X depends only on X up to linear equivalence.

Lemma 1. *Let G be a solvable group acting faithfully and transitively on a finite set X of square-free cardinality n. Then we have*

(a) *the group G is annihilated by $n\varphi(n)$.*

Suppose that A is a non-trivial normal p-subgroup of G for some prime p. Then we have

(b) *A is elementary abelian;*
(c) *all orbits of A on X have cardinality p;*
(d) *p divides n.*

Proof. We prove (b, c, d) first. All A-orbits of X have the same cardinality l because G acts transitively on X. Thus, this number l divides both n and the order of A. Since n is square-free and A acts faithfully, it follows that $l = p$ and $p \mid n$, which is the content of (c) and (d). The image of A in the permutation group of X is therefore contained in a group generated by pairwise disjoint p-cycles. Using again that A acts faithfully, we deduce that A is elementary abelian. This shows (b).

We now prove (a) by induction on the number of prime factors of n. If $n = 1$ the statement is trivial, so assume that $n > 1$. Then G is non-trivial, and since G is solvable there is a non-trivial normal p-subgroup A of G for some prime number p. Let K be the kernel of the action of G on $A\backslash X$. By (3) each A-orbit of X has size p. The normalizer in the symmetric group on p elements of a cyclic group of order p has order $p(p-1)$. Since any element of K normalizes the A-action on each A-orbit of X, it follows that K is annihilated by $p(p-1)$. But by the induction hypothesis, G acts on $A\backslash X$ through a group that is annihilated by $(n/p)\varphi(n/p)$. Since $\varphi(n) = (p-1)\varphi(n/p)$ statement (a) follows.

Lemma 2. *Let G be a solvable group acting faithfully and transitively on a finite set X of cardinality n for which n is coprime to $\varphi(n)$. Suppose that A is a normal p-subgroup of G for some prime p. Then*

(a) *G has a normal Sylow p-subgroup;*
(b) *for every (n/p)-element $s \in G$ the subset X^s of X is A-stable, and we have $(X^s)^a = X^{as}$ for all $a \in A$.*

Proof. From $\gcd(n, \varphi(n)) = 1$ it follows that n is squarefree. By Lemma 1 all A-orbits on X have cardinality p, and G acts on $A\backslash X$ through a group that is annihilated by $(n/p)\varphi(n/p)$. By our assumption on n, this number is coprime to p, so a Sylow p-subgroup S of the kernel K of the action of G on $A\backslash X$ is a Sylow p-subgroup of G. Since K has orbits of size p, and K acts on each orbit through a group of order dividing $p(p-1)$ that has a normal subgroup of order p, the group S is normal and hence characteristic in K. Therefore S is normal in G.

To prove (b), let $Z \subset X$ be an A-orbit that meets X^{as} for some $a \in A$. Then Z is s-stable. By Lemma 1(a), applied to the action of $\langle A, s\rangle$ on Z, we see that $s^{p(p-1)}$ acts trivially on Z. But by our assumption on n, the order of s is coprime to $p(p-1)$, so that s acts trivially on Z. With $a = 1$, it follows that X^s is a union of A-orbits. Also, one finds that $X^{as} \subset (X^s)^a$ for any $a \in A$; the inclusion $(X^s)^a \subset X^{as}$ is trivial, so this proves (b).

Lemma 3. *Let G be a finite solvable group acting on two finite sets X and Y of cardinality n. Assume that $\#X^g = \#Y^g$ for all n-elements $g \in G$, and that G acts transitively on X. Then G acts transitively on Y and the kernel of the G-action on Y is equal to the kernel of the G-action on X.*

Proof. For any positive integer n, a Hall n-subgroup of a finite group is a subgroup whose order is built up from primes dividing n and whose index is coprime to n. We will use that a solvable group G contains a Hall n-subgroup for every positive integer n; see [8, VI.1.8].

Let S be a Hall n-subgroup of G. For $x \in X$ let S_x and G_x be the stabilizers of x in S and in G. We have

$$n = [G : G_x] \mid [G : S_x] = [G : S][S : S_x],$$

so $n \mid [S : S_x]$, which implies that S acts transitively on X. Since X and Y are linearly equivalent over S, it follows that S acts transitively on Y as well. In particular, Y is a transitive G-set.

