Math 210A, Fall 2017
HW 2 Solutions
Written by Dan Dore

(If you find any errors, please email ddore@stanford.edu)

Question 1. Let R be a commutative ring, and let $I = \{r \in R \,|\, \exists k > 0 \text{ such that } r^k = 0\}$.

(a) Prove I is an ideal.

(b) Prove I is the intersection of all the prime ideals of R.
You may use without proof the following fact, a consequence of Zorn's lemma: if S is a subset of R satisfying $0 \notin S$ and $S \cdot S \subset S$, then the set of ideals $J \subset R$ for which $J \cap S = \emptyset$ has a maximal element.

Solution. (a) Let $f_1, f_2, f \in I, a \in R$. Then we need to show that $f_1 + f_2 \in I$ and $af \in I$ for every such f_1, f_2, f, a. Since $f_1, f_2, f \in I$, there are k_1, k_2, k such that $f_1^{k_1} = f_2^{k_2} = f^k = 0$. Then, we have

$$(af)^k = a^k f^k = 0$$

so $af \in I$. We also have:

$$(f_1 + f_2)^{k_1+k_2} = \sum_{i=1}^{k_1+k_2} \binom{k_1 + k_2}{i} f_1^i f_2^{k_1+k_2-i} = 0$$

Note that for each i, either $i > k_1$ or $k_1 + k_2 - i > k_2$, so either $f_1^i = 0$ or $f_2^{k_1+k_2-i} = 0$.

(b) First of all, if $f \in I$, then $f^k = 0$ for some k. If $\mathfrak{p}$ is a prime ideal, then $f^k = 0 \in \mathfrak{p}$, so either $f \in \mathfrak{p}$ or $f^{k-1} \in \mathfrak{p}$ by the definition of a prime ideal. By induction, this implies that $f \in \mathfrak{p}$.

Conversely, let $x \in \bigcap \mathfrak{p}$. We want to show that $x^k = 0$ for some k. I'll give two proofs of this, with the first proof more concrete and the second one more conceptual - you should think about why they're **actually just the same proof**.

Proof (i): Otherwise, let's consider the set $S = \{x^k \mid k \in \mathbf{N}\}$. This doesn't contain 0 by hypothesis, and clearly $S \cdot S \subseteq S$. So, by the fact listed in the hint, we know that the set of ideals $J \subset R$ such that $J \cap S = \emptyset$ contains a maximal element J_0. To get a contradiction, we want to show that J_0 is prime, since by assumption $x \in \bigcap \mathfrak{p}$, the intersection of all prime ideals.

We know that J_0 is a proper ideal of R, since it does not contain the element x. So let $y, z \in R$ such that $yz \in J_0$. If $y \notin J_0$, then $J_0 + (y)$ is a strictly larger ideal than J_0. Since J_0 is maximal among ideals not containing a power of x, we know $J_0 + (y)$ must contain a power of x; so we have $x^m = ay + b$ with $a \in R, b \in J_0$. But then, we have $x^m z = ayz + bz \in J_0$, since $yz, b \in J_0$. Now consider the ideal[1]

$$Q = \{w \in R \,|\, x^m w \in J_0\}.$$

This ideal Q certainly contains J_0, so either it is equal to J_0 or it contains x^k for some k. For the latter to be true would mean that $x^{m+k} \in J_0$, contrary to hypothesis. So we must have $Q = J_0$. In particular, we have $z \in J_0$. This concludes the proof that J_0 is a prime ideal. But we have asssumed both that $x \notin J_0$ and that x is in every prime ideal, a contradiction.

[1] In Atiyah–Macdonald this Q is called an "ideal quotient" and would be written $(J_0 : (x^m))$.

Proof (ii): Let $S = \{x^k \mid k \in \mathbf{N}\}$, and form the ring $R[\frac{1}{x}] = S^{-1}R$. If $x^k \neq 0$ for any k, this is not the zero ring. (In general, a localization $S^{-1}R$ is the zero ring $\iff 0 \in S$: to have $1 = 0$ in $S^{-1}R$ means that $\frac{1}{1} = \frac{0}{1}$, which by our explicit construction happens iff there exists some $s \in S$ for which $s \cdot (1 \cdot 1 - 0 \cdot 1) = s$ equals 0.) Note that $\ell(x) = \frac{x}{1}$ is invertible in $R[\frac{1}{x}]$ by construction, so it is not contained in any proper ideals.

However, since $R[\frac{1}{x}] \neq 0$, it does have a maximal ideal $\mathfrak{m}$. Since maximal ideals are prime, $\mathfrak{m}$ is a prime ideal of $R[\frac{1}{x}]$. Now, let $\ell \colon R \to R[\frac{1}{x}]$ be the canonical map $r \mapsto \frac{r}{1}$, and consider the ideal $\ell^{-1}(\mathfrak{m})$. Since $\ell(x) \notin \mathfrak{m}$ we know that $x \notin \ell^{-1}(\mathfrak{m})$. However, for any homomorphism $f \colon A \to B$ of commutative rings and any prime ideal $\mathfrak{p}$ of B, the ideal $f^{-1}(\mathfrak{p})$ is a prime ideal of A.[2] [3] Therefore $\ell^{-1}(\mathfrak{m})$ is a prime ideal that does not contain x. This demonstrates that $0 \notin \{x^k\} \implies x \notin \bigcap \mathfrak{p}$, as desired.

[2] Proof 1: if $a_1 a_2 \in f^{-1}(\mathfrak{p})$, then $f(a_1 a_2) = f(a_1) f(a_2) \in \mathfrak{p}$ so by the fact that $\mathfrak{p}$ is prime, either $f(a_1) \in \mathfrak{p}$ or $f(a_2) \in \mathfrak{p}$, which is the same thing as saying $a_1 \in f^{-1}(\mathfrak{p})$ or $a_2 \in f^{-1}(\mathfrak{p})$. Also, $1 \notin \ell^{-1}(\mathfrak{p})$ since $\ell(1) = 1 \notin \mathfrak{p}$.

