todo

- review important examples of groups
- recognition theorems for direct / semi-direct products, cyclic groups, etc.

Chapter 1

Analysis

1.1 7/16/18: Ordinary differential equations

Problem 1.1.1 (Gronwall's inequality)**.** Suppose f is a differentiable function from the reals into the reals. Suppose $f'(x) > f(x)$ for all $x \in \mathbb{R}$, and $f(x_0) = 0$. Prove that $f(x) > 0$ for all $x > x_0$.

Solution 1: The direct proof that first came to my mind goes as follows: consider $f^{-1}\{0\} \cap (x_0, \infty)$. Show that this set has a minimum; call it x_1.

Then use the mean value theorem to deduce that f' vanishes between x_0 and x_1. But then f must be negative there, and from here we can derive a contradiction. □

Solution 2: This is the solution Albert gave in class. Basically, rearrange the inequality as

$$f'(x) - f(x) > 0$$

and then introduce an "integrating factor" so that the LHS is the derivative of a product:

$$e^{-x} f'(x) - e^{-x} f(x) > 0$$
$$\frac{\mathrm{d}}{\mathrm{d}x}(e^{-x} f(x)) > 0.$$

Observe that $e^{-x} f(x)$ is positive and strictly increasing for $x > x_0$. The same is true of the function e^x, so we deduce their product $f(x)$ is positive and strictly increasing as well for $x > x_0$. □

Remark. If one has an inequality like $u'(t) < \beta(t)u(t)$, one first finds v which solves $v'(t) = \beta(t)v(t)$ and then computes the derivative of u/v to deduce that this ratio is increasing or decreasing (as the case may be). Then compare to its initial value at t_0.

Problem 1.1.2. Let n be an integer larger than 1. Is there a differentiable function on $[0, \infty)$ whose derivative equals its nth power and whose value at the origin is positive?

Solution: The differential equation is

$$\frac{\mathrm{d}y}{\mathrm{d}x} = y^n; \quad y(0) > 0.$$

The conditions of Picard's theorem are satisfied so we have local existence and uniqueness. The latter is the useful deduction—the above differential equation is easy to solve directly. Simply observe that the solutions all have vertical asymptotes at positive x, so there can be no continuous solution defined on all of $[0, \infty)$. □

Problem 1.1.3. Prove that the initial value problem

$$\frac{\mathrm{d}x}{\mathrm{d}t} = 3x + 85\cos x; \quad x(0) = 77$$

has a solution $x(t)$ defined for all $t \in \mathbb{R}$.

Solution: For this problem, it is very useful to have a quantitative form of Picard's theorem. Suppose we have a differential equation of the form

$$\frac{\mathrm{d}x}{\mathrm{d}t} = f(x, t),$$

i.e. a "slope field" given by f, defined on some rectangle $[t_0 - a, t_0 + a] \times [x_0 - b, x_0 + b]$.

If f is continuous with respect to t and uniformly Lipschitz with respect to x (in the sense that the Lipschitz constant may be picked independently of t) then there is a unique solution passing through (t_0, x_0) defined for $t \in [t_0 - \alpha, t_0 + \alpha]$ where

$$\alpha = \min(a, b/(\sup|f|)).$$

In our problem, by picking b large enough, we can always ensure that $b/\sup f > 1/4$ for example. So repeated application of Picard's theorem shows that there is a (unique) solution $x(t)$ defined for all $t \in \mathbb{R}$. □

Problem 1.1.4. Let $f\colon \mathbb{R} \to \mathbb{R}$ be a continuous nowhere vanishing function, and consider the differential equation

$$\frac{\mathrm{d}y}{\mathrm{d}x} = f(y).$$

1. For each real number c, show that this equation has a unique continuously differentiable solution $y = y(x)$ on a neighborhood of 0 which satisfies the initial condition $y(0) = c$.

2. Deduce the conditions on f under which the solution y exists for all $x \in \mathbb{R}$, for every initial value c.

Solution:

1. The idea is that we can just "solve" this differential equation by "separation of variables." To be rigorous, we will invoke the inverse function theorem.

   Let us instead consider the differential equation

   $$\frac{\mathrm{d}x}{\mathrm{d}y} = \frac{1}{f(y)}.$$

   The RHS is a continuous function; consider $x(y) = \int_c^y \frac{\mathrm{d}t}{f(t)}$. This function is continuously differentiable, and is the *unique* solution to the above equation with $x(c) = 0$. Moreover, $x'(c) \neq 0$ so the inverse function theorem tells us that it (locally) has a continuously differentiable inverse $y(x)$ which satisfies $y(0) = c$ and the differential equation

   $$\frac{\mathrm{d}y}{\mathrm{d}x} = f(y)$$

   as desired. Uniqueness also follows from the IFT.

2. The function $x(y)$ defined previously is either strictly increasing or strictly decreasing. In order for $y(x)$ to be defined for all $x \in \mathbb{R}$, it is necessary and sufficient for $x(y)$ to be surjective.

□

Problem 1.1.5. Consider the equation

$$\frac{\mathrm{d}y}{\mathrm{d}x} = y - \sin y.$$

Show that there is an $\epsilon > 0$ such that if $|y_0| < \epsilon$, then the solution $y = f(x)$ with $f(0) = y_0$ satisfies

$$\lim_{x \to -\infty} f(x) = 0.$$

Solution: Actually, ϵ can be taken to be anything—the result holds for any y_0.

Albert mentioned that there isn't a specific tool or theorem that immediately knocks out this problem. The strategy here is more or less to slowly chip away at the problem. Drawing a picture helps *a lot*.

Note that $y - \sin y$ is an odd function. If $y = f(x)$ is a solution to the differential equation, then so is $y = -f(x)$. Also, the hypotheses of Picard's theorem are satisfied, so solutions are locally unique. The function $y = 0$ is the solution with $y_0 = 0$.

So we may as well assume $y_0 > 0$. The solution y cannot cross the x-axis, as that would violate uniqueness of solutions. Thus it is always positive, and the differential equation also tells us that it is strictly increasing.