Let K be the kernel of the G-action on X and let N be the normal subgroup of G generated by the n-elements of K. Using that a surjective map of finite groups remains surjective when restricted to n-elements, one proves that $[K : N]$ is coprime to n. By our assumption, N is also contained in the kernel of the action of G on Y, so that G/N acts on Y. Since K/N is normal in G/N and G/N acts transitively on Y, all orbits of K/N on Y have the same cardinality l. Thus l divides $\#Y = n$, and it also divides $\#(K/N)$. It follows that $l = 1$ and that K acts trivially on Y. By the same argument, the kernel of the action of G on Y acts trivially on X. This proves Lemma 3.

Lemma 4. *Let A be an abelian p-group, and let X and Y be linearly equivalent A-sets all of whose A-orbits have cardinality p. Then X and Y are isomorphic as A-sets.*

Proof. Let B be a subgroup of A of index p. On each A-orbit of X the group B either acts transitively or trivially. The number $n_B(X)$ of A-orbits of X that are A-isomorphic to A/B therefore satisfies

$$(p^2 - p) \cdot n_B(X) = p \cdot \#(B\backslash X) - \#X.$$

The right side depends only on X up to linear equivalence, so it follows that $n_B(X) = n_B(Y)$ for all subgroups B of index p in A. This implies the lemma.

Before moving to the main proof in this section, we recall a property of the Fitting group of a solvable group. A finite group is said to be nilpotent if it is a product of groups of prime power orders. Two normal subgroups of a finite group G whose orders are powers of distinct prime numbers, centralize each other. One deduces that G has a unique maximal normal nilpotent subgroup F, which is called the Fitting group of G. We will use that for a finite solvable group G the centralizer of F in G is contained in F, so that G/F canonically embeds into the group $\operatorname{Out} F$ of outer automorphisms of F. We refer to [8, III.4.2] for a proof.

Proposition. *Let n be a positive integer for which $\varphi(n)$ is coprime to n. Let G be a finite solvable group acting transitively on a set X of cardinality n. Suppose that G also acts on a finite set Y and that for all n-elements $g \in G$ we have $\#X^g = \#Y^g$. Then X and Y are isomorphic as G-sets.*

Proof. We prove this by induction on the number of primes dividing the square-free number n. If $n = 1$ the result is trivial.

By Lemma 3 the G-set Y is transitive, and the kernels of the G-actions on X and on Y are the same. Since all n-elements of a quotient of G are images of n-elements of G, we may assume that G acts faithfully on both X and Y.

Let F be the Fitting group of G. We see from Lemma 1(a, d), that F is the product of elementary abelian normal subgroups of G of prime power orders, and that all primes dividing $\#F$ also divide n. First consider the case that F is cyclic. Then the order of F divides n. The group G/F embeds into $\operatorname{Out} F$, and $\operatorname{Aut} F$ has order coprime to n, so $[G : F]$ is coprime to n. But n divides $\#G$, so we must have $\#F = n$. It follows that the point stabilizers in G of points in X and Y are complements to F. Since $\#F$ is coprime to $[G : F]$ we have $H^1(G/F, F) = 0$, so all such point stabilizers are conjugate; cf. [13, Chap. I, §5.2]. We conclude that X and Y are isomorphic as G-sets if F is cyclic.

Now assume that F is not cyclic. Then there is a prime number p for which G has a non-cyclic normal p-subgroup. By Lemma 2(a) the group G contains a normal non-cyclic Sylow p-subgroup A. Lemma 1 implies that A is elementary abelian, and that the orbits of A on X and on Y all have cardinality p.

We come to the key step of the proof, which is to consider a 'block' of X consisting of elements with the same stabilizer in A. More precisely, take $x_0 \in X$, let B be the stabilizer of x_0 in A, and let $X_0 = \operatorname{Fix}_B X$. For $g \in G$ we have $gx_0 \in X_0$ if and only if B is contained in the stabilizer of gx_0 in A, which is gBg^{-1}; this occurs if and only if g belongs to the normalizer G_0 of B in G. Hence G_0 acts transitively on X_0 and contains the stabilizer of x_0 in G. We put $n_0 = \#X_0 = n/[G : G_0]$. The group B is non-trivial because A is not cyclic. Since B acts faithfully on X it follows that $n_0 < n$.

