Lecture 3. Group Actions

PCMI Summer 2015 Undergraduate Lectures on Flag Varieties

Lecture 3. The category of groups is discussed, and the important notion of a group action is explored.

Definition 3.1. A *group* is a set G with a composition operation (generally but not always written as a product), such that:

(i) Composition is associative: $f \cdot (g \cdot h) = (f \cdot g) \cdot h \ \ \forall f, g, h$.

(ii) There is an element $\mathrm{id} \in G$ such that: $g \cdot \mathrm{id} = g = \mathrm{id} \cdot g$ for all g.

(iii) Every element of G has a (two-sided) inverse.

Alternatively.... It is also true (and tempting) to define:

- A *monoid* is a category with one object, and
- A *group* is the collection of invertible morphisms of a monoid

Example 3.1. (a) $\mathrm{Perm}(n)$ or $\mathrm{GL}(V)$, or **any** of the automorphism groups $\mathrm{Aut}(X)$ of any object X of any category $\mathcal{C}$.

(b) A field k or vector space V with the addition operation.

(The group operation in this case is addition. It's the exception proving the rule that the operation is usually written as a product.)

(c) The units $k^* = k - \{0\}$ of a field with the multiplication operation.

(d) The group with two elements: $\{\pm 1\}$ with $(-1) \cdot (-1) = 1$.

(e) The group $\{1\}$ (analogous to the empty set or the zero space).

Definition 3.2. A map of groups $\phi : G \to G'$ is a *homomorphism* if:

(i) $\phi(\mathrm{id}_G) = \mathrm{id}_{G'}$ and

(ii) $\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2)$ for all $g_1, g_2 \in G$.

Example 3.2. (a) The (natural) logarithm is a group homomorphism

$$\ln : \mathbb{R}^{>0} \to \mathbb{R}$$

from the positive reals (with multiplication) to $\mathbb{R}$ (with addition). It is an isomorphism, with inverse the exponential function $e^x : \mathbb{R} \to \mathbb{R}^{>0}$. On the other hand, the complex exponential $e^z : \mathbb{C} \to \mathbb{C}^*$ is a group homomorphism that is only "locally" invertible by a logarithm.

(b) The permutation matrices of the previous lecture are the images of the homomorphism $\phi : \mathrm{Perm}(n) \to \mathrm{GL}(n, k)$ given by $\phi(\tau) = P_\tau$.

(c) The sign and determinant are group homomorphisms:

$$\mathrm{sgn} : \mathrm{Perm}(n) \to \{\pm 1\}, \ \det : \mathrm{GL}(n, k) \to k^*$$

Moment of Zen. The category $\mathcal{G}roups$ of groups consists of:

(a) The collection of all groups, and (b) All group homomorphisms.

Definition 3.3. A group G is *abelian* if the operation is commutative.

Example 3.3. Consider the four–element *Klein group*:

$$K_4 := \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \subset \mathrm{Perm}(4)$$

This is an abelian group, with, for example:

$$(1\ 2)(3\ 4) \circ (1\ 3)(2\ 4) = (1\ 4)(2\ 3) = (1\ 3)(2\ 4) \circ (1\ 2)(3\ 4)$$

and every element squares to the identity.

Definition 3.4. An abelian group G is *cyclic* if there is an element $g \in G$ whose positive and negative powers fill up G, i.e.

$$\{...., g^{-2}, g^{-1}, \mathrm{id}, g, g^2, g^3, ...\} = G$$

and such an element g is said to *generate* the cyclic group G.

Example 3.4 (Cyclic Groups).

(a) The integers, $\mathbb{Z}$, with addition, generated by 1 (or -1).

(b) The integers (mod n), $\mathbb{Z}/n\mathbb{Z}$, with addition, generated by **any** integer (mod n) that is relatively prime to n.

(c) The nonzero elements, k^*, of a **finite** field k, with multiplication, which is cyclic, but without an obvious choice of generator!

