

- (1) The main mistake was in the implication (i) implies (iii), i.e. ACC implies maximal principle. A common argument was to take a nonempty set  $S$  of ideals and prove it's inductive by taking a chain and applying the ACC to it. Then, one applies Zorn's lemma. However, the ACC only applies to chains which are indexed by  $\mathbb{N}$ , which is insufficient to apply Zorn's lemma. For instance, consider the set

$$X = \{S \subseteq \mathbb{R} : S \text{ is countable}\}$$

with the  $\subseteq$  relation making it to a poset. This set surely has no maximal element. Indeed, for  $S \in X$  take some  $a \in \mathbb{R} - S$ , which exists as  $\mathbb{R}$  is uncountable. Then  $S < S \cup \{a\}$ , and  $S \cup \{a\}$  is still countable and is hence in  $X$ . However, if  $\mathcal{C} \subseteq X$  is a *countable* chain then  $\bigcup_{S \in \mathcal{C}} S$  is countable, as it's a countable union of countable sets. Thus, all countable chains have an upper bound, but Zorn's lemma fails here.

A better way to do this is by contraposition, where we consider a nonempty set  $S$  of ideals which has no maximal element. As  $S$  is nonempty, it contains some  $I_0$ . As  $S$  has no maximal element it contains some  $I_1 > I_0$ . As  $S$  has no maximal element it contains some  $I_2 > I_1$ . Continue recursively to find a sequence  $I_0 < I_1 < I_2 < \dots$ , contradicting the ACC. By the way, this uses the axiom of choice (or really, a weaker form called the axiom of dependent choice).

- (2) There weren't many mistakes made in this problem, so I'll just make some general suggestions.

For one, there were two main methods people used, the maximum principle or the ascending chain condition. I'd recommend knowing both methods. Morally they are the same proof, but before you believe this moral statement you ought to get evidence by seeing both sides. For the maximum principle, take the set of counterexamples and suppose it's nonempty. For the ACC, suppose there was an element  $r$  which is not a product of irreducible elements. As it is not irreducible, decompose it into a product  $r = r_0 r_1$  and iterate this procedure. That is, write  $r_0 = r_{00} r_{01}$  and  $r_1 = r_{10} r_{11}$ . Eventually this process will terminate, because of the ACC. That is, the leaves the binary tree I am constructing will end up being irreducible.

Another suggestion is to know where the hypothesis of  $R$  being a domain is used. A perfectly valid answer is that Prof. Elman only defines irreducible elements when in a domain, but it's worth considering why this is the case. I think one way this hypothesis was hidden in many people's proofs was that in a domain  $R$  with elements  $a$  and  $b$ , we have  $(a) = (b) \iff a = ub$  for a unit  $u \in R^*$ . The implication  $\Leftarrow$  holds in any ring, but the converse uses the cancellation property. Many proofs involved factoring some  $r$  in  $R$  as  $r = ab$  with  $a, b$  nonzero nonunits, and then concluding that  $(r) < (a)$  and  $(r) < (b)$ , but this is secretly using cancellation. Try to find a counterexample to  $\implies$  above in a nondomain!

Also, it's pretty cool that factorization is automatic in any domain, even though being a UFD is quite a unique property. It turns out that a Noetherian domain  $R$  is a UFD if and only if every nonzero minimal (under inclusion) prime is principal. Therein lies the key to the uniqueness in factorization. I don't remember how hard this is to prove (namely, you may need a result from commutative algebra called Krull's principal ideal theorem), but it's worth considering.

- (3) Not many mistakes here. I'll say first that in terms of algebraic geometry, if we take  $R$  to be  $\mathcal{O}(X)$  for some variety  $X$ , then this says any algebraic subset  $V(I)$  is contained in  $V(\mathfrak{p}_1 \dots \mathfrak{p}_n)$  for some prime ideals  $\mathfrak{p}_i$ . We have  $V(\mathfrak{p}_1 \dots \mathfrak{p}_n) = \bigcup V(\mathfrak{p}_i)$ . Hence, any algebraic subset is contained in a union of  $V(\mathfrak{p}_i)$ , which are "irreducible" algebraic subsets in the sense that they are not a union of two smaller algebraic subsets (equivalently, see the topological notion I describe in problem (4)). In fact, any algebraic subset is uniquely the union of irreducible algebraic subsets, as proven in (4).