Hence the limit in question is the infimum of the range of y. We have already established that 0 is a lower bound. Moreover, if $L > 0$ is a lower bound, then y' is *also* bounded below thanks to the differential equation. But then, by the mean value theorem for instance, we must have that y crosses the x-axis, a contradiction. Therefore 0 is indeed the desired infimum and we are done. □

1.2 7/20/18: Metric spaces

Problem 1.2.1. Let $X \subseteq \mathbb{R}^n$ be compact and let $f: X \to \mathbb{R}$ be continuous. Given $\epsilon > 0$, show there is an M such that for all $x, y \in X$,

$$|f(x) - f(y)| \leq M|x - y| + \epsilon.$$

Solution: A continuous function on a compact set is uniformly continuous, and also is bounded (by some C). So there exists $\delta > 0$ for which $|x - y| < \delta \implies |f(x) - f(y)| < \epsilon$.

Then pick M large enough so that $M\delta > 2C$. □

Problem 1.2.2. Let K be a continuous function on the closed unit square satisfying $|K(x, y)| < 1$ for all x and y. Show that there is a continuous function $f(x)$ on $[0, 1]$ such that we have

$$f(x) + \int_0^1 K(x, y) f(y) \mathrm{d}y = e^{x^2}.$$

Can there be more than one such function f?

Solution: The fact that $|K(x, y)| < 1$ is a hint that the fixed point theorem for a contraction may be involved. According to Albert, this theorem is a common way of answering these integral equation type problems.

Consider the operator T defined as

$$T(f)(x) = e^{x^2} - \int_0^1 K(x, y) f(y) \mathrm{d}y.$$

We claim that $T: C([0, 1]) \to C([0, 1])$ is a contraction, where $C([0, 1])$ is equipped with the supremum norm. There are two parts to this claim: the fact that $T(f)$ is a continuous function of x, and that T is a contraction. Both parts essentially rely on compactness of the unit square, which tells us that

- $|K(x, y)|$ is uniformly continuous. This can be used to show that $T(f)$ is continuous.
- $|K(x, y)|$ has a maximum strictly less than 1. This is used to show that T is a contraction. Note that the definition of a contraction is *not* that $d(T(f), T(g)) < d(f, g)$, but that there is a constant $\alpha < 1$ such that $d(T(f), T(g)) \leq \alpha d(f, g)$.

Finally, we use the fact that $C([0, 1])$ is a complete metric space. This can probably just be cited, but the proof is not difficult: it just uses the fact that if continuous functions converge uniformly to another function, then that other function is also continuous.

With all these ingredients, we can invoke the fixed point theorem to deduce that T has a *unique* fixed point which is then the solution to the integral equation. □

Lemma 1.2.1. *In a metric space, a compact set and a closed set can be separated by a positive distance.*

Problem 1.2.3. Let X be a compact metric space and $f: X \to X$ an isometry. Show that $f(X) = X$.

Solution: Assume otherwise, and chase an element $x \in X \setminus f(X)$ around using f. Note that x has some positive distance away from $f(X)$, which is compact. □

Problem 1.2.4. Let F be a uniformly bounded, equicontinuous family of real valued function on the metric space (X, d). Prove that the function

$$g(x) = \sup\{f(x) : f \in F\}$$

is continuous.

Solution: The hypotheses appearing in this question suggest the usage of Arzela-Ascoli, but that is actually a red herring. This can be easily proved directly by noting that if $x, \epsilon > 0$ are given and δ is picked as in the definition of equicontinuity, then for $|x - y| < \delta$ we have

$$g(y) = \sup_f f(y) \leq \sup_f (f(x) + \epsilon) = \sup_f f(x) + \epsilon = g(x) + \epsilon$$
$$g(y) = \sup_f f(y) \geq \sup_f (f(x) - \epsilon) = \sup_f f(x) - \epsilon = g(x) - \epsilon.$$

□

Problem 1.2.5. Let $X \subseteq \mathbb{R}^n$ be a closed set and r a fixed positive real number. Let $Y = \{y \in \mathbb{R}^n : \exists x \in X, |x - y| = r\}$. Show that Y is closed.

Solution: Show that for a fixed point $p \in \mathbb{R}^n$, the function $d(p, -)$ is closed, using Lemma 1.2.1 and compactness of the sphere. If $p \notin Y$, then $d(p, X)$ is closed and does not contain r. So pick a ball around $r \in \mathbb{R}$ which doesn't meet $d(p, X)$, and consider the ball around $p \in \mathbb{R}^n$ of the same radius. This ball will be disjoint from Y by the triangle inequality. Thus Y is closed.

Well, you could reorganize this argument and just show that the sphere of radius r around p is separated by some $\epsilon > 0$ from X. □

1.3 7/25/18: Real analysis 1

Problem 1.3.1.

1. Prove that there is no continuous map from the closed interval $[0, 1]$ onto the open interval $(0, 1)$.
2. Find a continuous surjective map from the open interval $(0, 1)$ onto the closed interval $[0, 1]$.
3. Prove that no map in Part 2 can be bijective.

Solution:

1. Continuous image of compact set is compact.
2. "Start" at 1/2, go down to 0, go up to 1, "end" at 1/2.
3. If you want to be super-overkill, you could invoke Invariance of Domain in the 1-dimensional case. But I think the proof of that probably uses the IVT in some way anyway, so may as well prove it with IVT.

   Mildly clever IVT proof: let $f(a) = 0$, $f(b) = 1$. From IVT deduce that $f([a,b]) = [0,1]$ (or $f([b,a]) = [0,1]$, as the case may be).

   Less clever "intuitive" IVT proof: consider $f(a) = 0$ and look at some small interval around a and argue non-injectivity using that.

