Lecture 1. The Category of Sets

PCMI Summer 2015 Undergraduate Lectures on Flag Varieties

Lecture 1. Some basic set theory, a moment of categorical zen, and some facts about the permutation groups on n letters.

A *set* is a collection of *elements*. The *standard* finite sets are:

$$[n] := \{1, 2, 3, ..., n\}$$

i.e. the collections of the first n natural numbers.

Remark. The empty set $\emptyset$ is the unique set with zero elements.

Notation. $|S|$ is the number of elements (cardinality) of a finite set S.

A *map*:

$$f : S \to T$$

is a rule for assigning a unique element $t \in T$ to each element $s \in S$. This is written in "function notation" as: $f(s) = t$.

The map f is *injective*, *surjective* or *bijective*, respectively, if:

(inj) Each $t \in T$ is assigned to **at most** one $s \in S$.

(surj) Each $t \in T$ is assigned to **at least** one $s \in S$.

(bij) Each $t \in T$ is assigned to **exactly** one $s \in S$.

Maps can be composed. If $f : S \to T$ and $g : T \to U$, then:

$$(g \circ f)(s) = g(f(s))$$

defines the *composition* $g \circ f : S \to U$, and if $h : U \to V$, then:

$$h \circ (g \circ f) = (h \circ g) \circ f$$

In other words, composition of maps is an associative operation.

Every set S comes equipped with the *identity* self-map:

$$\mathrm{id}_S : S \to S \quad \mathrm{id}_S(s) = s$$

Evidently, $f \circ \mathrm{id}_S = f$ and $\mathrm{id}_T \circ f = f$ for all maps $f : S \to T$.

Each bijective map $b : S \to T$ has a two-sided *inverse* $b^{-1} : T \to S$, i.e.

$$b^{-1} \circ b = \mathrm{id}_S \text{ and } b \circ b^{-1} = \mathrm{id}_T$$

Remark. The fact that the left and right inverses of a bijection are the same is a consequence of associativity and the properties of the identity. If b_l^{-1} and b_r^{-1} are "left" and "right" inverses of b, respectively, then:

$$b_l^{-1} = b_l^{-1} \circ \mathrm{id}_T = b_l^{-1} \circ (b \circ b_r^{-1}) = (b_l^{-1} \circ b) \circ b_r^{-1} = \mathrm{id}_S \circ b_r^{-1} = b_r^{-1}$$

so they are the same!

Moment of Zen. The *category* of sets consists of the two collections:
(a) The collection of **all** sets, (b) The collection of **all** maps of sets
which we visualize as a universe of points (sets) and arrows (maps).

More precisely:

Definition 1.1. A *category* $\mathcal{C}$ consists of two collections:

(a) The collection $ob(\mathcal{C})$ of *objects* X of $\mathcal{C}$, and

(b) The collection $mor(\mathcal{C})$ of *morphisms* $f : X \to Y$ between objects equipped with a composition law with the following properties:

(i) The composition law is associative (in the sense we discussed).

(ii) Each object has an identity morphism $\mathrm{id}_X : X \to X$ such that

$$f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f \text{ for all objects } X, Y \text{ and morphisms } f : X \to Y$$

(iii) By the argument above, inverses (when they exist) are two-sided.

This is **designed** so that sets and maps form the category $\mathcal{S}ets$.

The morphisms from an object to itself are called *endomorphisms* and the morphisms with (two-sided) inverses are called *isomorphisms*. An *automorphism* is an endomorphism that is also an isomorphism.

Let:

$$\mathrm{End}(S) \text{ and } \mathrm{Aut}(S)$$

be the sets of endomorphisms and automorphisms of a set S.

