

COPYRIGHT NOTICE:

A. Ash & R. Gross: Fearful Symmetry

is published by Princeton University Press and copyrighted, © 2008, by Princeton University Press. All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from the publisher, except for reading and browsing via the World Wide Web. Users are not permitted to mount this file on any network servers.

Follow links for Class Use and other Permissions. For more information send email to: permissions@press.princeton.edu

PART ONE

*Algebraic
Preliminaries*

*Preliminaries
Algebraic*

PART ONE

*Chapter 1 Introduction***REPRESENTATIONS***Road Map*

To start our journey, we discuss the basic concept of *representation* from a formal point of view. This is the key concept underlying the number-theoretic methods of *Galois representations* that are our goal. To flesh out the abstract formalism, we go through an example: The ordinary act of counting can be viewed as a representation of sets. So we give (or review) mathematical definitions of *sets*, *functions*, *morphisms*, and *representations*, which will be with us for the whole book.

The Bare Notion of Representation

Before we narrow our focus to mathematical concepts, we start by discussing the general concept of a representation. In philosophy, the concept of one thing representing or misrepresenting another thing is a central concern. The distinction between truth and appearance, the thing-in-itself and its representation, is a keynote of philosophy. It plays a critical role in the works of such figures as Plato, Kant, Schopenhauer, and Nietzsche. Generally speaking, for these philosophers the “appearance” of something is thought to be an impediment or veil, which we wish to penetrate through to the reality acting behind it. But in mathematics, matters stand somewhat differently.

Consider, in an abstract way, the relationship that occurs when one thing represents another. Say B represents A . We have three

terms that stand together in some kind of relationship: A , B , and the fact that B represents A . We can call this fact X . It is important to remember that, in a representation, the three terms A , B , and X are usually distinct.

For example, A may be a citizen of Massachusetts, B her state representative, and X the legal fact that B represents A by voting in the legislature on her behalf. Or, to jump ahead, A may be an abstract group, B a group of matrices, and X a morphism from A to B . (We will define these terms later.)

It can happen, though, that $A = B$. For instance, B may be said to (also) represent herself in the state legislature. Or A may be a group of matrices and B the same group of matrices. But whether $A = B$ or $A \neq B$, we call these relationships “representations.”¹ Note that the fact of representation, X , is always going to be different from A and B , because A and B are objects and X is a fact of representation.

Now, what would be a good picture of A , B , and X ? We can view X as an arrow going from A to B . This captures the one-way quality of the relationship, showing that B is representing A , not vice versa:

$$A \longrightarrow B.^2$$

We can abstract even further, if we do not want to name A and B and we just want to visualize their relationship. We can picture them with dots. Then the picture of a representation becomes

$$\bullet \longrightarrow \bullet$$

which is the ultimate in abstraction. The dots are just placeholders for the names of the objects. The two dots can stand for two different objects or the same object. The dot or object from which the arrow emanates is called the *source* of that arrow, and the dot or object to which the arrow goes is called the *target* of that arrow.

In normal life, if A represents B , B and A can be very different kinds of things. For instance, a flag can represent a country, a

¹It may not seem to make sense for an object to represent itself, or it may seem like the best, most exact possible representation. Mathematicians do not take sides in this debate. We just agree to call it a representation even when A represents itself.

²It *could* happen that, at the same time, A also represents B , and we would picture that as $B \longrightarrow A$. But this is a different representation from the previous one. Its “fact of representation” Y is not equal to X .

slogan on a T-shirt can represent an idea, and a mental image can represent a beloved person. In mathematics, the situation is different. All the mathematical entities we encounter or invent are considered to be on the same plane and have the same degree and type of reality or ideality: They are all mathematical entities.

What are representations used for? They explain one thing by means of another. The object we want to understand is the “thing”: the thing-in-itself, the source. The object that we know quite a bit about already, to which we compare the source via a representation, we call the *standard object*. It is the site of appearance, the target.

Our conventions might not correspond to your expectations. The target, the object at the head of the arrow, is the piece of the picture that we understand better. We will derive information about the source by using properties of both the arrow and the target.

An Example: Counting

We look at the simplest possible example, one that goes back to prehistory: counting. Suppose we have a sack of potatoes or a flock of sheep. We want to know how many potatoes or sheep we have.

This is a much more sophisticated question than knowing whether they are the same in number as another sack of potatoes or another flock of sheep. We start with the less sophisticated question. Suppose we want to know whether the flock of sheep being herded home this evening is the same size as the herd we let out to the pasture in the morning. In the morning, we put a small pebble in our pouch for each sheep as it went out of the fold. Now we take a pebble out of the pouch as each sheep returns to the fold.

We were careful to make sure the pouch was empty in the morning before we began, and careful not to put anything in or take anything out during the day. So if the pouch becomes empty exactly as the last sheep comes in, we are happy. A mathematician says that we have demonstrated the existence of a *one-to-one correspondence* from the sheep in the morning to the sheep in the evening.