(d) The group of rotational symmetries of a regular polygon.

Evidently a cyclic group is abelian, but not conversely:

Products. Given groups $G_1, ..., G_n$, the *product* $G_1 \times ... \times G_n$ is the set of n-tuples $(g_1, ..., g_n) \mid g_i \in G_i$ with coordinate-wise multiplication:

$$(g_1, ..., g_n) \cdot (h_1, ..., h_n) = (g_1 \cdot h_1, ..., g_n \cdot h_n) \text{ and } \mathrm{id} = (\mathrm{id}, ..., \mathrm{id})$$

Definition 3.5. The *order* of a finite group G is the number $|G|$.

Chinese Remainder. A product of finite cyclic groups is cyclic if and only if the orders of the cyclic groups are pairwise relatively prime. Thus, if $n = \prod_{i=1}^{k} p_i^{m_i}$ is the prime factorization of n as a product of powers of distinct primes, then:

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/p_1^{m_1}\mathbb{Z} \times ... \times \mathbb{Z}/p_k^{m_k}$$

Example 3.5. The Klein group is not cyclic (it is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$).

Groups are far more complicated than sets or vector spaces. For an indication of the complexity of groups, consider the analogue of the standard sets $[n]$ and the standard vector spaces k^n.

Definition 3.6. The *free group* $F(n)$ on generators $x_1, ..., x_n$ is the set of *words* made up of letters $x_1, x_1^{-1}, ..., x_n, x_n^{-1}$ (mod cancellation) with *concatenation* as the operation (and the empty word as the identity).

Remark. The group analogue of $\mathrm{Perm}(n)$ or $\mathrm{GL}(n, k)$, namely the group $\mathrm{Aut}(F(n))$ of *automorphisms* of $F(n)$, is **extremely** complicated.

Definition 3.7. A group G is *finitely generated* if there is a surjective homomorphism: $\phi : F(n) \to G$ (for some value of n). A *relation* is an equation of two words that holds in G (after applying ϕ). A set of relations is complete if every equality of words in G (after applying ϕ) is a consequence of the given set of relations.

Example 3.6. (a) Cyclic groups are generated by one element x, with no non-trivial relations in the infinite case and one complete relation ($x^n = \mathrm{id}$) in the case of the cyclic group of order n.

(b) The *dihedral group* D_{2n} is generated by x, y with relations:

$$(i)\ x^n = \mathrm{id}, \quad (ii)\ y^2 = \mathrm{id}, \quad (iii)\ yx = x^{-1}y$$

There are $2n$ distinct elements of D_{2n} :

$$\{\mathrm{id}, x, x^2, \ldots, x^{n-1}, y, xy, x^2y, \ldots, x^{n-1}y\}$$

Moreover, it follows that each x^iy squares to zero, since:

$$(x^iy)^2 = x^i(yx^i)y = x^i(x^{-i}y)y = \mathrm{id}$$

Notice that if $n > 2$, then the dihedral group D_{2n} is not abelian.

(c) $\mathrm{Perm}(n)$ is generated by $t_1 = (1\ 2), t_2 = (2\ 3), ..., t_{n-1} = (n-1\ n)$. This takes some thought. For example:

$$(1\ 3) = t_1t_2t_1 = t_2t_1t_2, (1\ 4) = t_1t_2t_3t_2t_1, \ldots,$$

and a complete set of relations is given by:

$$t_i^2 = \mathrm{id},\ t_it_{i+1}t_i = t_{i+1}t_it_{i+1}\ , t_it_j = t_jt_i \text{ if } |i - j| > 1$$

(d) Dropping the relations $t_i^2 = \mathrm{id}$ in (c) but keeping the others defines the *braid group* on n strands. This is an infinite group which is finitely generated (with a complete set of finitely many relations).

The most commonly studied groups fall, roughly, into three types:

(i) Finite Groups

(ii) Finitely Generated Infinite Groups (e.g. $F(n)$ and braid groups)

(iii) Continuous Groups (e.g. the real numbers with addition)

We'll be interested here in groups of type (i) and (iii).