[3] Proof 2: $A/f^{-1}(\mathfrak{p})$ injects into $B/\mathfrak{p}$, which is a domain because $\mathfrak{p}$ is prime, so its subring $A/f^{-1}(\mathfrak{p})$ is a domain as well. These are really the same proof.

Question 2. Let $R = C^0([0,1])$ be the ring of real-valued continuous functions on the closed interval $[0,1]$. For every point $p \in [0,1]$, we obtain a maximal ideal $\mathfrak{m}_p = \{f \in R \mid f(p) = 0\}$.

Prove that *every* maximal ideal of R is of the form $\mathfrak{m}_p$ for a unique $p \in [0,1]$.

(Hint: You may wish to recall that $[0,1]$ is compact, which means that for any collection of open intervals covering it, there is some finite sub-collection that still covers it.)

Note that this means that you can recover the set $[0,1]$ just from the *ring* R.
(This actually works for any compact Hausdorff space, not just $[0,1]$; the proof is the same.)

(Optional, to think about: can you also recover the *topology* on $[0,1]$ from the ring R?)

Solution. Let $\mathfrak{m}$ be a maximal ideal of $R = C^0\left([0,1]\right)$, and assume that $\mathfrak{m} \neq \mathfrak{m}_x$ for any $x \in [0,1]$. Since $\mathfrak{m}$ is maximal, this means $\mathfrak{m} \not\subset \mathfrak{m}_x$, so for each $x \in [0,1]$ there is some $f_x \in \mathfrak{m}$ such that $f_x(x) \neq 0$. Since f_x is continuous, there is an open interval $U_x \subseteq [0,1]$ containing x such that $f_x|_{U_x}$ is non-vanishing. Then since for each $x \in [0,1]$, $x \in U_x$, we have $\bigcup_x U_x = [0,1]$; i.e. the U_x form an *open cover* of $[0,1]$. Since $[0,1]$ is compact, this has a finite subcover: there are $x_1, \ldots, x_n$ such that $[0,1] = \bigcup_{i=1}^n U_{x_i}$. That means that for any $x \in [0,1]$, at least one of the functions $f_{x_1}, \ldots, f_{x_n}$ is non-zero at x. Now, let

$$f = \left(f_{x_1}\right)^2 + \cdots + \left(f_{x_n}\right)^2$$

Since $f(x) = 0$ iff $f_{x_i} = 0$ for all i, this implies that $f(x) \neq 0$ for any $x \in [0,1]$. Therefore $g(x) = \frac{1}{f(x)}$ is well-defined and continuous on $[0,1]$, so f is invertible. But this is a contradiction since $f \in \mathfrak{m}$, a maximal ideal.

In fact, the map $x \mapsto \mathfrak{m}_x$ gives a *bijection* from $[0,1]$ to the set of maximal ideals of R. We just saw that this is surjective. To see that it is injective is easy in this setting: let $x \neq y$, and we want to show that $\mathfrak{m}_x \neq \mathfrak{m}_y$. But consider the function $f(t) = t - x$. This is certainly continuous on $[0,1]$, so it is an element of R. Since $f(x) = 0$ but $f(y) = y - x \neq 0$, $f \in \mathfrak{m}_x$ but $f \notin \mathfrak{m}_y$, so $\mathfrak{m}_x \neq \mathfrak{m}_y$.

We can actually also recover the *topology* of $[0,1]$ this way. For any $f \in R$, we get an open set $U_f := \{x \in [0,1] \mid f(x) \neq 0\}$. Under the bijection $x \mapsto \mathfrak{m}_x$, U_f corresponds to the set of maximal ideals which do not contain f (since every maximal ideal is of the form $\mathfrak{m}_x$, and $f \in \mathfrak{m}_x$ iff $f(x) = 0$ by definition). Now, let (a,b) be any open interval in $[0,1]$. We can pick some f such that $U_f = (a,b)$: for example, f could be a piecewise linear function which is the zero function on $[0,a] \cup [b,0]$ and positive elsewhere. (Draw a picture if you don't believe me!). Now, any open set in $[0,1]$ is a union of intervals, so any open set is a union of open sets of the form U_f. This means that U_f is a *basis* for the topology of $[0,1]$. In conclusion, if we were just handed the ring R and not told that it was a ring of continuous functions, we could construct the *topological space* $[0,1]$ out of R by taking as the underlying set the set of maximal ideals and defining a set to be open iff it is the union of sets of the form $U'_f = \{\mathfrak{m} \mid f \notin \mathfrak{m}\}$.

Our results apply to the following more general setting: Let X be a compact Hausdorff space, and let $R = C^0(X)$ its ring of continuous functions. Then for every $x \in X$, there is a maximal ideal $\mathfrak{m}_x$ of R consisting of functions that vanish at x. Again every maximal ideal of R is of this form — you can simply replace $[0,1]$ by X everywhere in the above argument to get this far (this needs only compactness of X). To get injectivity of the map $x \mapsto \mathfrak{m}_x$, and to see that we can recover the topology on X, we need the following lemma from topology:

Lemma 1 (Urysohn's Lemma)**.** If Z_1, Z_2 are disjoint closed subsets of a compact Hausdorff space[4] X, then there is a continuous, real-valued function $f \in C^0(X)$ such that $f|_{Z_1} \equiv 0$ and $f|_{Z_2} \equiv 1$.

First of all, the map $x \mapsto \mathfrak{m}_x$ from points of X to the set of maximal ideals of R is bijective. We just proved that it is surjective. To see that it is injective, let $x \neq y$ be two points of X. Since X is Hausdorff, $\{x\}$ and $\{y\}$ are closed, so there is some continuous function f such that $f(x) = 0$ and $f(y) \neq 0$. But this means that the set of functions vanishing at x is not the same as the set of functions vanishing at y, so $\mathfrak{m}_x \neq \mathfrak{m}_y$ (this is an abstract version of the argument we gave above).