□

Problem 1.3.2. Let f be a C^2 function on the real line. Assume f is bounded with bounded second derivative. Let

$$A = \sup_{x\in\mathbb{R}} |f(x)|, \quad B = \sup_{x\in\mathbb{R}} |f''(x)|.$$

Prove tha

$$\sup_{x\in\mathbb{R}} |f'(x)| \le 2\sqrt{AB}.$$

Solution: As Albert mentioned, if you see "C^2," chances are it's a Taylor expansion problem. Another hint is that we're asked to relate various derivatives of the function to one another, and the Taylor expansion gives a good way of doing that.

Then for every x, h, there exists a ξ between x and $x+h$ such that

$$f(x+h) = f(x) + f'(x)h + \frac{f''(\xi)h^2}{2!}$$

which means

$$\begin{aligned} |f'(x)| &= \left| \frac{1}{h} \left(f(x+h) - f(x) - \frac{f''(\xi)h^2}{2} \right) \right| \\ &\le \frac{2A}{h} + \frac{Bh}{2} \end{aligned}$$

for all h. If you compute the minimum of the RHS, you'll find that it's $2\sqrt{AB}$ as desired. □

Remark. Here are some ways to prove convergence.

- If you're working in a complete metric space, you could show that the sequence is Cauchy. This may be useful if there's no clear putative limit.

- Monotone and bounded.
- Squeeze liminf and limsup together; i.e. show $\liminf \geq \limsup$ so they must be equal.

Problem 1.3.3. Let x_n be a sequence of real numbers so that $\lim_{n\to\infty}(2x_{n+1} - x_n) = x$. Show that $\lim_{n\to\infty} x_n = x$.

Solution 1: There's a "slick" proof that Albert showed, but I put the word slick in quotes because it actually ends up being kind of long. The idea is that we have a wishful method that doesn't really quite work, but we use it to slowly approach a method which does work.

The wishful approach is fueled by an "addition by zero" trick:

$$\begin{aligned}\lim_{n\to\infty} x_n &= \lim_{n\to\infty}\left(x_n - \frac{x_{n-1}}{2} + \frac{x_{n-1}}{2}\right)\\ &= \frac{x}{2} + \frac{1}{2}\lim_{n\to\infty} x_n\end{aligned}$$

and then to solve for $\lim_{n\to\infty} x_n$.

We can't legally make this manipulation because we don't even know the limits are defined! Reducing to the problem of existence is actually not much of a reduction... However, we can do a similar argument using liminf and limsup. These are always defined, and the condition for them to be finite (so we can manipulate them as above) is just for x_n to be bounded. Let's first assume that's the case, and see how the argument would go:

$$\begin{aligned}\limsup_{n\to\infty} x_n &\leq \limsup_{n\to\infty}\left(x_n - \frac{x_{n-1}}{2}\right) + \limsup_{n\to\infty}\frac{x_{n-1}}{2}\\ &= \frac{x}{2} + \frac{1}{2}\lim_{n\to\infty} x_n\\ \limsup_{n\to\infty} x_n &\leq x.\end{aligned}$$

Similarly one deduces $\liminf_{n\to\infty} x_n \geq x$, so the limit in fact exists and is equal to x.

All that remains is to explain why x_n is bounded. For that we can do "addition by zero" repeatedly to write

$$x_n = \sum_{i=1}^{n} 2^{i-n-1}\left(2x_i - x_{i-1}\right) + 2^{-n}x_0.$$

Since $(2x_i - x_{i-1})$ is convergent, it is bounded—and from there it is straightforward to show that x_n is bounded as well. □

Solution 2: My direct proof just used the definition of convergence. If you go out far enough, $(x_n - 2x_{n-1})$ is within an ϵ-neighborhood of x; use that to show $x_n - x$ ends up within some small neighborhood (e.g. 2ϵ) of 0. □

Problem 1.3.4. Let a and x_0 be positive numbers, and define the sequence $(x_n)_{n=1}^{\infty}$ recursively by

$$x_n = \frac{1}{2}\left(x_{n-1} + \frac{a}{x_{n-1}}\right).$$

Prove that this sequence converges, and find its limit.

Solution: Bless the bit of dynamical systems work I did in high school... if you draw a picture (a graph of the recursion $f(x)$ together with the diagonal $y = x$) and play around with it, this problem is very easy, especially since the minimum of the recursion coincides with its fixed point: $\sqrt{a}$.

Steps of the proof:

1. Reduce to the case $x_0 \geq \sqrt{a}$ since if that isn't the case, you get it by applying f once.
2. Show that if $\sqrt{a} \leq x_n$, then $\sqrt{a} \leq x_{n+1} \leq x_n$. This can be done just by noting, in some way, that the graph of f is below the diagonal for $x_0 \geq \sqrt{a}$.
3. Deduce convergence (monotone and bounded).
4. Note that since f is continuous, if a sequence of iterates converges, it must be to a fixed point. Or use the limit trick from the preceding problem (this time we're fine since we already know it exists); i.e. just take the limit of the recursion as $n \to \infty$. Or argue by contradiction, as in Problem 1.1.5, to show that it can't converge to anything strictly higher than $\sqrt{a}$.

□

Problem 1.3.5. Suppose f is a continuous real valued function. Show that

$$\int_0^1 f(x)x^2 \mathrm{d}x = \frac{1}{3}f(\xi)$$

for some $\xi \in [0,1]$.

Solution: It was a little confusing to wrap my head around the IVT hint, but really you proceed by writing down what little you can deduce from such weak assumptions:

$$\frac{m}{3} = m\int_0^1 x^2 \mathrm{d}x \leq \int_0^1 f(x)x^2 \mathrm{d}x \leq M\int_0^1 x^2 \mathrm{d}x = \frac{M}{3}.$$

where m, M are the minimum and maximum of f on $[0,1]$. It follows that, by IVT, there must be some ξ between m and M inclusive such that $\frac{f(\xi)}{3}$ is equal to the middle expression.