Abelian groups, on the other hand, are less complicated:

Theorem 3.1. Every finitely generated abelian group G is isomorphic to a product of cyclic groups:

$$\mathbb{Z}^n \times \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_m\mathbb{Z}$$

for unique n and $d_1, ..., d_m$ such that each d_i divides d_{i+1}.

Still, the group $\mathrm{GL}(n, \mathbb{Z}) = \mathrm{Aut}(\mathbb{Z}^n)$ is plenty complicated.

Definition 3.8. A homomorphism $\rho : G \to \mathrm{Aut}(X)$ is called an *action* of the group G on an object X (of a category $\mathcal{C}$). Examples include permutation actions $\phi : G \to \mathrm{Aut}(S)$ on a set and linear actions, or *representations* $\rho : G \to \mathrm{GL}(V)$ on a vector space.

Example 3.7. (a) For each $0 \le m < n$, the map:

$$\chi_m : C_n \to \mathbb{C}^* = \mathrm{Aut}(\mathbb{C}^1);\ \chi_m(x) = e^{\frac{2\pi i m}{n}}$$

defines a one-dimensional complex representation of C_n.

(b) The dihedral group D_{2n} has a two-dimension real representation:

$$\rho(x) = \begin{bmatrix} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \\ \sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{bmatrix},\ \rho(y) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

(rotation counterclockwise by $2\pi/n$ and reflection across the x-axis).

This is well-defined since $\rho(x)^n = \mathrm{id} = \rho(y)^2$ and:

$$\rho(y) \cdot \rho(x) = \begin{bmatrix} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \\ -\sin(\frac{2\pi}{n}) & -\cos(\frac{2\pi}{n}) \end{bmatrix} = \rho(x)^{-1}\rho(y)$$

(c) D_{2n} also acts on the set $[n]$ via:

$$\phi(x) = (1\ 2\ ...\ n),\ \phi(y) = (1\ n-1)(2\ n-2)\cdots$$

which is well-defined because $\phi(x)^n = \mathrm{id} = \phi(y)^2$ and

$$\phi(y)\phi(x) = (1\ n-2)(2\ n-3)...(n-1\ n) = \phi(x)^{-1}\phi(y)$$

This is the "induced action" from (b) on the vertices of a regular n-gon centered at the origin, numbered counterclockwise, ending at $n = (1, 0)$.

Definition 3.9. A subset $H \subset G$ is a *subgroup* if $\mathrm{id} \in H$ and H is closed under inverses and the group operations.

Definition 3.10. An action $\phi : G \to \mathrm{Aut}(S)$ on a set S is *transitive* if, for each pair $s, t \in S$, there is an element $g \in G$ such that $\phi(g)(s) = t$, or equivalently, if there is no proper (nonempty) subset $T \subset S$ that is left fixed by the action. The *stabilizer* H_s of an element $s \in S$ is the subgroup of elements $h \in G$ with the property that $h(s) = s$.

Proposition 3.1. If $\phi : G \to \mathrm{Aut}(S)$ is a transitive action of a finite group, and if H_s is the stabilizer of any $s \in S$, then $|G| = |S| \cdot |H_s|$.

Proof. For each $t \in S$, choose $g_t \in G$ such that $g_t(s) = t$. Then:

$$G = \bigcup_{t \in S} g_t H_s \text{ where } g_t H_s = \{g_t \cdot h \mid h \in H_s\}$$

and this is a disjoint union of $|S|$ sets, each of size $|H_s|$.

Corollary 3.1 (Lagrange's Theorem) If $H \subset G$ is a subgroup of a finite group, then $|H|$ divides $|G|$.