Next, we can actually determine the topology of X via R by considering the open sets $U_f = \{x \in X \mid f \neq 0\}$ for various $f \in R$. This is a *basis* for the topology on X, which means that for any open set $V \subseteq X$ and any $x \in V$, there is some f such that $x \in U_f \subseteq V$. This says exactly that for any closed set Z ($Z = X \setminus U$) and any point $x \notin Z$, there is some continuous function f such that $f|_Z = 0$ and $f(x) \neq 0$, and this is another case of Urysohn's Lemma.

Note that since we established a bijection between the points of X and the maximal ideals in R, we can think of the topology generated by the U_f (i.e. the open sets are unions of U_f's; the fact that these form a basis says exactly that this topology is the given topology on X) as giving us a topology on the set of maximal ideals of R. This is called the *Zariski Topology*, and appears in algebraic geometry as well.

These remarks show us that there is a nice correspondence between compact Hausdorff spaces and certain kinds of rings. In fact, it's possible to go further and to characterize exactly which kinds of rings show up this way, and to prove that we actually get an equivalence of categories (a continuous map $X \to Y$ induces a ring homomorphism from $C(Y)$ to $C(X)$ by sending g to $g \circ f$).[5] An analogous (and easier) result in algebraic geometry says that there is an order-reversing equivalence of categories between the category of affine algebraic varieties over a field k and polynomial functions between them and the category of finitely generated k-algebras and maps of k-algebras. This fact is the starting point of modern algebraic geometry.

[4] more generally, X can be any space with the property that any two disjoint closed subsets have disjoint open neighborhoods

[5] To actually make this work, you need to replace real-valued functions with complex-valued functions and require the maps on the ring side to keep track of some additional structure, namely the norm and complex conjugation operation which come from the fact that the ring is an algebra of complex-valued functions. This structure on a ring is called a *C^*-algebra*, and this result is called *Gelfand Duality*. I have no idea if an analogous result can be made to work where we stick to real-valued functions, and if anyone does, I'd be curious to find out.

Question 3 (optional, replaces Q2)**.** [This question is very hard, **100% optional**, and cannot be done without material from outside this course.]

Let $R = C^\infty(S^1; \mathbf{C})$ be the ring of complex-valued smooth functions on the circle S^1, which for concreteness I will realize as smooth 1-periodic functions on R:

$$R \cong \{f \in C^\infty(\mathrm{R}; \mathbf{C}) \mid f(x+1) = f(x)\}.$$

The proof of Q2 applies in exactly the same way to R, showing that every maximal ideal of R is of the form $\mathfrak{m}_p = \{f \in R \mid f(p) = 0\}$ for a unique $p \in [0, 1) \approx S^1$; you do not have to prove this. (The complex-valued vs real-valued is not an important point, it just simplifies the following.)

For any $f \in R$ we can define complex numbers $a_n \in \mathbf{C}$ for all $n \in \mathbb{Z}$ by $a_n = \int_0^1 f(x)e^{-2\pi inx}\,dx$. (Remark: It is a fact that these numbers decay rapidly as $n \to \infty$,
in the sense that for all $k \geq 0$ we have $n^k|a_n| \to 0$ and $n^k|a_{-n}| \to 0$ as $n \to +\infty$.)

Let $S \subset R$ be the subring consisting of those functions for which $a_{-1} = a_{-2} = \cdots = 0$, i.e.

$$S = \left\{ f \in R \;\middle|\; \int_0^1 f(x)e^{-2\pi inx}\,dx = 0 \text{ for all } n < 0 \right\}$$

(You do not have to prove that S is a subring of R, though you might benefit from thinking about why it is.)
For every $p \in [0, 1)$, we still have a maximal ideal $\mathfrak{m}_p \subset S$ given by $\mathfrak{m}_p = \{f \in S \mid f(p) = 0\}$.

Exhibit a maximal ideal of S that is *not* of this form, and ideally exhibit *two* such maximal ideals. (If you really want a challenge: can you classify *all* maximal ideals of S? Warning: I do not know that this is possible using things you know. But you could at least come up with a guess, even if you can't completely prove it's correct.)

Solution. (Solution by TC, edits by DD. "I" means TC. These solutions try to cover many many different directions you might have taken this; **no one** was expected to come up with all this by themselves.)

[First, why does the proof of Q2 not work here? The key difference is that if you just know that a function $f \in S$ is nonzero everywhere on S^1, then $\frac{1}{f}$ is a perfectly nice function, but it doesn't have to lie in S. Simple example: $f = e^{2\pi ix}$ is in S and nowhere vanishing on S^1; but $\frac{1}{f} = e^{-2\pi ix}$ has $a_{-1} = 1$ so $\frac{1}{f} \notin S$.]

The formula for $a_n = a_n(f)$ should suggest Fourier series (as does the fact that we're talking about periodic functions in the first place). In fact the a_n are exactly the Fourier coefficients of f. Note that the rapid decay of the coefficients guarantees that the sum $\sum_{n\in\mathbb{N}} a_n(f)e^{2\pi inx}$ converges to $f(x)$ uniformly/absolutely/however nicely you could possibly want. And it's straightforward to check that our formula for a_n lets us go back and forth between these descriptions; that is, if $g(x) = \sum_{n\in\mathbb{N}} b_n e^{2\pi inx}$ then $\int_0^1 g(x)e^{-2\pi imx}\,dx = b_m$.

