Review: Basic Terminology and Results

Also: Group Actions

(Handout January 12, 2009)

A *multiplicative group* is a set G on which multiplication is defined (and closed, so that $xy \in G$ for all $x, y \in G$) such that

(i) For all $x, y, z \in G$, we have $(xy)z = x(yz)$.

(ii) There exists $1 \in G$ such that for all $x \in G$, we have $x1 = x = x1$.

(iii) For all $x \in G$, there exists $x^{-1} \in G$ such that $xx^{-1} = x^{-1}x = 1$.

The operation we have denoted by *juxtaposition* (i.e. simply writing the elements x and y next to each other, as in 'xy'). In other examples of groups, juxtaposition may be replaced by a symbol such as '$*$', '$\circ$', '$+$', etc. for the binary operation. (A *binary operation* on G is a map $G \times G \to G$, i.e. taking every ordered pair of elements of G to an element of G; thus closure is implicitly required.) Thus a *group* is a set G with a binary operation which is associative, for which G has an identity element, and every element of G has an inverse in G. All groups are taken to be multiplicative unless otherwise specified.

A group G is *abelian* if $xy = yx$ for all $x, y \in G$. The *order* of G is its cardinality $|G|$, whether finite or infinite. The *order* of an element $x \in G$ is the smallest integer $k \geqslant 1$ such that $x^k = 1$; or if no such integer k exists, the order of x is *infinite* and we write $|x| = \infty$. A *subgroup* of G is a subset $H \subseteq G$ which is a group, if the binary operation of G is restricted to H; in this case we write $H \leqslant G$. We know that a nonempty subset of G is a subgroup iff it is closed under taking products and inverses. Note that the intersection of two subgroups of G, or any collection of subgroups of G, is again a subgroup of G. The *trivial subgroup* $\{1\} \leq G$ is usually denoted simply as $1 = \{1\}$.

Given a subset $S \subseteq G$, we denote by $\langle S \rangle$ (`$\langle S\rangle$` in TEX) the unique smallest subgroup of G containing S; this consists of 1 together with all elements of S, inverses of elements of S, and their various products of arbitrarily many factors. We call $\langle S \rangle$ the *subgroup generated by* S. In particular if $\langle S \rangle = G$, we say that G is *generated by* S. A *cyclic group* is a group generated by a single element; thus a cyclic group is either

(i) a finite cyclic group of order n, i.e. $\{1, x, x^2, x^3, \ldots, x^{n-1}\}$ where $x^n = 1$, or

(ii) an infinite cyclic group $\{\ldots, x^{-2}, x^{-1}, 1, x, x^2, x^3, \ldots\}$.

In both cases, note that $|\langle x\rangle| = |x|$, so the two meanings of 'order' are compatible: the order of an element is the order of the subgroup that it generates.

The *centralizer* of an element $g \in G$ is the subgroup $C_G(g) = \{x \in G : xg = gx\}$. More generally if $S \subseteq G$ is any subset, the *centralizer* of S in G is the subgroup

$$C_G(S) = \{x \in G : xs = sx \text{ for all } s \in S\}.$$

A *right coset* of a subgroup $H \leqslant G$ is a subset of the form $Hx = \{hx : h \in H\}$ for some $x \in G$. All the right cosets of H have cardinality $|H|$, and they partition the set G. This proves *Lagrange's Theorem:*

$$|G| = [G : H]|H|$$

where $[G : H]$ denotes the *index* of H in G, i.e. the number of right cosets of H in G. In particular if G is finite, then every subgroup of G has order dividing $|G|$. One could just as well use left cosets $xH = \{xh : h \in H\}$ in place of right cosets, giving another partition of G.

A subgroup $K \leqslant G$ is *normal* (denoted $K \trianglelefteq G$) if the left and right cosets of K coincide: $xK = Kx$ for all $x \in G$. In this case $(Kx)(Ky) = Kxy$ for all $x, y \in G$, and it is not hard to see that the set of cosets $G/K = \{Kx : x \in G\}$ is a group, called the *quotient group* of G by K. If $H \leqslant G$ and $K \trianglelefteq G$ then $HK \leqslant G$ (here $HK = \{hk : h \in H,\ k \in K\}$). If $H, K \trianglelefteq G$ then $HK \trianglelefteq G$.

