

Throughout we assume that  $R$  is a commutative ring with identity  $1 \neq 0$ .

1. Recall that  $S^{-1}R$  is defined to be the set of equivalence classes in  $R \times S$  with the equivalence relation  $(r, s) \sim (r', s')$  if there exists an element  $t \in S$  such that  $t(rs' - r's) = 0$ . Prove that the multiplication  $(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2)$  is a well-defined operation on  $S^{-1}R$ . Let  $(r, s) \sim (r', s')$  and choose  $t$  so that  $t(rs' - r's) = 0$ . Then we compute:

$$\begin{aligned}(r, s)(a, b) &= (ra, sb) \\ (r', s')(a, b) &= (r'a, s'b).\end{aligned}$$

I claim that  $(r'a, s'b) \sim (ra, sb)$ . Indeed,  $t(r'asb - ras'b) = t(r's - rs')ab = 0 \cdot ab = 0$ . So multiplication is well-defined on  $S^{-1}R$ .

2. Define  $\Phi$  to be the function which takes a subset of  $R$  to a subset of  $S^{-1}R$  in the following way:

$$\Phi(I) = \{(x, s) \mid x \in I, s \in S\}.$$

- Prove that if  $I$  is an ideal in  $R$ , then  $\Phi(I)$  is an ideal in  $S^{-1}R$ . Suppose that  $I$  is an ideal in  $R$ . Let  $(x, s), (y, s') \in \Phi(I)$  and  $(r, s'') \in S^{-1}R$ . By definition,  $x, y \in I$ . Then  $(x, s) + (r, s'')(y, s') = (xs' + sry, ss's')$  is in  $\Phi(I)$  since  $xs' \in I$  and  $sry \in I$ . Also  $(0, 1) \in \Phi(I)$  since  $0 \in I$ .
  - Prove that if  $P$  is a prime ideal that does not intersect  $S$ , and  $S$  has no zero divisors, then  $\Phi(P)$  is a prime ideal in  $S^{-1}R$ . Suppose that  $P$  is a prime ideal not intersecting  $S$  and that  $S$  has no zero divisors. Suppose that  $(x, s)(y, s') \in \Phi(P)$ . Then  $(xy, ss') \in \Phi(P)$ , i.e., there is an element  $r \in P$  such that  $(xy, ss') \sim (r, s'')$  for some  $s''$ . This implies there exists a  $t \in S$  such that  $t(xys'' - rss') = 0$ . Since  $S$  has no zero-divisors,  $xys'' = rss' \in P$  since  $r \in P$ . Since  $s'' \notin P$ , this implies  $xy \in P$ , so either  $x \in P$  or  $y \in P$ .
3. Suppose that  $S \subset R$  is a multiplicative set in  $R$ . Prove that the homomorphism  $\phi : R \rightarrow S^{-1}R$  is injective if and only if  $S$  contains no zero-divisors. Suppose that  $\phi$  is injective and that  $s \in S$  such that  $rs = 0$  for some  $r \in R$ .

$$\begin{aligned}(0, 1) &= \phi(0) \\ &= \phi(rs) \\ &= (rs, 1).\end{aligned}$$

Since  $s \in S$ , there is an element  $(1, s)$  in  $S^{-1}R$  with the property that  $(1, s)(s, 1) = (s, s) = (1, 1)$  (the latter equality due to the fact that  $t(s - s) = 0$  for any  $t$  we choose). Multiplying both sides of the equation by this element yields

$$\begin{aligned}(0, 1)(1, s) &= (r, 1)(s, 1)(1, 2) \\ (0, s) &= (r, 1).\end{aligned}$$

Hence,  $\phi(r) = 0$ , which implies  $r = 0$ . Thus,  $s$  is not a zero-divisor. Next, suppose that  $S$  has a zero divisor  $t$  such that  $tr = 0$  for some non-zero  $r \in R$ . Then I claim that  $(r, 1) = (0, 1)$  in  $S^{-1}R$ . Indeed,  $t(r \cdot 1 - 0 \cdot 1) = tr = 0$ . So  $\phi(r) = (r, 1) = 0$ . Hence,  $\phi$  is not injective.

4. Let  $p$  be a prime integer, and consider the ring  $R = \mathbb{Z}$ . Let  $S = \mathbb{Z} \setminus p\mathbb{Z}$ . The ring  $S^{-1}R$  is called the localization of  $\mathbb{Z}$  at  $p$ . Find all of the ideals of this ring, and describe the maximal ideal (there is only one). We proved in class that  $\Phi$  from problem 2 is a bijection between ideals in  $R$  not intersecting  $S$  and ideals in  $S^{-1}R$ . Let  $n\mathbb{Z}$  be an ideal in  $\mathbb{Z}$  such that  $n\mathbb{Z} \cap S = \emptyset$ . Then

$$\begin{aligned} n\mathbb{Z} \cap (\mathbb{Z} \setminus p\mathbb{Z}) &= \emptyset \\ \Rightarrow n\mathbb{Z} \setminus n\mathbb{Z} \cap p\mathbb{Z} &= \emptyset \\ \Rightarrow n\mathbb{Z} \setminus np\mathbb{Z} &= \emptyset \\ \Rightarrow n &= kp \exists k \in \mathbb{Z}. \end{aligned}$$

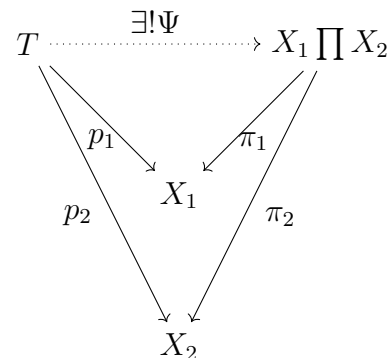
So the ideals in  $S^{-1}R$  are the ideals generated by a multiple of  $p$ . These are all contained in  $p\mathbb{Z}$ , so this is the unique maximal ideal.