In particular, we can use this to check that

$$a_n(fg) = \sum_{p+q=n} a_p(f)a_q(g) \tag{$*$}$$

[the so-called "convolution formula"] by expanding

$$\begin{aligned} f(x)g(x) &= \Big(\sum_{p\in\mathbb{N}} a_p(f)e^{2\pi ipx}\Big)\Big(\sum_{q\in\mathbb{N}} a_q(g)e^{2\pi iqx}\Big) \\ &= \sum_{n\in\mathbb{N}}\big(\sum_{p+q=n} a_p(f)a_q(g)\big)e^{2\pi inx} \end{aligned}$$

Note that we don't actually need a particularly strong convergence of the Fourier series to verify this convolution identity. In particular, a continuous function on S^1 is bounded, so it is in L^p for all $1 \leq p \leq \infty$. In particular, if f, g are continuous functions on S^1, then f, g, and fg are all L^2 functions. We want to show the following integral identity for any $n \in \mathbf{Z}$:

$$\int_0^1 f(x)g(x)e^{-2\pi inx}\,dx = \sum_{p+q=n,p,q\geq 0}\left(\int_0^1 f(x)e^{-2\pi ipx}\,dx\right)\left(\int_0^1 g(x)e^{-2\pi iqx}\,dx\right)$$

But both sides of the formula give a *bounded*[6], hence continuous, bilinear form on $L^2(S^1)$, so the above proof works as soon as we know that the Fourier series $\sum_{p\in\mathbf{N}} a_p(f)e^{2\pi ipx}$ converges to f in the L^2 norm, which Wikipedia says is called the Reisz-Fischer theorem, and is true for any L^2 function f. This lets us fiddle around with the regularity condition in the definition of R in order to get various different function spaces with similar properties.

In other words, the map from S to the power series ring $\mathbf{C}[[t]]$ sending $f \in S$ to the formal sum $\sum_{n\in\mathbb{N}} a_n(f)t^n$ is a ring homomorphism. [7] [8]

In particular, this interpretation suggests one evident maximal ideal, namely (t). This corresponds to the homomorphism $S \to \mathbf{C}$ given by $f \mapsto a_0(f)$, i.e. which sends f to its *average* $\operatorname{avg}(f) = \int_0^1 f(x)\,dx$. I feel like it should be possible to prove directly that $\operatorname{avg}(fg) = \operatorname{avg}(f)\operatorname{avg}(g)$, but in any case it follows from the convolution formula above.

[6] You can check by Hölder's inequality and Cauchy-Schwarz for finite sums that both sides are bounded by $\|f\|_{L^2}\|g\|_{L^2}$

[7] It turns out that this is actually an *isomorphism* between S and the subring of $\mathbf{C}[[x]]$ consisting of power series whose coefficients decay rapidly. One needs to check surjectivity, i.e. that any rapidly decaying coefficients arise from a smooth function (which is true even without assuming that $a_{-1} = a_{-2} = \cdots = 0$). Indeed, knowing only $\sum |a_n| < \infty$ is enough to guarantee uniformly-absolute convergence of the sum $\sum_{n\in\mathbb{N}} a_n e^{2\pi ix}$ (which thus converges to some continuous function f). In light of the identity $a_n(f') = (-2\pi in)a_n(f)$ (integration by parts), knowing $|a_n| \leq \frac{c}{n^{k+\varepsilon}}$ guarantees that the resulting function is C^{k-1}. So rapid decay guarantees that $f \in C^\infty$. But this is not necessary for the question.

[8] One could apply this to all of R to get elements that are some sort of "double-ended" power series "$\sum_{n\in\mathbb{Z}}$"$a_n t^n$; however, in general such power series **do not form a ring** because multiplication does not make sense (coefficients would be infinite sums). So one has to use the rapid decay property to even show multiplication is defined. This ends up giving some sort of ring of Laurent series: if there are only finitely many negative terms, everything works and we go into the localized ring $\mathbf{C}[[t]][\frac{1}{t}]$, otherwise we end up in some ring of complex functions with possibly essential singularities.

To see other maximal ideals, note that for *any* complex number $z \in D$ in the open unit disk (i.e. $|z| < 1$), the sum $\sum_{n\in\mathbb{N}} a_n(f)z^n$ converges absolutely. This defines a function $\pi_z\colon S \to \mathbf{C}$ sending $f \mapsto \sum_{n\in\mathbb{N}} a_n(f)z^n$, and the formula for $a_n(fg)$ in $(*)$ above shows that this is a ring homomorphism. So we obtain one maximal ideal $\mathfrak{m}_z = \{f \in S \mid \sum_{n\in\mathbb{N}} a_n(f)z^n = 0\}$ for each $z \in D$. But note that $\mathfrak{m}_0$ is the ideal we found above, corresponding to $f \mapsto \operatorname{avg}(f)$ [more on this in next paragraph].

Incidentally, for $f \in S$ the function $F\colon D \to \mathbf{C}$ given by $\sum_{n\in\mathbb{N}} a_n(f)z^n$ is actually **holomorphic** on the open disk D, and it turns out that our ring S is isomorphic to the ring of holomorphic functions on the open disk D that extend to a smooth function on the boundary S^1. (Our Fourier expansion is simply the Taylor expansion of the holomorphic function around 0, which always has radius of convergence ≥ 1. Note that when you plug in a complex number $z = e^{2\pi it} \in S^1$, the Taylor series is literally equal to the Fourier series since $\left(e^{2\pi it}\right)^n = e^{2\pi int}$, so by convergence of the Fourier series, you recover the original function.) In particular, the fact that evaluation $g \mapsto g(0)$ at $z = 0$ coincides with the average $\operatorname{avg}(g|_{S^1})$ is the *mean value property* for harmonic functions (recall holomorphic functions are harmonic).

A natural conjecture is then the claim that the maximal ideals all come from evaluation at a point of $\mathbf{D} \cup S^1$. Note that some functions in S have radius of convergence 1, so there are no ideals coming from points outside the unit disk. (For example, take $a_n = \frac{1}{n^{\log n}}$. Since $\sum_n |a_n|$ converges (compare it to $\frac{1}{n^2}$), the Fourier series $\sum a_n e^{2\pi inx}$ converges to a continuous function, and since $|a_n|$ decays faster than $\frac{1}{n^k}$ for any fixed k, this function is smooth.)