If $xH = Hx$, we say that x *normalizes* H. The *normalizer* of H in G is the set of elements of G which normalize H, i.e. $N_G(H) = \{x \in G : xH = Hx\}$. Note that $H \trianglelefteq N_G(H) \leqslant G$, and we have the equality $N_G(H) = G$ iff $H \trianglelefteq G$.

The *centre* of G is the subgroup $Z(G) = \{z \in G : zg = gz \text{ for all } g \in G\}$. Clearly $Z(G) \trianglelefteq G$, and equality holds iff G is abelian.

If G and H are groups, a *homomorphism* from G to H is a map $\theta : G \to H$ such that $\theta(xy) = \theta(x)\theta(y)$ for all $x, y \in G$. In this case the image is a subgroup $\theta(G) \leqslant H$, and the *kernel* is a normal subgroup $\ker(\theta) = \{g \in G : \theta(g) = 1\} \trianglelefteq G$. In fact, every normal subgroup is the kernel of some homomorphism; so a normal subgroup is the same thing as the kernel of a homomorphism. Indeed, if $K \trianglelefteq G$ then K is the kernel of the *canonical homomorphism* $G \to G/K$, $x \mapsto Kx$.

A group G is *simple* if its only normal subgroups are the trivial subgroup 1, and G itself. A Herculean effort by dozens of mathematicians has led to the classification of finite simple groups (CFSG). The proof of this result, the longest written proof in the history of mathematics, occupies tens of thousands of pages. The list of finite simple groups includes several infinite families, and 26 sporadic groups, the largest of which (the Monster) has order 808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000.

A homomorphism $\theta : G \to H$ is one-to-one iff its kernel is the trivial subgroup 1. A homomorphism θ is called an *isomorphism* if it is bijective. If there exists an isomorphism $\theta : G \to H$ then we say G is isomorphic to H, and we write $G \cong H$. This relation between groups (of isomorphism) is an equivalence relation. Isomorphism preserves all the intrinsic properties of a group (such as whether a group is abelian, the number of elements of a given order, etc.)

We have the *First Isomorphism Theorem:* If $\theta : G \to H$ is any group homomorphism, then

$$G/\ker(\theta) \cong \theta(G).$$

The *Second Isomorphism Theorem* asserts that if $H \leqslant G$ and $K \trianglelefteq G$, then

$$H/(H \cap K) \cong HK/K.$$

(Note that $H \cap K \trianglelefteq H$; also HK is a subgroup of G containing K, so that $K \trianglelefteq HK$.)

The *Third Isomorphism Theorem* asserts that if $K \trianglelefteq G$ and L is another normal subgroup of G contained in K (so that in particular $L \trianglelefteq K$), then

$$(G/L)\Big/(K/L) \cong G/K\,.$$

(Note that $K/L \trianglelefteq G/L$.)

An *automorphism* of G is an isomorphism from G to itself. The automorphisms of G form a group under composition, denoted $\operatorname{Aut} G$. Given $g \in G$, define $\psi_g : G \to G$ by $\psi_g(x) = gxg^{-1}$. Then ψ_g is bijective (its inverse is $\psi_{g^{-1}}$) and

$$\psi_g(xy) = (gxg^{-1})(gyg^{-1}) = g(xy)g^{-1}$$

so ψ_g is an automorphism. (Note that ψ_g is the identity map on G, iff $g \in Z(G)$.) Automorphisms of the form ψ_g are called *inner*; automorphisms not of this form are called *outer*. It is easily checked that $\psi_g \circ \psi_h = \psi_{gh}$ and $(\psi_g)^{-1} = \psi_{g^{-1}}$; thus the inner automorphisms of G form a subgroup $\operatorname{Inn} G \leqslant \operatorname{Aut} G$. In fact this is a normal subgroup: $\operatorname{Inn} G \trianglelefteq \operatorname{Aut} G$.