Since G_0 normalizes B, it acts also on $Y_0 = \operatorname{Fix}_B Y$. We shall apply the induction hypothesis to G_0 acting on X_0 and Y_0. For this, we need to check that $\#X_0^g = \#Y_0^g$ for any n_0-element $g \in G_0$. Let g be such, and write $g = ts$ for suitable powers t and s of g so that t is a p-element and s is an (n/p)-element. Note that $t \in A$ because A is the normal Sylow p-subgroup of G. Since A is normal, as is an n-element for any $a \in A$, so we have $\#X^{as} = \#Y^{as}$. By Lemma 2(b) this implies that X^s and Y^s are linearly equivalent A-sets, so by Lemma 4 they are isomorphic as A-sets. Therefore we have $\#\operatorname{Fix}_{\langle t,B\rangle}(X^s) = \#\operatorname{Fix}_{\langle t,B\rangle}(Y^s)$. But again from Lemma 2(b), we have

$$X_0^g = \operatorname{Fix}_{\langle ts,B\rangle} X = \operatorname{Fix}_{\langle t,s,B\rangle} X = \operatorname{Fix}_{\langle t,B\rangle}(X^s),$$

and likewise $Y_0^g = \operatorname{Fix}_{\langle t,B\rangle}(Y^s)$. It follows that $\#X_0^g = \#Y_0^g$, as desired.

Now the induction hypothesis implies that X_0 and Y_0 are isomorphic as G_0-sets. The stabilizer H of x_0 in G is contained in G_0, so H stabilizes a point in Y_0. Thus, both X and Y are G-isomorphic to G/H. This completes the proof of the proposition, and the proof of the implication (3) $\Rightarrow$ (5) of Theorem 2 in the case n is coprime to $\varphi(n)$.

4. The case $n = pq$

In this section we prove the implication (3) $\Rightarrow$ (5) of Theorem 2 for the remaining case. We let $n = pq$ for two not necessarily distinct prime numbers p and q. We have a solvable group G acting transitively on a set X of cardinality n. It is also given that G acts on a finite set Y and that for all n-elements $g \in G$ we have $\#X^g = \#Y^g$. We shall prove that X and Y are isomorphic as G-sets.

As in the proof of the proposition in Section 3, we may assume that the action of G is faithful and transitive on both X and Y. We will first treat two special cases, and then deduce the general case.

Case 1. *There is an abelian normal subgroup A of G that acts transitively on X.*

Since A is transitive and abelian, any element a of A that fixes a point in X fixes all points of X, so that $a = 1$. Therefore X and Y are both A-isomorphic to the A-set A. This readily implies that A is equal to its own centralizer in G. In other words, the canonical map $G/A \to \operatorname{Aut}(A)$ is injective. Note that $\operatorname{Aut} A$ is isomorphic to $\mathbb{F}_p^* \times \mathbb{F}_q^*$, to $\mathrm{GL}_2(\mathbb{F}_p)$, or to $(\mathbb{Z}/p^2\mathbb{Z})^*$. By switching p and q if $p > q$ we can achieve that $p = q$ or $q \nmid \#\operatorname{Aut} A$. Let $S \subset G$ be the preimage in G of a Sylow p-subgroup of G/A. Then S/A is cyclic and $[G : S]$ is coprime to $n = pq$.

The elements of S are n-elements, so X and Y are linearly equivalent over S. But X and Y have cyclic point stabilizers in S, and therefore X and Y are isomorphic as S-sets. This implies that point stabilizers in G of X and Y give classes in $H^1(G/A, A)$ that restrict to the same element of $H^1(S/A, A)$. But this restriction map is injective, because $[G : S]$ and $\#A$ are coprime [13, Chap. I, §2.4]. This completes the proof for Case 1.

Case 2. *There is a normal p-subgroup A of G that is not cyclic, and whose orbits on X have cardinality p.*

We first prove that the G-sets $\bar{X} = A\backslash X$ and $\bar{Y} = A\backslash Y$ are isomorphic. If $g \in G$ is a q-element then X and Y are linearly equivalent as $\langle g, A\rangle$-sets, so $\bar{X}$ and $\bar{Y}$ are also linearly equivalent as $\langle g, A\rangle$-sets, and $\#\bar{X}^g = \#\bar{Y}^g$. It follows from the proposition in Section 3, applied to G acting on $\bar{X}$ and $\bar{Y}$, that $\bar{X}$ and $\bar{Y}$ are isomorphic as G-sets. From $\#Y/\#\bar{Y} = \#X/\#\bar{X} = p$ we see that all orbits of A on Y have cardinality p. By Lemma 4 of Section 3 it follows that X and Y are isomorphic as A-sets.

