1. Basic definitions

In the first week, I reviewed the basic definitions and rephrased them in a categorical framework. The purpose of this was two-fold. First, I wanted to make the preliminaries more interesting for those of you who already know the basic concepts. Second, I want students to feel more comfortable with category theory so that I can use it later to explain more difficult concepts.

1.1. Rings and endomorphisms.

First of all, an *additive group* is defined to be an abelian group in which the composition law is written as addition and the neutral element is called "0". When the group law is written as multiplication, it is called a *multiplicative group* whether or not it is abelian.

Definition 1.1. A *ring* is an additive group R together with a biadditive, associative multiplication law with unity. More precisely, a ring is: $(R, +, \cdot, 0, 1)$ where

(1) $(R, +, 0)$ is an additive group.
(2) $(R, \cdot, 1)$ is a monoid. I.e., multiplication is associative and has unit 1.
(3) Multiplication distributes over addition from the left and the right. I.e.,

$$a(b + c) = ab + ac \qquad (a + b)c = ac + bc$$

This condition is called *bi-additivity* since the multiplication mapping $(x, y) \mapsto xy$ is additive (a homomorphism) in each variable.

Lang allows $1 = 0$. I don't. But there is only one ring with this property, namely the zero ring, since any ring with $1 = 0$ has the property that

$$x = 1x = 0x = 0$$

for all $x \in R$.

To make a category we need homomorphisms.

Definition 1.2. If R, S are rings, a *ring homomorphism* $\phi : R \to S$ is a set mapping which is

(1) additive: $\phi(r + s) = \phi(r) + \phi(s)$
(2) multiplicative: $\phi(rs) = \phi(r)\phi(s)$
(3) unital: $\phi(1) = 1$.

I pointed out that the image of a ring homomorphism is a *subring* of S, i.e., a subset of S which is closed under addition, subtraction,

multiplication and contains 1. The *kernel* of ϕ is a (two-sided) *ideal* in R, i.e., a subset $I \subseteq R$ so that I is an additive subgroup of R and $RI = I = IR$.

One example of a ring is given by the endomorphism ring of any nonzero (!) additive group. If A, B are additive groups, then $\mathrm{Hom}_{\mathcal{A}dd}(A, B)$ is also an additive group where addition is defined pointwise:

$$(f + g)(x) = f(x) + g(x).$$

Here $\mathcal{A}dd$ is the category of additive groups and homomorphisms. In the case $A = B$, homomorphisms $f : A \to A$ are called *endomorphisms* of A and we write $\mathrm{End}(A) = \mathrm{Hom}(A, A)$. Being a Hom set, it is an additive group. But now we also have a composition law

$$\circ : \mathrm{End}(A) \times \mathrm{End}(A) \to \mathrm{End}(A).$$

The composition law distributes over addition on both sides for different reasons:

(1) Distributivity from the left comes from the fact that these are homomorphisms:

$$f(g + h)(x) = f(g(x) + h(x)) = fg(x) + fh(x) = (fg + fh)(x).$$

(2) Distributivity from the right comes from the definition of addition in $\mathrm{End}(A)$:

$$(f + g)h(x) = fh(x) + gh(x) = (fh + gh)(x).$$

Composition of mappings is always associative and the identity mapping acts as unity $id : A \to A$. Therefore, $(\mathrm{End}_{\mathcal{A}dd}(A), +, \circ, 0, id)$ is a ring (provided that $A \neq 0$).

The idea is that $\mathrm{End}(A)$ has addition and multiplication (given by composition) satisfying a list of conditions. *Rings* are subsets $R \subseteq \mathrm{End}(A)$ which has all of this structure. I.e., R is closed under addition, subtraction, multiplication and contains 0 and 1.

Question: If we start with a ring R then what is A?

Answer: We can take $A = (R, +)$, the underlying additive group of R. Then we have a ring monomorphism

$$\phi = \lambda : R \to \mathrm{End}(R, +)$$

given by $\phi(r) = \lambda_r$ which is left multiplication by r. This is an additive endomorphism of R by left distributivity:

$$\lambda_r(a + b) = r(a + b) = ra + rb = \lambda_r(a) + \lambda_r(b).$$

The additivity of the mapping $\phi = \lambda$ follows from right distributivity (in R):

$$\phi(r+s)(x) = \lambda_{r+s}(x) = (r+s)x = rx+sx = \lambda_r(x)+\lambda_s(x) = (\phi(r)+\phi(s))(x).$$

The fact that ϕ is multiplicative follows from the associativity of multiplication in R:

$$\phi(rs)(x) = (rs)x = r(sx) = \phi(r)\phi(s)(x).$$

The fact that ϕ is a monomorphism follows from the fact that 1 is a right unity:

$$(\forall x \in R)(\phi(r)(x) = 0) \Rightarrow \phi(r)(1) = r1 = r = 0.$$

The fact that $\phi(1) = 1$ follows from the fact that 1 is a left unity:

$$\phi(1)(x) = 1x = x.$$

Thus, all of the properties of a ring (the ones which involve the multiplication), are included in the statement that $\phi = \lambda : R \to \mathrm{End}(R, +)$ is a ring homomorphism.

1.2. **Modules.** When we think of R as being a subring of $\mathrm{End}_{\mathcal{A}dd}(A)$, the additive group A is called an R-module.

Definition 1.3. An *R-module* is an additive group M together with a ring homomorphism $\phi : R \to \mathrm{End}_{\mathcal{A}dd}(M)$.

This is usually stated in longhand as follows. For every $r \in R, x \in M$ there is $rx \in M$ with the following properties for all $r, s \in R$ and $x, y \in M$.

(1) $r(x + y) = rx + ry$ (I.e., $\phi(r)$ is additive, or equivalently, ϕ is a set mapping.)
(2) $(r + s)x = rx + sx$ (I.e., ϕ is additive.)
(3) $(rs)x = r(sx)$ (I.e., ϕ is multiplicative.)
(4) $1x = x$ (I.e., $\phi(1) = id = 1$.)

For example, R is an R-module and any left ideal in R is an R-module. (A *left ideal* is a proper additive subgroup $I \subset R$ so that $RI = I$.)