The *commutator* of two elements $x, y \in G$ is the element $[x, y] = x^{-1}y^{-1}xy \in G$. Note that $[x, y] = 1$ iff x and y commute. For two subgroups H and K, we denote

$$[H, K] = \big\langle [h, k] \,:\, h \in H,\ k \in K \big\rangle.$$

The *derived subgroup of* G is the normal subgroup $G' = [G, G] \trianglelefteq G$. The quotient G/G' is abelian, and is called the *abelianization of* G. In fact, G' is the unique smallest normal subgroup whose quotient is abelian.

The *external direct product* of two groups H and K is the group

$$H \times K = \{(h, k) : h \in H,\ k \in K\}$$

with componentwise multiplication. Here we may identify H and K with $H \times \{1\}$ and $\{1\} \times K$ respectively, so we have a group $H \times K$ having two normal subgroups with trivial intersection, but whose product is the entire group $H \times K$. Likewise if G is any group having normal subgroups H and K such that $H \cap K = \{1\}$ and $HK = G$, then we say G is the *internal direct product* of H and K, and we write $G = H \times K$. The distinction between internal and external direct products is merely a matter of viewpoint; hence we have essentially one notion of a *direct product* of groups.

Every abelian group is a direct product of cyclic groups.

Let p be prime. A *p-group* is a group of order p^k for some $k \geqslant 1$. An *elementary abelian p-group* is a direct product of cyclic groups of order p, where p is prime. A *p-subgroup* of a finite group G is a subgroup $H \leqslant G$ such that H is a p-group. A *Sylow p-subgroup of G* is a p-subgroup $H \leqslant G$ whose index $[G : H]$ is not divisible by p.

A subgroup $H \leqslant G$ is *characteristic* (denoted $H \blacktriangleleft G$) if $\theta(H) = H$ for every $\theta \in \operatorname{Aut} G$. Every characteristic subgroup is normal, but not conversely. We say G is *characteristically simple* if its only characteristic subgroups are the trivial subgroup 1 and G itself. Every such group is a direct product of isomorphic simple groups.

Group Actions

If X is any set, the set of permutations of X (i.e. bijections $X \to X$) forms a group under composition. This group, denoted $\operatorname{Sym} X$, is the *symmetric group on X*. When X is a finite set, we often take $X = \{1, 2, 3, \ldots, n\}$, in which case $\operatorname{Sym} X$ is denoted S_n, the *symmetric group of degree n*. A *permutation group* is a subgroup $G \leqslant \operatorname{Sym} X$ for some X; in this case the *degree* of the permutation group is the cardinality $|X|$. Given $g \in G$ and $x \in X$, we write $g : x \mapsto x^g$. (Some authors write instead $x \mapsto g(x)$. Below we explain the differences between these two notational conventions.) The *orbit* of a point $x \in G$ is the subset

$$x^G = \{x^g : g \in G\} \subseteq X.$$

The orbits of G on X form a partition of X. If there is only one orbit (i.e. X itself), we say G is *transitive*. The *stabilizer* of a point $x \in X$ is the subgroup

$$G_x = \{g \in G : x^g = x\} \leqslant G.$$

The size of an orbit is the index of the corresponding stabilizer:

$$|x^G| = [G : G_x].$$

More generally, let X be any set, and let G be a group. We say that G *acts on* X if there is a rule that assigns to every $g \in G$ a permutation of X (denoted $x \mapsto x^g$ as above) in such a way that $(x^g)^h = x^{gh}$ for all $x \in X$ and $g, h \in G$. The reason this is slightly more general than the situation described above, is that we sometimes allow distinct elements of G to give the same permutation of X. More precisely, an *action* (or *representation* of G on X is a homomorphism $\theta : G \to \operatorname{Sym} X$. Here each $g \in G$ gives a permutation $\theta(g) : X \to X$, $x \mapsto x^{\theta(g)}$. (We write simply x^g in place of $x^{\theta(g)}$ if the choice of action θ is clear from context.) If θ is one-to-one, we say the action θ is *faithful*; in this case we may identify G with the permutation group $\theta(G) \leqslant \operatorname{Sym} X$ and we are back in the situation described above. But in general we define orbits and stabilizers for any group action, just as we do for permutation groups.