5. This problem is to help us look ahead. Let  $\varphi(n)$  denote the number of units in  $\mathbb{Z}/n\mathbb{Z}$ . (From previous homework, we know this is the same as computing the number of integers  $1 \leq k < n$  that are relatively prime to  $n$ .)
- (a) Compute  $\varphi(p^k)$  when  $p$  is prime and  $k$  is a non-negative integer. Write the element  $m \in \mathbb{Z}/p^k\mathbb{Z}$  as  $\sum_{i=0}^{k-1} a_i p^i$  where  $a_i \in \{0, \dots, p-1\}$ . Then  $m$  is a unit if and only if  $a_0 \neq 0$ . This yields  $(p-1)p^{k-1}$  elements.
- (b) Compute  $\varphi(n)$  for  $n \in \{6, 10, 12, 18, 24, 36\}$  and make a conjecture about the relationship between  $\varphi(n)$  and the prime power decomposition of  $n$ . Good guess:  $\varphi(n) = \prod_i \varphi(p_i^{k_i})$  when  $n = \prod_i p_i^{k_i}$ .

Here I'll recall the universal property that defines a product, and introduce a new one that defines the coproduct.

**Definition:** Let  $X_1, X_2$  be objects in a category  $\mathcal{C}$ . Define  $X_1 \amalg X_2$  to be the object with the following universal property: There are morphisms  $\pi_i : X_1 \amalg X_2 \rightarrow X_i$  such that if there is any other object  $T$  with morphisms  $\varphi_i : T \rightarrow X_i$  for  $i \in \{1, 2\}$ , then there is a unique morphism  $\Psi : T \rightarrow X_1 \amalg X_2$  such that  $\pi_i \circ \Psi = \varphi_i$ .

This is conveniently captured in the diagram to the right, and is read to mean that you start with the object  $X_1 \amalg X_2$  and its morphisms to  $X_1$  and  $X_2$  set in stone. Any time there is an object  $T$  with morphisms as in the diagram, there is a morphism  $\Psi$  that can fill in that dotted arrow so that the diagram commutes, meaning any two ways to get to the same place produce the same morphism.

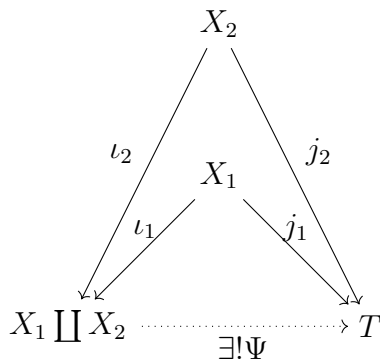


6. Prove that if  $R_1$  and  $R_2$  are rings, then the product ring  $\{(r_1, r_2) \mid r_1 \in R_1, r_2 \in R_2\}$  is actually the object  $R_1 \amalg R_2$ . I.e., verify that it satisfies the universal

property. Clearly we have maps  $f_i : R_1 \times R_2 \rightarrow R_i$  given by  $f_i(r_1, r_2) = r_i$ . Now suppose that  $T$  is a ring with homomorphisms  $p_i : T \rightarrow R_i$ . Then define  $\Phi : T \rightarrow R_1 \times R_2$  via  $\Phi(t) = (p_1(t), p_2(t))$ . We verify:  $\pi_i(\Phi(t)) = p_i(t)$ , so the diagram commutes. Furthermore, if  $f(t) = (f_1(t), f_2(t))$ , then  $\pi_i(f(t)) = f_i(t)$ , so in order for the commutativity to hold,  $f_i(t) = p_i(t)$ . Hence,  $\Phi = f$ , so  $\Phi$  is the unique morphism making the commutativity hold.

7. Consider now the category  $\mathcal{C}$  whose objects are positive integers and so that
- $$\text{Mor}_{\mathcal{C}}(n, m) = \begin{cases} \{m/n\} & \text{if } n \mid m \\ \emptyset & \text{otherwise} \end{cases}.$$
- Given two integers  $n, m$ , compute  $m \amalg n$  in this context (i.e., what integer has the desired universal property).

If you really like the last problem, awesome. You can try your hand at a new one. This is just for the superfans. Try to write what you think the universal property of the coproduct should be given just the diagram:



Then, compute  $m \amalg n$  for objects  $m, n$  in  $\mathcal{C}$ . Suppose that  $m, n \in \mathbb{Z}_{>0}$ . I claim that  $m \amalg n = \gcd(m, n)$ . First, since  $\gcd(m, n) \mid m$  and  $\gcd(m, n) \mid n$ , we have morphisms  $\pi_m : \gcd(m, n) \rightarrow m$  and  $\pi_n : \gcd(m, n) \rightarrow n$  (encoded as  $m/\gcd(m, n)$  and  $n/\gcd(m, n)$ ). Now suppose that there is an integer  $t$  and morphisms  $p_m : t \rightarrow m$  and  $p_n : t \rightarrow n$ . By definition, then,  $t \mid m$  and  $t \mid n$  (and they are encoded as  $m/t$  and  $n/t$ ). If this is the case, then  $t \mid \gcd(m, n)$ , so there is a morphism  $\Phi : t \rightarrow \gcd(m, n)$  (encoded as  $\gcd(m, n)/t$ ). Note that  $\pi_m \circ \Phi$  is encoded as  $(m/\gcd(m, n))(\gcd(m, n)/t) = m/t$  and similarly for  $n$ . Thus,  $\pi_\star \Phi = p_\star$ , and since the morphism sets here are singletons,  $\Phi$  is unique.