Cambridge University Press
978-1-107-62944-8 - Classical Groups, Derangements and Primes
Timothy C. Burness and Michael Giudici
Excerpt
More information

1

Introduction

The study of derangements in transitive permutation groups has a long and rich history, which can be traced all the way back to the origins of probability theory in the early eighteenth century. In 1708, the French mathematician Pierre de Montmort wrote one of the first highly influential books on probability, entitled *Essay d'Analyse sur les Jeux de Hazard* [106], in which he presents a systematic combinatorial analysis of games of chance that were popular at the time. Through studying the card game *treize* (and variations), he calculates the proportion of derangements in the symmetric group S_{13} in its natural action on 13 points, and he proposes the general formula

$$\frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}$$

for the natural action of S_n. In a second edition, published in 1713, he reports on his correspondence with Nicolaus Bernoulli, who proved the above formula using the inclusion-exclusion principle (see [117] for further details). In particular, it follows that the proportion of derangements in S_n tends to $1/e$ as n tends to infinity.

In the context of permutation group theory, derangements have been widely studied since the days of Jordan in the nineteenth century, finding a range of interesting applications and connections in diverse areas such as graph theory, number theory and topology. In more recent years, following the Classification of Finite Simple Groups, the subject has been reinvigorated and our understanding of derangements has advanced greatly. As we shall see, many new results on the proportion of derangements in various families of groups have been obtained, and there has been a focus on studying the existence of derangements with special properties.

In the first three sections of this introductory chapter we will briefly survey some of these results and applications, focusing in particular on derangements of prime order. Given a fixed prime number r, we will see that the problem of determining the existence of a derangement of order r in a finite transitive permutation group G can essentially be reduced to the case where G is a primitive almost simple group of Lie type. In this book, we aim to provide a detailed analysis of derangements of prime order in classical groups; the basic problem is introduced in Section 1.4, and we present a brief summary of our main results in Section 1.5 (with more detailed results given later in the text).

1.1 Derangements

We start by recalling some basic notions. We refer the reader to the books by Cameron [35], Dixon and Mortimer [48] and Wielandt [120] for excellent introductions to the theory of permutation groups.

Let G be a permutation group on a set Ω, so G is a subgroup of $\mathrm{Sym}(\Omega)$, the group of all permutations of Ω. We will use exponential notation for group actions, so α^g denotes the image of $\alpha \in \Omega$ under the permutation $g \in G$. The cardinality of Ω is called the *degree* of G.

We say that G is *transitive* on Ω if for all $\alpha, \beta \in \Omega$ there exists an element $g \in G$ such that $\alpha^g = \beta$. The *stabiliser in* G *of* α, denoted by G_α, is the subgroup of G consisting of all the permutations that fix α. The familiar Orbit-Stabiliser Theorem implies that if G is transitive then Ω can be identified with the set of (right) cosets of G_α in G. Moreover, the action of G on Ω is equivalent to the natural action of G on this set of cosets by right multiplication.

Given a subgroup H of G, we will write H^g to denote the conjugate subgroup $g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$. It is easy to see that $G_{\alpha^g} = (G_\alpha)^g$ for all $\alpha \in \Omega$, $g \in G$. In particular, if G is transitive then G_α and G_β are conjugate subgroups for all $\alpha, \beta \in \Omega$.

The notion of primitivity is a fundamental indecomposability condition in permutation group theory. We say that a transitive group G is *imprimitive* if Ω admits a nontrivial G-invariant partition (there are two trivial partitions, namely $\{\Omega\}$ and $\{\{\alpha\} \mid \alpha \in \Omega\}$), and *primitive* otherwise. Equivalently, G is primitive if and only if G_α is a maximal subgroup of G. The finite primitive groups are the basic building blocks of all finite permutation groups.

Notice that if N is a normal subgroup of G, then the set of orbits of N on Ω forms a G-invariant partition of Ω. Thus, if G is primitive, every nontrivial normal subgroup of G is transitive. We can generalise the notion of primitivity by defining a group to be *quasiprimitive* if every nontrivial normal subgroup is transitive.