Example: Fractional Linear Transformations

Let $X = \mathbb{C} \cup \{\infty\}$, the one-point compactification of the complex numbers. (We refer to X as the *Riemann sphere,* or as the *complex projective line.*) Let $G = GL_2(\mathbb{C})$, the group of all invertible 2×2 complex matrices. Consider the action of G on X by fractional linear transformations: the matrix $g = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ maps

$$z \mapsto z^g = \begin{cases} \frac{az+c}{bz+d}\,, & \text{if } z \in \mathbb{C} \text{ and } bz + d \neq 0; \\ \infty, & \text{if } z \in \mathbb{C} \text{ and } bz + d = 0; \\ \frac{a}{b}\,, & \text{if } z = \infty. \end{cases}$$

(The exceptional values of the fractional linear transformation $X \to X$ are chosen so as to ensure continuity with respect to the topology of X, which is that of the Riemann sphere. Here an open neighbourhood of $\infty \in X$ is simply the complement,in X, of a closed bounded subset of $\mathbb{C}$.) This action is transitive, i.e. every point of X can be mapped to every other point by some fractional linear transformation. The stabilizer of ∞ is the subgroup consisting of lower-triangular matrices $\left[\begin{smallmatrix} a & 0 \\ c & d \end{smallmatrix}\right]$ with $ad \neq 0$; the stabilizer of 0 is the subgroup consisting of upper-triangular matrices $\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right]$ with $ad \neq 0$. The action is not faithful since if λ is any nonzero complex number, then the matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{bmatrix}$$

give the same fractional linear transformation. In fact, the kernel of the action of G on X (the set of all matrices fixing every point of X) is just the set of scalar matrices $\lambda I = \left[\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right]$ for $\lambda \neq 0$. These matrices comprise the centre $Z(G)$, and so $G/Z(G) = PGL_2(\mathbb{C})$ is the group of permutations induced by G.

Example: The Regular Action

Let G be any group. Then G acts on G itself by left-multiplication: the element $g \in G$ gives the map $\lambda_g : G \to G$, $x \mapsto gx$. Note that λ_g is bijective (its inverse is $\lambda_{g^{-1}}$) and that $\lambda_g \circ \lambda_h = \lambda_{gh}$, so we do indeed have an action of G on G. This action is transitive, and the stabilizer of any point $x \in G$ is the trivial subgroup $\{1\}$, so the action is faithful. We may therefore regard G as a permutation group on G. This gives *Cayley's Representation Theorem*: every group is isomorphic to a permutation group. And for a finite group G, we see that G is isomorphic to a permutation group of degree $n = |G|$; hence G is isomorphic to a subgroup of S_n.

The action $g \mapsto \lambda_g$ is called the *left-regular action of G on G*. We may similarly define the right-regular action of G on G, if we are careful to distinguish between left and right actions (see comments below).

Example: Conjugation

Let a group G act on G itself by conjugation. Thus each $g \in G$ gives the permutation $\psi_g : G \to G$, $x \mapsto gxg^{-1}$. The orbits of this action are simply the *conjugacy classes* of G. The stabilizer of $x \in G$ is simply its centralizer $C_G(x)$. From the formula for the orbit size, we have

$$|x^G| = [G : C_G(x)].$$

Thus every conjugacy class has size dividing the group order (it is in fact the index of the corresponding centralizer). The kernel of the action of G on itself by conjugation is $Z(G)$. In particular the action is faithful iff G has trivial centre.

Left and Right Actions

Let G be a group, and X a set. A *left action* of G on X is a map $G \times X \to X$, $(g, x) \mapsto gx$ such that

$$g(h(x)) = (gh)(x)$$

for all $g, h \in G$ and $x \in X$. (We may write $g(x)$ in place of gx.) A *right action* of G on X is a map $X \times G \to X$, $(x, g) \mapsto xg$ such that

$$(xg)h = x(gh)$$

for all $g, h \in G$; $x \in X$. It is natural in this case to write x^g in place of xg. The essential notational difference here is that for left actions, function composition is performed right-to-left; for right actions, function composition is performed left-to-right. Expressed in this way, the distinction between left and right actions seems a rather minor notational issue.