I (DD this time, not TC) have no idea whether all maximal ideals come from evaluation at a point of $\overline{\mathbf{D}}$ for the ring S we're considering, but there are some analogous cases where this is true and some where this is false. The rest of this solution is DD's attempt to present a lot of complicated analysis arguments he found on the Internet and does not fully understand, so for the analysis-minded among you, please let him know if you find any mistakes or simplifications, and especially if you manage to settle the question for S.

(I) To see an example where this is false, consider the ring $\mathscr{O}(\mathbf{D})$ of all holomorphic functions on the unit disk, with no condition whatsoever about their behavior on the boundary S^1. Then it's a theorem that every *finitely generated* maximal ideal of this ring is the ideal of functions vanishing at some point in $\mathbf{D}$. This is not so terribly hard to prove, and is proven for example in the book *Classical Topics in Complex Function Theory* by Remmert, around p. 136.[9] The key fact is that if $u, v \in \mathscr{O}(\mathbf{D})$ are two holomorphic functions with no common zeros, then there are $a, b \in \mathscr{O}(\mathbf{D})$ such that $au + bv = 1$. Unfortunately, the method used to produce these a, b (via writing the meromorphic function $\frac{1}{uv}$ in a *Mittag-Leffler series*, i.e. a normally convergent series of meromorphic functions where each term has only a single pole with the same principal part at that pole as $\frac{1}{uv}$) does not provide any boundary regularity (as far as DD can tell!).

To see a maximal ideal that is not of this form, let $f_0 \in \mathscr{O}(\mathbf{D})$ be a function which vanishes exactly on an infinite discrete set $\{x_n\} \subset D$ (necessarily accumulating at a point on S^1). Such a function exists by the Weierstrass product theorem for the unit disk, or we can construct one by using the Cayley transformation to map the (open!) unit disk bi-holomorphically to the (open!) upper half-plane, where we can take the function $\sin(2\pi ix)$, which vanishes exactly when $x = in$ for an integer n. Let I be the ideal of functions which vanish at infinitely many x_n. This is certainly a proper ideal

[9] Stanford students can access this book by clicking here:
https://stanford.idm.oclc.org/login?url=http://link.springer.com/10.1007/978-1-4757-2956-6.

(since $1 \notin I$) so it is contained in some maximal ideal $\mathfrak{m}$. However, there is no point $z \in \mathbf{D}$ such that $f(z) = 0$ for all $f \in I$: we can multiply f_0 by the meromorphic function $\frac{1}{(z-x_n)^{\operatorname{ord}_{x_n} f_0}}$ to get a function in I which does not vanish at x_n (this function is holomorphic on $\mathbf{D}$ since away from x_n it is the product of meromorphic functions, and near x_n we can write $f_0(z) = (z - x_n)^{\operatorname{ord}_{x_n} f_0} g(z)$ with $g(z)$ holomorphic and non-vanishing at x_n). So I contains a function which does not vanish at x_n for each n, and also I contains f_0, which does not vanish anywhere other than on the x_n. So, this maximal ideal is not given by evaluation at a point. However, if there were some f_0 as above with continuous (let alone smooth) restriction to S^1, this counterexample would go through and contradict the next result, so such a function cannot exist. Somebody who is better at complex analysis than DD is could probably prove this fact directly, perhaps using some sharper version of the maximum modulus principle.

(II) To see an example where this is true, consider the ring $A(\mathbf{D})$ of all holomorphic functions on the open unit disk $\mathbf{D}$ with *continuous* extension to the boundary. By the more general argument given above, this ring is isomorphic to a ring of continuous functions on S^1 with all negative Fourier coefficients equal to 0 (more care needs to be taken here to see that the associated power series of a continuous function f on S^1 really defines a holomorphic function $\widetilde{f}$ such that $\widetilde{f}$ restricts to f on S^1: this should be possible to show using the Cauchy integral formula to *define* the holomorphic function, which implies that the power series expansion is given by the a_n. Convergence of the integral must be checked.). This ring is nice because it is a *Banach algebra* with respect to the supremum norm. That is to say that the function $\|f\| = \sup_{z \in \overline{\mathbf{D}}} |f(z)|$ is a norm, Cauchy series with respect to this norm converge, and addition and multiplication are both sub-additive with respect to this norm. The key fact we'll use from functional analysis is that any maximal ideal of a Banach algebra $\mathscr{A}$ is necessarily closed, so $\mathscr{A}/\mathfrak{m}$ is a field which is also a Banach algebra. Then, the Gelfand-Mazur[10] Theorem implies that $\mathscr{A}/\mathfrak{m} \simeq \mathbf{C}$, so that the maximal ideal $\mathfrak{m}$ defines a *continuous* homomorphism from $\mathscr{A}$ to $\mathbf{C}$. This means that its values are determined on any dense set. In order to conclude, we'll need a special case of a hard fact from complex analysis: this is Mergelyan's theorem, which says that if $K \subseteq \mathbf{C}$ is compact with $\mathbf{C} \setminus K$ connected, then any continuous function on K which is holomorphic in the interior of K can be uniformly approximated by polynomials.[11] Uniform convergence is the same thing as convergence in the supremum norm, so this implies that polynomials are dense in the Banach algebra $A(\mathbf{D})$. Now, our maximal ideal $\mathfrak{m}$ of $A(\mathbf{D})$ gives a continuous homomorphism $\chi \colon A(\mathbf{D}) \to \mathbf{C}$, and so it is determined by its values on the polynomial subring $\mathbf{C}[z] \subseteq A(\mathbf{D})$ (polynomials certainly are continuous on S^1 and holomorphic in the disk!). Now, the restriction of χ to $\mathbf{C}[z]$ is still a homomorphism of $\mathbf{C}$-algebras, and it is surjective because $\mathbf{C}[z]$ contains the constant functions. Now, it is true that any surjective homomorphism of $\mathbf{C}$-algebras from $\mathbf{C}[z]$ to $\mathbf{C}$ is given by $f \mapsto f(z_0)$ for some $z_0 \in \mathbf{C}$ (prove it!). Let's show that $|z_0| \leq 1$. We can return to the previous example with $f(z) = 1 + \sum_{n=1}^{\infty} \frac{1}{n^{\log n}} z^n$. Let f_n be the n-th partial sum of this power series, and note that $\|f_m - f_n\|$ for $m \geq n$ is bounded above by $\sum_{k=n}^{m} \left| \frac{1}{k^{\log k}} \right|$, so since the series $\sum_{n=1}^{\infty} \frac{1}{k^{\log k}}$ converges absolutely, this is a Cauchy sequence in

[10] Sorry, *not* Barry Mazur, although he has worked in a ton of different fields. This is Stanislaw Mazur, a mid-20th century Polish mathematician.

