

**GROUP ACTIONS ON SETS
WITH APPLICATIONS TO FINITE GROUPS**

NOTES OF LECTURES GIVEN AT THE UNIVERSITY OF MYSORE

ON 29 JULY, 01 AUG, 02 AUG, 2012

K. N. RAGHAVAN

ABSTRACT. The notion of the action of a group on a set is a fundamental one, perhaps even more so than that of a group itself: groups derive their interest from their actions. We first define this notion and give some examples. The structure of an action can be understood by means of orbits and stabilisers. We introduce these and make some observations about them. While in themselves so elementary as to be self-evident, these observations nevertheless lead to interesting consequences when combined effectively in the right context.

After discussing Lagrange's theorem in the language of group actions, we come to the class equation, which is the main technical result in these notes. We apply the class equation to derive some standard basic results in the theory of finite groups: that the centre of a p -group is non-trivial, theorems of Cauchy and Sylow on the existence of subgroups of prime power orders, and those of Sylow about the number and conjugacy of subgroups named after him.

Up to date version of these notes is available from the author's home page at <http://www.imsc.res.in/~knr/>. Corrections and other suggestions for improvement are solicited and may please be emailed to knr@imsc.res.in.

Notation. Throughout these notes, G denotes a group and X, Y denote sets. We use symbols g, g_1, g', \dots to denote elements of G ; similarly x, x_1, x', \dots , to denote elements of X , and y, y_1, y', \dots to denote elements of Y .

The basic definitions. An *action* of G on X is a map $G \times X \rightarrow X$ denoted $(g, x) \mapsto gx$ such that $1x = x$ and $g(hx) = (gh)x$ for all x in X and g, h in G . Given an action of G on X , we call X a G -set. A G -map between G -sets X and Y is a map $f : X \rightarrow Y$ of sets that *respects the G -action*, meaning that, $f(gx) = gf(x)$ for all x in X and g in G .

To give an action of G on X is equivalent to giving a group homomorphism from G to the group of bijections of X .

Examples. Here are some examples:

- *Trivial action:* the prescription $gx = x$ for all g and x defines a G -action on X .
- *The defining action:* Most groups come with a natural action that helps define them. For example, the *symmetric group* \mathfrak{S}_X is defined as the set of bijections from X to itself, the multiplication being composition. By the very definition we have a map $\mathfrak{S}_X \times X \rightarrow X$, namely $(f, x) \mapsto f(x)$, that satisfies the axioms for an action.
- The group $GL_2(\mathbb{R})$ of invertible 2×2 matrices with real entries acts on the vector space of column matrices of size 2×1 with real entries: the action map is just the usual matrix multiplication. More generally, the group $GL_n(\mathbb{R})$ of invertible $n \times n$ matrices with real entries acts by usual matrix multiplication on the space of column matrices of size $n \times 1$ with real entries.
- The previous example is in fact properly thought of as a defining action. If V is a vector space of finite dimension n over the real numbers, then $GL(V)$ is defined as the group of vector space isomorphisms from V to itself (multiplication is composition). So there is a defining action of $GL(V)$ on V . By the choice of a basis for V , we may identify V with real column matrices of size $n \times 1$ and $GL(V)$ with invertible real matrices of size $n \times n$. The action of $GL(V)$ on V is then identified as the action by matrix multiplication of $GL_n(\mathbb{R})$ on real $n \times 1$ column matrices.
- *Left regular action:* G acts on itself: putting $X = G$, it is readily checked that the map $G \times G \rightarrow G$ defining the multiplication operation of G satisfies the action axioms.
- *Right regular action:* Again put $X = G$. Define $\rho : G \times G \rightarrow G$ by $\rho(g, x) := xg^{-1}$. We have $\rho(1, x) = x1^{-1} = x$ and $\rho(g, \rho(h, x)) = (\rho(h, x))g^{-1} = (xh^{-1})g^{-1} = x(h^{-1}g^{-1}) = x(hg)^{-1} = \rho(hg, x)$, so ρ defines an action.
- *Conjugation action:* Yet again put $X = G$. This time define $G \times G \rightarrow G$ by $(g, x) \mapsto {}^g x := gxg^{-1}$. It is easily checked that ${}^1 x = x$ and ${}^g ({}^h x) = ({}^{gh}) x$.
- *Action on left cosets:* Let H be a subgroup of G . The set G/H of left cosets is naturally a G -set: $G \times G/H \rightarrow G/H$ is given by $(g, xH) \mapsto gxH$.