Left actions are typically preferred in undergraduate courses, where the experience with function notation that most students acquire comes from pre-calculus and calculus courses. At the more advanced levels, left actions are generally favored by analysts; and right actions are generally favored by algebraists. However one often wants to consider both left and right actions in the same context, and then we cannot really learning about the subtle distinction. Moreover because different authors have different personal preferences, it is best for us to confront this issue head-on.

As a first example, let us denote by $F^{1\times n}$ the space of row vectors of length n over a field F; and by $F^{n\times 1}$, the space of column vectors of length n. The group $GL_n(F)$ consisting of invertible $n \times n$ matrices over F, acts naturally on $F^{1\times n}$ on the right; it also acts on $F^{n\times 1}$ on the left.

For another example, any group G naturally acts on itself by both left and right multiplication. We have defined the left regular representation of G on itself as the permutation action where $g \in G$ acts on G by way of the permutation $\lambda_g : G \to G$, $x \mapsto gx$. The associative property for G then yields

$$\lambda_g(\lambda_h(x)) = g(hx) = (gh)x = \lambda_{gh}(x)$$

so that $\lambda_{gh} = \lambda_g \circ \lambda_h$ as expected. We try to do the same for right-multiplication: given $g \in G$, a naive first attempt to define right-multiplication by g would be $\rho_g : G \to G$, $x \mapsto xg$. We check that

$$\rho_g(\rho_h(x)) = (xh)g = x(hg) = \rho_{hg}(x)$$

so that $\rho_g \circ \rho_h = \rho_{hg}$ rather than ρ_{gh}. The failure to obtain ρ_{gh} here can be expressed by saying that the map $g \mapsto \rho_g$ is not a homomorphism; or equivalently, the usual right-multiplication of G on G does not satisfy the usual rules for a left-action (where composition of maps is right-to-left as in undergraduate calculus courses). We will remedy this situation by instead defining

$$\rho_g(x) = xg^{-1}.$$

We now check that

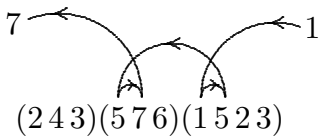
$$\rho_g \circ \rho_h = \rho_{gh}$$

as before. In fact this trick can be used to turn any right action into a left action, and vice versa. Note that the conjugation action $\psi_g(x) = gxg^{-1}$ simply becomes $\psi_g = \lambda_g \circ \rho_g = \rho_g \circ \lambda_g$ in this setting. Although we have defined conjugation as a left action (with right-to-left composition $\psi_g \circ \psi_h = \psi_{gh}$), sometimes it is preferable to use instead right action:

$$x^g = g^{-1}xg$$

so that $(x^g)^h = x^{gh}$.

And why would right action ever be preferable to left action? We show how cycle notation for S_n works using both conventions, and how left action has at least two problems which are resolved using right actions. Let's consider the composition of (243)(576) with (1523), using both conventions. If we use left action then we must compose right-to-left, thus: (243)(576)(1523) = (176543). To find the image of each point of $X = \{1, 2, \ldots, 7\}$ under this composite permutation requires careful zig-zagging back and forth; for example we check that $1 \mapsto 7$ under the composite map:



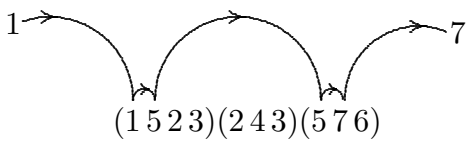
Using the standard representation of functions acting on the left, we may equivalently write

$$(243)(576)\big((1523)(1)\big) = (243)(576)(5) = 7.$$

Here the notation is ambiguous as the expressions (1) and (5) are easily misinterpreted as cycles of length 1! Both of these difficulties disappear with right action:

$$(1^{(1523)})^{(243)(576)} = 5^{(243)(576)} = 7.$$

Here the left-to-right composition of cycles is consistent with the left-to-right interpretation of each cycle, thus:



Reference

G. Eric Moorhouse, *Abstract Algebra I,* course notes for Math 5550.
http://www.uwyo.edu/moorhouse/handouts/algebra.pdf (932 KB)