Another perspective from Albert: precisely *because* the assumptions are so weak (you only know f is continuous) and you are asked for existence of something in some interval, chances are IVT is involved somehow. □

Problem 1.3.6. Let $0 \le a \le 1$ be given. Determine all nonnegative continuous functions f on $[0,1]$ which satisfy the following three conditions:

$$\int_0^1 f(x)\mathrm{d}x = 1, \quad \int_0^1 xf(x)\mathrm{d}x = a, \quad \int_0^1 x^2 f(x)\mathrm{d}x = a^2.$$

Solution 1, Cauchy-Schwarz: This one is kind of tricky, in that it was the one problem on this sheet I couldn't figure out any solution to (not even an ugly one) before Albert went over them in class.

Reverse engineering motivation (a.k.a. hindsight is 20/20): we're dealing with a bunch of integrals of products of various similar-looking functions—perhaps we could interpret the integral as a pairing and make use of CS. The first thing you might try to do is

$$\left(\int_0^1 x^n f(x)\mathrm{d}x\right)^2 \le \int_0^1 x^{2n}\mathrm{d}x \int_0^1 f(x)^2\mathrm{d}x$$

but this manipulation isn't very useful, mostly because we don't know anything about $\int_0^1 f(x)^2\mathrm{d}x$. The trick is to instead split $xf(x)$ as $x\sqrt{f(x)}\cdot\sqrt{f(x)}$ (which we can do because we are told that f is non-negative, a fact that we otherwise would not have used!), in which case CS gives

$$\left(\int_0^1 xf(x)\mathrm{d}x\right)^2 \le \int_0^1 x^2 f(x)\mathrm{d}x \int_0^1 f(x)\mathrm{d}x$$

That looks much better. With the constraints in the problem, we actually have equality, and equality only happens in CS when the two vectors being paired are linearly dependent. But this is clearly impossible: if $f(x)$ is nonzero for at least two different values of x, then $x\sqrt{f}$ and $\sqrt{f}$ cannot be linearly dependent. And of course, this must be the case since $\int f = 1$. □

Solution 2, Jensen's: Incidentally, apparently the "J" in "Jensen" is pronounced as a "Y." I feel like I probably should've known this, given how many times I've seen this inequality used in lectures before... but still, worth taking a note of, I guess.

This one is a bit easier to reverse engineer motivation for: anyone that has taken a probability class should recognize those integrals as moments! The constraints of the problem tell us that f can be thought of as a probability distribution on $[0,1]$, with first moment a and second moment a^2. But $\mathbb{E}[X^2] - \mathbb{E}[X]^2 \ge 0$ and equality occurs only when X has no variance whatsoever. That would require f to be a point mass distribution, i.e. the Dirac delta distribution centered at a. But that's not even a function, let alone a continuous one. This is a similar conclusion to what we reached in the other solution.

These two solutions actually feel pretty similar... they're probably "equivalent" in some sense. □

1.4 7/30/18: Real analysis 2

Problem 1.4.1. Prove that a real valued C^3 function f on $\mathbb{R}^2$ whose Laplacian,

$$\frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2},$$

is everywhere positive, cannot have a local maximum.

Solution: I don't see what's wrong with just considering $f(x_0, y)$ and $f(x, y_0)$ for a fixed point (x_0, y_0). Perhaps the issue has to do with the definition of C^3?

Albert's solution is more roundabout and uses the Taylor expansion

$$f(\vec{x}) = f(\vec{x}_0) + \nabla f(\vec{x}_0)(\vec{x} - \vec{x}_0) + (\vec{x} - \vec{x}_0)\nabla^2 f(\vec{x}_0)(\vec{x} - \vec{x}_0) + \cdots.$$

□

Problem 1.4.2. Define $f: \mathbb{R}^2 \to \mathbb{R}$ by $f(x, 0) = 0$ and

$$f(x, y) = \left(1 - \cos \frac{x^2}{y}\right)\sqrt{x^2 + y^2}$$

for $y \neq 0$.

1. Show that f is continuous at $(0, 0)$.
2. Calculate all directional derivatives of f at $(0, 0)$.
3. Show that f is not differentiable at $(0, 0)$.

Solution:

1. It suffices to observe that $|f| \leq 2\sqrt{x^2 + y^2}$.
2. The *definition* of directional derivative at the origin, in the direction v, is $\frac{\mathrm{d}}{\mathrm{d}t} f(tv)\Big|_{t=0}$. If $v = (a, b)$ with $b \neq 0$ then this is

$$\frac{\mathrm{d}}{\mathrm{d}t}\left(1 - \cos \frac{a^2 t}{b}\right) t|v|.$$

   which evaluates to 0 at $t = 0$. If $b = 0$ then the derivative is also 0.
3. Because all directional derivatives are equal to 0, one might be tempted to conclude that the function is differentiable, with derivative 0. Indeed, if it *were* differentiable, this would have to be the derivative. But this is not the case, because we can consider the curve $r(t) = (t, t^2)$. $f(r(t))/|r(t)|$ does not approach 0 as $t \to 0$.

□

I'm too lazy to write out explicit solutions for the rest, so I'll just summarize the takeaways.

If you're asked to show that the image of a function contains a neighborhood of some point, it's a good bet that you'll need to use the Inverse Function Theorem (show that the Jacobian at the appropriate point has nonzero determinant).

If you need to compute the derivative of a matrix function, you could write it out explicitly, or you can make use of directional derivatives. Namely, we can compute the derivative of F in the direction of A at the point B via

$$(D_B F)A = \frac{\mathrm{d}}{\mathrm{d}t} f(B + tA)\Big|_{t=0}.$$

The RHS is univariate, so it is easy to differentiate.

If X is some *connected* space and you want to show that some set $S \subset X$ is the entirety of X, you could try showing that S is both open and closed (and non-empty).

It's easy to show that if the Jacobian of a map is everywhere invertible, then the map is open.

Proper maps are closed. Argument: if y is a limit point of $f(C)$, take $y_n \to y$ inside $f(C)$. Note that $\{y_n\} \cup \{y\}$ is compact, so by properness its preimage is as well. So pick $x_n \mapsto y_n$ where $x_n \in C$ and consider a convergent subsequence...