Definition 1.1.1 Let G be a group acting on a set Ω. An element of G is a *derangement* (or *fixed-point-free*) if it fixes no point of Ω. We write $\Delta(G)$ for the set of derangements in G. In addition, if G is finite then $\delta(G) = |\Delta(G)|/|G|$ denotes the proportion of derangements in G.

Note that if G is transitive with point stabiliser H then

$$\Delta(G) = G \setminus \bigcup_{g \in G} H^g \tag{1.1.1}$$

so an element $x \in G$ is a derangement if and only if $x^G \cap H$ is empty, where $x^G = \{g^{-1}xg \mid g \in G\}$ is the conjugacy class of x in G. We also observe that $\Delta(G)$ is a normal subset of G.

Let G be a finite group acting transitively on a set Ω with $|\Omega| \geqslant 2$. By the Orbit-Counting Lemma we have

$$\frac{1}{|G|} \sum_{x \in G} |\mathrm{fix}_{\Omega}(x)| = 1$$

where $\mathrm{fix}_{\Omega}(x) = \{\alpha \in \Omega \mid \alpha^x = \alpha\}$ is the set of fixed points of x on Ω. Since $|\mathrm{fix}_{\Omega}(1)| = |\Omega| \geqslant 2$, there must be an element $x \in G$ with $|\mathrm{fix}_{\Omega}(x)| = 0$ and thus G contains a derangement. This is a theorem of Jordan, which dates from 1872 (see [82]).

Theorem 1.1.2 *Let G be a finite group acting transitively on a set Ω with $|\Omega| \geqslant 2$. Then G contains a derangement.*

In particular, every nontrivial finite transitive permutation group contains a derangement. In view of (1.1.1), Jordan's theorem is equivalent to the fact that

$$G \neq \bigcup_{g \in G} H^g \tag{1.1.2}$$

for every proper subgroup H of a finite group G.

It is easy to see that Jordan's theorem does *not* extend to transitive actions of infinite groups:

(i) Let $\mathrm{FSym}(\Omega)$ be the *finitary symmetric group* on an infinite set Ω; it comprises the permutations of Ω with finite support (that is, the permutations that move only finitely many elements of Ω). Clearly, this transitive group does not contain any derangements.

(ii) Let V be an n-dimensional vector space over $\mathbb{C}$ and let $G = \mathrm{GL}(V)$ be the general linear group of all invertible linear transformations of V. Let Ω be the set of complete flags of V, that is, the set of subspace chains

$$\{0\} = V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_{n-1} \subset V_n = V$$

where each V_i is an i-dimensional subspace of V. The natural action of G on V induces a transitive action of G on Ω. For each $x \in G$ there is a basis of V in which x is represented by a lower-triangular matrix (take the Jordan canonical form of x, for example), so x fixes a complete flag and thus G has no derangements.

(iii) More generally, consider a connected algebraic group G over an algebraically closed field K of characteristic $p \geqslant 0$, and let B be a Borel subgroup of G. Then every element of G belongs to a conjugate of B, so G has no derangements in its transitive action on the flag variety G/B. In fact, by a theorem of Fulman and Guralnick [55, Theorem 2.4], if G is a simple algebraic group acting on a coset variety G/H, then G contains no derangements if and only if one of the following holds:
   (a) H contains a Borel subgroup of G;
   (b) $G = \mathrm{Sp}_n(K)$, $H = \mathrm{O}_n(K)$ and $p = 2$;
   (c) $G = G_2(K)$, $H = \mathrm{SL}_3(K).2$ and $p = 2$.

   Moreover, if G is simple then [55, Lemma 2.2] implies that $\Delta(G)$ is a dense subset of G (with respect to the Zariski topology) if and only if H does not contain a maximal torus of G.

As observed by Serre, Jordan's theorem has some interesting applications in number theory and topology (see Serre's paper [113] for further details).

(i) *A number-theoretic application.* Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial over $\mathbb{Q}$ with degree $n \geqslant 2$. Then f has no roots modulo p for infinitely many primes p.

