QUOTIENT SPACES

MATH 433, KEN BROWN

1. Introduction

Quotients are ubiquitous in modern algebra. A familiar example is the construction of $\mathbb{Z}_n$, the set of integers mod n. Informally, $\mathbb{Z}_n$ is obtained by taking the set $\mathbb{Z}$ of ordinary integers and identifying n with 0. This identification, of course, forces us to make others. If $n = 3$, for example, we must identify -1 with 2 because $-1 = 2 - 3$; we express this identification by writing $-1 \equiv 2 \bmod 3$ and saying -1 is *congruent* to 2 mod 3. In general, we construct $\mathbb{Z}_n$ by identifying two integers a, b whenever $a - b$ is a multiple of n, in which case we write $a \equiv b \bmod n$. Let's spell out what it means to "identify" two integers. A reference for what follows is Appendix A.3 of your text.

2. Equivalence relations

Congruence mod 3 (or mod any fixed integer n) has the same formal properties as equality:

- reflexivity: $a \equiv a$.
- symmetry: $a \equiv b \implies b \equiv a$.
- transitivity: $a \equiv b$ and $b \equiv c \implies a \equiv c$.

A relation with these three properties is called an *equivalence relation*. As we will see, there is then a sensible way to "identify" equivalent elements, i.e., to regard them as equal.

Given a set X with an equivalence relation $\equiv$, an *equivalence class* is a set of the form

$$E_x := \{y \in X : y \equiv x\}$$

for fixed $x \in X$. For example, congruence mod 3 on $\mathbb{Z}$ yields three equivalence classes: $E_0 = \{\dots, -3, 0, 3, 6, \dots\}$, $E_1 = \{\dots, -2, 1, 4, 7, \dots\}$, and $E_2 = \{\dots, -1, 2, 5, 8, \dots\}$. More briefly, the three sets are $3\mathbb{Z}$, $1 + 3\mathbb{Z}$, and $2 + 3\mathbb{Z}$. Note that there are many other names for these sets. For instance, $E_1 = E_4 = E_{-2} = -2 + 3\mathbb{Z} = \cdots$. You might find it helpful to plot the integers using three different colors to represent the three equivalence classes.

As illustrated by this example, it is always true that X is partitioned into equivalence classes; in other words, every $x \in X$ belongs to a *unique* equivalence class, namely, E_x. You should check this as an exercise or see Appendix A.3 of the text. The *quotient* of X by the equivalence relation is the set Y of equivalence classes. Read that sentence again: Y is a set whose elements are sets. Picture the equivalence classes as boxes; then Y is the set of these boxes. Putting equivalent elements into the same box is the mathematical mechanism for "identifying" them.

Date: August 2000.

In the case of $\mathbb{Z}$ with the relation of congruence mod 3, the quotient is denoted $\mathbb{Z}_3$ and called the set of integers mod 3. It is a set whose three elements are the sets $3\mathbb{Z}$, $1+3\mathbb{Z}$, $2+3\mathbb{Z}$.

3. Operations on quotients

We do arithmetic in $\mathbb{Z}_3$ by doing operations on representative integers. For example, to compute the sum of two equivalence classes A, B, choose representatives $a \in A$ and $b \in B$ and form the sum $c = a + b$. Then c is in a unique equivalence class C, and we define $A + B = C$. For example,

$$(1+3\mathbb{Z}) + (2+3\mathbb{Z}) = (3+3\mathbb{Z}) = 3\mathbb{Z}.$$

It's customary to label the equivalence classes by our favorite representatives $0, 1, 2$ and to write, for instance, $1 + 2 = 0$ in $\mathbb{Z}_3$. When we write this, of course, we are really thinking, "$1 + 2 = 3$, which is in the same box as 0."

Our definition of addition requires some justification, since it is potentially ambiguous. How do we know we get the same box C no matter which representatives a, b we choose? What has to be checked is that addition is compatible with congruence:

$$a \equiv a' \text{ and } b \equiv b' \implies a + b \equiv a' + b'.$$

You can check this in your head or on scratch paper.

Similar remarks apply to multiplication, and we obtain a rigorous construction of the field with three elements. It would be a good exercise to verify that $\mathbb{Z}_3$ satisfies the field axioms (associativity, commutativity, etc.) as a *formal consequence* of the fact that these properties hold in $\mathbb{Z}$. The only exception is the existence of multiplicative inverses, which doesn't hold in $\mathbb{Z}$ but which happens to hold in $\mathbb{Z}_3$ (but not in $\mathbb{Z}_4$).

4. Quotient vector spaces

We now replace $\mathbb{Z}$ by a vector space V and $3\mathbb{Z}$ by a subspace $W \subseteq V$. We wish to construct a *quotient space* V/W in which all the vectors in W get identified with the zero-vector. By analogy with the number theory example, we define a relation of "congruence mod W" on V by declaring that

$$\mathbf{v} \equiv \mathbf{w} \iff \mathbf{v} - \mathbf{w} \in W.$$

You should be able to check that this is an equivalence relation. The equivalence classes are the *affine subspaces* (also called *flats*) $\mathbf{v} + W$. For example, if $V = \mathbb{R}^2$ and W is a 1-dimensional subspace (line through the origin), then the equivalence relation partitions $\mathbb{R}^2$ into a family of parallel lines.

The quotient space V/W defined by congruence mod W has one element for each affine subspace $\mathbf{v}+W$. You can visualize it by imagining a subspace W' orthogonal to W, cutting across these affine subspaces and giving a set of representatives for them. Think of V/W as obtained by collapsing each affine subspace $\mathbf{v} + W$ to a single point, represented by the intersection of $\mathbf{v} + W$ with W'. How would you visualize V/W if $V = \mathbb{R}^3$ and W is 1-dimensional?

So far V/W is just a set. To make it a vector space, we proceed as in Section 3, by choosing representatives. Concisely, the definitions read

$$(\mathbf{v} + W) + (\mathbf{w} + W) := (\mathbf{v} + \mathbf{w}) + W, \qquad a(\mathbf{v} + W) := a\mathbf{v} + W.$$

One must check that these operations are well-defined, independent of the choice of representatives $\mathbf{v}, \mathbf{w}$. Once we've done this, it becomes a routine matter to verify that V/W satisfies the axioms for a vector space.

5. Conclusion

If you've never seen quotients before, this construction might seem quite strange. For now, just view it as an exercise in abstract thinking. Later we will see many situations where quotients arise naturally.

6. Exercises

We continue the notation of Section 4: V is a vector space (over an arbitrary field) and W is a subspace.

1. Verify that congruence mod W is an equivalence relation and that the equivalence classes are the affine subspaces $\mathbf{v} + W$.

2. Prove that addition and scalar multiplication in V/W are well-defined.

3. What's the zero-vector in V/W?

4. If V has finite dimension n and W has dimension k, prove that V/W has dimension $n - k$. [Hint: Start with a basis for V that contains a basis for W.]

5. (extra credit) Discuss root adjunction from the point of view of quotients. [Hint: Given a field F, the set $F[x]$ of polynomials with coefficients in F can be viewed as obtained from F by adjoining a new element x, subject to no relations. If we're trying to create a root of a given polynomial f, we want to identify $f(x)$ with 0.]