As in the proof in Section 3, we now consider a block of X consisting of elements with the same stabilizer in A. Let $x_0 \in X$, and let B be the stabilizer of x_0 in A. As in the previous section, B is non-trivial because A is not cyclic, and $\#\operatorname{Fix}_B X$ is a divisor of $n = pq$ that is smaller than n. Also, $\operatorname{Fix}_B X$ is a union of A-orbits, so p divides $\#\operatorname{Fix}_B X$. It follows that $\#\operatorname{Fix}_B X = p$ and that $Ax_0 = \operatorname{Fix}_B X$. Applying an A-isomorphism $X \to Y$, we find $y_0 \in Y$ with $Ay_0 = \operatorname{Fix}_B Y$.

Let H be the stabilizer of x_0 in G. The group H normalizes $H \cap A = B$, so it acts on $\operatorname{Fix}_B X = Ax_0$ and on $\operatorname{Fix}_B Y = Ay_0$. Therefore H fixes the elements $\bar{x}_0$ and $\bar{y}_0$ of $\bar{X}$ and $\bar{Y}$. Since $\bar{X} \cong_G \bar{Y}$ it follows that $\bar{X} - \{\bar{x}_0\} \cong_H \bar{Y} - \{\bar{y}_0\}$.

Let S be a Sylow p-subgroup of H. The group B acts transitively on each A-orbit in $X - Ax_0$ and $Y - Ay_0$. Since S contains B, this implies that all S-orbits of $X - Ax_0$ and $Y - Ay_0$ are closed under the action of A. It follows that S has the same number of orbits on the four sets $X - Ax_0$, $\bar{X} - \{\bar{x}_0\}$, $\bar{Y} - \{\bar{y}_0\}$, and $Y - Ay_0$. Because X and Y are linearly equivalent over S, the number of S-orbits on X and Y is also the same. It follows that S has the same number of orbits on Ax_0 and Ay_0. But S is a p-group fixing x_0, and since $\#Ax_0 = \#Ay_0 = p$, the group S acts trivially on Ax_0 and Ay_0.

The action of H on Ay_0 is therefore an action on a set of p elements that normalizes the group generated by a p-cycle, and whose Sylow p-subgroup acts trivially. That is only possible if H fixes a point in Ay_0, so that the G-sets X, Y, and G/H are all isomorphic. This completes the proof of Case 2.

Proof of the general case. We consider the Fitting subgroup F of G. First suppose that F acts transitively on X. If the center Z of F acts transitively on X then we are done by Case 1. So suppose Z does not act transitively on X. The primes p and q divide the order of the center Z of F, because they divide $\#F$, and Z acts freely on X. It follows that $\#Z = p = q$, and that F is a p-group. Thus $Z\backslash X$ has cardinality p, and F acts transitively on $Z\backslash X$ through a group of order p. Let A be the kernel of this action. Then A is normal in G of order $\#F/p$, and it contains Z. Since its orbits on X have cardinality p and A acts faithfully on X, the group A is elementary abelian. Because F is non-abelian, we have

$p^3 \mid \#F$ and $p^2 \mid \#A$. Hence A is non-cyclic, and Case 2 applies.

Now suppose that F does not act transitively on X. Since G/F embeds into $\operatorname{Out} F$ we know that $F \neq \{1\}$, so all F-orbits in X have the same prime cardinality, which, after possibly switching p and q, we may assume to be p. If F is non-cyclic then Case 2 applies, so assume that F is cyclic of order p. Then $\operatorname{Out} F$ and therefore G/F are also cyclic, and we have $p \nmid [G : F]$. It follows that G has only one subgroup S of index q, so that all points in $F\backslash X$ or $F\backslash Y$ have stabilizer S in G. The point stabilizers in G of points in X or Y are contained in S, so they are complements of F in S. But such point stabilizers are then conjugate in S because $H^1(S/F, F) = 0$. Thus X and Y are isomorphic as G-sets. This completes the proof of Theorem 2.