An interesting class of rings related to this problem are Dedekind domains. One definition of a Dedekind domain is a Noetherian domain  $R$  which is not a field where all nonzero primes  $\mathfrak{p}$  are maximal and so that the localization  $R_{\mathfrak{p}}$  is a PID. Being a Dedekind domain implies that every nonzero ideal  $I$  can be uniquely factored as the product of prime ideals  $I = \prod \mathfrak{p}_i^{e_i}$ . As we will see in HW4, rings of the form  $\mathbb{Z}[\sqrt{d}]$  needn't be UFDs, which makes number theory difficult as factoring is typically a key technique. But so long as  $d$  is not 1 mod 4, these rings will be Dedekind domains, so if we can translate our problems into purely ideal-theoretic language, we can use unique factorization! In algebraic geometry, Dedekind domains appear as the coordinate rings of smooth curves.

- (4) Not many mistakes here. My main comment here is that the proof written here is exactly how you prove problem (2), assuming you used the maximal principle there. Similarly to (2), it's worth proving this result using ACC as well, in which case the proof you write down will be the same as if you proved (2) with the ACC.

Another application of the exact same technique is the following topological fact, which is critically used in algebraic geometry. First,

**Definition 0.1.** A topological space  $X$  is called Noetherian if it satisfies the descending chain condition on closed subsets.

One can prove (exactly as in (1)) that a space is Noetherian if and only if it satisfies the “minimal condition” on closed subsets. This condition is exactly opposite to the condition on ideals from the problem. The topological notion of irreducibility will, similarly, be the ideal-theoretic notion of irreducibility, but reversed.

**Definition 0.2.** A nonempty closed subset  $Y$  of a topological space  $X$  is called irreducible if  $Y = Z_1 \cup Z_2$  for  $Z_i$  closed in  $X$  implies that  $Y = Z_1$  or  $Y = Z_2$ .

With this set up, the proof of problems (2) and (4) directly yield the following:

**Theorem 0.1.** *Let  $X$  be a nonempty Noetherian topological space. Then  $X$  is a finite union of irreducible closed subsets.*

In algebraic geometry, this means that any variety is a finite union of irreducible varieties. Indeed, a variety  $X$  with the Zariski topology is Noetherian, as its coordinate ring  $\mathcal{O}(X)$  is Noetherian (by the Hilbert basis theorem). There is also a uniqueness statement if we insist none of the irreducible closed subsets contain each other.

One can probably phrase this as a general result on “Noetherian posets”, i.e. posets satisfying the ACC (equivalent in this generality to the maximal condition) which admits “joins”, i.e. the infimum of any two elements exists and is unique. I've never seen this myself, but it seems like a natural abstraction.

- (5) The only main issue I saw was not proving that whatever maximal ideal was written is not principal. Just because an ideal is written with two or more generators doesn't mean a sneaky element in the ideal cannot generate it! Consider, for instance, in  $\mathbb{Z}$  the result  $(n, m) = (\gcd(n, m))$ . This requires Bezout's identity, so you need a pretty sophisticated understanding of the arithmetic of  $\mathbb{Z}$  to get this principal generator. In the problem, you should take a maximal ideal like  $(2, x)$ , suppose that  $(f) = (2, x)$  and use that  $2 \in (f)$  and  $x \in (f)$  to derive a contradiction.

I also want to present first my personal belief on the most conceptually clear approach to checking maximality/primality, and then some interesting geometric interpretations/analogies of the fact that maximal ideal are not principally generated in this ring.

First, I think the best way to get maximal and prime ideals here is to define ring homomorphisms out of  $\mathbb{Z}[t]$ . In a previous discussion section, I explained that ring homomorphisms  $\mathbb{Z}[t] \rightarrow R$  are in one to one correspondence with elements of  $R$ . Every ring homomorphism  $\mathbb{Z}[t] \rightarrow R$  is of the form  $f(t) \mapsto f(r)$  for some unique  $r \in R$ . Think through what  $f(r)$  means and why this makes sense in  $R$ .