New G -sets from old. From a given G -set X , we may cook up other related G -sets. In fact, any set obtained from X by a *natural* set operation is also *naturally* a G -set.¹ Here are some examples:

- the Cartesian square $X \times X$ with action being defined by $g(x, x') := (gx, gx')$; more generally, $X^n := X \times \dots \times X$ (n times) with G -action $g(x_1, \dots, x_n) := (gx_1, \dots, gx_n)$ becomes a G -set.
- the power set 2^X of X : for Y a subset of X , we let $gY := \{gy \mid y \in Y\}$.
- The set of all functions (say, complex valued) on X : if f is such a function and g an element of G , define gf by $(gf)(x) := f(g^{-1}x)$ for x in X .

¹Although the words “natural” and “naturally” in this sentence have precise mathematical meanings, the first time reader may want not to dwell too much upon them, preferring instead to take them in the sense of everyday language.

- if Y is a G -set too, the set X^Y of maps from Y to X is naturally also a G -set: given $f : Y \rightarrow X$ and $g \in G$, we define gf by $(gf)(y) := g(f(g^{-1}y))$.

Restricting the action. The following remarks may seem innocuous but can be used to good effect:

- if H is a subgroup of G , any G -set may be considered to be also a H -set by just *restricting* the action to H .
- a subset Y of a G -set X is *G -invariant* if $gy \in Y$ whenever $y \in Y$. A G -invariant subset is naturally itself a G -set.

G -invariant subset

Here are some examples of the use of the second item above:

- Consider the collection of all subsets of a given cardinality of a G -set X . Being a G -invariant subset of the power set of X , this itself is a G -set.
- Consider the action of $GL(V)$ on a vector space V discussed above. The subspace of linear functionals is a $GL(V)$ -invariant in the space of all complex valued functions on V , and so is a $GL(V)$ -set.
- Let V be a vector space of finite dimension n (over some field). For an integer r , $0 \leq r \leq n$, consider the collection denoted $\mathbb{G}(r, V)$ of all linear subspaces of dimension r of V . For example, $\mathbb{G}(0, V)$ is a singleton whose only element is $\{0\}$; and $\mathbb{G}(1, V)$ is the collection of all “lines through the origin” in V . Now, $\mathbb{G}(r, V)$ is a $GL(V)$ -invariant subset of the power set of V , and so in its own right a $GL(V)$ -set.

Notation. As already mentioned, G denotes a group throughout. In what follows, X denotes a G -set. Neither G nor X is assumed to be finite for now: finiteness assumptions will be explicitly mentioned wherever imposed.

Orbits and their structure, stabilizers. For x an element of X , the *orbit of x* or the *orbit through x* is the subset $Gx := \{gx \mid g \in G\}$ of X . We have:

- x is in the orbit through x ;
- if y is in the orbit through x , then x is in the orbit through y ;
- if y is in the orbit through x and z in the orbit through y , then z is in the orbit through x .

Thus, the relation on X defined by

$$y \sim x \text{ if } y \text{ is in the orbit through } x$$

is an equivalence relation. The equivalence classes are called *orbits*. Being equivalence classes, the orbits partition X into a union of pairwise disjoint subsets:

$$(1) \quad X = \coprod \text{orbits}$$

The orbits form a partition of the G -set X . \coprod stands for disjoint union.

Orbits are G -invariant subsets of X (in the sense defined above of G -invariance), and are therefore themselves G -sets: in fact, a subset of X is G -invariant precisely when it is a union of orbits. Equation (1) therefore has the following implication, at least philosophically if not also practically:

to understand the structure of any G -set, it is enough if we understand the structures of all possible G -orbits, for after all each G -set is pieced together from its orbits.

