Groups, Fields, and Vector Spaces

General Themes

- Avoid the appearance of accidents
- Find natural coordinates based on the intrinsic features of the problem. These will typically lead to more incisive analyses, and descriptions of the data that suggest generalization, not the specific features of the experiment, measuring devices, etc.
- Use appropriate mathematics: Everything in the lab is finite and discrete, but mathematical concepts and models typically involve infinities and continua. So the mathematical constructs should allow for a smooth transition between large but finite and infinite, and a smooth transition between sampled and continuous

Overview

Three kinds of mathematical structures

In order of increasing number of kinds of components:

- Groups: one kind of element, one operation
- Fields: one kind of element, two operations ("addition" and "multiplication")
- Vector spaces: two kinds of elements (vectors and scalars); scalars form a field, and operations that apply to (vector, vector) pairs and to (vector, scalar) pairs

A particularly interesting kind of vector space is the set of mappings from elements of a group to a field.

Structure-preserving transformations and natural coordinates

These are the key to identifying natural "coordinates." Here, "coordinates" is used in a very general way, essentially as "labels".

Structure-preserving transformations can be sought for groups, fields, or vector spaces. Structure-preserving transformations always form a group, in their own right. This is a useful way to understand the generic nature of groups, rather than some of the simpler examples (real numbers under addition), since these "simpler examples" often have properties that are not generic to groups.

We will look at structure-preserving transformations of certain vector spaces, and use them to identify particularly natural basis sets for the vector spaces. We will apply this to

vector spaces consisting of mappings from a group to a field. Fourier theory falls out from this.

Looking ahead: for a group $G = \mathbb{Z}_n$ (the integers, with addition as the group operation), we will get the discrete Fourier transform. For $G = \Re$ (the real numbers, with addition as the group operation), we will get the Fourier transform. For G ={rotations of a circle}, we will get Fourier series.

Other groups lead to other useful constructs, though we won't pursue them here. For example, with G ={rotations of a sphere}, we get spherical harmonics. With G ={permutations of *n* objects}, translations in Euclidean *n*-space, or translations and rotations in Euclidean *n*-space, we get other useful things.

Groups

Group axioms

A group is a set of elements *a*, *b*, …, along with an operation $\circ$ that is a mapping from a pair of elements to a third element, i.e. $a \circ b = c$ (formally, $\circ : G \times G \to G$), for which the following hold:

G1: Associativity: $a \circ (b \circ c) = (a \circ b) \circ c$.
G2: Identity: There is a special element $e \in G$ for which, for every *a* in *G*, $a \circ e = a$ and $e \circ a = a$.
G3: Existence of inverses. For every *a* in *G*, there is a corresponding group element a^{-1} for which $a \circ a^{-1} = e$ and $a^{-1} \circ a = e$.

Other properties that many groups have, but are not required:

The group operation need not be commutative (i.e., satisfy $a \circ b = b \circ a$). A commutative group is also called an Abelian group.

A group may have a finite or an infinite number of elements.

An infinite group may, or may not, have a notion of "nearness" of elements. A group which has a notion of nearness (appropriately defined) is called a Lie group. (The notion of "nearness" must be preserved by the group operation. That is, if *a* is near *b*, then $a \circ c$ must be near $b \circ c$ (and similarly for $c \circ a$ and $c \circ b$).

A set that satisfies G1 but not G2 or G3 is a "semigroup". You can always make it satisfy G2 by adding an identity element, if it doesn't already have one.