(ii) *A topological application.* Let $f : T \to S$ be a finite covering of a topological space S, where f has degree $n \geqslant 2$ (so that $|f^{-1}(s)| = n$ for all $s \in S$) and T is path-connected and non-empty. Then there exists a continuous map $\varphi : \mathbb{S}_1 \to S$ from the circle $\mathbb{S}_1$ that cannot be lifted to the covering T.

In view of Jordan's theorem, two natural questions arise:

Question 1. *How abundant are derangements in transitive groups?*

Question 2. *Can we find derangements with special properties, such as a prescribed order?*

Both of these questions have been widely investigated in recent years, and in the next two sections we will highlight some of the main results.

Remark 1.1.3 We will focus on Questions 1 and 2 above. However, there are many other interesting topics concerning derangements that we will not discuss. Here are some examples:

(i) *Normal coverings.* Let G be a finite group and recall that if H is a proper subgroup of G then $\bigcup_{g \in G} H^g$ is a proper subset of G (see (1.1.2)). A collection of proper subgroups $\{H_1, \ldots, H_t\}$ is a *normal covering* of G if

$$G = \bigcup_{i=1}^{t} \bigcup_{g \in G} H_i^g$$

and we define $\gamma(G)$ to be the minimal size of a normal covering of G. By Jordan's theorem, $\gamma(G) \geqslant 2$, and this invariant has been investigated in several recent papers (see [15, 16, 42], for example). The connection to derangements is transparent: if $\{H_1, \ldots, H_t\}$ is a normal covering then each $x \in G$ has fixed points on the set of cosets G/H_i, for some i.

(ii) *Algorithms.* Given a set of generators for a subgroup $G \leqslant S_n$, it is easy to determine whether or not G is transitive. If G is transitive and $n \geqslant 2$, then Jordan's theorem implies that G contains a derangement, and there are efficient randomised algorithms to find a derangement in G. In a recent paper, Arvind [2] has presented the first elementary *deterministic* polynomial-time algorithm for finding a derangement.

(iii) *Thompson's question.* A finite transitive permutation group $G \leqslant \mathrm{Sym}(\Omega)$ is *Frobenius* if $|G_\alpha| > 1$ and $G_\alpha \cap G_\beta = 1$ for all distinct $\alpha, \beta \in \Omega$. By a theorem of Frobenius, $\{1\} \cup \Delta(G)$ is a normal transitive subgroup and thus $\Delta(G)$ is a transitive subset of G. The following, more general question, has been posed by J. G. Thompson.

Question. *Let* $G \leqslant \mathrm{Sym}(\Omega)$ *be a finite primitive permutation group. Is* $\Delta(G)$ *a transitive subset of* G*?*

This is Problem 8.75 in the Kourovka Notebook [84]. It is easy to see that the primitivity condition here is essential; there are imprimitive groups G such that $\Delta(G)$ is intransitive. For instance, take the natural action of the alternating group A_4 on the set of 2-element subsets of $\{1, 2, 3, 4\}$.

1.2 Counting derangements

Let G be a transitive permutation group on a finite set Ω with $|\Omega| = n \geqslant 2$. Recall that $\Delta(G)$ is the set of derangements in G, and $\delta(G) = |\Delta(G)|/|G|$ is the proportion of derangements. In general, it is difficult to compute $\delta(G)$

precisely. Of course, Jordan's theorem (Theorem 1.1.2) implies that $\delta(G) > 0$, and stronger lower bounds have been obtained in recent years. In [37], for example, Cameron and Cohen use the Orbit-Counting Lemma to show that $\delta(G) \geqslant 1/n$, with equality if and only if G is *sharply* 2*-transitive*, that is, either $(G,n) = (S_2,2)$, or G is a Frobenius group of order $n(n-1)$, with n a prime power. This has been extended by Guralnick and Wan (see [73, Theorem 1.3]).

Theorem 1.2.1 *Let G be a transitive permutation group of degree $n \geqslant 2$. Then one of the following holds:*

(i) $\delta(G) \geqslant 2/n$;
(ii) *G is a Frobenius group of order $n(n-1)$ with n a prime power;*
(iii) $G = S_n$ *and* $n \in \{2,4,5\}$.

