How To Make Rings That Do Terrible Things

1. Counterexample Constructions

Suppose you want to construct a ring that does something very specific and terrible. Often the easiest way to do this is to start with the integers, throw in a bunch of extra elements, and then quotient out by relations that force the extra elements to act the way you want them to.

Definition: If X is a set of elements, then $\mathbb{Z}\langle X\rangle$ is the collection of objects of the form

$$\sum_{w\in\langle X\rangle} a_w w,$$

where $\langle X\rangle$ is the collection of noncommuting monomials with letters in X. Addition and multiplication are given by

$$\left(\sum_{w\in\langle X\rangle} a_w w\right) + \left(\sum_{w\in\langle X\rangle} b_w w\right) = \sum_{w\in\langle X\rangle} (a_w + b_w)w,$$

$$\left(\sum_{w\in\langle X\rangle} a_w w\right)\left(\sum_{w\in\langle X\rangle} b_w w\right) = \sum_{w\in\langle X\rangle}\left(\sum_{uv=w} a_u b_v\right) w$$

Example 1: Suppose I want to create a ring with a left zero-divisor that is not a right zero-divisor? I can take

$$\mathbb{Z}\langle x, y\rangle/(xy)$$

Example 2: If I want a ring with a left unit that is not a right unit, I can take

$$\mathbb{Z}\langle x, y\rangle/(xy - 1)$$

Example 3: If I want a ring with a left unit that is also a right zero divisor, I can take

$$\mathbb{Z}\langle x, y, z\rangle/(xy, zx - 1)$$

2. Now Hold On Just A Second There...

Okay, I'm lying. That third example totally doesn't work. If we have $xy = 0$ and $zx = 1$, then we have

$$y = (zx)y = z(xy) = 0,$$

so our relations accidentally cllapsed y to zero, and we didn't actually create the ring we thought we'd created. But what about our first two examples? Do they actually work? How can we tell when our construction goes through properly?

Related Question: Let R be a ring in which, if $2x = 0$ and $3x = 0$, then $x = 0$. Suppose a, b, c, and $(a + b + c)$ are all idempotent[1] Does it follow that $ab = 0$?

Here's one way to think about this problem: I take the ring $\mathbb{Z}\langle a, b, c\rangle$ and I quotient out by the ideal

$$I = \left((a^2 - a), (b^2 - b), (c^2 - c), \left((a + b + c)^2 - (a + b + c)\right)\right).$$

Did I accidentally collapse ab to zero?

All of these qeustions come down to the same basic problem: Given a ring $\mathbb{Z}\langle X\rangle$ and a set of relations of the form $p = q$, how can we tell which elements become equal?

3. Reduction Systems

A **reduction system** S is a collection of ordered pairs $\sigma = (W_\sigma, f_\sigma)$, where $W_\sigma \in \langle X\rangle$ and $f \in \mathbb{Z}\langle X\rangle$.

For any $A, B \in \langle X\rangle$, and any $\sigma \in S$, we can define a **simple reduction** $r_{A\sigma B}$ from $\mathbb{Z}\langle X\rangle$ to itself, which takes the monomial $AW_\sigma B$ to $Af_\sigma B$, and fixes everything else. Notice that when we perform the simple reduction $r_{A\sigma B}$, essentially what we're doing is adding $A(f_\sigma - W_\sigma)B$. If we wanted to undo it, we would add $A(W_\sigma - f_\sigma)B$.

If r is any composition of simple reductions, then we will call it a **reduction**.

Notice: Given a reduction r, it is clear that for any $p, q \in \mathbb{Z}\langle X\rangle$, and any $n \in \mathbb{Z}$, we will have

$$r(np + q) = nr(p) + r(q)$$

We say a reduction r **acts trivially** on an element $p \in \mathbb{Z}\langle X\rangle$ if $r(p) = p$. We say p is **irreducible** under S if every reduction is trivial on p. We will write $\mathbb{Z}\langle X\rangle_{irr}$ to denote the irreducible elements of $\mathbb{Z}\langle X\rangle$.

A reduction r is said to be **final** on p if $r(p) \in \mathbb{Z}\langle X\rangle_{irr}$. We call p **reduction unique** if its image under any final reduction is the same. In this case, we will denote the common value $r_S(p)$.

What we would like to do is take our ideal I and use it to construct a reduction system S in which every element of $\mathbb{Z}\langle X\rangle$ is reduction unique. If we can do this, then to check whether two elements p and q of our ring $\mathbb{Z}\langle X\rangle/I$ are the same, all we have to do is check to see whether $r_S(p) = r_S(q)$.