Tuple Notation. Each map $f : [n] \to S$ "is" the n-tuple of its values:

$$(f(1), f(2), \dots, f(n)) \in S^n$$

In particular, an n-tuple of elements of $[n]$ is an element $f \in \mathrm{End}([n])$, and if the elements are distinct, then $f \in \mathrm{Aut}([n])$. We conclude that

$$|\mathrm{End}([n])| = n^n \text{ and } |\mathrm{Aut}([n])| = n!$$

Since every pair of endomorphisms can be composed, we can form a composition table for the endomorphisms of a finite set:

Example 1.1. The elements of $\mathrm{End}([2])$ are $(1,1), (1,2), (2,1), (2,2)$ with composition table:

$g \circ f$	$g = (1,1)$	$(1,2)$	$(2,1)$	$(2,2)$
$f = (1,1)$	$(1,1)$	$(1,1)$	$(2,2)$	$(2,2)$
$(1,2)$	$(1,1)$	$(1,2)$	$(2,1)$	$(2,2)$
$(2,1)$	$(1,1)$	$(2,1)$	$(1,2)$	$(2,2)$
$(2,2)$	$(1,1)$	$(2,2)$	$(1,1)$	$(2,2)$

Notice that already in this case, composition is **not** commutative!

Our first interesting example of a representation is the following:

Definition 1.2: Let $f \in \mathrm{End}([n])$. Then:

$$\mathrm{sgn}(f) = \prod_{\text{pairs } i<j} \frac{f(j) - f(i)}{j - i}$$

is the *characteristic sign function* of the endomorphism.

Remark. We could have also chosen $i > j$ in a pair, since:

$$\frac{f(j) - f(i)}{j - i} = \frac{f(i) - f(j)}{i - j}$$

Proposition 1.1. (a) $\mathrm{sgn}(f) = 0$ if and only if $f \notin \mathrm{Aut}([n])$.

(b) Otherwise $\mathrm{sgn}(f) = \pm 1$.

(c) sgn is a multiplicative function, i.e.

$$\mathrm{sgn}(f \circ g) = \mathrm{sgn}(f) \cdot \mathrm{sgn}(g)$$

for all pairs of endomorphisms f, g.

Proof. Since $[n]$ is finite, f fails to be an automorphism if and only if it fails to be injective, and f fails to be injective if and only if the numerator of some factor of $\mathrm{sgn}(f)$ is zero. This is (a).

For (b), let $f \in \mathrm{Aut}([n])$. Then the pairs $\{f(i), f(j)\}$ vary over all two-element subsets of $[n]$ as the pairs $\{i, j\}$ vary over all two-element subsets. It follows that $\prod_{i<j} |f(j) - f(i)| = \prod_{i<j} |j - i|$ and therefore that $\prod_{i<j}(f(j) - f(i)) = \pm \prod_{i<j}(j - i)$, which gives (b). Notice that it may be the case that $i < j$ but $f(i) > f(j)$. In fact, the number of such "crossings" determines whether $\mathrm{sgn}(f)$ is $+1$ or -1.

Let $h = f \circ g$. If f or g is not an automorphism, then h is not, and:

$$\mathrm{sgn}(h) = 0 = \mathrm{sgn}(f) \cdot \mathrm{sgn}(g)$$

Otherwise, g in particular is an automorphism, and:

$$\mathrm{sgn}(h) = \prod_{i<j} \frac{f(g(j)) - f(g(i))}{j - i} = \prod_{i<j} \frac{f(g(j)) - f(g(i))}{g(j) - g(i)} \cdot \frac{g(j) - g(i)}{j - i}$$

The product of the second factors gives $\mathrm{sgn}(g)$, and the product of the first factors (and the remark above) gives $\mathrm{sgn}(f)$. $\square$

Remark. The inverse of a composition of automorphisms satisfies:

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1}$$

Notation. Self-compositions of an automorphism are written as powers:

$$f^2 = f \circ f,\ \ f^3 = f \circ f \circ f,\ \text{etc}$$

Definition 1.3. $\mathrm{Aut}([n])$ is called the *permutation group* $\mathrm{Perm}(n)$.

Example 1.2. $\mathrm{Perm}(3)$ consists of six elements:

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

These elements fall into three distinct "classes:"

(id) $\mathrm{id} = (1,2,3)$ fixes each element.