5. Non-solvable groups and asymptotic results

Write $\mathcal{R}$ for the set of positive integers n for which there exists a group G with two non-isomorphic linearly equivalent transitive G-sets of cardinality n. In Theorem 1 we described the subset $\mathcal{S}$ of $\mathcal{R}$ that consists of those n that arise from solvable groups G. It turns out that both $\mathcal{S}$ and $\mathcal{R}$ have density 1 in the set of positive integers. We will make this more precise below.

In order to produce elements in $\mathcal{R} - \mathcal{S}$ we describe two additional constructions of groups G with two non-isomorphic linearly equivalent transitive G-sets. Let L be a finite field, q its cardinality, and let V be a vector space over L of dimension $d \geq 2$. We put $G = \operatorname{GL} V$. Every element $g \in G$ fixes the same number of elements in V and its dual $V^* = \operatorname{Hom}_L(V, L)$. This implies that $V - \{0\}$ and $V^* - \{0\}$ are linearly equivalent transitive G-sets of cardinality $q^d - 1$. For any divisor m of $q - 1$ we can divide out by the action of a subgroup of index m in L^*. This leads to two linearly equivalent transitive G-sets of cardinality $m(q^d - 1)/(q - 1)$. It is easy to check that these G-sets are not isomorphic if and only if $m + d \geq 4$. Multiplying the groups and sets by any group of order $k \geq 1$ we find that the set

$$\mathcal{T} = \{km(q^d - 1)/(q - 1) : q \text{ is a prime power, } d \geq 2,\ m \mid q - 1,\ m + d \geq 4,\ k \geq 1\}$$

is a subset of $\mathcal{R}$.

For the second construction we take $G = \operatorname{PSL}(2, L)$, where L is a finite field in which $6 \neq 0$ so that $q = \#L$ is ± 1 modulo 5. A result of Dickson [8, II.8.27] implies that G contains a subgroup H that is isomorphic to A_5. We now let K be a conjugate of H by an element of $\operatorname{PGL}(2, L)$ that is not contained in G. We claim that G/H and G/K are non-isomorphic linearly equivalent G-sets. Let us sketch a proof. Linear equivalence follows from the fact that for each $l \in \{2,3,5\}$ all subgroups of order l in G are conjugate. Now suppose that G/H and G/K are isomorphic, so that H and K are conjugate. Then one first proves that the centralizer of H in $\mathrm{PGL}(2,L)$ is trivial. The normalizer of H in $\mathrm{PGL}(2,L)$ is bigger than the normalizer of H in G, and it injects to $\mathrm{Aut}\, A_5 = S_5$. So this injection is an isomorphism. But since in S_5 any two elements of order 5 are conjugate, it follows that some element of order 5 in G is $\mathrm{PGL}(2,L)$-conjugate to its square. Lifting this element to $\mathrm{SL}(2,L)$ and considering its eigenvalues one readily obtains a contradiction. This proves the claim. It follows that the set

$$\mathcal{U} = \{kq(q^2-1)/120 : q \text{ is a prime power coprime to } 6,\ q \equiv \pm 1 \bmod 5,\ k \geq 1\}$$

is contained in $\mathcal{R}$. Unfortunately, this does not give much more information than the inclusion $\mathcal{S} \cup \mathcal{T} \subset \mathcal{R}$ that we knew already, since $\mathcal{U} - (\mathcal{S} \cup \mathcal{T})$ is contained in the set of multiples of 11 and $29 \cdot 59$, which arise from $q = 11$ and $q = 59$.

The three constructions tell us that $\mathcal{S} \cup \mathcal{T} \cup \mathcal{U} \subset \mathcal{R}$. We do not know if equality holds. The combined results of Feit, Guralnick, and Wales [4, 5, 6] say that

$$(*) \qquad \{n \in \mathcal{R} : n \text{ is the product of at most two primes}\} \subset \mathcal{T} \cup \mathcal{U}$$

if the classification of finite simple groups is valid. This represents our only tool in proving that integers do *not* belong to $\mathcal{R}$.

We now come to the asymptotic results. For two positive real-valued functions f, g that are defined on $\mathbb{R}_{\geq a}$ for some $a \in \mathbb{R}$, we say that $f(x) \lesssim g(x)$ as $x \to \infty$ if $\limsup_{x\to\infty} f(x)/g(x) \leq 1$, and we say that $f(x) \sim g(x)$ as $x \to \infty$ if $\lim_{x\to\infty} f(x)/g(x) = 1$. We write $\log^k$ for the k-fold iteration $\log \circ \ldots \circ \log$ for any positive integer k, and γ for Euler's constant.