For metric spaces, a continuous map is proper if and only if every sequence that escapes to infinity is mapped to such a sequence as well. (Escapes to infinity: for every compact set S, only finitely many of the points are inside S.)

In problems involving periodic functions, consider using the Fourier transform. By the way, the equidistribution theorem about numbers like $a + b\alpha$ ($a, b \in \mathbb{Z}$, α irrational) is proved using Fourier series. Probably the most useful sufficient criterion about Fourier series convergence is as follows: if the function f is continuous and its Fourier coefficients are absolutely summable, then its Fourier series converges uniformly to f. The Fourier coefficients are given by

$$\int_I e^{-2\pi i n x} f(x) \mathrm{d}x$$

up to some appropriate constant (which can easily be determined by thinking of the expression as an inner product). For playing around with these integrals, shifting the variable of integration and exploiting periodicity can be helpful.

L'Hopital's rule *assumes* the existence of $\lim f'/g'$. The existence of $\lim f/g$ does not necessitate the existence of $\lim f'/g'$. Example: $f(x) = x^2 \sin(1/x)$ (a very common counterexample) and $g(x) = x$.

1.5 8/3/18: Complex analysis 1

Morera's theorem is a useful way of proving that something is holomorphic when you aren't given much else about the function. Holomorphic functions enjoy many properties that real differentiable functions do not: for example the uniform limit of holomorphic functions is also holomorphic, while the analogous statement for real functions is

blatantly false by Stone-Weierstrass (any continuous function on a closed interval can be approximated uniformly by polynomials).

By the way, for Morera's theorem, you need only show that the integral is zero on all elements of a family $\mathcal{F}$ of toy contours which is closed under translation and dilation. So for example, the family of all circles would suffice.

If a holomorphic function is bounded near a singularity, then that singularity is removable. A singularity a is removable, by definition, when $\lim_{z\to a}(z-a)f(z) = 0$.

Open mapping theorem: If U is a domain (connected open subset) and $f: U \to \mathbb{C}$ is holomorphic and *non-constant*, then it is open. Contrast this with the real case (consider a parabola for example).

By the way, that means that if you have a non-constant holomorphic map from an open set to any set $C \subset \mathbb{C}$, the image of the map lands in the interior of C. This is useful if C is the closed unit disk for example, because then we can use many of the below tools on the open unit disk.

Conformal map: holomorphic with everywhere nonzero derivative. Note that this is a local condition: preserving angles. Some people use conformal to mean "one-to-one and holomorphic," which is stronger and involves a global condition that is not satisfied by e.g. the exponential function. Why is this stronger? One-to-one and holomorphic implies nonzero derivative everywhere. This can proved by contradiction using series expansion and Rouché's theorem.

Schwarz lemma: should be considered for just about any problem about the open unit disk $\mathbb{D}$. Let $f: \mathbb{D} \to \mathbb{D}$ be holomorphic and $f(0) = 0$. Then $|f(z)| \le |z|$ and $|f'(0)| \le 1$. Moreover, if equality holds for either of the preceding inequalities for *some* value of z, then f is in fact a rotation.

If you're asked to find the maximum possible value of some holomorphic function at a given point given some constraints on the function, this lemma may be useful.

Blaschke factor: often used in tandem with the preceding. Special function with nice properties:

- $f_{z_0}: \mathbb{D} \to \mathbb{D}$ is an automorphism. In fact, it is its own inverse.
- $f_{z_0}(z_0) = 0$.

The formula is given by

$$f_{z_0}(z) = \frac{z - z_0}{\overline{z_0} z - 1}, \quad z_0 \in \mathbb{D}$$

though often times just knowing such a function exists is enough to solve problems.

Mobius transformation: useful for mapping between half-plane and unit disk. We construct a map from the upper half-plane to the unit disk by

$$\frac{z - i}{z + i}$$

since points in the upper half-plane are closer to i than to $-i$. There is a map $GL(2,\mathbb{C}) \to Aut(\hat{\mathbb{C}})$ which sends

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \frac{az+b}{cz+d}$$

that is, in fact, a group homomorphism. In particular, this gives a convenient way of composing/inverting Mobius transformations.

Maximum modulus principle: if f is holomorphic at z_0, then we cannot have $|f(z_0)| \geq |f(z)|$ for all z in any neighborhood of z_0. This can be proven easily using the open mapping theorem. Minimum modulus is fine too, provided it's nonzero. Also useful to state as: a function obtains its maximal modulus along boundary (of closed bounded domain).

Liouville's theorem: an entire bounded function is constant. Proved by using Cauchy's integral formula for the derivative along arbitrarily large circles around any given point.

If you're given constraints on the real part of a function, consider exponentiation. Or if you have constraints on the imaginary part, first multiply by i and then exponentiate.

1.6 8/8/18: Complex analysis 2

S&S has the following example of a function which is holomorphic on $\mathbb{D}$, can be extended continuously to $\overline{\mathbb{D}}$, but cannot be extended holomorphically past:

$$\sum_{n=0}^{\infty} 2^{-n\alpha} z^{2^n}$$

for some $0 < \alpha < \infty$. Trying to *prove* this, however, is not that easy (I haven't done it). It's a particularly pathological example involving a nowhere-differentiable function.

There are three kinds of actual singularities: removable, pole, and essential. They can be distinguished using the Laurent series about the singularity: consider what happens to behavior around the point after multiplying the function by $(z-z_0)^n$. If using $n=1$ causes the function to approach 0 at z_0, then it's removable. If this is achieved by some higher power, then it's a pole (if $n=2$, then we have a simple pole, corresponding to the $a_{-1}/(z-z_0)$ term being the lowest in the series expansion). If this is not achieved by any value of n, then the singularity is essential.