It is worth noting that this strengthening of the lower bound on $\delta(G)$ from $1/n$ to $2/n$ requires the classification of the finite 2-transitive groups, which in turn relies on the Classification of Finite Simple Groups. As explained in [73], Theorem 1.2.1 has interesting applications in the study of algebraic curves over finite fields.

Inspired by Montmort's formula

$$\delta(S_n) = \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}$$

(with respect to the natural action of S_n), it is natural to consider the asymptotic behaviour of $\delta(G)$ when G belongs to an interesting infinite family of groups. From the above formula, we immediately deduce that $\delta(S_n)$ tends to $1/e$ as n tends to infinity. Similarly, we find that $\delta(A_n) \geqslant 1/3$ and $\delta(\mathrm{PSL}_2(q)) \geqslant 1/3$ for all $n,q \geqslant 5$, with respect to their natural actions of degree n and $q+1$ (see [12, Corollary 2.6 and Lemma 2.8]). In these two examples, we observe that G belongs to an infinite family of finite simple groups, and $\delta(G)$ is bounded away from zero by an absolute constant.

In fact, a deep theorem of Fulman and Guralnick [55, 56, 57, 58] shows that this is true for *any* transitive simple group.

Theorem 1.2.2 *There exists an absolute constant $\varepsilon > 0$ such that $\delta(G) \geqslant \varepsilon$ for any transitive finite simple group G.*

This theorem confirms a conjecture of Boston *et al.* [12] and Shalev. The asymptotic nature of the proof does not yield an explicit constant, although [57, Theorem 1.1] states that $\varepsilon \geqslant 0.016$ with at most finitely many exceptions. It is speculated in [12, p. 3274] that the optimal bound is $\varepsilon = 2/7$, which is realised by the standard actions of $\mathrm{PSL}_3(2)$ and $\mathrm{PSL}_3(4)$, of degree

7 and 21, respectively. In fact, it is easy to check that the action of the Tits group $G = {}^2F_4(2)'$ on the set of cosets of a maximal subgroup $2^2.[2^8].S_3$ yields $\delta(G) = 89/325 < 2/7$, and we expect $89/325$ to be the optimal constant in Theorem 1.2.2.

Fulman and Guralnick also establish strong asymptotic results. For instance, they show that apart from some known exceptions, $\delta(G)$ tends to 1 as $|G|$ tends to infinity (the exceptions include $G = A_n$ acting on the set of k-element subsets of $\{1,\ldots,n\}$ with k bounded, for example). Further information on the limiting behaviour of the proportion of derangements in the natural action of S_n or A_n on k-sets is given by Diaconis, Fulman and Guralnick [44, Section 4], together with an interesting application to card shuffling.

As explained in [55, Section 6], one can show that the above theorem of Fulman and Guralnick does *not* extend to almost simple groups. For example, let p and r be primes such that r and $|\mathrm{PGL}_2(p)| = p(p^2-1)$ are coprime, and set $G = \mathrm{PGL}_2(p^r){:}\langle\phi\rangle$ and $\Omega = \phi^G$, where ϕ is a field automorphism of $\mathrm{PGL}_2(p^r)$ of order r. By [71, Corollary 3.7], the triple $(G, \mathrm{PGL}_2(p^r), \Omega)$ is *exceptional* and thus [71, Lemma 3.3] implies that every element in a coset $\mathrm{PGL}_2(p^r)\phi^i$ (with $1 \leqslant i < r$) has a unique fixed point on Ω. Therefore

$$\delta(G) \leqslant \frac{|\mathrm{PGL}_2(p^r)|}{|G|} = \frac{1}{r}$$

and thus $\delta(G)$ tends to 0 as r tends to infinity.

It is worth noting that Theorem 1.2.2 indicates that the proportion of derangements in simple primitive groups behaves rather differently to the proportion of derangements in more general primitive groups. Indeed, by a theorem of Boston *et al*. [12, Theorem 5.11], the set

$$\{\delta(G) \mid G \text{ is a finite primitive group}\}$$

is dense in the open interval $(0,1)$.