(tr) $(1,3,2), (2,1,3)$ and $(3,2,1)$ each "transpose" two elements.

(cyc) $(2,3,1), (3,1,2)$ each "cycle" through all the elements.

Permutations have an extremely useful *cycle* notation:

Definition 1.4. Let $s \in S$ and $f \in \mathrm{Aut}(S)$. The sequence:

$$s, f(s), f^2(s), f^3(s), \ldots$$

of elements of S is the *orbit* of s under the automorphism f.

Proposition 1.2. The orbit of each $i \in [n]$ cycles under a permutation $\sigma \in \mathrm{Perm}(n)$, i.e. there is a distinct sequence $i_1, \ldots, i_k \in [n]$ so that:

$$\sigma(i) = i_1, \sigma^2(i) = i_2, \ldots, \sigma^k(i) = i_k = i$$

Proof. Because $[n]$ is finite, the elements of the orbit $i, \sigma(i), \sigma^2(i), \ldots$ eventually repeat. Suppose the **first** repetition is:

$$\sigma^m(i) = \sigma^n(i) \text{ with } m < n$$

Then composing both sides with the permutation $(\sigma^m)^{-1} = (\sigma^{-1})^m$ gives $i = \sigma^{n-m}(i)$, and the Proposition holds with $k = n - m$. $\square$

Cycle Notation. The *cycle* notation for $\sigma \in \mathrm{Perm(n)}$ lists the distinct elements of the orbit of 1 (in parentheses without commas), followed by the distinct elements of the orbit of the first element not contained in the orbit of 1, etc. until all elements of $[n]$ are exhausted.

For example, in cycle notation the elements of $\mathrm{Perm}(3)$ are:

$$(1,2,3) = (1)(2)(3)$$

$$(1,3,2) = (1)(2\ 3), (2,1,3) = (1\ 2)(3), (3,2,1) = (1\ 3)(2)$$

$$(2,3,1) = (1\ 2\ 3),\ \ (3,1,2) = (1\ 3\ 2)$$

Simplification. Singleton orbits are left out of the cycle notation, with the assumption that any missing element is fixed by the permutation.

For example: $(1,3,2) = (1)(2\ 3) = (2\ 3)$ in the simplified notation.

The composition table for the six elements of Perm(3) is:

$g \circ f$	$g = \mathrm{id}$	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$f = \mathrm{id}$	id	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$(1\ 2)$	$(1\ 2)$	id	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(1\ 3)$	$(2\ 3)$
$(1\ 3)$	$(1\ 3)$	$(1\ 3\ 2)$	id	$(1\ 2\ 3)$	$(2\ 3)$	$(1\ 2)$
$(2\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$	id	$(1\ 2)$	$(1\ 3)$
$(1\ 2\ 3)$	$(1\ 2\ 3)$	$(2\ 3)$	$(1\ 2)$	$(1\ 3)$	$(1\ 3\ 2)$	id
$(1\ 3\ 2)$	$(1\ 3\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2)$	id	$(1\ 2\ 3)$

Example 1.3. The 24 elements of Perm(4) fit into one of five classes:

(i) The identity id

(ii) Transpositions

$$(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)$$

(iii) Three-cycles

$$(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)$$

(iv) Four-cycles

$$(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)$$

(v) Transposition pairs

$$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$$

We leave the 24×24 composition table for Perm(4) as an exercise.

Exercise 1.1. The sign of a transposition (for any n) is:

$$\mathrm{sgn}(i\ j) = -1$$

Corollary 1.1. The sign of an m-cycle is $(-1)^{m-1}$.

Proof. An m-cycle is a composition of $m - 1$ transpositions:

$$(i_1\ i_2\ i_3\ ...\ i_m) = (i_1\ i_m) \circ \cdots \circ (i_1\ i_3) \circ (i_1\ i_2)$$

so by the Exercise and Prop 1.1, we have $\mathrm{sgn}(i_1\ i_2\ i_3\ ...\ i_m) = (-1)^{m-1}$. □

Corollary 1.2. Every permutation $\sigma \in \mathrm{Perm}(n)$ is a composition of transpositions. Although the number of such transpositions is not well-defined, the parity (even or odd) of the number is well-defined.