Proof. Let $S = \{gH \mid g \in G\}$ be the set of left cosets of $H \subset G$. Then G acts on S by left multiplication: $g'(gH) = (g'g)H$, the action is transitive, and the stabilizer of $H \in S$ is H, so $|G| = |S| \cdot |H|$. $\square$

In Proposition 2.3, the cosets of a subspace formed a vector space. Here, they are just a set (and not usually a group). But see below!

Example 3.8. There are two obvious subgroups of D_{2n}, namely:

$$C_n = \{1, x, x^2, ..., x^{n-1}\} \text{ and } C_2 = \{1, y\}$$

The cosets of C_n are: $\{1, x, x^2, \ldots, x^{n-1}\}$ and $\{y, yx, \ldots, yx^{n-1}\}$.
The cosets of C_2 are $\{1, y\}, \{x, xy\}, ..., \{x^{n-1}, x^{n-1}y\}$.

Definition 3.11. The *conjugation action* of G on itself is the map:

$$c : G \to \mathrm{Aut}(G), \; c(h)(g) = hgh^{-1}$$

This is an action *in the category of groups* since:

$$c(h)(gg') = h(gg')h^{-1} = hgh^{-1} \cdot hg'h^{-1} = c(h)(g) \cdot c(h)(g')$$

i.e. each $c(h)$ is automorphism of G **as a group**. The image of the conjugation action is called the group of *inner* automorphisms of G.

Example 3.9. (a) The conjugation action of an abelian group G on itself is trivial (i.e. the image of $c : G \to \mathrm{Aut}(G)$ is $\{\mathrm{id}\}$), since:

$$c(h)(g) = hgh^{-1} = (hh^{-1})g = g$$

More generally, if $g \in G$ commutes with all other elements of G, then g is said to be in the *center* of G, and is fixed by the conjugation action.

(b) The conjugation action of the permutation group. If $h \in \mathrm{Perm}(n)$ (thought of as a bijection $h : [n] \to [n]$) and $g \in \mathrm{Perm}(n)$ is written in cycle notation, then the cycle notation for hgh^{-1} has the same "shape" as the cycle notation for g, but with each i replaced with $h(i)$.

For example, if $h = (1\ 2\ 3) \in \mathrm{Perm}(3)$, then

$$h(1\ 2)h^{-1} = (h(1)\ h(2)) = (2\ 3) \text{ and } h(1\ 3)h^{-1} = (2\ 1) = (1\ 2)$$

As a consequence, it follows that the *classes* of elements of $\mathrm{Perm}(n)$ are preserved by the conjugation action, and the conjugation action is transitive on each *conjugacy class* of elements.

For example, consider the conjugacy classes of elements in $\mathrm{Perm}(4)$:

$$\mathrm{id}, (*\,*), (*\ \ *\ \ *), (*\ \ *\ \ *\,*), (*\,*)(*\,*)$$

We've seen that these classes have $1, 6, 8, 6, 3$ elements, respectively. We can write down the stabilizers of elements in each class:

$\mathrm{Stab}(\mathrm{id}) = \mathrm{Perm}(4)$

$\mathrm{Stab}(1\ 2) = \{\mathrm{id}, (1\ 2), (1\ 2)(3\ 4), (3\ 4)\}$

$\mathrm{Stab}(1\ 2\ 3) = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$

$\mathrm{Stab}(1\ 2\ 3\ 4) = \{\mathrm{id}, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}$

$\mathrm{Stab}((1\ 2)(3\ 4)) =$ Exercise... note that it has $24/3 = 8$ elements

Let $\mathrm{Sub}(G)$ be the set of subgroups $H \subset G$. Because it acts by group automorphisms, the conjugation action induces an action on the set of subgroups:

$$\phi : G \to \mathrm{Aut}(\mathrm{Sub}(G));\ \ \phi(g) = gHg^{-1}$$

i.e. conjugating a subgroup produces another subgroup!