Given this, we can define a maximal ideal of  $\mathbb{Z}[t]$  by trying to surject it onto a field. The simplest field I can think of here is  $\mathbb{Z}/2\mathbb{Z}$ , so we try defining the map  $\mathbb{Z}[t] \rightarrow \mathbb{Z}/2\mathbb{Z}$  by sending  $t \rightarrow 0 + 2\mathbb{Z}$ . Check that this is onto with kernel  $(2, t)$  - proving maximality. Similarly, to find a prime but nonmaximal ideal, we need to surject  $\mathbb{Z}[t]$  onto a domain which is not a field. The simplest one here is  $\mathbb{Z}$ , and we can map  $\mathbb{Z}[t] \rightarrow \mathbb{Z}$  by, for instance  $t \rightarrow 17$ . This is into with kernel  $(t - 17)$ .

Generally, I think using maps is a great approach to ring theory. As for how to define maps, I think using “universal properties”, like the correspondence between maps  $\mathbb{Z}[t] \rightarrow R$  and elements of  $R$ , is the best. The other universal property you’ll want to use is that if  $f : R \rightarrow S$  vanishes on an ideal  $I \subseteq R$  then there is an induced map  $\bar{f} : R/I \rightarrow S$  sending  $r + I \mapsto f(r)$ . In fancy terms, the following commutes.

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ \downarrow & \nearrow \exists! \bar{f} & \\ R/I & & \end{array}$$

Often times the ring  $R$  we want to map out of will be a quotient of a polynomial ring by some ideal  $I$ , so we define a map out of it by choosing where the variables (generators) go and ensuring that the ideal  $I$  is sent to 0 (the relations are satisfied). By the way, if  $I$  is given by an explicit generating set  $S$ , we need only check that the elements of  $S$  are mapped to 0, so this is often not so bad. I’d suggest getting comfortable with this method, as well as the usage of the correspondence principle and the third isomorphism theorem. These are the heart of such ring theoretic computations.

Now, the geometric part. The key observation is that you can do basically the exact same thing here if you replace  $\mathbb{Z}$  with any PID  $R$  which is not a field. For instance, as a challenging exercise you can try determining all prime ideals of  $R[t]$  for  $R$  a PID. Consider  $R = \mathbb{C}[x]$  and  $R[y] = \mathbb{C}[x, y]$ . Given the edifice of algebraic geometry, maximal ideals of  $\mathbb{C}[x, y]$  are of the form  $(x - a, y - b)$  for a point  $(a, b) \in \mathbb{C}^2$ . We can consider the surjection  $\mathbb{C}[x, y] \rightarrow \mathbb{C}$  via  $f \mapsto f(a, b)$  and show that  $(x - a, y - b)$  is precisely its kernel to prove maximality.

To explain why such an ideal is not principal, consider some  $(f) \subseteq \mathbb{C}[x, y]$ . The corresponding variety  $V(f)$  will, intuitively, be one dimensional (a *curve*) if  $f$  is not zero ( $f = 0$  iff  $V(f) = \mathbb{C}^2$ ) or not a unit ( $f \in \mathbb{C}[x, y]^*$  iff  $V(f) = \emptyset$ ). You can think of this in terms of linear algebra - imposing a single linear constraint like  $2x + 3y = 0$  cuts down the dimension by 1. The same idea holds true in geometry, but you need to make a more subtle argument, perhaps reducing to the linear algebra by using tangent spaces. Try plotting some examples!

Anyways, given this dimension result, I see the reason maximal ideals in this ring are not principal as a manifestation of the clear geometric fact that points are not one dimensional. If

a maximal ideal  $\mathfrak{m} = (x - a, y - b)$  was principally generated by  $\mathfrak{m} = (f)$ , then the varieties they define would be the same. That is,  $V((x - a, y - b)) = V(f)$ , but the left hand side is the point  $(a, b)$  and the right hand side is a curve. To formalize this argument uses quite a lot of machinery (such as Krull's principal ideal theorem), but it's quite beautiful when it works out.

An incredible development in algebraic geometry and number theory arose in the mid 20<sup>th</sup> century which allowed geometric arguments like the above to be phrased elegantly for any commutative ring. This is the theory of “affine schemes”. Let's return to  $\mathbb{Z}[x]$ . Just as  $\mathbb{C}[x, y]$  is the ring of coordinate functions on  $\mathbb{C}^2$ , the machinery of schemes will allow us to view  $\mathbb{Z}[x]$  as the ring of functions on a very bizarre space called  $\text{Spec } \mathbb{Z}[x]$ . Much like the classical story with  $\mathbb{C}^2$  and  $\mathbb{C}[x, y]$ , the zero-dimensional points of  $\text{Spec } \mathbb{Z}[x]$  will correspond to maximal ideals of  $\mathbb{Z}[x]$ . We visualize  $\mathbb{Z}[x]$  as a two dimensional space, with one axis corresponding to  $x$  and another corresponding to  $\mathbb{Z}$ . This is like how we visualize  $\mathbb{C}^2$  as having one axis corresponding to  $x$  and another to  $y$ . We are replacing  $\mathbb{C}[x]$  by  $\mathbb{Z}$ !

