AFS AT MEPCO DEC 2022

CHAPTER 6 OF ARTIN'S ALGEBRA: "MORE GROUP THEORY"

NOTES AND TUTORIAL SHEET 1

Abstract. Group actions: G-sets and G-maps; symmetries and defining actions; actions of a group on itself: the left regular action and the conjugation action, Cayley's theorem; action on cosets; orbits and stablisers; structure of a transitive action and the counting formula; the class equation and its application to p-groups.

Throughout, let G denote a group (not necessarily finite) and X, Y, ... sets (not necessarily finite).

(1) We say that X is a G-set or that G acts on X if there exists a map $G \times X \to X$ given by $(g, x) \mapsto gx$ satisfying the following axioms[1]:
(a) $g(hx) = (gh)x$ and (b) $1x = x$, for all g, h in G and all x in X.
A map $f : X \to Y$ between G-sets is called a G-map if $f(gx) = gf(x)$ (for all g in G and all x in X).

(2) Groups arise naturally in mathematics as symmetries of objects. The mathematical objects with which we are familiar are sets with some additional structure. Consider, for instance, the following hierarchy of three examples: a set, a vector space, and an inner product space. A symmetry of an object is a self-map, a bijection of the underlying set that preserves all the structures. Being a bijection, the inverse of a symmetry is defined, and it too should preserve all the structures (if this isn't clear, we demand it). A composition of two symmetries is also a symmetry. Thus the symmetries of any object form a group called the symmetry group. For instance:
  (a) The symmetry group of a set X is just the group $\mathfrak{S}_X$ of bijections from X to X. It is called the "symmetric group". If X a finite set with n elements, say $[n] := \{1, \ldots, n\}$, this is just the familiar "symmetric group" $\mathfrak{S}_n$ on the n symbols $1, \ldots, n$.
  (b) The symmetry group of a vector space V is $GL(V)$, the group of invertible linear transformations from V to V. It is called the "general linear group".
  (c) The symmetry group of an inner product space W is the "orthogonal group" $O(W)$ of invertible linear transformations that preserve the inner product $\langle u, v\rangle$: $O(W) := \{g \in GL(W) \mid \langle gu, gv\rangle = \langle u, v\rangle\}$.

Given an object, it may be useful to strip it of some of its structures and consider only what is left. For example, an inner product space W may be considered as just a vector space or even just a set. In such a forgetful situation,

[1]The notation gx for the result of the action of g on x is natural and suggestive. There are certain contexts, however, in which it could cause confusion, and in such situations some such alternative notation as $g \cdot x$ or ${}^g x$ is used. For an instance of such usage, consider the conjugation action of a group on itself (one of the items below).

there are natural inclusions of the symmetry groups: $O(W) \subseteq GL(V) \subseteq \mathfrak{S}_V$. Similarly, for a vector space V, we have $GL(V) \subseteq \mathfrak{S}_V$.

(3) The symmetry group of an object naturally acts on the object. Such an action is called the defining action, because it helps to define the group itself.

(4) If G acts on X, one can use this to define a group homomorphism from G to the symmetric group $\mathfrak{S}_X$. Conversely, given such a homomorphism, there is a corresponding action of G on X. The action is called faithful if the homomorphism $G \to \mathfrak{S}_X$ is injective, or, equivalently, the kernel of the homomorphism is the trivial subgroup $\{1\}$ of G.

(5) A group acts on itself in multiple ways. Here are two ways that we will immediately consider:
   (a) This action is variously called left action, left regular action, left regular action: the result gx of g acting on x is the product gx in the group.
   (b) The conjugation action: ${}^g x = gxg^{-1}$. (Here we have used ${}^g x$ to denote the result of g acting on x, for it would be confusing to use gx for that purpose in this context.)
   (c) CAYLEY'S THEOREM: For any group G, the left regular action of G on itself being faithful (check this), we get an injection of G into $\mathfrak{S}_G$.

(6) Let H be a subgroup of G and G/H the set of (left) cosets of H. We have a natural action of G on G/H, with $g(xH) := gxH$.

(7) Let X be a G-set.
   (a) Given elements x and y of X, we say that y is the orbit of X (or G-orbit of x in case we want to emphasise the action of G) and write $x \sim y$, if there exists g in G such that $gx = y$. The relation $x \sim y$ is symmetric, reflexive, and transitive. In other words, it is an equivalence relation on X. The equivalence classes are called orbits. We suggestively use Gx to denote the orbit of x.
   (b) The orbits being equivalence classes (for an equivalence relation), they form a partition of X. In other words, X is the disjoint union of its orbits.
   (c) A subset Y of X is said to be G-stable if $gy \in Y$ for all $g \in G$ and $y \in Y$. A subset Y is G-stable if and only if it is a union of orbits. Given a G-stable set Y, we can consider Y itself as a G-set. To analyse the G-action on X, we could consider the partition of X into orbits, and analyse each orbit separately. This motivates the next definition.
   (d) The action of G on X is said to be transitive if the whole of X is a single orbit, or, equivalently, given any two elements x and y of X, there exists an element g in the group such that $gx = y$. The action of G on the set G/H of cosets of a subgroup H is transitive. This is significant, since, as we will presently show, every transitive action is isomorphic to an action on cosets.

