18.704 Supplementary Notes
February 4, 2005

Groups and actions

It was perhaps Felix Klein more than a hundred years ago who first understood that groups were absolutely fundamental to all kinds of mathematics. Speaking about geometry in particular, he said that studying a certain kind of geometry *means* studying a certain kind of symmetry group: that you should specify the symmetries first, and they'll tell you what the geometry is. In order to follow this philosophy perfectly, I should define first not an abstract group but a symmetry group. However, I'm a slave to the demands of pedagogy, and it's pedagogically a bit easier to start with abstract groups. So here they are.

Definition 1. A *group* is a set G equipped with a binary operation $\cdot$ called *multiplication* satisfying the following axioms.

(1) (associative law) For all elements a, b, and c in G, we have

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

(2) (identity element) There is an element $1 \in F$ such that for every element a in G, we have

$$1 \cdot a = a \cdot 1 = a.$$

(3) (inverses) For every element a in G there is an element a^{-1} so that

$$a \cdot a^{-1} = a^{-1} \cdot a = 1.$$

A *subgroup* of G is a subset $H \subset G$ which is a group under the restriction of the multiplication law for G. This amounts to three requirements on H:

(1) (closure) For all elements a and b in H, the product $a \cdot b$ belongs to H.
(2) (identity element) The identity element 1 of G belongs to H.
(3) (inverses) For every element a of H, the inverse a^{-1} also belongs to H.

You might think that the second requirement is unnecessary, because it seems to be a consequence of the first and the third. That's not quite correct, however; why not?

The numbered items in Definition 1 are the *axioms* for a group. To make an example of a group, we need to describe the set G, describe the multiplication $\cdot$, and check that all of the axioms are satisfied. The best examples are groups of symmetries, however. To talk about those, we need one more abstract definition.

Definition 2. Suppose that G is a group and X is a set. An *action* of G on X is a map

$$G \times X \to X, \qquad (g, x) \mapsto g \cdot x, \tag{A}$$

subject to the following requirements.

(1) For all g and h in G and x in X, we have

$$g \cdot (h \cdot x) = (g \cdot h) \cdot x.$$

Here on the left side, both dots represent the action of G: first h acts, then g acts. On the right side, the first dot is the multiplication law in G, and the second is the action of G on X: first multiply g and h, then let the product act on X.

(2) For all $x \in X$, we have $1 \cdot x = 1$: the identity element of G acts by doing nothing.

The action is said to be *faithful* if for every $g \neq 1$ in G there is an $x \in X$ so that $g \cdot x \neq x$. The action is *transitive* if X is non-empty, and for all x and y in X there is an element g in G so that $g \cdot x = y$.

Suppose $x \in X$. The *orbit of* x is the subset

$$G \cdot x = \{g \cdot x \mid g \in G\} \subset X.$$

The *isotropy subgroup* for the action at x is

$$G_x = \{g \in G \mid g \cdot x = x\}.$$

Here are some examples.

Example 1. Suppose X is any set. A *permutation of* X is one-to-one function g from X onto X:

$$g\colon X \to X, \qquad g(x_1) = g(x_2) \Rightarrow x_1 = x_2, \quad \text{and}$$

$$\text{for every } y \text{ in } X \text{ there is an } x \text{ in } X \text{ so that } g(x) = y.$$

Write $\Sigma(X)$ for the collection of all permutations of X. We want to make $\Sigma(X)$ a group. The multiplication operation is composition of functions: $g \cdot h = g \circ h$. It is not difficult to check that the composition of two permutations is in fact a permutation: so compostion is in fact a binary operation on $\Sigma(X)$. Composition of functions satisfies the associative law whenever it is defined, so condition (1) of Definition 1 is satisfied. The identity function $1_X(x) = x$ is a permutation, and it is an identity element for compostion of functions; so condition (2) is satisfied. Finally, every permutation g has an inverse function, defined by

$$g^{-1}(y) = \text{unique element } x \text{ such that } g(x) = y.$$

This element x exists by the second condition defining a permutation, and it is unique by the first condition. We have

$$g^{-1} \circ g = g \circ g^{-1} = 1_X,$$

so condition (3) is satisfied, and $\Sigma(X)$ is a group.

The permutation group $\Sigma(X)$ acts on X, by

$$g \cdot x = g(x) \qquad (g \in \Sigma(X), x \in X).$$

Requirement (1) in the definition of an action reads

$$g(h(x)) = (g \cdot h)(x) \qquad (g, h \in \Sigma(X), x \in X).$$

This is just the statement that the group law for multiplying permutations is composition. Requirement (2) is immediate from the definition of the identity element 1_X above.