Proposition. *We have*

$$\text{(a)} \qquad \#\{n \leq x : n \in \mathcal{R}\} \sim \#\{n \leq x : n \in \mathcal{S}\} \sim x$$

and

$$\text{(b)} \qquad \frac{x \log^2 x}{\log x} \lesssim \#\{n \leq x : n \notin \mathcal{R}\} \leq \#\{n \leq x : n \notin \mathcal{S}\} \sim \frac{x\mathrm{e}^{-\gamma}}{\log^3 x}$$

for $x \to \infty$*, assuming* $(*)$ *for the first inequality in* (b).

We sketch the proof of the proposition. By Theorem 1 every positive integer n outside $\mathcal{S}$ satisfies $n = pq$, for primes p and q, or $\gcd(n, \varphi(n)) = 1$. These two properties have known asymptotic behavior: we have

$$\#\{n \le x : n = pq \text{ for primes } p,\, q\} \sim \frac{x \log^2 x}{\log x} \quad \text{as } x \to \infty$$

by Theorem 437 in Hardy and Wright [7], and

$$\#\{n \le x : n \ge 1,\ \gcd(n, \varphi(n)) = 1\} \sim \frac{x\mathrm{e}^{-\gamma}}{\log^3 x} \quad \text{as } x \to \infty$$

by Erdős [3]. Since for every real number $\epsilon > 0$ we have $(\log^2 x)/\log x \lesssim \epsilon/\log^3 x$ as $x \to \infty$, the rightmost "$\sim$" in (b) follows. The second inequality in (b) is trivial. The results in (a) follow immediately because $1/\log^3 x$ tends to zero as $x \to \infty$.

It remains to show the first inequality in (b). Let $\mathcal{Q}$ be the set of products of two primes. By Theorem 437 from [7], quoted above, it suffices to show that $\mathcal{R} \cap \mathcal{Q}$ is "negligible" by comparison with $\mathcal{Q}$, in the sense that

$$\frac{\#\{n \le x : n \in \mathcal{R} \cap \mathcal{Q}\}}{\#\{n \le x : n \in \mathcal{Q}\}} \to 0 \qquad \text{as } x \to \infty.$$

Let $\mathcal{P}$ be the set of prime numbers, and put $\mathcal{V} = \{(q^d - 1)/(q - 1) : q \text{ is a prime power}, d \ge 3\}$. If $(q^d - 1)/(q - 1) \le x$, with $d \ge 3$ and $q \ge 2$, then one has $q^{d-1} \le x$, so $q \le \sqrt{x}$ and $d - 1 \le (\log x)/\log 2$. This implies that $\#\{n \le x : n \in \mathcal{V}\} \le \sqrt{x} \cdot (\log x)/\log 2$, which shows that $\mathcal{V} \cap \mathcal{P}$ and $\mathcal{V} \cap \mathcal{Q}$ are negligible by comparison with $\mathcal{P}$ and $\mathcal{Q}$, respectively. Writing $\mathcal{F}$ for the set of Fermat primes, one deduces from $(*)$ in a straightforward manner that $\mathcal{R} \cap \mathcal{Q}$ is contained in the union of the three sets

$$\{29 \cdot 59\}, \qquad \mathcal{V} \cap \mathcal{Q}, \qquad \{pq : p \in \mathcal{P},\, q \in \{11\} \cup \mathcal{F} \cup \big(\mathcal{V} \cap \mathcal{P}\big)\}.$$

The first two of these sets are negligible by comparison with $\mathcal{Q}$. Also, from the fact that each of $\{11\}$, $\mathcal{F}$, and $\mathcal{V} \cap \mathcal{P}$ is negligible by comparison with $\mathcal{P}$, it follows by an easy argument that the third set is negligible by comparison with $\mathcal{Q}$ as well. The proposition follows.