(e) For an element x in X, the stabiliser of x (also called the isotropy at x), denoted G_x, is defined by $G_x := \{g \in G \mid gx = x\}$.
   (i) G_x is a subgroup of G.
   (ii) We have an isomorphism of G-sets: $G/G_x \simeq Gx$ given by $gG_x \mapsto gx$. In particular, we have, when G is finite, the following counting formula: $|G| = |G_x| \cdot |Gx|$.

(8) By the counting formula, the cardinality of any orbit under the action a finite group G divides the order of G. In particular, the cardinality of any conjugacy class of G divides the order of G.

(9) Analyse the orbits and stabilisers for the actions that have been introduced up to now (and all those that will be introduced from now on). For the conjugacy action of G on itself, for example, the orbits are the conjugacy classes, and the stabiliser of an element is its centraliser. Thus, by the counting formula, for an element x in a finite group G, we have

$$|G| = |\text{conjugacy class of } x| \cdot |\text{centraliser of } x|$$

(10) Let H be a subgroup of a group G. For g an element of G, let ${}^gH$ denote the conjugate gHg^{-1} of the subgroup H.
- The G-sets G/H and $G/{}^gH$ with their natural G-actions are isomorphic as G-sets. (The map $xH \mapsto xHg^{-1} = xg^{-1}\,{}^gH$ defines an isomorphism).
- Conversely, if, for a subgroup H' of G, the G-sets G/H and G/H' are isomorphic (as G-sets) then $H' = {}^gH$ for some $g \in G$.

(11) In this item we discuss various versions of the class equation of a finite group G. Consider the conjugation action of a such a group on itself. The orbits in this case are the conjugacy classes. Let $C_1, \ldots, C_k$ be all the conjugacy classes, listed in some order. Since these form a partition of G, we have:

$$|G| = |C_1| + \cdots + |C_k| \tag{1}$$

Every summand on the right side is a divisor of $|G|$ (as observed above).

The identity element forms a (conjugacy) class by itself. More generally, any element in the centre of G forms a class by itself. In fact, the converse is also true: if an element forms a class by itself, then it belongs to the centre. We may therefore write:

$$|G| = |\text{centre of } G| + \sum_{|C|>1} |C| \tag{2}$$

where the sum on the right side is taken over all non-singleton conjugacy classes. Every summand on the right side is a divisor of $|G|$; we emphasise that each of the summands $|C|$ in Eq. (2) is a divisor of G bigger than 1.

(12) A finite group G is called a p-group (where p is understood tacitly to denote a prime number) if its order is a power of p. Use the class equation to show that any p-group (that is not itself trivial) has non-trivial centre. (Hint: Consider

Eq. (2) for a p-group G with $|G| > 1$. In this case, $|G| \equiv 0 \bmod p$ and $|C| \equiv 0 \bmod p$ for each C in Eq. (2), so $|\text{centre of } G| \equiv 0 \bmod p$. In particular, $|\text{centre of } G| > 1$.)

(13) (FIXED POINT THEOREM FOR p-GROUP ACTIONS) Suppose that a p-group G acts on a finite set X. Show that $|X| \equiv |X^G| \bmod p$, where $X^G := \{x \in X \mid gx = x \text{ for all } g \in G\}$. In particular, if $|X| \not\equiv 0 \bmod p$, then X^G is non-empty.

(14) Let p be a prime number. Any group of order p^2 is abelian. There are exactly two groups of order p^2 up to isomormphism: namely, the cyclic group and $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$.

(15) Give a proof of Lagrange's theorem using the language of group actions.

(16) Let G denote the cyclic group of order m. For n a positive integer let $q(n)$ be the number of G-isomorphism classes of G-sets of cardinality n. Set $q(0) = 1$ (by definition). Show that the generating function $Q(t) := \sum_{n \geqslant 0} q(n) t^n$ equals

$$Q(t) = \frac{1}{\prod_{d \mid m} (1 - t^d)}$$

A few afterthoughts

Let G be a group and X a G-set.

(1) For two elements of X belonging to the same orbit, the stabiliser subgroups at these points are conjugate: in fact, ${}^{g}(G_x) = G_{gx}$.

(2) Let $\mathbb{F}$ be a finite field with q elements. Let V be a vector space of finite dimension n over $\mathbb{F}$. Let k be an integer $0 \leqslant k \leqslant n$. What is the number of k-dimensional subspaces in V? (Hint: It may help to try this for $k = 1$ and $k = 2$ first.)