This is far too vast of a story to explain here, so I'll leave you with David Mumford's drawing of  $\text{Spec } \mathbb{Z}[x]$ , often called his “treasure map”, seen below.

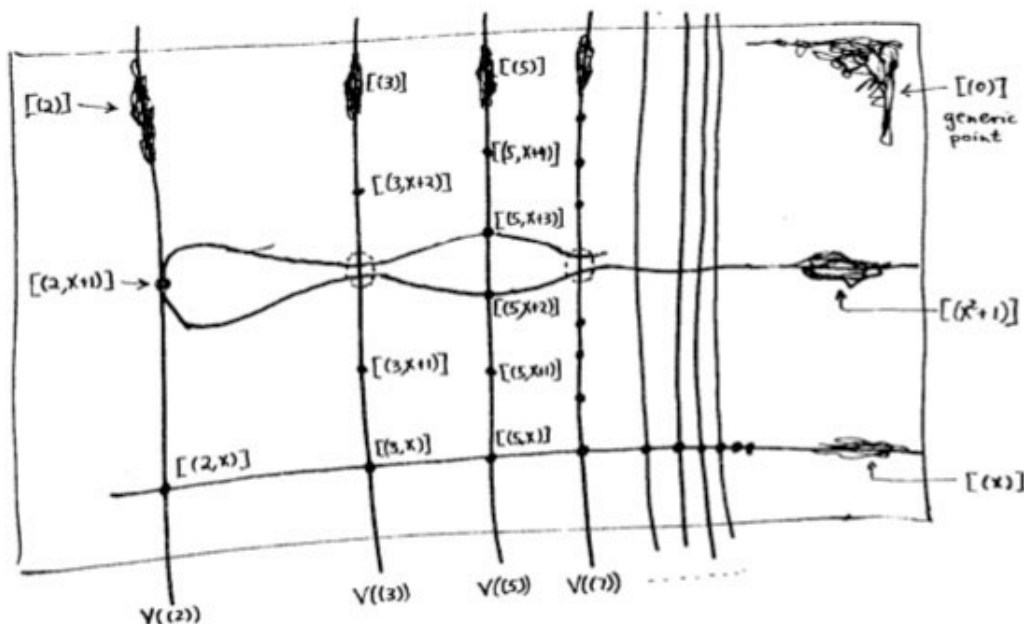


Figure 1: Mumford's “treasure map” depicting  $\text{Spec } \mathbb{Z}[x]$

To give a few details, when Mumford writes  $[I]$  for an ideal  $I \subseteq \mathbb{Z}[x]$ , he means the “vanishing set” of  $I$  in  $\text{Spec } \mathbb{Z}[x]$ , which we called  $V(I)$  when we were working with complex varieties. Notice the labels  $[(2, x)]$ ,  $[(3, x)]$ ,  $[(5, x)]$ ,  $[(3, x + 2)]$ , etc. at the zero-dimensional points of this space. These are maximal ideals in  $\mathbb{Z}[x]$ . Notice also that the one-dimensional curves in here are all given by a principal ideal - some are polynomials like  $(x)$  or  $(x^2 + 1)$  and others are prime numbers, like  $(2)$  or  $(5)$ . The same geometric proof above that explained why  $(x - a, y - b)$  was not principal in  $\mathbb{C}[x, y]$  can be ported over to this setting to prove that the maximal ideals in  $\mathbb{Z}[x]$ , such as  $(2, x)$  are not principal.

Given one of these labels, try to think about what the quotient of  $\mathbb{Z}[x]$  by that ideal is. Recall that in the classical setting, a variety  $Y = V(I)$  in  $\mathbb{C}^2$  has coordinate ring  $\mathbb{C}[x, y]/I$ . So for

instance, the leftmost vertical line (labeled  $[(2)]$ ) has “coordinate ring”  $\mathbb{Z}[x]/(2) \cong \mathbb{Z}/2\mathbb{Z}[x]$ . For instance,  $(2) = (1+i)^2$  as ideals in the Gaussian integers, and the intersection of the line  $V((2))$  with this curve looks sorta like  $y = x^2$ !