[11] Perhaps this is easier to do on the closed unit disk than for a general compact domain, and someone who likes complex analysis could try to do so.

$A(\mathbf{D})$, so $f_n \to f$ in the norm of $A(\mathbf{D})$. Thus, $\chi(f_n) \to \chi(f)$. Now assume that $\chi(p(z)) = p(z_0)$ for any polynomial p with $z_0 \in \mathbf{C}$. Then

$$\chi(f) = \lim_{N\to\infty} \chi(f_N) = \lim_{N\to\infty} \sum_{n=1}^{N} \frac{1}{n^{\log n}} (z_0)^n$$

Since the radius of convergence of this power series is 1, as we can check by evaluating

$$\limsup_{n\to\infty} \sqrt[n]{n^{\log n}} = \limsup_{n\to\infty} e^{(\log n)^2/n} = 1,$$

this limit must diverge for $|z_0| > 1$, hence $z_0 \in \overline{\mathbf{D}}$. Finally, since $f \mapsto f(z_0)$ and $f \mapsto \chi(f)$ are both continuous homomorphisms which agree on all polynomials, they must agree, so our maximal ideal is the ideal of functions vanishing at some $z_0 \in \mathbf{D}$.

Why doesn't this proof extend to the case of smooth functions? The first problem is that functions with smooth boundary are not a Banach space: a uniform limit of holomorphic functions which are smooth on the boundary need not be smooth (e.g. all polynomials are smooth on the boundary and we just saw that they can converge uniformly in $\overline{\mathbf{D}}$ to anything which is continuous on S^1 and holomorphic on $\mathbf{D}$), so we have to control convergence of all of the derivatives as well. This involves an infinite family of norms, so we just get a Fréchet algebra, not a Banach algebra. Now, maximal ideals need not be smooth in this setting, so the homomorphisms into fields may not be continuous, so the preceding argument does not apply. If we relax the smooth boundary condition to a C^k boundary condition for some finite k, then we only need to control finitely many derivatives, so we can put all of their supremum norms together into a norm and get a Banach algebra again. However, it's not clear (to DD) that we can reduce the problem to polynomials as we did above: Mergelyan's theorem does not require the derivatives to converge. Perhaps a better analyst than DD could show by hand that a holomorphic function on $\mathbf{D}$ with C^k boundary condition can be approximated uniformly, along with all of its derivatives, by smooth functions.

Question 4. Let $a \in \mathbf{Z}$ and $b \in \mathbf{Z}$ be coprime. Let C be any abelian group, and let

$$f\colon (\mathbf{Z}/a\mathbf{Z}) \times (\mathbf{Z}/b\mathbf{Z}) \to C$$

be a $\mathbb{Z}$-bilinear map. Prove that $f = 0$.

Solution. Note that a bilinear map must satisfy $f(0, z) = 0$ for any z. Since a, b are coprime, a is a unit in the ring $\mathbf{Z}/b\mathbf{Z}$, so there is some $c \in \mathbf{Z}/b\mathbf{Z}$ such that $ac = 1$. (In elementary terms, because a and b are coprime, we can find n and m in $\mathbf{Z}$ such that $na + mb = 1$.) Now, let x, y be arbitrary elements of $\mathbf{Z}/a\mathbf{Z}, \mathbf{Z}/b\mathbf{Z}$ respectively. We have:

$$f(x, y) = f(x, (ac)y) = f(x, a(cy)) = f(ax, cy) = f(0, cy) = 0$$

To get from $f(x, a(cy))$ to $f(ax, cy)$ we used the bilinearity of f, and then the fact that $ax = 0$ for all $x \in \mathbb{Z}/a\mathbb{Z}$. We'll see once we learn about tensor products that this statement is equivalent to the statement that

$$\big(\mathbf{Z}/a\mathbf{Z}\big) \otimes_{\mathbf{Z}} \big(\mathbf{Z}/b\mathbf{Z}\big) = 0.$$

Question 5. Let N be a submodule of the R-module M. Prove that if N is finitely generated and M/N is finitely generated, then M is finitely generated.

Solution. Let $[m_1], \ldots, [m_\ell]$ be a finite generating set of M/N (here, the notation $[m_i]$ means "the equivalence class mod N including m_i"). Choosing representatives arbitrarily gives us elements $m_1, \ldots, m_\ell$ in M. In addition, let $n_{\ell+1}, \ldots, n_{\ell+k}$ be a generating set of $N \subseteq M$. Now, we have the set of $\ell + k$ elements $S = \{m_1, \ldots, m_\ell, n_{\ell+1}, \ldots, n_{\ell+k}\}$ of M. Let's show that S generates M.

From the fact that the $[m_i]$ generate M/N, we know that for any $m \in M$, we can write $[m]$ in M/N as:

$$[m] = r_1[m_1] + \cdots + r_\ell[m_\ell]$$

Thus, the elements m and $r_1 m_1 + \cdots + r_\ell m_\ell$ have the same image in M/N, so their difference is an element n of N. Since the n_j generate N, we can write:

$$m = r_1 m_1 + \cdots + r_\ell m_\ell + n = r_1 m_1 + \cdots + r_\ell m_\ell + r_{\ell+1} n_{\ell+1} + \cdots + r_{\ell+k} n_{\ell+k}$$

Thus, m is an R-linear combination of elements of S, so S generates M and in particular M is finitely generated.