Proof. The cycle notation presents a permutation as a composition of (disjoint) cycles. Each cycle is a composition of transpositions, as in the Proof of Corollary 1.1 above. The parity is determined by the sign of σ, which was well-defined in Definition 1.2. □

Exercises.

1.1. Prove that the sign of a transposition $(i\ j) \in \mathrm{Perm}(n)$ is -1.

1.2. Work out the composition table for $\mathrm{Perm}(4)$.

A subset of $\mathrm{Perm}(n)$ that contains the identity $\mathrm{id}_{[n]}$ and is closed under inverses and compositions is a *subgroup*.

1.3. Find all the subgroups of $\mathrm{Perm}(3)$ and $\mathrm{Perm}(4)$.

Hint: The number of elements in a subgroup of $\mathrm{Perm}(n)$ divides $n!$.

The *order* of $\sigma \in \mathrm{Perm}(n)$ is the smallest value of k so that $\sigma^k = \mathrm{id}_{[n]}$.

1.4. (a) Obtain the order of $\sigma \in \mathrm{Perm}(n)$ from its cycle notation.

(Conclude that the order of any permutation is finite!)

(b) Find the largest order of an element of $\mathrm{Perm}(n)$ for small n.

A nonempty set S is *finite* if there is a surjective map $f : [n] \to S$.

1.5. (a) If S is finite and non-empty, contemplate why there is a bijective map $f : [m] \to S$ for a unique integer m.

(b) Find two infinite sets that have no bijection between them.

(c) Find an injection from the set $\mathbb{Z}$ to itself that is **not** a bijection.

(d) Show that (c) cannot happen for finite sets.

And now for some zenmaster problems.

1.6. Let S be a fixed set and consider the following pair of collections:

(a) The collection of subsets of S, (b) Inclusions of subsets

This is a category! Draw pictures of it when $S = [2]$ and $[3]$.

What are compositions and isomorphisms in this category?

1.7. The *Cartesian product* of two sets S and T is the set:

$$S \times T = \{(s,t) \mid s \in S \text{ and } t \in T\}$$

of ordered pairs. This comes equipped with "projection" maps:

$$p : S \times T \to S \text{ and } q : S \times T \to T$$

defined by setting $p(s,t) = s$ and $q(s,t) = t$.

(a) Show that this data (the set $S \times T$ with the maps p and q) is *universal* in the category $\mathcal{S}ets$ in the following sense. Suppose (U, a, b) is another triple, consisting of a set U with maps $a : U \to S$ and $b : U \to T$, then there is a **unique** map $f : U \to S \times T$ with the property that $p \circ f = a$ and $q \circ f = b$. (Draw a picture!)

(a) Show that if (U, a, b) happens to **also** be universal, then the **unique** map f is a bijection, and so U is indistinguishable from $S \times T$.

We say that objects X, Y of a category $\mathcal{C}$ have a product in $\mathcal{C}$ if there exists (U, a, b) with the universal property above. Notice that this gives a **categorical** notion of the product, which can apply even in categories in which the objects are not sets!

(b) Show that in the category of subsets of S (from Exercise 1.6.), the **intersection** $T_1 \cap T_2$, together with the inclusions into T_1 and T_2, is the product of T_1 and T_2.

(c) What universal property holds for **unions** $T_1 \cup T_2$ together with the inclusions $i : T_1 \subset T_1 \cup T_2$ and $j : T_2 \subset T_1 \cup T_2$ in the category of subsets of S? A triple satisfying this property is called a **coproduct**.

(d) Are there coproducts of sets in the category of sets?

1.8. We tacitly assumed that S and T were not empty when we formed their Cartesian product. What happens if one or the other is empty? What's the product, and does it still satisfy the universal properties? How many maps from the empty set to another set are there? Are there any maps from a nonempty set to the empty set?