Similarly, the weird horizontal looking curve this (labeled  $[(x^2 + 1)]$ ) has “coordinate ring”  $\mathbb{Z}[x]/(x^2 + 1)$ , which is isomorphic to the Gaussian integers. Consider the intersection of that curve with the various vertical lines, labelled by the primes. Then try factoring these primes, 2, 3, and 5, in the Gaussian integers. So we can think of that as the affine line over the field  $\mathbb{Z}/2\mathbb{Z}$ , much like how we think of  $\mathbb{C}^1$  as the affine line over the field  $\mathbb{C}$  with its coordinate ring  $\mathbb{C}[x]$ .

All of this is meant to be tremendously vague, and all by analogy. Understanding it in detail is a significant undertaking, and if you have any questions about what this is or where to learn about it, ifeel free to ask me!

- (6) The main difficulty was in proving that all proper subgroups of  $\mathbb{Z}_{p^\infty}$  are of the form  $\langle \frac{1}{p^r} + \mathbb{Z} \rangle$  for  $r \geq 0$ . Most people had the right idea, but there were often some technical errors or skipped details, so I’ll try to explain how this proof should go.

Let  $H$  be a proper subgroup of  $\mathbb{Z}_{p^\infty}$ . To show that it is of the desired form, we must find a candidate in  $H$  that we will show generates it. Indeed, a cyclic group is generated by any element of maximal order in that group, so we will seek an  $x \in H$  of maximal order.

We must justify that such an element exists (for instance,  $\mathbb{Z}_{p^\infty}$  has no element of maximal order). To do so, we will first analyze what the elements of order  $p^r$  look like. Indeed, take some  $x$  of order  $p^r$ .  $x$  is representable as  $\frac{a}{b} + \mathbb{Z}$ . WLOG take  $a$  and  $b$  to be coprime. Then for  $x$  to have order  $p^r$  means in particular that  $p^r x = 0$  in  $\mathbb{Z}_{p^\infty}$ , i.e.  $p^r \frac{a}{b} \in \mathbb{Z}$ . As  $a$  and  $b$  are coprime, this means that  $b = p^e$  for some  $0 \leq e \leq r$ . But then  $p^e \frac{a}{b}$  is surely an integer, so  $p^e x = 0$  in  $\mathbb{Z}_{p^\infty}$ , proving that the order of  $x$  divides  $p^e$ . Hence,  $r = e$ , so the elements of  $\mathbb{Z}_{p^\infty}$  of order  $p^r$  are precisely those of the form  $\frac{a}{p^r}$  with  $a$  coprime to  $p$ . Thus, all the elements of  $\mathbb{Z}_{p^\infty}$  are in the group  $\langle \frac{1}{p^r} + \mathbb{Z} \rangle$ . It follows that this subgroup is exactly the set of elements of  $\mathbb{Z}_{p^\infty}$  with order at dividing  $p^r$ .

Now, suppose  $H$  contains elements of arbitrarily large order. Let  $x \in \mathbb{Z}_{p^\infty}$ . Then  $x$  has order  $p^r$  for some  $r \geq 0$ . Then by hypothesis, there is some  $N \geq r$  and some  $y \in \mathbb{Z}_{p^\infty}$  so that  $y$  has order  $p^N$ . Then  $p^{N-r}y$  has order  $p^r$  and thus lies in  $\langle \frac{1}{p^r} + \mathbb{Z} \rangle$ . So  $p^{N-r}y$  generates  $\langle \frac{1}{p^r} + \mathbb{Z} \rangle$ . As such,  $\langle \frac{1}{p^r} + \mathbb{Z} \rangle \subseteq H$ . Because  $x \in \langle \frac{1}{p^r} + \mathbb{Z} \rangle$  we have shown  $x \in H$  for all  $x \in \mathbb{Z}_{p^\infty}$ . This contradicts our hypothesis that  $H$  is proper in  $\mathbb{Z}_{p^\infty}$ .