With this definition in hand, we can say roughly what a "symmetry group" is.

Vague Definition 3. Suppose X is a set with some additional structure. The *symmetry group of the structure* consists of all permutations of X that preserve the structure.

What's vague here is the word "structure." It's meant to cover an enormous range of possibilities. Instead of trying to make some very general definition, it's better to give some examples.

Example 2. Suppose X is a circle. More precisely, suppose that X is the unit circle centered at the origin in the xy plane. That is

$$X = \{P = (x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}.$$

The structure that I want to look at is distance: between any two points P and Q of the circle there is a well defined distance $d(P, Q)$. For example, $d((1, 0), (0, 1)) = \sqrt{2}$. The "symmetry group of the circle" means all permutations of the circle that preserve distances:

$$G = \{g \in \Sigma(X) \mid d(g \cdot P, g \cdot Q) = d(P, Q) \quad (P, Q \in X)\}.$$

An example of a permutation in G is the rotation r_θ by an angle of θ:

$$r_\theta(x, y) = (x \cos\theta + y \sin\theta, -x \sin\theta + y \cos\theta).$$

Proving that this permutation preserves distance is an elementary analytic geometry exercise, using the identity $\cos^2\theta + \sin^2\theta = 1$. A more interesting exercise is to compute the composition of two rotations:

$$r_\theta \cdot r_\phi = r_{\theta+\phi}.$$

This one requires the addition formulas for sin and cos. The most interesting exercise of all is to find some additional symmetries of the circle (preserving distance, but not given by rotation).

Example 3. Suppose that X is the two-dimensional vector space $\mathbb{R}^2$. The structure that I want to look at is the vector space structure: vector addition and scalar multiplication. The "symmetry group of the vector space $\mathbb{R}^2$" means all permutations of the plane that preserve addition and scalar multiplication:

$$G = \{g \in \Sigma(X) \mid g \cdot (P + Q) = g \cdot P + g \cdot Q, \quad g \cdot (rP) = r(g \cdot P) \quad (P, Q \in \mathbb{R}^2, r \in \mathbb{R})\}.$$

An example of a permutation in G is multiplication by an invertible matrix

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad (a, b, c, d \in \mathbb{R}, ad - bc \neq 0)\}$$

$$g_T \cdot (x, y) = (ax + by, cx + dy).$$

Are there other permutations in G?

It's a good exercise to check that composition of these permutations corresponds to matrix multiplication: $g_S \cdot g_T = g_{ST}$. This fact is the reason that matrix multiplication is defined the way it is. It also explains why matrix multiplication is associative: because it corresponds to composition of functions.

Examples 2 and 3 are meant to illustrate two very different kinds of "structure" whose symmetry we might want to study. The first one looks like geometry, and the second one like linear algebra. Despite these fundamental differences, the formula for the action in Example 2 looks a lot like the formula for the action in Example 3. (Can you find some precise way to express a relation between the examples?) This is meant to illustrate the fact that we can do a lot of geometry by doing linear algebra. That's a central theme of this seminar.

Story Problem 4. (cf. `http://michel.delord.free.fr/toom_wp.pdf`) There is a tour group consisting of seven people: two married couples and three single individuals. Each couple is to share a double hotel room, and each of the three single individuals is to have a single room. The tour operator is about to distribute their seven room keys, but he has lost the labels on the keys. Rather than admit this mistake, he intends to distribute the keys at random. What is the probability that no harm will be done? (And what in the world does this have to do with group actions?)

One way to proceed is to let X be the set of seven room keys; we can call them

$$X = \{A, B, C, D, E, F, G\}.$$

The structure on X is that there are two pairs of keys that go to double rooms; say for example that the keys $\{A, B\}$ and $\{C, D\}$ are for these rooms. Mixing up the keys amounts to picking a permutation in $\Sigma(X)$ are random. Doing no harm amounts to picking a permutation that preserves the structure:

$$G = \text{permutations of } X \text{ preserving the pairs of double room keys.}$$

The probability of doing no harm is therefore equal to

$$\text{cardinality of } G/\text{cardinality of } \Sigma(X).$$

So what remains is to find a way to count the elements in each of these two groups. That's a great thing for you to think about, but I won't say more about how to do it now. The answers are 48 and 5040, so the chance of doing no harm is less than one percent.