We finally illustrate our knowledge of $\mathcal{R}$ by considering small numbers. It was first shown by Perlis [12] that 7 and 8 are the two smallest elements of $\mathcal{R}$. The elements of $\mathcal{T} \cup \mathcal{U}$ below 100 that are not in $\mathcal{S}$ are

$$7,\ 11,\ 13,\ 14,\ 15,\ 21,\ 22,\ 26,\ 31,\ 33,\ 35,\ 39,$$
$$49,\ 51,\ 55,\ 57,\ 62,\ 65,\ 73,\ 77,\ 85,\ 91,\ 93.$$

By $(*)$ the following are not in $\mathcal{R}$:

$$9,\ 10,\ 17,\ 19,\ 23,\ 25,\ 29,\ 34,\ 37,\ 38,\ 41,\ 43,\ 46,\ 47,\ 53,\ 58,$$
$$59,\ 61,\ 67,\ 69,\ 71,\ 74,\ 79,\ 82,\ 83,\ 86,\ 87,\ 89,\ 94,\ 95,\ 97.$$

In [6] this list is given up to 40, with 34 omitted by mistake. At the time of [6] it was unknown whether $18 \in \mathcal{R}$. We now know that $18 \in \mathcal{S} \subset \mathcal{R}$, and that the list above is equal to $\{7, 8, \cdots, 100\} - \mathcal{R}$. With the help of $(*)$ it is not hard to find $\{n \in \mathcal{R} : n \leq 2000\}$ explicitly. The subset $\mathcal{S} \cup \mathcal{T} \cup \mathcal{U}$ of $\mathcal{R}$ contains 1303 elements up to 2000, of which 1083 are in $\mathcal{S}$. The remaining 697 numbers up to 2000 are products of at most two prime numbers, so that $(*)$ implies that they are not in $\mathcal{R}$.

Below 4000 there are only 8 values of n for which we cannot decide whether $n \in \mathcal{R}$ only on the basis of $(*)$ and the inclusion $\mathcal{S} \cup \mathcal{T} \cup \mathcal{U} \subset \mathcal{R}$:

$$\begin{array}{ll} 2001 = 3 \cdot 23 \cdot 29 & 3335 = 5 \cdot 23 \cdot 29 \\ 2185 = 5 \cdot 19 \cdot 23 & 3515 = 5 \cdot 19 \cdot 37 \\ 2755 = 5 \cdot 19 \cdot 29 & 3567 = 3 \cdot 29 \cdot 41 \\ 2829 = 3 \cdot 23 \cdot 41 & 3657 = 3 \cdot 23 \cdot 53. \end{array}$$

References

1. W. Bosma, B. de Smit, *Arithmetically equivalent fields of small degree*, in preparation.
2. J. W. S. Cassels and A. Fröhlich (eds), *Algebraic number theory*, Academic Press, London, 1967.
3. P. Erdős, *Some asymptotic formulas in number theory*, J. Indian Math. Soc. **12** (1948), 75–78.
4. W. Feit, *Some consequences of the classification of finite simple groups*, pp. 175–181 in: B. Cooperstein and G. Mason (eds), *The Santa Cruz conference on finite groups 1979*, Proc. Sympos. Pure Math. **37**, Amer. Math. Soc., Providence, RI, 1980.
5. R. M. Guralnick, *Subgroups inducing the same permutation representation*, J. Algebra **81** (1983), 312–319.
6. R. M. Guralnick and D. B. Wales, *Subgroups inducing the same permutation representation, II*, J. Algebra **96** (1985), 94–113.
7. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fourth edition, Oxford University Press, London, 1971.
8. B. Huppert, *Endliche Gruppen I*, Grundlehren Math. Wiss. **134**, Springer-Verlag, Berlin, 1967.

9. I. M. Isaacs, *Fixed points and* Π*-complements in* Π*-separable groups*, Arch. Math. (Basel) **39** (1982), 5–8.
10. V. V. Ishkhanov, B. B. Lur′e, and D. K. Faddeev, *The embedding problem in Galois theory*, Transl. Math. Monogr. **165**, Amer. Math. Soc., Providence, RI, 1997 [translation of 1990 Russian original].
11. N. Klingen, *Arithmetical similarities*, Oxford University Press, Oxford, 1998.
12. R. Perlis, *On the equation* $\zeta_K(s) = \zeta_{K'}(s)$, J. Number Theory **9** (1977), 342–360.
13. J-P. Serre, *Cohomologie galoisienne*, Lecture Notes in Math. **5**, fifth edition, Springer-Verlag, Berlin, 1994.