So the orders of elements in  $H$  are bounded. Let  $x \in H$  be an element of  $H$  of maximal order  $p^r$ . Then  $x \in \langle \frac{1}{p^r} + \mathbb{Z} \rangle$ , and in fact generates this group, so  $\langle \frac{1}{p^r} + \mathbb{Z} \rangle \subseteq H$ . Every element of  $H$  has order dividing  $p^r$  and is hence in  $\langle \frac{1}{p^r} + \mathbb{Z} \rangle$ , so  $H \subseteq \langle \frac{1}{p^r} + \mathbb{Z} \rangle$ . Hence, all proper subgroups of  $\mathbb{Z}_{p^\infty}$  are of this form.

Onto the asides. For one, we can describe  $\mathbb{Z}_{p^\infty}$  using the correspondence principle for groups. Indeed, let  $\pi : \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z}$  be the quotient map. What is  $\pi^{-1}[\mathbb{Z}_{p^\infty}]$ ? By definition, it consists of the  $x \in \mathbb{Q}$  so that  $\pi(x) \in \mathbb{Z}_{p^\infty}$ . These are precisely the  $x \in \mathbb{Q}$  which can be written as  $a/p^r$  for some  $r \geq 0$ . That is,  $\pi^{-1}[\mathbb{Z}_{p^\infty}] = \mathbb{Z}[1/p]$ . So the correspondence principle says

$$\frac{\mathbb{Z}[1/p]}{\mathbb{Z}} = \mathbb{Z}_{p^\infty}$$

as subgroups of  $\mathbb{Q}/\mathbb{Z}$ . Elements of  $\mathbb{Z}[1/p]$  can be thought of as base  $p$  expansions where we allow (finitely many!) negative powers of  $p$ . That is, elements expansions of the form

$$\sum_{i=n}^m a_i p^i$$

for  $0 \leq a_i < p$  and  $n, m \in \mathbb{Z}$ . We can think of modding out by  $\mathbb{Z}$  as throwing out all the nonnegative powers of  $p$ , so the elements of  $\mathbb{Z}[1/p]/\mathbb{Z}$  are represented by expansions of the form

$$\sum_{i=n}^{-1} a_i p^i$$

with  $0 \leq a_i < p$  and  $n \leq -1$ . In other words, this is the base- $p$  fractional part! Using the decimal notation in base  $p$ , this is like truncating 1232.4331 to 0.4331 (say, in base 5).

Furthermore, the subgroup  $\langle \frac{1}{p^r} + \mathbb{Z} \rangle$  is equal to  $\frac{1}{p^r}\mathbb{Z}/\mathbb{Z}$  as subgroups of  $\mathbb{Q}/\mathbb{Z}$ . The isomorphism  $\frac{1}{p^r}\mathbb{Z}/\mathbb{Z}$  that most people gave can be thought of as multiplication by  $p^r$ . Formally, we can consider the isomorphism  $\mathbb{Q} \rightarrow \mathbb{Q}$  given by multiplication by  $p^r$ . By restriction, this yields an isomorphism  $\frac{1}{p^r}\mathbb{Z} \rightarrow \mathbb{Z}$ . The subgroup  $\mathbb{Z} \subseteq \frac{1}{p^r}\mathbb{Z}$  maps to the subgroup  $p^r\mathbb{Z} \subseteq \mathbb{Z}$  via this isomorphism, which in turn yields the isomorphism

$$\frac{\frac{1}{p^r}\mathbb{Z}}{\mathbb{Z}} \xrightarrow{\sim} \mathbb{Z}/p^r\mathbb{Z}$$

as desired.

In terms of base  $p$  decimal expansions, elements of  $\frac{1}{p^r}\mathbb{Z}$  are represented by finite base  $p$  expansions where there are at most  $r$  numbers after the decimal point.