Definition 3.12. (a) Two subgroups $H, H' \in \mathrm{Sub}(G)$ are *conjugate* if:

$$gHg^{-1} = H' \text{ for some } g \in G$$

i.e. if $\phi(g)(H) = H'$. The set of subgroups that are conjugate to H is called the *conjugacy class* of H. By definition, then, a group G acts transitively on each conjugacy class of **subgroups** of G, just as it does on each conjugacy class of **elements** of G.

(b) A subgroup $H \subset G$ is *normal* if it is fixed by conjugation, i.e. if the conjugacy class of H consists of H iself.

Example 3.10. The normal subgroups of $\mathrm{Perm}(4)$ are $\{\mathrm{id}\}$, K_4 and:

$$A_4 := \{\mathrm{id}, (*\,*)(*\,*), (*\ \ *\ \ *)\} \text{ (12 elements)}$$

i.e. all elements $\sigma \in \mathrm{Perm}(4)$ such that $\mathrm{sgn}(\sigma) = 1$.

As with vector spaces, we have the following:

Definition 3.13. Let $\phi : G \to G'$ be a group homomorphism.

(i) The kernel of ϕ is the subgroup $\phi^{-1}(\mathrm{id}_{G'}) \subset G$.

(ii) The image of ϕ is the subgroup $\mathrm{im}(\phi) \subset G'$.

The following is easily checked (see Proposition 2.2).

Proposition 3.2. ϕ is injective if and only if $\ker(\phi) = \{\mathrm{id}_G\}$.

However, there is a new wrinkle:

Proposition 3.3. The kernel of a homomorphism $\phi : G \to G'$ is a **normal** subgroup of G and conversely, if $H \subset G$ is a normal subgroup, there is a surjective homomorphism $q : G \to G'$ with $H = \ker(\phi)$.

Proof. Suppose $h \in \ker(\phi)$ and $h' = ghg^{-1}$ for some g. Then:

$$\phi(h') = \phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = \phi(g) \cdot \mathrm{id}_{G'} \cdot \phi(g)^{-1} = \mathrm{id}_{G'}$$

so $h' \in \ker(\phi)$. This implies that H is normal.

Conversely, suppose $H \subset G$ is normal, and consider again:

$$G/H = \{gH \mid g \in G\}, \text{ the set of cosets}$$

I claim that H being a *normal* subgroup is exactly the condition that is needed in order for multiplication of cosets to make G/H a group:

$$(gH) \cdot (g'H) = g(g'Hg'^{-1})g'H = (gg')H$$

Then the proof proceeds as in Proposition 2.3, with: $q : G \to G/H$ given by $q(g) = gH$ the surjective homomorphism with kernel H. $\square$

Example 3.11. The Klein subgroup $K_4 \subset \mathrm{Perm}(4)$ is normal, so it is the kernel of a group homomorphism. Looking around, we find it:

$$\phi : \mathrm{Perm}(4) \to \mathrm{Aut}(\{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\})$$

namely, the conjugation action on the conjugacy class $(*\,*)(*\,*)$. This is a surjective homomorphism to a group of order 6, with K_4 in the kernel (since K_4 is commutative), hence K_4 is the kernel ($4 \times 6 = 24$).

Definition 3.14. (a) The *alternating group* $\mathrm{Alt}(n) \subset \mathrm{Perm}(n)$ is the kernel of the sign homomorphism (permutations of sign 1).

(b) The *special linear group* $\mathrm{SL}(n, k) \subset \mathrm{GL}(n, k)$ is the kernel of the determinant, i.e. the matrices A with $\det(A) = 1$.

Example 3.12. Consider $\mathrm{Alt}(5)$ with $60 = 5!/2$ elements in classes:

$$\mathrm{id}, (*\ *\ *), (*\,*)(*\,*), (*\ *\ *\ *\ *)$$

of $\mathrm{Perm}(5)$ with $1, 20, 15, 24$ elements, respectively. This group has many subgroups but it is *simple*, meaning that it has no (non-trivial) normal subgroups. Indeed, the groups $\mathrm{Alt}(n)$ for $n \geq 5$ are all simple. This is not obvious, but you could prove it with the tools you have.