In a slightly different direction, if G is a transitive permutation group of degree $n \geqslant 2$, then $\Delta(G)$ is a normal subset of G and we can consider the number of conjugacy classes in $\Delta(G)$, which we denote by $\kappa(G)$. Of course, Jordan's theorem implies that $\kappa(G) \geqslant 1$. In [31], the finite primitive permutation groups with $\kappa(G) = 1$ are determined (it turns out that G is either sharply 2-transitive, or $(G,n) = (A_5, 6)$ or $(\mathrm{PSL}_2(8){:}3, 28)$), and this result is used to study the structure of finite groups with a nonlinear irreducible complex character that vanishes on a unique conjugacy class. We refer the reader to [31] for more details and further results.

An extension of the main theorem of [31] from primitive to transitive groups has recently been obtained by Guralnick [69]. He shows that every transitive group G with $\kappa(G) = 1$ is primitive, so no additional examples arise.

1.3 Derangements of prescribed order

In addition to counting the number of derangements in a finite permutation group, it is also natural to ask whether or not we can find derangements with special properties, such as a specific order.

1.3.1 Prime powers

The strongest result in this direction is the following theorem of Fein, Kantor and Schacher [52], which concerns the existence of derangements of prime power order.

Theorem 1.3.1 *Every nontrivial finite transitive permutation group contains a derangement of prime power order.*

This theorem was initially motivated by an important number-theoretic application, which provides another illustration of the utility of derangements in other areas of mathematics. Here we give a brief outline (see [52] and [87, Chapter III] for more details; also see [68] for further applications in this direction).

Let K be a field and let A be a central simple algebra (CSA) over K, so A is a simple finite-dimensional associative K-algebra with centre K. By the Artin–Wedderburn theorem, A is isomorphic to a matrix algebra $M_n(D)$ for some positive integer n and division algebra D. Under the *Brauer equivalence*, two CSAs A and A' over K are equivalent if $A \cong M_n(D)$ and $A' \cong M_m(D)$ for some n and m, and the set of equivalence classes forms an abelian group under tensor product. This is called the *Brauer group* of K, denoted $\mathscr{B}(K)$.

Let L/K be a field extension. The inclusion $K \subseteq L$ induces a group homomorphism $\mathscr{B}(K) \to \mathscr{B}(L)$, and the *relative Brauer group* $\mathscr{B}(L/K)$ is the kernel of this map. The connection to derangements arises from the remarkable observation that Theorem 1.3.1 is equivalent to the fact that $\mathscr{B}(L/K)$ is infinite for any nontrivial finite extension of global fields (where a *global field* is a finite extension of $\mathbb{Q}$, or a finite extension of $\mathbb{F}_q(t)$, the function field in one variable over a finite field $\mathbb{F}_q$).

In order to justify this equivalence, as explained in [52, Section 3], there is a reduction to the case where L/K is separable, and by a further reduction one can assume that $L = K(\alpha)$. Let E be a Galois closure of L/K, let Ω be the set of roots in E of the minimal polynomial of α over K, and let G be the Galois group $\mathrm{Gal}(E/K)$. Then G acts transitively on Ω, and [52, Corollary 3] states that $\mathscr{B}(L/K)$ is infinite if and only if G contains a derangement of prime power order. More precisely, if r is a prime divisor of $|\Omega|$ then the r-torsion subgroup of $\mathscr{B}(L/K)$ is infinite if and only if G contains a derangement of r-power order.

Although the existence of derangements in Theorem 1.1.2 is an easy corollary of the Orbit-Counting Lemma, the extension to prime powers in Theorem 1.3.1 appears to require the full force of the Classification of Finite Simple Groups.

The basic strategy is as follows. First observe that if $G \leqslant \mathrm{Sym}(\Omega)$ is an imprimitive permutation group and every $x \in G$ of prime power order fixes a point, then x must also fix the set that contains this point in an appropriate G-invariant partition of Ω. Hence the primitive group induced by G on a maximal G-invariant partition also has no derangements of prime power order, so the existence problem is reduced to the primitive case. We now consider a minimal counterexample G. If N is a nontrivial normal subgroup of G, then N acts transitively on Ω (by the primitivity of G), so the minimality of G implies that $N = G$ and thus G is simple. The proof now proceeds by working through the list of finite simple groups provided by the Classification. It would be very interesting to know if there exists a Classification-free proof of Theorem 1.3.1.