For x in X , define its *stabilizer* G_x by

$$G_x := \{g \in G \mid gx = x\}$$

stabilizer G_x

It is clearly a subgroup of G . Consider the space G/G_x of left cosets of G_x with its natural G -action $(g, g'G_x) \mapsto gg'G_x$. The G -set structure of the orbit Gx of x can be understood in terms of that of G/G_x . In fact, as is readily verified, we have a G -set isomorphism:

$$(2) \quad G/G_x \simeq Gx \text{ as } G\text{-sets via } gG_x \leftrightarrow gx$$

Structure of an orbit

The upshot is:

To understand the G -set structure on an arbitrary G -orbit, it is enough to understand the G -set structure of the left coset spaces G/H for all subgroups H of G .

Transitive actions and homogeneous spaces. The whole of X is a single G -orbit if and only if, given any two elements x and x' of X , there exists an element g of G such that $gx = x'$. In this case, the G -action is said to be *transitive*, and X is called a *homogeneous space* for G . In view of (2), every homogeneous space for G is of the form G/H for some subgroup H .

Lagrange's theorem. Let H be a subgroup of G . Consider G as an H -set with the left regular action: $(h, g) \mapsto hg$. The following facts are readily verified:

- the orbits for this action are precisely the right cosets of H ;
- each right coset has cardinality the same as that of H : if Hx is a right coset, $h \leftrightarrow hx$ defines a bijection between H and Hx .

By equation (1), G is a disjoint union of right cosets of H , so²

$$(3) \quad |G| = |H||H \backslash G| \quad \text{where } H \backslash G \text{ denotes the set of right cosets of } H$$

Considering instead of the left regular action the right one of H on G given by $(h, g) \mapsto gh^{-1}$, we conclude similarly that

$$(4) \quad |G| = |H||G/H|$$

By (2), any G -orbit is of the form G/H for some subgroup H , so in view of (4):

$$(5) \quad \text{the order of any } G\text{-orbit divides the order of the group } G$$

Lagrange's theorem

From (3) and (4) we also conclude:

$$(6) \quad \begin{array}{l} \text{the order of any subgroup } H \text{ divides the order of the group;} \\ \text{the number of left cosets of } H \text{ equals the number of its right cosets.} \end{array}$$

The class equation. Let us rewrite in a slightly modified form the right side of equation (1). Divide the orbits into two classes: singleton orbits and non-singleton orbits. Obviously, an element x forms an orbit by itself if and only if it is *fixed* by every element of G : $gx = x$ for all g in G . Let us denote by X^G the *fixed point set* of X , that is the collection of all fixed points:

fixed point set X^G

$$X^G := \{x \in X \mid gx = x \forall g \in G\}$$

With this notation, equation (1) can be written as:

$$(7) \quad X = X^G \coprod \text{non-singleton orbits}$$

By taking cardinalities of both sides of the equation,³ we get

$$(8) \quad |X| = |X^G| + \sum |\text{orbit}| \quad (\text{where the sum is over non-singleton orbits})$$

Centre of G
 $:= \{g \in G \mid gh = hg \forall h \in G\}$

Let us now apply the above considerations to the situation when $X = G$ acted upon by conjugation. The orbits are the conjugacy classes, and the fixed point set X^G is the centre of G . The last equation in this situation becomes

The class equation

$$(9) \quad |G| = |\text{centre}(G)| + \sum |\text{conjugacy class}| \quad (\text{sum is over non-singleton classes})$$

²Here and in the sequel, we will be considering relations between cardinalities of various sets. While cardinalities make sense even without finiteness assumptions, the reader may just want to assume the sets whose cardinalities are in consideration to be finite.

³As already mentioned, this operation makes sense even when X is not finite, but the reader may just want to think of the special case when X is finite.