Notice that the $\mathrm{Perm}(5)$ conjugacy class $(*\ *\ *\ *\ *)$ **cannot** be a conjugacy class for $\mathrm{Alt}(5)$ acting on itself, since 24 does not divide 60. In fact, it splits in two.

Exercises.

1. Show that an action of a group G on a set S is the same as a map from the Cartesian product:

$$a : G \times S \to S; \quad \text{written} \quad a(g, s) = gs$$

with the property that $g_1(g_2 s) = (g_1 g_2)s$ for all $g_1, g_2 \in G$. If $S = V$ is a vector space over k, then the action is a representation if in addition, multiplication by g is linear, i.e. $g(\vec{v}+\vec{w}) = g\vec{v}+g\vec{w}$ and $g(c\vec{v}) = cg(\vec{v})$.

2. If G acts transitively on S and H_s and $H_{s'}$ are stabilizers of $s, s' \in S$, prove that H_s and $H_{s'}$ are *conjugate* subgroups of G. Conversely, if $H = gH_s g^{-1}$ is conjugate to H_s, for some $g \in G$, prove that $H = H_{s'}$ for some $s' \in S$. Thus, S indexes the elements in the conjugacy class of the stabilizer of (any) element $s \in S$.

3. Prove that the left multiplication action of G on itself is transitive, but is *only* an automorphism of G as a set, and not an action in the category of groups (in contrast to the conjugation action).

4. Prove that the group of units (denoted k^*) of a finite field is cyclic.

Hint: If $n = |k^*|$, then every element of k^* is a root of $x^n - 1$.

If $g \in k^*$ is **not** a generator, then g is a root of $x^d - 1$ for some d that properly divides n (by Lagrange's Theorem). The problem now follows from counting and the fact that a polynomial of degree d with coefficients in a field has **no more** than d roots in that field.

5. Prove the Chinese Remainder result.

6. For the dihedral groups D_{2n}:

(a) Find all the conjugacy classes of elements $g \in D_{2n}$.

(b) Find all the normal subgroups $H \subset D_{2n}$.

7. Find all conjugacy classes of elements of (a) Alt(4) (b) Alt(5).

8. Find the stabilizer of $(1\ 2)(3\ 4) \in \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ for the conjugation action of Perm(4). (It is a group with 8 elements).

9. Find Aut(G) (in the category of groups) for the groups C_n and D_{2n}.

10. Identify the groups of "rotational" symmetries of:

(a) A regular tetrahedron.

(b) A cube.

(c) A regular dodecahedron.

Hint: Two are alternating groups and one is a permutation group.

Zen master problems.

11. Show that a product of two groups as defined just above Definition 3.5 is a product in the category of groups.

A functor $F : \mathcal{C} \to \mathcal{D}$ is *faithful* if F is injective on objects and each

$$(*)\ F : \mathrm{Hom}(X, Y) \to \mathrm{Hom}(F(X), F(Y))$$

is also injective. In other words, each object and arrow from $\mathcal{C}$ has a unique image in $\mathcal{D}$. It is **fully faithful** if each of the maps $(*)$ is also **surjective** (but F is still only required to be injective on objects).

12. Show that the forgetful functors from vector spaces over k to sets, as well as the forgetful functor from groups to sets, are all faithful but not fully faithful. Notice that all groups and vector spaces are pointed, i.e. they have a distinguished elements, so forgetful functors to the category of sets pass through a category whose objects consist of sets with a distinguished point (what are the morphisms?). However, even the functor from the category of sets with a distinguished point to sets (forgetting the point) is not fully faithful.

13. Let $\mathcal{A}b$ be the category of abelian groups. Show that the forgetful functors from vector spaces over any k to $\mathcal{A}b$ are all faithful, but not fully faithful, but in contrast, show that the functor from abelian groups to groups **is** fully faithful.