Examples of groups

Some examples of groups in which the group operation is familiar addition or multiplication

- The (positive and negative) integers $\mathbb{Z}$, $\circ$ is ordinary addition
- The rational numbers $\mathbb{Q}$, $\circ$ is ordinary addition
- The real numbers $\Re$, $\circ$ is ordinary addition
- The complex numbers $\mathbb{C}$, $\circ$ is ordinary addition
- $\mathbb{Q}$, $\Re$, or $\mathbb{C}$ with 0 omitted, $\circ$ is ordinary multiplication
- $m \times n$ matrices with entries drawn from $\mathbb{Z}$, $\mathbb{Q}$, $\Re$, or $\mathbb{C}$, $\circ$ is matrix addition
- $m \times m$ invertible matrices with entries drawn from $\mathbb{Q}$, $\Re$, or $\mathbb{C}$, $\circ$ is matrix multiplication

Some examples of groups in which the group operation is the composition of transformations:

- Rotations of a regular *k*-gon
- Rotations of a circle (limiting case of the above, "$k \to \infty$")
- Rotations and reflections of a regular *k*-gon
- Rotations and reflections of a circle
- Translations along a line
- Translations and rotations in Euclidean *n*-space
- Rotations of an *n*-sphere
- Permutations of a set of *n* objects

Which of the above are commutative?
Are any of the above abstractly identical?
Which of the have an infinite number of elements? Of those, which have a notion of "nearness"?

Some basic group properties

We're doing this not just to provide "practice" with the group axioms, but also because of what they mean.

There is only one identity element. For if *e* and *f* were both identitiy elements, then
$e \circ f = e$ by G2, since *f* is an identity
$e \circ f = f$ by G2, since *e* is an identity
from which it follows that $e = f$.

An element can have only one inverse. For if $a \circ b = e$, then
$b = e \circ b$ by G2, since *e* is the identity

$b = (a^{-1} \circ a) \circ b$ by G3, since a^{-1} is an inverse of a
$b = a^{-1} \circ (a \circ b)$ by G1
$b = a^{-1} \circ e$ since we assumed that $a \circ b = e$
and hence,
$b = a^{-1}$ by G2, since e is the identity.

No element can have a "private" left or right identity. In other words, if an element f is an identity for some group element a, then it is the identity e for all of the group. For if $a \circ f = a$ (f is a "right identity"), then
$f = e \circ f$ by G2, since e is the identity
$f = (a^{-1} \circ a) \circ f$ by G3
$f = a^{-1} \circ (a \circ f)$ by G1
$f = a^{-1} \circ a$ since we assumed that f was a private identity for a, i.e., $a \circ f = a$,
and hence,
$f = e$, i.e., f is the group identity. (A similar argument works if we had assumed $f \circ a = a$, i.e., that f is a "left identity"). Another consequence of this (that we will use below) is that if $f \circ f = f$, then $f = e$. This is because $f \circ f = f$ means that f is a "private: identity for f.

The group operation is one-to-one. That is, if $a \circ c = b \circ c$, then $a = b$. This, essentially, allows us to "cancel." Equivalently, if $x \circ z = y$, then $x = y \circ z^{-1}$
To show this: if $a \circ c = b \circ c$, then
$(a \circ c) \circ c^{-1} = (b \circ c) \circ c^{-1}$, then
$a \circ (c \circ c^{-1}) = b \circ (c \circ c^{-1})$ by G1,
$a \circ e = b \circ e$ by G3
$a = b$ by G2

The inverse of the product is the product of the inverses, in reverse order. To show this, we need to show that $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$, i.e., that $(a \circ b) \circ (b^{-1} \circ a^{-1}) = e$.
$(a \circ b) \circ (b^{-1} \circ a^{-1}) = \left((a \circ b) \circ b^{-1}\right) \circ a^{-1} = \left(a \circ (b \circ b^{-1})\right) \circ a^{-1}$, each step by G1
$\left(a \circ (b \circ b^{-1})\right) \circ a^{-1} = (a \circ e) \circ a^{-1} = a \circ a^{-1} = e$, by G3, G2, and G3.

Intrinsic properties of group elements

The "order" of a group element a is the least (nonzero) integer n for which an n-fold product $a \circ a \circ \ldots \circ a$ is the identity, i.e., $a^n = e$. Note that associativity means that we don't have to specify how to put parentheses around $a \circ a \circ \ldots \circ a$; any way of doing it gives the same answer.