There's another kind of "singularity" to keep in mind: branch points. Basically, some functions can't be defined globally (for topological reasons or otherwise), or more specifically, in a neighborhood around a specific point. Consider $f(z) = \sqrt{z}$, which cannot be defined in a neighborhood of the origin. Such examples can be useful for exhibiting holomorphic functions that can't be extended in certain ways.

Identity theorem: if a holomorphic function vanishes on a domain with an accumulation point, then it is identically zero.

Schwarz reflection principle: often used in tandem with the preceding. If $f(z)$ is holomorphic, so is $\overline{f}(\overline{z})$. That's the trivial form: a less trivial form states that it's possible to extend a holomorphic function across the real axis if it takes real values on the real

axis. The subtlety is holomorphicity along the axis, but that can be shown using Morera's theorem.

Generalized Liouville's theorem: if there exists c such that $|f(z)| \leq c|z|^n$ for sufficiently large $|z|$, then f is a polynomial of degree at most n. Proved using induction, with ordinary Liouville's as base case.

Got a pole at infinity? Consider the function $f(1/z)$ instead to get a pole at zero.

Laurent expansion is a powerful tool that is worth trying, especially for analyzing singularities.

For an essential singularity, for *any* complex number w, it is possible to pick a sequence converging to the singularity whose image under f converges to w. Little/great Picard's theorems. Little: an entire and non-constant function misses at most one point. Great: on any punctured neighborhood of an essential singularity, the image of f misses at most one point. Great can be used to prove little by considering polynomial and non-polynomial cases separately.

Rouché's theorem: a useful tool for counting roots with multiplicity. Might as well remember the symmetric version: if

$$|f(z) - g(z)| < |f(z)| + |g(z)|$$

everywhere on the simple contour ∂K for some bounded region K, then f, g have the same number of roots counting multiplicity inside K. Proof: homotopy invariance of winding number (which counts number of roots with multiplicity).

Chapter 2

Algebra

2.1 7/18/18: Group theory

Problem 2.1.1. Let G be a finite group of order n with the property that for each divisor d of n there is at most one subgroup in G of order d. Show G is cyclic.

Solution: First we reduce to the case that $|G| = p^\alpha$ for some prime p. Note that if

$$|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

then we can invoke the Sylow theorems to deduce that each Sylow p-subgroup is normal, and that G is the direct product of them. So, if we show the result for p^α, then the general case follows from the Chinese Remainder Theorem for instance.

Next is essentially a counting argument. If G has no elements of order p^α, then it can have at most one subgroup of each of the orders $1, p, \dots, p^{\alpha-1}$, and each element must belong to one of these subgroups. But

$$1 + p + \cdots + p^{\alpha-1} = \frac{p^\alpha - 1}{p - 1} < p^\alpha$$

so this is impossible. □

Problem 2.1.2.

1. Let G be a finite group and let X be the set of pairs of commuting elements of G

$$X = \{(g, h) \subset G \times G : gh = hg\}.$$

   Prove that $|X| = c|G|$ where c is the number of conjugacy classes in G.

2. Compute the number of pairs of commuting permutations on five letters.

Solution:

1. For each $g \in G$, we count the number of elements that commute with g. Consider the action of G on itself by conjugation. The elements which commute with g is then $\mathrm{Stab}(g)$. The orbit-stabilizer theorem tells us

$$[G : \mathrm{Stab}(g)] = |C_g|$$

where C_g is the conjugacy class of g. Hence we sum $|G|/|C_g|$ over all elements $g \in G$. But the sum over each conjugacy class is $|G|$, so the total sum is $c|G|$ as claimed.

2. The number of conjugacy classes in S_5 is the number of partitions of the number 5: there are 7 of these. Hence by the preceding part the answer is $5!7 = 840$.

□

Problem 2.1.3. Prove that every group of order 30 has a cyclic subgroup of order 15.

Solution: Intense Sylow bashing. Essentially there are two steps: first show that every group of order 30 has a subgroup of order 15, and then that the only group of order 15 is $\mathbb{Z}/15$.

First step: let H be a Sylow 3-subgroup and K be a Sylow 5-subgroup. Use counting to show that one of these has no conjugates (it is the unique Sylow p-group). Then HK is a subgroup of order 15.

Second step: use Sylow theorems again to show that every group of order 15 has only one Sylow 3-group and one 5-group, so they are both normal and the group is the direct product $\mathbb{Z}/15$. □

Problem 2.1.4. Find the smallest n for which the permutation group S_n contains a cyclic subgroup of order 111.

Solution: Asking for a cyclic subgroup of order 111 is the same as asking for an element of order 111. Every element of S_n has a disjoint cycle decomposition, and the order of an element is the LCM of the cycle lengths in this decomposition.

Since $111 = 3 \cdot 37$, the answer is $3 + 37 = 40$. An element such as

$$(1\,2\,3 \cdots 37)(38\,39\,40)$$

will do the trick. □

Problem 2.1.5 (Poincare's Theorem)**.** Let G be a group and $H \leq G$ a subgroup of finite index n. Show that G contains a normal subgroup N such that $N \leq H$ and the index of N is $\leq n!$.

Solution: The presence of $n!$ strongly suggests that we do something with S_n. Consider the (left) action of G on the (left) cosets of H. This action defines a map $\alpha: G \to S_n$. Note that the only elements of G which fix the coset containing the identity 1 are the elements of H. Thus $N \coloneqq \ker \alpha \subseteq H$. Since $G/N \cong \alpha(G)$, we have

$$|G/N| = |\alpha(G)| \leq |S_n| = n!$$

as wanted. □

Problem 2.1.6.

1. Let G be a non-abelian finite group. Show that $G/Z(G)$ is not cyclic, where $Z(G)$ is the center of G.
2. If $|G| = p^n$, with p prime and $n > 0$, show that $Z(G)$ is not trivial.
3. If $|G| = p^2$, show that G is abelian.