Question 6. Let M be a finitely generated R-module. Let $\pi\colon M \twoheadrightarrow R^n$ be a surjective homomorphism, and let $K = \ker(\pi)$. Prove that the R-module K is finitely generated.

Solution.

Step 1: Because R^n is a free module, there exists a *section* $i\colon R^n \to M$, meaning a homomorphism i such that $\pi \circ i = \mathrm{id}_{R^n}$.

Why does this section i exist? We can pick a basis $e_1, \ldots, e_n$ of R^n. Because π is surjective, for each e_j we can choose some $i(e_j)$ (non-uniquely) in M such that $\pi(i(e_j)) = e_j$. Because R^n is free, this choice of where to send basis vectors uniquely extends to a map $i\colon R^n \to M$. (we don't need uniqueness right now, just the fact that it extends) Furthermore, since $\pi(i(e_j)) = e_j$ for each j, the two R-module homomorphisms $\pi \circ i$ and id_{R^n} from R^n to R^n agree on the generating set $\{e_1, \ldots, e_n\}$. So by one of the equivalent characterizations of what it means for a set to generate a module from HW1, this implies that $\pi \circ i = \mathrm{id}_{R^n}$.[12]

Step 2: The existence of a splitting implies that $M \simeq K \oplus R^n$, with the injection $K \hookrightarrow M$ corresponding to the map $k \mapsto (k, 0)$ and the surjective homomorphism $\pi\colon M \to R^n$ corresponding to the map $(k, a) \mapsto a$. An isomorphism $\varphi\colon K \oplus R^n \to M$ is given by sending K to $K \subseteq M$ and mapping R^n into M by i. The map φ is injective, since if $\varphi(k, a) = 0$, then $k + i(a) = 0$, so $\pi(k) + \pi(i(a)) = a = 0$, since $\pi \circ i = \mathrm{id}_{R^n}$ and $\pi|_K = 0$. It is surjective because if $m \in M$, then $\pi(i(\pi(m))) = \pi(m)$, so $m - i(\pi(m)) = k \in K$. Thus, $m = \varphi(k, \pi(m))$.

Step 3: It is true more generally that if K, N are R-modules such that $M := K \oplus N$ is finitely generated, then K and N are already finitely generated.

To see this, note that $M = K \oplus N$ has a surjective homomorphism $\pi_K\colon K \oplus N \twoheadrightarrow K$ given by $\pi_K(k, n) = k$. [13] So the image $\pi_K(S)$ of a finite generating set for M will be a finite generating set for K (by the first condition on HW1 Q1). The same argument applies by symmetry to N.

[12] We'll see later that there is a more general class of modules P such that every short exact sequence $0 \to K \to M \to P \to 0$ admits a splitting; these modules are called *projective*.

[13] In a sense, we are using here that the finite direct sum $K \oplus N$ coincides with the finite product $K \times N$.

Question 7. Let R be a commutative ring, and let $S \subset R$ be a multiplicative set ($S \cdot S \subset S$). Let M be a finitely generated R-module. Prove that the localization $S^{-1}M$ satisfies

$$S^{-1}M = 0 \qquad \iff \qquad \exists s \in S \text{ with } s \cdot M = 0.$$

Solution. The elements of $S^{-1}M$ are all of the form $\frac{m}{s}$ with $m \in M, s \in S$. By the construction of the localization, we know that $\frac{m}{s} = 0 = \frac{0}{1}$ iff there is some $s' \in S$ such that $s'(1 \cdot m - s \cdot 0) = s' \cdot m = 0$. This means that $S^{-1}M = 0$ iff for every $m \in M$, there is some $s_m \in S$ such that $s_m \cdot m = 0$. This immediately shows that the $\Leftarrow$ direction is true, since if $s \cdot M = 0$, we can take $s_m = s$ for all $m \in M$. So far, this much is true without using the fact that M is finitely generated.

Now we are reduced to showing that if for every $m \in M$, there is some s_m such that $s_m \cdot m = 0$, then in fact there is a *single* s such that $s \cdot m = 0$ for all $m \in M$. The key is to observe that if X is a generating set of M, then

$$s \cdot x = 0 \text{ for all } x \in X \qquad \Longrightarrow \qquad s \cdot M = 0.$$

One way to see this is that multiplication by s is an R-module homomorphism from M to M (since R is commutative!), so it is determined by its values on a generating set — but our hypothesis says it agrees with the zero homomorphism on the generating set X.

Now suppose that we have a *finite* generating set $\{m_1, \ldots, m_n\}$. By hypothesis, there is some $s_1, \ldots, s_n$ such that $s_i \cdot m_i = 0$. Now, S is multiplicatively closed, so the product of all these elements $s := s_1 \cdot s_2 \cdot (\cdots) \cdot s_n$ belongs to S. And this product satisfies $s \cdot m_i = 0$ for $i = 1, \ldots, n$ (we can use commutativity of R to put s_i last in the expression for s). So $s \cdot M = 0$, as desired.

Question 8. Let $f\colon X \to Y$ be a homomorphism of R-modules.

(a) Consider all pairs (A, α) of an R-module A and a homomorphism $\alpha\colon A \to X$ with $f \circ \alpha = 0$.

$$\begin{tikzcd}
A \arrow[r, "\alpha"] \arrow[dr, "0"'] & X \arrow[d, "f"] \\
& Y
\end{tikzcd}$$

You will prove that these exists a "universal" such pair. Specifically, you must construct some $(M, \mu\colon M \to X)$ with $f \circ \mu = 0$ with the property that:
for any $(A, \alpha\colon A \to X)$ with $f \circ \alpha = 0$, there exists a unique $a\colon A \to M$ such that $\alpha = \mu \circ a$.

$$\begin{tikzcd}
A \arrow[r, "a"'] \arrow[rr, bend left, "\alpha"] \arrow[drr, "0"'] & M \arrow[r, "\mu"'] \arrow[dr, "0"] & X \arrow[d] \\
& & Y
\end{tikzcd}$$

(We might abbreviate this property as saying roughly: "Every α with $f \circ \alpha = 0$ factors uniquely through M".)