Application to the structure of finite groups. Assume the group G to be finite. Suppose that for a prime p the following hypothesis is satisfied:⁴

$$(10) \quad \text{every proper subgroup of } G \text{ has index divisible by } p$$

Then, by (2), every non-singleton G -orbit has cardinality divisible by p . This applies in particular to every non-singleton conjugacy class in G . Reading equations (8) and (9) modulo p , we get:

$$(11) \quad |X| \equiv |X^G| \pmod{p} \quad |\text{centre}(G)| \equiv 0 \pmod{p}$$

Since $|\text{centre}(G)|$ is positive—the identity element of the group always belongs to the centre—we conclude that the centre is non-trivial.

When G is a p -group (that is, $|G|$ is a power of a prime p), the hypothesis (10) is satisfied (by (6)). From the previous paragraph we conclude:

$$(12) \quad \text{the centre of a } p\text{-group is non-trivial (that is, has cardinality more than 1)}$$

Groups of order p^2 are in fact abelian—see item (2) in the appended tutorial sheet. There do exist groups of order p^3 that are not abelian (irrespective of p)—see item (8) in the tutorial sheet.

On the existence or lack thereof of subgroups of given orders: theorems of Cauchy and Sylow. We continue to assume that G is finite. By Lagrange (6), the order of any subgroup H is a factor of the order of G . It is natural to ask whether, given a factor of $|G|$, there exists a subgroup of that order. This is false in general, as easy examples show: see item (9) in the tutorial sheet. However, we have the following:

$$(13) \quad \text{If } G \text{ is abelian and } d \text{ divides } |G|, \exists \text{ a subgroup of } G \text{ of order } d.$$

$$(14) \quad \text{If } q = p^e \text{ (} e \geq 0 \text{) is a prime power dividing } |G|, \exists \text{ a subgroup of } G \text{ of order } q.$$

In the proofs of these statements, we use the following observation:

If N is a normal subgroup of G , then the preimages in G of elements of G/N under the natural quotient map $G \rightarrow G/N$ are the (left/right) cosets of N ; so they form a partition of G into subsets each of cardinality $|N|$. In particular, the preimage in G of a subgroup K of G/N is a subgroup of cardinality $|N||K|$.

Let us first prove (13) in the case when d is a prime p . Proceed by induction on $|G|$: there being no prime dividing 1, we assume that $|G| > 1$. It is enough to find an element z in G whose order f is divisible by p , for then $z^{f/p}$ has order p . Choose $1 \neq x$ in G . If p divides the order of x , we are done. If not, consider G/X where X is the subgroup generated by x . By induction, there exists y in G/X of order p . Any pre-image z in G of y has order a multiple of p , and (13) is proved in the case when d is a prime.

For the proof of (13) in the general case, proceed by induction on d . The case $d = 1$ being obvious, assume $d \geq 2$, let p be a prime dividing d , and choose subgroup N of G of order p . By induction, there exists subgroup of order d/p of G/N . Its pre-image in G is a subgroup of order d , and we are done.

We now prove (14). Proceed by induction on $|G|$. The case $|G| = 1$ being obvious, assume $|G| > 1$. We are done by induction if there is a proper subgroup with index coprime to p . So we may assume that hypothesis (10) holds for G . By (11), we conclude that p divides the cardinality of the centre of G . Applying (13), choose subgroup N of order p of the centre of G . By induction, there exists a subgroup of G/N of order q/p . Its pre-image in G is a subgroup of order q , and we are done.

The case $e = 1$ of (14) is *Cauchy's theorem*; the case when q is the highest power of p dividing $|G|$ is *Sylow's theorem*.

⁴At the end of the day—see (14) below—it turns out that the only groups that satisfy this hypothesis are those of order a power of p . The hypothesis is thus merely a provisional one that enables the proofs.

Sylow p -subgroups: their conjugacy and number. Let G be finite and p a prime. Write $|G| = p^e m$ with m coprime to p . Thus p^e is the highest power of p dividing $|G|$, the case $e = 0$ not being excluded from consideration.

A subgroup of order p^e of $|G|$ is called a *Sylow p -subgroup* in honour of Sylow who proved not only their existence (14) but also:

(15) Any two Sylow p -subgroups are conjugate.

(16) The number of Sylow p -subgroups divides m and is congruent to 1 mod p .