Solution:

1. This is easy to show by contradiction; suppose that $G/Z(G)$ is cyclic and generated by an element $[\alpha]$, where $\alpha \in G$. Then any element of G can be written in the form $\alpha^k z$ where $z \in Z(G)$. But elements of this form commute, so G must be abelian.
2. Use the "class equation," which is to say we consider partitioning G into its conjugacy classes. The singleton conjugacy classes correspond to elements of $Z(G)$. Since the identity is in its own conjugacy class, there must be at least p singletons, as the size of each conjugacy class must divide $|G| = p^n$.
3. The center cannot be of size p by the first part, and it cannot be trivial by the second. So it must be of size p^2, i.e. the whole group.

□

Problem 2.1.7. Use the simplicity of A_6 to show that A_6 does not have an index 3 subgroup. Then show that there are no simple groups of order 120.

Solution: The first part is an immediate consequence of Poincare's theorem (a previous problem in this section). If you don't want to invoke the theorem, you can prove this statement in the same fashion.

For the second part, consider the Sylow 5-groups of a group G of order 120. There can either be 1 or 6 of them. In the former case, we have a normal subgroup so G is not simple. In the latter, G acts on the Sylow 5-groups by conjugation, producing a map $G \to S_6$. If this map is not injective, then its kernel is a proper normal subgroup. If the image strictly contains A_6, then the preimage of A_6 is a normal subgroup. Otherwise we have an embedding of G within A_6. But A_6 has no index 3 subgroups, so this is impossible. □

2.2 7/23/18: Rings 1

Problem 2.2.1. Let F be a field and let $M_n(F)$ be the ring of $n \times n$ matrices with coefficients in F. Prove that $M_n(F)$ has no nontrivial (two-sided) ideals. What can you conclude about ring homomorphisms from $M_n(F)$?

Solution: Suppose $\mathfrak{a}$ is a nonzero ideal, and let $A \in \mathfrak{a}$. Multiply A (on both sides as needed) by matrices which are entirely zero except for a single 1 in one spot in order to get a matrix with only one non-zero entry. Then use permutation matrices (again on both sides as needed) to move that non-zero entry to all diagonal locations—take the sum and scale to get the identity. Thus $\mathfrak{a} = (1)$.

It follows that ring homomorphisms from $M_n(F)$ are always injective (provided that the target is not the zero ring).

We remark that the statement of the problem is certainly untrue if we consider one-sided ideals: consider the ideal of matrices whose kernels contain a fixed subspace of F^n, for example (or whose images are contained within a fixed subspace). □

Problem 2.2.2. Let R be the set of complex numbers of the form

$$a + 3bi, \quad a, b \in \mathbb{Z}.$$

Prove that R is a subring of $\mathbb{C}$ and that R is an integral domain but not a unique factorization domain.

Solution: To see that it is a subring of $\mathbb{C}$, one needs only check closure, which we omit. The fact that R is an integral domain is obvious, because $\mathbb{C}$ is one (indeed, it is a field).

To show that R is *not* a UFD, as in the words of my former algebra professor Andrei Negut, "use the norm!". (The "norm" we use is actually the "norm squared" but it's more convenient because it's an integer and still enjoys the multiplicative properties of the norm.)

$$N(a + 3bi) \coloneqq a^2 + 9b^2.$$

The possible values of N are $0, 1, 4, 9, \ldots$. Now consider

$$(1 + 3i)(1 - 3i) = 10 = 2 \cdot 5.$$

If R were a UFD, since $N(2) = 4$ is irreducible, it must divide one of the two terms on the left. This is because we have "unique factorization into irreducibles, up to units," or alternatively that irreducibles are prime in a UFD. But norm considerations show that this is impossible. □

Problem 2.2.3. Let m and n be positive integers. Prove that the ideal generated by $x^m - 1$ and $x^n - 1$ in $\mathbb{Z}[x]$ is principal.

Remark. The division algorithm works in $R[x]$ provided the thing we're dividing by is monic (leading coefficient is a unit).

Solution: Use the Euclidean algorithm to show that $x^{\gcd(m,n)} - 1 \in (x^m - 1, x^n - 1)$. Then we conclude

$$(x^{\gcd(m,n)} - 1) = (x^m - 1, x^n - 1)$$

because the other inclusion is obvious by divisibility. □

Problem 2.2.4. Let R be a finite commutative ring with unity which has no zero-divisors and contains at least one element other than 0. Prove that R is a field.

Solution: We know that R is not the zero ring, so to show that R is a field, we need only show that every element of R is a unit (has an inverse). To that end, let $r \in R$ and consider the map "multiplication by r." Since R has no zero-divisors, we deduce

$$- \cdot r \colon R \to R$$

is injective. But R is *finite*, so that means it's also surjective. Hence r has an inverse, as desired.

The statement is obviously untrue without the finiteness assumption; consider $R = \mathbb{Z}$. □

Problem 2.2.5. Let F be a field and X a finite set. Let $R(X, F)$ be the ring of all functions from X to F, endowed with pointwise operations. What are the maximal ideals of $R(X, F)$?

Solution: There are a number of ways that one could show the ideals of $R(X, F)$ are precisely sets of the form $I(S)$ where $S \subseteq X$ and I denotes "ideal vanishing on." Possibly the most direct and elementary way is by considering "supports" and then using multiplication by indicator functions.

Alternatively, one can use, in some form, $\operatorname{Spec} \prod = \coprod \operatorname{Spec}$ for finite products. The ideals of a product are products of ideals, and the prime ideals are a prime ideal in one of the rings, times all the other rings. □

Problem 2.2.6. Let R be a principal ideal domain and let I and J be nonzero ideals. Show that $IJ = I \cap J$ if and only if $I + J = R$.

Solution: The implication $I + J = R \implies IJ = I \cap J$ does not require that R is a PID. Just note that $i + j = 1$ for some $i \in I$ and $j \in J$, and then for $x \in I \cap J$ we have

$$x = x(i + j) = xi + xj \in IJ.$$

Of course, it is always true that $IJ \subseteq I \cap J$.