For finite groups, every element has a (finite) order. To see this, consider the series $a^0 = e$, a^1, a^2, a^3,…. Since the group is finite, eventually it must repeat. So say $a^m = a^n$. Then (assuming $m < n$),
$a^m = a^n$ implies
$e = (a^m)^{-1} \circ a^m = (a^m)^{-1} \circ a^n = (a^m)^{-1} \circ (a^m \circ a^{n-m}) = \left((a^m)^{-1} \circ (a^m)\right) \circ a^{n-m} = a^{n-m}$
so the order of *a* is at most $n - m$.

We can do better than this: for a finite group, the order of a group element is a factor of the size of the group. Here, size means number of elements, $\#(G)$.

We show this by showing something more general. First, define a subgroup: a subgroup of a group *G* is a subset of *H* of *G* that is, in its own right, a group. (Similarly: subfield, subspace, etc.) Note that the associativity law is automatic, so what must be shown is that *H* is closed under the group operation, and that it contains the identity (of *G*), and inverses of everything in itself.

Note also that if *a* is an element of *G*, and *n* is its order, then $H = \left\{e, a, a^2, \ldots a^{n-1}\right\}$ is a subgroup of *G*, and $\#(H) = n$. (Check: what is the group operation table for *H*? are inverses always in *H*?) *H* is also known as a "cyclic" group.

So if we can show that the size of every subgroup is a factor of the size of the group, then we will have also shown that the order of every element is a factor of the size of the group.

We'll show this (that $\#(H)$ is a factor of $\#(G)$) by a counting argument: we will divide *G* up into pieces, each of which have the same size as *H*. The pieces are "cosets": for any element *b* in *G*, the coset *Hb* are all of the elements *g* of *G* that can be written in the form $g = h \circ b$, for some element *h* in *H*.

Every element in *G* is in some coset: *g* is in the coset *Hg*, since $g = e \circ g$, and the identity, *e*, is in *H*.

So we now have to show that the cosets, are non-overlapping. That is, either two cosets are disjoint, or they are identical. Say *Hb* and *Hc* are two cosets that are not disjoint. Then there is at least one element in common, i.e., for some h' and h'' $h' \circ b = h'' \circ c$. This means that $b = (h')^{-1} \circ h'' \circ c$. Now we can see that every element in *Hb* is contained in *Hc*: A typical element $g = h \circ b$ is also
$g = h \circ \left((h')^{-1} \circ h'' \circ c\right) = \left(\left(h \circ (h')^{-1}\right) \circ h''\right) \circ c$ (after several applications of the associative law); the latter shows that *g* is also in *Hc*.

So *G* is a disjoint union of cosets of any subgroup *H*. So its size must be a multiple of the size of *H*.

Several notes, in order of increasing importance to us:

Here we used "right cosets". We also could have used "left cosets" *bH*. Note that a left coset *bH is* not necessarily the same as the right coset *Hb*. A left coset and a right coset can overlap but not be identical.

We can use facts about the order of group elements as an elementary way to establish the possibilies for the structure of groups of a given size. For prime numbers *p*, there is only one group (abstractly) that has size *p*, namely, the group generated by an element of order *p*. Can think of this as the rotations of a *p*-gon. Other possibilities of course for non-prime sizes, see homeworks for a few.

We used a counting argument here, and counting arguments won't work for infinite groups. But the notion of "disjoint union" does work. Similarly, summing over a group (for a finite group) turns into averaging over a group (for an infinite group).

This basic idea above – cosets –is a model for building larger structures out of smaller ones, Think of *G* as a space, *H* as a special plane in *G* that runs through the origin, and the cosets of *H* as planes that are parallel to *G*.

Relationships among groups: homomorphisms

A (group) *homomorphism* is a **structure-preserving map** between two groups. Formally: if *G* and *H* are groups (*H* not necessarily a subgroup of *G*), then $\varphi : G \to H$ is a mapping from *G* to *H* for which

$\varphi(g_1 \circ g_2) = \varphi(g_1) \circ \varphi(g_2)$. Note that on the left side of the equation, $\circ$ is the group operation in *G*; on the right, $\circ$ is the group operation in *H*.