We will prove a stronger result than (15), to state which, let P be an arbitrary Sylow p -subgroup and H an arbitrary p -subgroup.⁵ Then:

(17) H is contained in some conjugate of P .

In proving (17) and (16), we make use of the following observation:

(18) If H normalizes P , then $H \subseteq P$.

We first prove (18). Consider the subgroup PH of G . Being a quotient of $P \times H$, it is a p -group. On the other hand it contains P . Since p^e is the highest power of p that divides $|G|$, we conclude that $PH = P$, in other words that $H \subseteq P$, and (18) is proved.

To prove (17), consider the conjugation action of G on its set of subgroups. Since the cardinality of a subgroup doesn't change under the G -action, the Sylow p -subgroups form a G -invariant subset. The conjugates of P form a G -orbit, which let us denote X . The stabiliser of P being its normalizer $N(P)$, we have $X \simeq G/N(P)$ as G -sets by (2). Since $P \subseteq N(P)$, it follows that $|G/N(P)|$ divides m :

(19) $|X|$ divides m

In particular, $|X|$ is non-zero modulo p . Now consider X as an H -set and apply (11) to conclude that $|X^H|$ is non-zero, which means that there exists a conjugate of P , say P' , that is normalized by H . By (18), we have $H \subseteq P'$, and (17) is proved (and so in particular is (15)).

To prove (16), let us look back at the above proof of (17) in the light of (15). We see that X must be the set of all Sylow p -subgroups. So the first half of (16) follows from (19). To proof the second half, consider X as a P -set and apply (11). By (18), the only Sylow- p subgroup that P normalizes is itself, so $X^P = \{P\}$, and we are done.

⁵A p -subgroup is a subgroup which is a p -group, in other words, a subgroup whose order is a power of p .

TUTORIAL SHEET: GROUP ACTIONS ON SETS

- (1) Let G be a group, X a G -set, and x, y be two elements of X .

If x and y belong to the same orbit of G , then their stabilizers G_x and G_y are conjugate: in fact, writing $y = gx$ for g in G , we have $G_y = G_{gx} = {}^gG_x$.

On the other hand, if the stabilizers G_x and G_y are conjugate, say ${}^gG_x = G_y$, then the orbits Gx and Gy are isomorphic as G -sets: in fact, $hgx \mapsto hy$ gives an isomorphism.

Notation: For $g \in G$ and H a subgroup of G , ${}^gH := gHg^{-1}$, the conjugate of H by g .

- (2) Let H be a subgroup of a group G . We may consider the group $H \times H$ acting on G as follows: $(h, k) \cdot g := h g k^{-1}$. Let $H \backslash G / H$ denote the set of orbits for this action. (These orbits are called the *double cosets*: each is of the form HgH for some $g \in G$.)

Let G/H denote, as usual, the set of left cosets of H . There is a natural action of G on G/H : $g \cdot xH := gxH$. Consider the induced action of G on the Cartesian product $G/H \times G/H$.

The G -orbits of $G/H \times G/H$ are in bijection with $H \backslash G / H$: $(xH, yH) \leftrightarrow Hxy^{-1}H$.

- (3) An action of G on X is said to be *faithful* if $gx = x$ for all x implies $g = 1$; equivalently if the map from G to the group of bijections of X is an injection. It is said to be *simply transitive* if it is both transitive and faithful.

The action of G on itself by left multiplication is faithful. If G acts simply transitively on X , then $X \simeq G$ as G -sets non-canonically (where G is a G -set by the left regular action).

The first assertion in item (3) is called *Cayley's theorem*.

- (4) Let G be a finite group and X a finite G -set. Prove the following result of Burnside:

$$\# \text{ of } G\text{-orbits in } X = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

where $X^g := \{x \in X \mid gx = x\}$.

- (5) (from Artin's Algebra p. 196, problem 8) Considering colourings of the vertices of the regular octagon by two colours, say red and blue. Consider two colourings to be equivalent if one is obtained by the other by either a rotation by an integer multiple of the angle $\pi/4$ or by reflection in an axis of symmetry (a line passing through two opposite vertices, or the mid-points of two opposite edges). Use Burnside's result above to determine the number of non-equivalent colourings.
- (6) Let p be a prime and G a p -group. Determine all non-negative integers n such that there is a set of cardinality n on which G acts transitively.
- (7) Let N be a central subgroup of a group G (this means that N is a subgroup contained in the centre). Then N is clearly normal. Suppose that G/N is cyclic. Show that G is abelian.