To make this mathematically precise, we make two definitions:

DEFINITION: A *set* is a collection of things, which are called the *elements* of the set.³

For example, the collection of all odd numbers is a set, and the odd number 3 is an element of that set.

DEFINITION: A *one-to-one correspondence* from a set A to a set B is a rule⁴ that associates to each element in A exactly one element in B , in such a way that each element in B gets used exactly once, and for exactly one element in A .

Digression: Definitions

A mathematician uses the term “definition” in a way that might be surprising to nonmathematicians. The *Oxford English Dictionary* defines “definition” as “a precise statement of the essential nature of a thing.” Mathematicians agree that a definition should be “precise,” but we are not so sure about capturing the “essential nature.” Our definition of one-to-one correspondence above will let you recognize a one-to-one correspondence if one is shown to you. Suppose that A is the set {red, blue, green} and B is the set {1, 2, 3}. Then a one-to-one correspondence between the two sets is given by

red \rightarrow 1

blue \rightarrow 2

green \rightarrow 3.

You can check that this associates to each element of the set A a different element of the set B , and that each element of the set B is used once.

³A set may be described by listing all of its elements between curly braces, so that $\{1, a, b\}$ is the set with the three elements 1, a , and b . A set may also be described using a qualifier preceded by a colon, so that $\{x : x > 0 \text{ and } x \text{ is real}\}$ is the set of all positive real numbers.

⁴By “rule,” we mean any definite means of association. It need not be given by a formula. For example, it can be given by a list that tells which sheep in the morning and in the evening were counted by the same pebble.

Our definition of one-to-one correspondence, however, does not tell you the “essential nature” of a one-to-one correspondence. We have given you no clue why you should care about one-to-one correspondences, nor does our definition tell you how to make a one-to-one correspondence.

Even when a mathematical definition technically has all of the properties listed by the *OED*, it often strikes nonmathematicians as unusual. A mathematical definition can redefine a commonly used word to mean something else. For example, mathematicians refer to “simple” groups, which are in fact not particularly simple. They define the words “tree” and “quiver” in ways that have nothing to do with oaks and arrows.

Sometimes a mathematician defines an object in terms of its properties, and only then proves that an object with these properties exists. Here is an example: The *greatest common divisor* of two positive integers a and b can be defined to be a positive number d so that:

1. d divides a .
2. d divides b .
3. If c is any other number that divides both a and b , then c divides d .

With this definition, it is not obvious that the greatest common divisor exists, because there might not be any number d that satisfies all three properties. So right after making the definition, it should be proved that a number with the properties outlined actually exists.

Counting (*Continued*)

In our example, each pebble corresponded to one sheep in the morning and one sheep in the afternoon. This sets up the rule that associates to each morning sheep the afternoon sheep that shared its pebble. This rule is a one-to-one correspondence under the conditions of our story.

But we do not need to know any set theory, nor what a one-to-one correspondence is, to count sheep in this way. In fact, we do

not even need to know how to count! In a book about Sicily in the 1950s (Dolci, 1959), a young shepherd boy was interviewed who did not know how to count:

I can't count, but even when I was a long way away, I could see if one of my goats was missing. I knew every goat in my herd—it was a big herd, but I could tell every one of them apart. I could tell what kid belonged to what mother. . . . The master used to count them to see if they were all there, but I knew they were all there without counting them.

You can see that for the shepherd boy, counting was not necessary. Nor is it required if we want to sell our flock for one dollar a sheep. We just pair up the dollars and the sheep. And in the case of two sacks of potatoes, we can take one potato out of each sack and throw the pair of potatoes over our shoulders. We repeat until one sack is empty. If the other sack is also empty, we have confirmed that there were the same number of potatoes in each sack to begin with.

Counting Viewed as a Representation

But if there are thousands of potatoes, or if we want to keep a record, or tell someone far away how many sheep we have, something else needs to be done, involving language—in this case, mathematical language. The flock of sheep is our “thing,” our *source object*. For a target, we need a standard object that we know how to count in a standard way. This is the series of counting words, for example, in English, “one, two, three, . . .” As each sheep enters the fold, we count it with the next word in the series, and the last counting word that we utter is the number of sheep.

Again we have made a one-to-one correspondence, but this time with a standard object, so we have something to write home about. The folks at home have the same standard, so they will know how to interpret our report. (If we report our result to people who do not know the English counting words, they will not know how many sheep we have.)

In the case of the two sacks of potatoes, if we use the tossing-over-our-shoulders method, when we are done we will know whether the sacks contained the same number of potatoes or not, but the place will be strewn with potatoes and we will not know what that number is. If instead we use counting words, we can count the potatoes one sack at a time, neatly, and then compare the answers.

