

1 What's a Ring

I dunno.



Definition 1.1. A ring $(R, +, \cdot)$ is an abelian group $(R, +)$ along with a second binary operation (\cdot) which is associative and distributive over addition. (and with 1).

Notation. Call the additive identity 0 and the multiplicative identity 1.

Proposition 1.2. $\forall r \in R,$

$$\begin{aligned} r \cdot 0 &= 0 \cdot r = 0 \\ r \cdot 0 &= r \cdot (0 + 0) = r \cdot 0 + r \cdot 0 \\ &\Rightarrow r \cdot 0 = 0 \end{aligned}$$

Fact. The additive inverse of r is $(-1 \cdot r)$

We sure are doing rings here. Man I love rings. Also, I learned about a new L^AT_EX package, check this out: **FAX FAX FAX** We've even got  and . lol.

So anyway:

Definition 1.3. We say a ring has *multiplicative cancellation* if $\forall b \neq 0$ and $a \cdot b = c \cdot b$ then $a = c$.

Example 1.4. This isn't always true. In fact, notice $\mathbb{Z}/6\mathbb{Z}$ does not have multiplicative cancellation.

Definition 1.5. $a \in R$ is a *zero divisor* if $\exists b \in R, b \neq 0$ such that $a \cdot b = 0$

Proposition 1.6 (The worst proposition). $a \in R$ is not a zero divisor iff $a : R \rightarrow R$ by $a(b) = a \cdot b$ is injective.

Definition 1.7. An *integral domain* is a non-zero commutative ring without zero divisors.

So which cyclic rings are integral domains? Well notice that when n is nonprime, $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain.

Now let's look at some really wacky rings.

Example 1.8. Take S a set, and let $\mathcal{P}(S)$ be the power set of S . We can make this a ring with $A \cup B \setminus (A \cap B)$ as addition. Then the additive identity of this ring is the empty set, and a set's inverse is the set complement.

Then we define multiplication (which will also turn out to be commutative) as $A \cdot B = A \cap B$, whose identity is the whole set, and whose distributivity is a bit trick to prove.

Hint: Try drawing a Venn diagram or two.

Here's another nasty one:

Example 1.9. Let R be a ring, and S be a set.

Then R^S is the function ring of functions $S \rightarrow R$, with $(f + g)(s) = f(s) + g(s)$ and $(f \cdot g)(s) = f(s)g(s)$. Then the additive identity is $f(s) = 0_R$ and multiplicative is $f(s) = 1_R$. Then this ring has zero divisors in the form of function pairs which take a nonzero value whenever the other takes zero.

Then something is a (left or right) unit if $\exists v$ such that $u \cdot v = 1$ (or visa-versa). A division ring is a ring where every non zero element is a two sided unit.

Definition 1.10. A *Field* is a non zero commutative ring where every nonzero element is a unit.

2 Polynomial Rings

Let R be a ring. then $R[x]$ is the set of polynomials in indeterminate x (consider only polynomials with finitely many terms). Then if $f = \sum a_i x^i$ and $g = \sum b_i x^i$, then $f + g = \sum (a_i + b_i) x^i$, and $fg = \sum_{k \in \mathbb{N}} \sum_{i+j=k} a_i b_j x^k$. This is a ring. Have fun checking this you fucks lmao. Now in the same vein, $R[[x]]$ is the ring of formal power series in R .

3 Ring Homomorphisms

Definition 3.1. A *homomorphism of rings* is a map φ which is homomorphic on both the addition and the multiplication, and takes the identity of one category to the other.

And naturally an isomorphism is a homomorphism with rings.

Now we can talk about the category of rings, RING. thank god. Then in this category, \mathbb{Z} is initial. namely, we can construct a homomorphism $\mathbb{Z} \rightarrow R$ which maps $1 \mapsto 1_R$, $-1 \mapsto -1_R$, and $m \mapsto \underbrace{1_R + \dots + 1_R}_{m \text{ times}} = m1_R$. Notice that the additive homomorphism falls

out trivially. Then in order to get multiplication in general, we need to get that

$$\begin{aligned} \varphi(m)\varphi(n) &= m1_R \cdot n1_R \\ &= m \cdot n1_R1_R = mn1_R \\ &= \varphi(m \cdot n). \end{aligned}$$

Corollary 3.2. *Ring homomorphisms take units to units.*

Now we give a particularly interesting example, despite the fact that rings on their own are boring as shit.

Example 3.3. $\mathbb{Z}[X_1, \dots, X_n]$, the set of polynomials in some number n of indeterminants, is the analogue of free groups. And in particular this can be verified using the category \mathcal{R}_A .