Combine (12) with this argument to conclude that groups of order p^2 are abelian (where p is a prime).

- (8) Let p be a prime, $q = p^e$ a power of p with $e \geq 1$, and \mathbb{F}_q the finite field with q elements. Let $GL_n(\mathbb{F}_q)$ denote the group of invertible $n \times n$ matrices with entries in \mathbb{F}_q .
- $GL_n(\mathbb{F}_q)$ has order $(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-2})(q^n - q^{n-1})$. In particular, the cardinality of a Sylow- p subgroup of $GL_n(\mathbb{F}_q)$ is $q^{n(n-1)/2}$.
 - Consider the subgroup $U_n(\mathbb{F}_q)$ consisting of those elements of $GL_n(\mathbb{F}_q)$ that are upper triangular and all of whose diagonal entries are equal to 1. The cardinality of $U_n(\mathbb{F}_q)$ is clearly $q^{n(n-1)/2}$, so that it is a Sylow- p subgroup of $GL_n(\mathbb{F}_q)$.
 - $U_3(\mathbb{F}_p)$ has order p^3 and is not abelian.
- (9) The alternating group A_4 of even permutations of 4 letters has no subgroup of order 6.
- (10) Let G be a finite group, p a prime, and P a Sylow p -subgroup of G . It follows from (15) that P is normal if and only if it is the only Sylow p -subgroup. In

particular, P is the unique Sylow p -subgroup of its normalizer $N(P)$ in G . Show that the normalizer of $N(P)$ in G equals $N(P)$.

- (11) With notation as in item 8, let $B_n(\mathbb{F}_q)$ be the subgroup of $GL_n(\mathbb{F}_q)$ consisting of upper triangular matrices. Show that $B_n(\mathbb{F}_q)$ is the normalizer in $GL_n(\mathbb{F}_q)$ of $U_n(\mathbb{F}_q)$. Deduce from exercise (10) that $B_n(\mathbb{F}_q)$ is its own normalizer.
- (12) Find the orbits and stabilizers for the action of $GL_n(\mathbb{R})$ on $n \times 1$ real column matrices.
- (13) Let V be the real vector space of all real $n \times 1$ column matrices. Let \mathfrak{B} denote the collection of those subsets of cardinality n of V that form a basis for V . The induced action of $GL_n(\mathbb{R})$ on the power set of V leaves \mathfrak{B} invariant. Determine the orbits and stabilizers for the action of $GL_n(\mathbb{R})$ on \mathfrak{B} .
- (14) Let \mathfrak{S}_n be the symmetric group on n letters. Elements of \mathfrak{S}_n are called *permutations*. Every permutation is a product of disjoint cycles. The cardinalities of the cycles in such a decomposition (counted with multiplicity and including the singleton cycles) determines a partition of n , called the *cycle type* of the permutation. Two permutations are conjugate if and only if they have the same cycle type, and every partition arises as a cycle type. Thus conjugacy classes of permutations are in bijection with partitions. For $\lambda = 1^{m_1} 2^{m_2} \dots$ a partition, the centralizer of an element with cycle type λ has cardinality $1^{m_1} m_1! \cdot 2^{m_2} m_2! \cdot \dots$.
- (15) Let X be a finite set, say $[n] := \{1, 2, \dots, n\}$. Then the group $G = \mathfrak{S}_X = \mathfrak{S}_n$ of bijections of X acts on X (naturally of course). Consider the induced action of G in turn on each of the following. Determine in each case the orbits, stabilisers, and their cardinalities.
 - (a) the power set of X .
 - (b) Cartesian square $X \times X$.
 - (c) complex valued functions on X .
 - (d) higher Cartesian powers X^3, X^4 , etc.
 - (e) functions from X to X .

Warning: Answers to (d), (e) are a bit involved.