We can also think of this group geometrically. Recall the isomorphism  $\mathbb{R}/\mathbb{Z} \rightarrow S^1$  via  $t + \mathbb{Z} \mapsto e^{2\pi it}$ .  $\mathbb{Q}/\mathbb{Z}$  is the set of torsion elements of  $\mathbb{R}/\mathbb{Z}$ , and corresponds to the elements of  $S^1$  with rational angle. For an integer  $n$ , we let  $S^1[n] = \{g \in S^1 : g^n = 1\}$ . This is the set of  $n^{\text{th}}$  roots of unity, which visually are the vertices of a regular  $n$ -gon inscribed in the unit circle with one vertex at 1. We let  $S^1[p^\infty] = \{g \in S^1 : g^{p^r} = 1 \text{ some } r\}$ . This is, of course,  $\bigcup_r S^1[p^r]$ , so you can imagine drawing a regular  $p$ -gon with vertex at 1 in the unit circle, then drawing a regular  $p^2$ -gon, then a regular  $p^3$ -gon, etc. The union of these vertices is  $S^1[p^\infty]$ . The exponential map yields an isomorphism  $\mathbb{Z}_{p^\infty} \rightarrow S^1[p^\infty]$ , and it's useful to think of this group additively and multiplicatively like this.

On another tangent, an interesting note about the last part is that as stupid as the multiplication in the last part is, it is in fact the only map  $\mathbb{Z}_{p^\infty} \times \mathbb{Z}_{p^\infty} \rightarrow \mathbb{Z}_{p^\infty}$  which satisfies the distributive law given the additive structure on this group. Indeed, suppose we had such a map. Consider the product

$$\left(\frac{1}{p^n} + \mathbb{Z}\right) \left(\frac{1}{p^m} + \mathbb{Z}\right)$$

We know nothing about what element in  $\mathbb{Z}_{p^\infty}$  this is, other than the hypothesis that this proposed multiplication distributes over addition. To get some addition in here, we'll write

$$\begin{aligned} \frac{1}{p^n} &= p^m \frac{1}{p^{n+m}} \\ \frac{1}{p^m} &= p^n \frac{1}{p^{n+m}} \end{aligned}$$

where as usual,  $p^m x$  means to add  $x$  to itself  $p^m$  many times. Thus, we can compute this product to be

$$\begin{aligned}
\left(\frac{1}{p^n} + \mathbb{Z}\right) \left(\frac{1}{p^m} + \mathbb{Z}\right) &= \left(p^m \frac{1}{p^{n+m}} + \mathbb{Z}\right) \left(p^n \frac{1}{p^{n+m}} + \mathbb{Z}\right) \\
&= p^{n+m} \left(\frac{1}{p^{n+m}} + \mathbb{Z}\right) \left(\frac{1}{p^{n+m}} + \mathbb{Z}\right) \\
&= \left(p^{n+m} \frac{1}{p^{n+m}} + \mathbb{Z}\right) \left(\frac{1}{p^{n+m}} + \mathbb{Z}\right) \\
&= \left(\frac{p^{n+m}}{p^{n+m}} + \mathbb{Z}\right) \left(\frac{1}{p^{n+m}} + \mathbb{Z}\right) \\
&= 0 \left(\frac{1}{p^{n+m}} + \mathbb{Z}\right) \\
&= 0
\end{aligned}$$

The elements  $\frac{1}{p^n} + \mathbb{Z}$  generate this group, so this shows that the product of any two elements must be 0 (again, use distributivity to prove this). So the only possible rng structure on  $\mathbb{Z}_{p^\infty}$  is the 0 multiplication!

My final aside for this problem is to ask a somewhat bizarre question. Can you determine the set of group homomorphisms  $\mathbb{Z}_{p^\infty} \longrightarrow S^1$ , where  $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ ? Actually, this set forms a group by pointwise multiplication. As a hint, use part (iii) of this problem to write

$$\mathbb{Z}_{p^\infty} = \bigcup_{r \geq 1} \left\langle \frac{1}{p^r} + \mathbb{Z} \right\rangle$$

A map out of a cyclic group like  $\left\langle \frac{1}{p^r} + \mathbb{Z} \right\rangle$  is wholly determined by where you send the generator, so long as you map it to something of order dividing  $p^r$ . Try to think about the generator of  $\left\langle \frac{1}{p^r} + \mathbb{Z} \right\rangle$ , and how these generators relate to each other as you go “up the tower” in this union.

If you’re curious why I want you to find maps into  $S^1$ , you can look up “Pontryagin duality”. This relates to a beautiful area of math, with critical importance to algebraic number theory, where you can do Fourier analysis on topological abelian groups! To say why this has anything to do with Fourier analysis, note that  $x \mapsto e^{2\pi i x}$  is a continuous group homomorphism  $\mathbb{R} \longrightarrow S^1$ . This is exactly the factor appearing in the Fourier transform over  $\mathbb{R}$ .