An *onto* homomorphism φ (a.k.a. "surjective" homomorphism) is a homomorphism from *G* and *H* for which all members of *H* are some $\varphi(g)$.

An *isomorphism* is an "onto" homomorphism φ from *G* to *H* if there is also an "onto" homomorphism $\varphi^{-1} : H \to G$, for which $\varphi^{-1}(\varphi(g)) = g$ (and also, $\varphi(\varphi^{-1}(h)) = h$).

An *automorphism* is an isomorphism from a group *G* to itself.

Each of these can also be defined in an analogous fashion for other algebraic structures, such as fields and vector spaces.

Examples of homomorphisms

The log is a homomorphism from $\Re > 0$ (with $\circ$ as multiplication) to $\Re$ (with $\circ$ as addition).

$\varphi(n) = 2n$ is a homomorphism from $\mathbb{Z}$ (with $\circ$ as addition) to $\mathbb{Z}$ (with $\circ$ as addition).

$\varphi(n) = -n$ is a homomorphism from $\mathbb{Z}$ (with $\circ$ as addition) to $\mathbb{Z}$ (with $\circ$ as addition).

$\varphi(z) = e^z$ is a homomorphism from $\mathbb{C}$ (with $\circ$ as addition) to nonzero elements of $\mathbb{C}$ (with $\circ$ as multiplication)

The parity of a permutation is a homomorphism from any permutation group (with $\circ$ as composition) to $G = \{+1, -1\}$ (with $\circ$ as multiplication). Briefly, the "parity" of a permutation is defined as follows. Any permutation can be built from a sequence of pairwise swaps. If the number of pairwise swaps is even, the parity is +1. If the number of pairwise swaps is odd, the parity is -1. (One needs to show that this is in fact well-defined. We'll do that much later.)

Which of these are onto? Which are isomorphisms? Which are automorphisms?

The kernel

The kernel of a homomorphism $\varphi : G \to H$ is the set of elements of *G* for which $\varphi(g) = e_H$. Here, e_H is the identity for *H*. (Unfortunately, there is no obvious relationship to other uses of the term "kernel".)

The kernel of a homomorphism is always a subgroup. It's obviously a subset, so we need to show that G2 and G3 hold.

To show G2 (that there is an identity), we need to show that e is in the kernel. That is, we need to show that $\varphi(e)$ is the identity for *H*. $\varphi(e) = \varphi(e \circ e) = \varphi(e) \circ \varphi(e)$. So $\varphi(e) = e_H$, since it is the "private" identity for $\varphi(e)$.

To show G3 (that if *g* is in the kernel, then so is g^{-1}), we need to show that $\varphi(g) = e$ implies that $\varphi(g^{-1}) = e$. To do this:
$e_H \circ \varphi(g^{-1}) = \varphi(g) \circ \varphi(g^{-1}) = \varphi(g \circ g^{-1}) = \varphi(e) = e_H$. (Second equality uses the fact that a homomorphism is structure-preserving, last equality uses what we just showed, that $\varphi(e) = e_H$.

Objects playing several roles: automorphisms

We now show how the set of automorphisms of a group *G* can in turn be considered a group, which we will call $A(G)$. We need to define the group operation in $A(G)$, which must take a pair of automorphisms to a third. We'll use composition. (Here, we will use

$\circ$ to denote the group operation in $A(G)$, and justaposition (e.g., gh) to denote the group operation in G.) Formally, to define $\varphi_1 \circ \varphi_2$, we need to define how it acts on an element of G, and to show that this definition of $\varphi_1 \circ \varphi_2$ is itself an automorphism: $\varphi_1 \circ \varphi_2(g) = \varphi_1(\varphi_2(g))$.