4. Poooooset!

Example: Suppose we have a reduction system

$$S = \{(x^2, y + z), (y, -2z), (z, x)\},$$

and we start with the polynomial x^2. Then we can reduce in S to get the sequence

$$(x^2) \to (y + z) \to (-z) \to (-x^2) \to (-y - z) \to (x^2)$$

[1] An **idempotent** r is an element of a ring R satisfying $r^2 = r$.

Yeah... Notice that this does not appear to be doing much reducing. So we introduce a poset. Pooooset!

Let $<$ be a partial ordering on $\langle X \rangle$, satisfying

$$B \leq B' \Rightarrow ABC \leq AB'C$$

Then we say S is **compatible with** $<$ if for any $\sigma \in S$, any monomial M that appears in f_σ satisfies $M < W_\sigma$.

Now in our earlier example, assume that there had been a partial order $<$ compatible with S. We have

$$x^2 > y > z > x^2,$$

which is a contradiction. So the problem with our example is that S is actually not compatible with any partial ordering of $\langle X \rangle$.

5. Infinite Chains And Ambiguities

Let S be a reduction system, $<$ a partial ordering of $\langle X \rangle$ compatible with S. When we try to reduce our elements of $\mathbb{Z}\langle X \rangle$, there are two possible problems we can run into. The first problem arises when there is an element on which no reduction is final. We can avoid this by insisting that $<$ satisfy the **descending chain condition**. This says that any infinite descending chain in our poset must stabilize.

The other problem we could run into is a situation in which an element p of $Z\langle X \rangle$ has two final reductions r and r', with $r'(p) \neq r(p)$. This always occurs as the result of one of the following kinds of ambiguities:

Overlap Ambiguity: This occurs when I have monomials $A, B, C \in \langle X \rangle$, and elements $\sigma, \tau \in S$ with $W_\sigma = AB$ and $W_\tau = BC$. In this case, we can reduce ABC to either $f_\sigma C$ or Af_τ. We say that this overlap ambiguity is **resolvable** if there exist reductions r and r' with $r(f_\sigma C) = r(Af_\tau)$.

Inclusion Ambiguity: This occurs when I have monomials $A, B, C \in \langle X \rangle$, and elements $\sigma, \tau \in S$ with $W_\sigma = B$, and $W_\tau = ABC$. In this case, ABC can be reduced to either $Af_\sigma C$ or f_τ. We say that this inclusion ambiguity is **resolvable** if there exist reductions r and r' with $r(Af_\sigma C) = r'(f_\tau)$.

6. Finding Normal Forms In Quotient Rings

Theorem 1. *Let S be a reduction system on $\mathbb{Z}\langle X \rangle$ which is compatible with a partial order $<$ on $\langle X \rangle$, satisfying the descending chain condition. Let I be the ideal generated by the polynomials $(W_\sigma - f_\sigma)$, for all $\sigma \in S$. Then the following conditions are equivalent:*

a: *All ambiguities of S are resolvable.*

b: *All elements of $\mathbb{Z}\langle X \rangle$ are reduction-unique under S.*

c: *$\mathbb{Z}\langle X \rangle / I \cong \mathbb{Z}\langle X \rangle_{irr}$, where multiplication on $\mathbb{Z}\langle X \rangle_{irr}$ is given by*

$$r_S(p) r_S(q) = r_S(pq)$$

Proof. First we'll prove that **a** implies **b**. Assume that all ambiguities are resolvable relative to $<$. Let D be a monomial, and assume that all monomials $M < D$ are reduction-unique. We want to show that D is reduction-unique.[2]

Consider the collection of simple reductions on D. If there is more than one way to reduce D, then one of the following three things happens:

Case 1: $D = LABCM$, where $AB = W_\sigma$, and $BC = W_\tau$. Thus D can be reduced to $Lf_\sigma CM$ or to $LAf_\tau M$. Since this is an overlap ambiguity, and all ambiguities are resolvable, these will reduce to some common polynomial p. Since any monomial less than D is reduction unique, r_S is defined on all of these values, and

$$r_S(Lf_\sigma CM) = r_S(LAf_\tau M) = r_S(p)$$

Case 2: $D = LABCM$, where $B = W_\sigma$, and $ABC = W_\tau$. We resolve this in the same way.

Case 3: $D = LW_\sigma NW_\tau M$. This reduces to either $Lf_\sigma NW_\tau M$ or to $LW_\sigma Nf_\tau M$. However, these very clearly have a common reduction.

Thus any way we reduce D, we get a reduction-unique polynomial, and all these reduction-unique polynomials reduce to the same thing. Thus D is also reduction-unique. This means that all the monomials, and thus all the polynomials are reduction unique.