Remark 1.3.2 The finite primitive permutation groups with the property that *every* derangement has r-power order, for some fixed prime r, are investigated in [32]. The groups that arise are almost simple or affine, and the almost simple groups with this extremal property are determined in [32, Theorem 2].

1.3.2 Isbell's Conjecture

Let G be a finite transitive permutation group. Although Theorem 1.3.1 guarantees the existence in G of a derangement of prime power order, the proof does not provide any information about the primes involved. However, there are some interesting conjectures in this direction. For example, it is conjectured that if a particular prime power dominates the degree of G, then G contains a derangement that has order a power of that prime. This is known as *Isbell's Conjecture*.

Conjecture 1.3.3 *Let p be a prime. There is a function $f(p,b)$ with the property that if G is a transitive permutation group of degree $n = p^a b$ with $(p,b) = 1$ and $a \geqslant f(p,b)$, then G contains a derangement of p-power order.*

The special case $p = 2$ arises naturally in the study of n-player games, and the conjecture dates back to work of Isbell on this topic in the late 1950s [77, 78, 79]. The formulation of the conjecture stated above is due to Cameron, Frankl and Kantor [38, p. 150].

Following [78], let us briefly explain the connection to n-player games. A *fair game* (or *homogeneous game*) is a method for resolving binary questions without giving any individual player an advantage. If such a game has n players, then it can be modelled mathematically as a family $\mathscr{W}$ of subsets of a set X of size n, called *winning sets*, with the following four properties:

(a) If $A \subseteq B \subseteq X$ and $A \in \mathscr{W}$ then $B \in \mathscr{W}$.
(b) If $A \in \mathscr{W}$ then $X \setminus A \notin \mathscr{W}$.
(c) If $A \notin \mathscr{W}$ then $X \setminus A \in \mathscr{W}$.
(d) If $G \leqslant \mathrm{Sym}(X)$ is the setwise stabiliser of $\mathscr{W}$, then G is transitive on X.

For example, if n is odd then 'majority rules', where $\mathscr{W}$ is the set of all subsets of X of size at least $n/2$, is a fair game.

We claim that the existence of a fair game with n players is equivalent to the existence of a transitive permutation group of degree n with no derangements of 2-power order (see [77, Lemma 1]).

To see this, suppose that $\mathscr{W}$ is a fair game with n players and associated group G. Clearly, if n is odd then G has no derangements of 2-power order, so let us assume that n is even. A derangement in G of 2-power order would map some subset A of size $n/2$ to its complement, but this is ruled out by (b) and (c) above.

Conversely, suppose $G \leqslant \mathrm{Sym}(X)$ is a transitive permutation group of degree n with no derangements of 2-power order. As noted above, if n is odd then G preserves the fair game 'majority rules', so let us assume that n is even. Consider the action of G on the set of subsets of X of size $n/2$, and suppose that G contains an element g that maps such a subset to its complement. Then g is a derangement. Moreover, if the cycles of g have length $n_1, \ldots, n_k$, then g^m is a derangement of 2-power order, where $m = [n_1', \ldots, n_k']$ is the least common multiple of the n_i', and n_i' is the largest odd divisor of n_i. This is a contradiction. Therefore, the orbits of G on the set of subsets of size $n/2$ can be labelled

$$\mathscr{O}_1, \ldots, \mathscr{O}_\ell, \mathscr{O}_1^c, \ldots, \mathscr{O}_\ell^c$$

where $\mathscr{O}_i^c = \{X \setminus A \mid A \in \mathscr{O}_i\}$. Then

$$\mathscr{W} = \{A \subseteq X \mid B \subseteq A \text{ for some } B \in \mathscr{O}_i,\ 1 \leqslant i \leqslant \ell\}$$

is preserved by G and so it models a fair game with n players. This justifies the claim.

Isbell's Conjecture remains an open problem, although some progress has been made in special cases. For example, Bereczky [8] has shown that if $n = p^a b$, where p is an odd prime, $a \geqslant 1$ and $p+1 < b < \frac{3}{2}(p+1)$, then G contains