To show that this is an automorphism:

$\varphi_1 \circ \varphi_2(gh) = \varphi_1(\varphi_2(gh))$ (by the definition of the group operation in $A(G)$)
$= \varphi_1(\varphi_2(g)\varphi_2(h))$ (since φ_2 is a homomorphism)
$= \varphi_1(\varphi_2(g))\varphi_1(\varphi_2(h))$ (since φ_1 is a homomorphism)
$= (\varphi_1 \circ \varphi_2(g))(\varphi_1 \circ \varphi_2(h))$ (by the definition of the group operation in $A(G)$, applied to each factor)

We next need to show that this operation leads to a group structure on $A(G)$. Associativity follows from the fact that the operation is a composition. The presence of an identity in $A(G)$ follows from the fact that the trivial map from G to itself is an automorphism (but not an interesting one). The presence of inverses in $A(G)$ follows from the fact that an automorphism has an inverse (since it is an isomorphism).

A special set of automorphisms: the "inner" automorphisms. For any element α in G, let's look at the map $\varphi_\alpha(g) = \alpha g \alpha^{-1}$. It's easy to see that φ_α is an automorphism of G: It preserves structure:
$\varphi_\alpha(gh) = \alpha(gh)\alpha^{-1} = \alpha(g\alpha^{-1}\alpha h)\alpha^{-1} = (\alpha g \alpha^{-1})(\alpha h \alpha^{-1}) = \varphi_\alpha(g)\varphi_\alpha(h)$.

To see that the "inner" automorphism group contains identities and inverses (as automorphisms), we need to see how inner automorphisms compose:
$(\varphi_\alpha \circ \varphi_\beta)(g) = \varphi_\alpha(\varphi_\beta(g)) = \varphi_\alpha(\beta g \beta^{-1}) = \alpha\beta g \beta^{-1}\alpha^{-1} = \alpha\beta g(\alpha\beta)^{-1} = \varphi_{\alpha\beta}(g)$
so
$\varphi_\alpha \circ \varphi_\beta = \varphi_{\alpha\beta}$ (where the subscript on the right is the group operation in G).
As a consequence, $(\varphi_\alpha)^{-1} = \varphi_{\alpha^{-1}}$, i.e., φ_α is invertible and its inverse is also an inner automorphism.

We can think of the "inner" automorphisms as a model for change of coordinates.

Summing up: For any group G, we have a group of automorphisms $A(G)$, and a homomorphism from G into a subgroup of $A(G)$, the "inner" automorphisms: This mapping, the adjoint map, $Adj : G \to A(G)$, takes a group element α into the inner automorphism φ_α. The action of φ_α on G is defined by $\varphi_\alpha(g) = \alpha g \alpha^{-1}$.

What is the kernel of *Adj*? Say γ is in the kernel of *Adj*. This means that φ_γ is the identity transformation on *G*. That is, $\varphi_\gamma(g) = g$ for all *g* in *G*. That is, $\gamma g \gamma^{-1} = g$ for all *g* in *G*.Or, $\gamma g = g\gamma$. In other words, the kernel of *Adj* is the set of elements γ in *G* that commute with all elements in *G*. (This is known as the "center" of *G*).

If *G* is commutative (i.e., everything commutes), the center of *G* is *G* itself, and *Adj* is trivial – in other words, all inner automorphisms are the identity. But there may still be some nontrivial members of $A(G)$.

Examples of automorphisms, inner automorphisms, etc.

$\mathbb{Z}$ (with $\circ$ as addition): It is commutative, so all inner automorphisms are trivial. But $\varphi(n) = -n$ is an automorphism (that is nontrivial, and not an inner automorphism).

Invertible $m \times m$ matrices: For generic matrices *M*, $\varphi_M(G) = MGM^{-1}$ is a nontrivial inner automorphism. The center of the group of invertible $m \times m$ matrices, i.e., the matrices that commute with all others, and therefore lead to the trivial inner automorphisms, are multiples of the identity matrix.