(b) On the other side, consider all pairs $(B, \beta\colon Y \to B)$ with $\beta \circ f = 0$.

$$\begin{tikzcd}
X \arrow[d, "f"'] \arrow[dr, "0"] & \\
Y \arrow[r, "\beta"'] & B
\end{tikzcd}$$

Prove that these exists a "universal" such pair, by constructing
some $(N, \nu\colon Y \to N)$ with $\nu \circ f = 0$ with the property that:
for any $(B, \beta\colon Y \to B)$ with $\beta \circ f = 0$, there exists a unique $b\colon N \to B$ such that $\beta = b \circ \nu$.

$$\begin{tikzcd}
X \arrow[d, "f"'] \arrow[dr, "0"] \arrow[drr, "0"] & & \\
Y \arrow[r, "\nu"] \arrow[rr, bend right, "\beta"'] & N \arrow[r, "b"] & B
\end{tikzcd}$$

(We might abbreviate this property as saying roughly: "Every β with $\beta \circ f = 0$ factors uniquely through N".)

Solution. (a) We will define M to be the *kernel* of the homomorphism f, i.e. the submodule of X given by $\{x \in X \mid f(x) = 0\}$, and $\mu \colon M \to X$ the inclusion of this submodule. Certainly $f \circ \mu = 0$, since this is nothing other than $f|_M$, which is 0 by definition.

Now, let $\alpha \colon A \to X$ be a homomorphism such that $f \circ \alpha = 0$. This means that for all $b \in A$, $f(\alpha(b)) = 0$. This implies that $\alpha(b) \in M$. We can construct a homomorphism $a \colon A \to M$ by sending b to $\alpha(b) \in M$. This is a homomorphism since α is, and the operations in M are just the restrictions of the operations in X. In other words, we know that α is a homomorphism so $\alpha(r_1 b_1 + r_2 b_2) = r_1 \alpha(b_1) + r_2 \alpha(b_2)$ in X, but since all of these elements are actually in M, the same holds for the restricted map a. Next, we can check that $\mu \circ a = \alpha$ by checking this on every $b \in A$: we have $\mu(a(b)) = \mu(\alpha(b)) = \alpha(b)$, since μ is just the inclusion map.

Why is a unique? Let $a' \colon A \to X$ be another homomorphism such that $\mu \circ a' = \alpha$. This means that for all $b \in A$, $\mu(a'(b)) = \alpha(b)$. But since $\mu(m) = m$ for any $m \in M$, this says that $a'(b) = \alpha(b) = a(b)$ for all $b \in B$, so $a = a'$.[14]

(b) This time, N will be the *cokernel* of the homomorphism, i.e. the quotient module $Y/\operatorname{im}(f)$, where $\operatorname{im}(f) = \{y \in Y \mid \exists x \in X, y = f(x)\}$ (this is a submodule of Y because f is a homomorphism).[15] The map $\nu \colon Y \to N$ is the projection map $y \mapsto [y] = y + \operatorname{im}(f)$ (as usual, we think of elements of the quotient as equivalence classes mod $\operatorname{im}(f)$). Since f maps X into $\operatorname{im}(f)$, we have that $\nu \circ f = 0$ (i.e. $\nu(f(x)) = f(x) + \operatorname{im}(f) = 0 + \operatorname{im}(f)$).

Now, let $\beta \colon Y \to B$ be a homomorphism such that $\beta \circ f = 0$. We want to construct a homomorphism $b \colon N \to B$ such that $b \circ \nu = \beta$. Since $\beta \circ f = 0$, for any $x \in X$, $\beta(f(x)) = 0$, so $\beta|_{\operatorname{im}(f)} = 0$. This means that we get a well-defined function $b \colon N \to B$ by sending $[y]$ to $\beta(y)$, since $\beta(y) = \beta(y + f(x))$ for any $f(x) \in \operatorname{im}(f)$. This is a homomorphism because β is and because the operations on N are induced from those on Y. What this means explicitly is that

$$b\big(r_1[y_1] + r_2[y_2]\big) = b\big([r_1 y_1 + r_2 y_2]\big) = \beta(r_1 y_1 + r_2 y_2) = r_1 \beta(y_1) + r_2 \beta(y_2) = r_1 b([y_1]) + r_2 b([y_2]).$$

Now, we can check that $b \circ \nu = \beta$, since $(b \circ \nu)(y) = b([y]) = \beta(y)$.

Finally, we need to show that b is unique. Let b' be a homomorphism from N to B such that $b' \circ \nu = \beta$. Then for any $y \in Y$, $b'(\nu(y)) = b'([y]) = \beta(y) = b([y])$. Since every element of N can be written as $[y]$ for some $y \in Y$, this forces $b' = b$.[16]

[14] Note that this argument for uniqueness did not use anything in particular about α; in fact, we only need to know that μ is injective. For any injective homomorphism $\mu \colon M \to N$ of R-modules any homomorphisms $f, g \colon L \to M$ for some R-module L, $\mu \circ f = \mu \circ g$ iff $f = g$. The categorical term for this property is that μ is a *monomorphism*. In any category, these are typically morphisms which are "injective" in some sense depending on the type of category we're looking at.

[15] Incidentally, the reason for the term *cokernel* is because the property we're about to show for N is formally "dual" to the property from part (a) of the kernel.

[16] The dual of the footnote for the previous part applies here: we didn't use anything particular about β, and we only needed the surjectivity of ν. A surjective homomorphism ν of R-modules has the property that $f \circ \nu = g \circ \nu \implies f = g$, and the categorical term for this property is that ν is an *epimorphism*. This notion usually agrees with some suitable idea of surjectivity in sufficiently nice 'algebraic' categories like the category of R-modules, but is often weaker than surjectivity in 'geometric' settings. For example, in the category of topological Hausdorff spaces and continuous maps, a map is an epimorphism as soon as the image is *dense*.