Now we will show that **b** implies **c**. Assume that the elements of $\mathbb{Z}\langle X\rangle$ are reduction-unique under S. Then we have a map

$$r_S : \mathbb{Z}\langle X\rangle \to \mathbb{Z}\langle X\rangle_{irr}$$

If we define a multiplication on $\mathbb{Z}\langle X\rangle_{irr}$ by $r_S(p)r_S(q) = r_S(pq)$, then r_S will automatically preserve multiplication. Now we consider addition. Since $p + q$ is reduction-unique, there is some reduction r such that

$$r(p + q) = r_S(p + q).$$

Since p is reduction unique, there is some reduction r' such that

$$r'r(p) = r_S(p).$$

Since q is reduction unique, there is some reduction r'' such that

$$r''r'r(q) = r_S(q)$$

Thus we have

$$\begin{aligned} r_S(p+q) &= r(p+q) \\ &= r'r(p+q) \\ &= r''r'r(p+q) \\ &= r''r'r(p) + r''r'r(q) \\ &= r_S(p) + r_S(q) \end{aligned}$$

Thus r_S is a homomorphism.

We'd like to prove that the kernel of this homomorphism is I. Suppose $p \in \ker(r_S)$. Then by a sequence of reductions, I can get p to be equal to zero. If I would like to run my sequence

[2]This will actually suffice, since DCC implies the existence of a smallest non-reduction-unique vertex.

of reductions in reverse, I will repeatedly add elements of the form $A(W_\sigma - f_\sigma)B$ to my polynomial. Thus my polynomial p must consist of a sum of elements of this form, and thus be in I.

This shows that $\ker(r_S) \subseteq I$. Now suppose I have an element p of I. Then p is the sum of elements of the form $q_1(W_\sigma - f_\sigma)q_2$, for $q_1, q_2 \in \mathbb{Z}\langle X\rangle$. There is a reduction that will send each of these to zero, so p must be in $\ker(r_S)$. Thus $\ker(r_S) = I$, and we have **c**.

Conversely, if we assume **c** and assume that some p can be reduced to either q or q' in $\mathbb{Z}\langle X\rangle_{irr}$. Then since $\mathbb{Z}\langle X\rangle_{irr}$ is closed under addition, we have $q - q' \in \mathbb{Z}\langle X\rangle$. And since we can get from q to q' through a sequence of reductions and inverse-reductions, the difference between the two must be some element of I. Thus $q - q' \in \mathbb{Z}\langle X\rangle_{irr} \cap I = \{0\}$. Thus p is reduction-unique. Thus we have **b**.

Now we have **a**⇒**b**⇔**c**. A moment's thought is enough to verify that if every element of $\mathbb{Z}\langle X\rangle$ is reduction-unique, then every ambiguity is resolvable. And this completes our proof.

□

7. Cool! We Have Normal Forms! Now What?

. **Example 1:** $\mathbb{Z}\langle x, y\rangle/(xy)$. We take $S = \{(xy, 0)\}$. There are no ambiguities, and so anything without an xy in it cannot be reduced. In particular $yx \neq 0$.

Example 2: $\mathbb{Z}\langle x, y\rangle/(xy - 1)$. We take $S = \{(xy, 1)\}$. Again no ambiguities, and so anything without an xy can't be reduced. In particular, $yx \neq 0$.

Example 3: $\mathbb{Z}\langle x, y, z\rangle/(xy, zx - 1)$. We take $S = \{(xy, 0), (zx, 1)\}$. We have an overlap ambiguity in the monomial zxy. This produces a new equation that must be satisfied $0 = y$, which means we need to throw $(y, 0)$ into our reduction system S to make the ambiguity resolvable. This is why we accidentally collapsed y to 0.

Related Question: $\mathbb{Z}\langle a, b, c\rangle/I$, where

$$I = \left((a^2 - a), (b^2 - b), (c^2 - c), \left((a + b + c)^2 - (a + b + c)\right)\right).$$

We start with the reduction system

$$S = \{(a^2, a), (b^2, b), (c^2, c), (ba, -ab - bc - cb - ac - ca)\}$$

This has four ambiguities:

$$aaa, bbb, ccc, baa, bba$$

The first three are easily resolved. The third takes work. More work than I have time to do in the course of this class. Exercise!

My Favorite Example:

$$\mathbb{Z}\langle a, b, c, d, x, y, v, w\rangle/((ax - by), (cx - dy), (cv - dw))$$

This is a noncommutative domain that cannot be embedded in a division ring. Ask me why!