The Definition of a Representation

A one-to-one correspondence is an example of a *function* and of a *morphism*. We will be using these terms throughout this book. We will take a stab at defining them now, and refine and amplify the definitions as we continue.

DEFINITION: A *function* from a set A to a set B is a rule that assigns to each element in A an element of B . If f is the name of the function and a is an element of A , then we write $f(a)$ to mean the element of B that is assigned to a . A function f is often written as $f : A \rightarrow B$.

DEFINITION: A *morphism* is a function from A to B that captures at least part of the essential nature of the set A in its image in B .

We must be intentionally vague in this chapter about the way that a morphism “captures the essential nature” of A , mostly because it depends on the nature of the entities A and B . When we use the word “morphism” later in the book, our source A and target B will both be groups. After we have defined “group” in chapter 2, we will revisit the idea of a “morphism of groups” in chapter 12.

Some people may think “morphism” is an ugly word, but it is the standard mathematical term for this concept. The longer word “homomorphism” is also used, but we will stick with the shorter version. It derives from the Greek word for “form,” and we view the “essential nature” captured by a morphism as the “form” of A .

There are many kinds of functions, but the most useful ones for us are the morphisms from a source to a well-understood standard target. We will call this a *representation*. It is implicit that the target we choose is one that we know a lot about, so that from our knowledge that there is a morphism, and better yet our knowledge of some additional properties of the morphism, we can obtain new knowledge about the source object.

DEFINITION: A *representation* is a morphism from a source object to a standard target object.

Counting and Inequalities as Representations

Going back to the counting example, we think about finite sets—for example, {sun, earth, moon, Jupiter} or {1, Kremlin, π } or any set that contains a finite number of items. This collection of finite sets contains the special sets {1}, {1, 2}, {1, 2, 3}, and so on. In the context of counting, given any two finite sets A and B , a morphism is a one-to-one correspondence from A to B . A representation in this case is a morphism from the source (a given finite set, e.g., the set of sheep in your flock) to the target, which must be one of the special sets {1}, {1, 2}, {1, 2, 3}, and so on. The special property that we demand of the morphisms in the context of counting is that they should be one-to-one correspondences. For example, if you have a flock of exactly three sheep for your source, a representation of that flock *must* have {1, 2, 3} as its target. Thus, the “essential nature” of the source that is preserved by the morphism, *in this context*, is the number of elements it contains.

There are a lot of possible morphisms— $n!$ to be exact, where n is the number of elements in the source and target.⁵ When we are counting the number of elements in a set, we do not actually care about *which* morphism we grasp onto. But there is no choice about the target: it is {1, 2, 3, . . . , n } if and only if n is the number of elements in our source.

⁵The notation $n!$, pronounced “ n factorial,” means the product of all of the numbers from 1 through n . For example, $5!$ is $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$. For an exercise, you can find the six possible one-to-one correspondences from the set {red, blue, green} to the set {1, 2, 3}.

We could alter the counting process, and stipulate that a morphism be a one-to-one correspondence from the source to a *subset* of the target. But that would allow us to count the three oranges on our desk as “19, 3, 55,” for example, which is useless.

Or is it? If that is our count, then we know that there are three oranges, because $\{19, 3, 55\}$ is a set of three numbers. But how do we know how many numbers are in the set $\{19, 3, 55\}$? We still have to count them, so this technique has not helped us.

Suppose that we require the count to go in order of size. Then the above example is invalid, but “3, 19, 55” is valid. As always, knowing the last number in the count is the point. In this case, we would then know that the source has *at most* 55 objects. This leads to the concept of *less than or equal*. We could now generate the science of inequalities by using this kind of morphism.⁶

Summary

If A represents B , we have three things: two objects, A and B , which from now on will be sets, and the relation between them, which from now on will be a morphism. When A and B have some additional “structure”—e.g., they are *finite* sets, or *ordered* sets—and we restrict the possible morphisms from A to B to have something to do with that structure—e.g., morphisms must be one-to-one correspondences, or order-preserving functions—then the existence of a representation from A to B gives us some information about A in terms of the standard object B —e.g., we can find out how many elements are in A , or at most how many elements are in A . Another example of adding structure to a set, allowing a more profound study of that set, is given by the sets of permutations to which we will add a *group structure*; see chapter 3.

In this book we explore some very explicit examples of representations. The things we consider are always mathematical objects such as sets, groups, matrices, and functions between them. We

⁶For a nice discussion of counting and its extension to infinite sets, see *One, Two, Three . . . Infinity* (Gamow, 1989).

show you how this works in detail in one particular case that we develop throughout the book and that gets us to our goal: mod p linear representations of Galois groups. We explain how these representations help to clarify the general problem of solving systems of polynomial equations with integer coefficients, and how they can sometimes lead to definitive results in this area.

Besides the representations discussed in this book, there are many other kinds of representation theories used today in mathematics. Representation theory is often needed to formulate interesting problems, as well as to solve them.