For the other direction, we proceed more or less "directly." I had some trouble with this, mostly because I didn't "push aggressively enough" with the information provided. Write $I + J = (k)$ for some $k \in R$, and $I = (m)$ and $J = (n)$. So then we must have $m = kx$ and $n = ky$ for some $x, y \in R$. Now $kxy \in I \cap J \subseteq IJ$, meaning that it is a multiple of $(kx)(ky)$. Since we are working in a domain, it follows that 1 is a multiple of k, i.e. that k is a unit. so $I + J = R$.

There are some analogies with this argument to the intuitive lcm and gcd argument for $\mathbb{Z}$. □

Problem 2.2.7. By the fundamental theorem of algebra, the polynomial x^3+2x^2+7x+1 has three complex roots, α_1, α_2 and α_3. Compute $\alpha_1^3+\alpha_2^3+\alpha_3^3$.

Solution: When I saw this problem, I knew to write the desired expression in terms of elementary symmetric functions and to use Vieta's formulas. What I did *not* think of, however, is that I can first simplify the desired expression by using the fact that the α_i are roots of the given polynomial!

That makes the problem somewhat simpler (although the original approach would've worked too). The simplification would be a lot more important if the desired expression had very high degree. □

Problem 2.2.8. Let $\mathfrak{a}$ be the ideal in $\mathbb{Z}[x]$ generated by 5 and x^3+x+1. Is $\mathfrak{a}$ prime?

Solution: Let $R=\mathbb{Z}[x]$. We are interested in whether $R/\mathfrak{a}$ is an integral domain. We will use the fact that

$$R/\mathfrak{a} = \frac{R/(5)}{\mathfrak{a}/(5)} = (\mathbb{Z}/5)[x]/(x^3+x+1).$$

$\mathbb{Z}/5$ is a field, so $(\mathbb{Z}/5)[x]$ is a UFD and our question is equivalent to asking whether x^3+x+1 is irreducible. It doesn't have a root in $\mathbb{Z}/5$, so it is. □

Remark. There's a potentially useful "converse" of sorts; see Theorem 2.28 in Altman-Kleiman's CA notes.

Problem 2.2.9. Let $f_n(x)=x^{n-1}+x^{n-2}+\cdots+x+1$. Show that $f_n(x)$ is irreducible in $\mathbb{Q}[x]$ if n is prime. What if n is composite?

Solution: Apply the shift $x=(y+1)$, noting that

$$f_n(x) = \frac{x^n-1}{x-1} = ((y+1)^n-1)/y$$

satisfies Eisenstein's criterion for irreducibility. So the original (unshifted) polynomial is irreducible too.

If $n=mk$ is composite, then

$$f_n(x) = (x^{m-1}+\cdots+1)(x^{(k-1)m}+x^{(k-2)m}+\cdots+1).$$

I don't know if there's a motivated way of seeing this. □

Remark. Good idea to review cyclotomic polynomials, perhaps? Maybe that can offer some motivation.

Problem 2.2.10. Factor x^4+x^3+x+3 completely in $(\mathbb{Z}/5)[x]$.

Solution: It has no roots in $\mathbb{Z}/5$, so if it did factor, it must factor into two quadratics. Since $\mathbb{Z}/5$ is a field, we can assume that the two quadratics are monic:

$$(x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (d + ac + b)x^2 + (ad + bc)x + bd.$$

Is there anything better to do here than trial and error? We can eliminate a few possibilities since the quadratics need to be irreducible, but still...

There are 10 irreducible quadratics over $\mathbb{Z}/5$. They are

$$x^2 + 2, x^2 + 3, x^2 + x + 1, x^2 + x + 2,$$
$$x^2 + 2x + 3, x^2 + 2x + 4, x^2 + 3x + 3, x^2 + 3x + 4,$$
$$x^2 + 4x + 1, x^2 + 4x + 2.$$

There's no way to factor it. □

2.3 7/27/18: Rings 2

Problem 2.3.1. Prove that a finite subgroup of the multiplicative group of a field is cyclic.

Problem 2.3.2. Let F be a field of characteristic $p > 0$, $p \neq 3$. If α is a zero of the polynomial $f(x) = x^p - x + 3$ in an extension field of F, show that $f(x)$ has p distinct zeros in the field $F(\alpha)$.

Problem 2.3.3. Exhibit infinitely many pairwise nonisomorphic quadratic extensions of $\mathbb{Q}$ and show they are pairwise nonisomorphic.

Problem 2.3.4. Let $\mathbb{Q}$ be the field of rational numbers. For θ a real number, let $F_\theta = \mathbb{Q}(\sin\theta)$ and $E_\theta = \mathbb{Q}(\sin\frac{\theta}{3})$. Show that E_θ is an extension field of F_θ and determine all possibilities for $\dim_{F_\theta} E_\theta$. (Use trigonometric identities.)

Problem 2.3.5. Show that the field $\mathbb{Q}(t_1, \ldots, t_n)$ of rational functions in n variables over the rational numbers is isomorphic to a subfield of $\mathbb{R}$.

Problem 2.3.6. Let $\mathbb{F}$ be a finite field of cardinality p^n, with p prime and $n > 0$, and let G be the group of invertible 2×2 matrices with coefficients in $\mathbb{F}$.

1. Prove that G has order $(p^{2n} - 1)(p^{2n} - p^n)$.
2. Show that any $p - Sylow$ subgroup of G is isomorphic to the additive group of F.

Problem 2.3.7. Let p be a prime and $\mathbb{F}_p$ the field of p elements. How many elements of $\mathbb{F}_p$ have square roots in $\mathbb{F}_p$? Cube roots? (You may separate into cases for p.)

Problem 2.3.8. Let $n \geq 2$ be an integer such that $2^n + n^2$ is prime. Prove that

$$n \equiv 3 \pmod 6.$$

Problem 2.3.9. Determine the rightmost decimal digit of

$$A = 17^{17^{17}}.$$

Problem 2.3.10. Let ϕ be Euler's function. Let a and k be two integers, with $a > 1, k > 0$. Prove that k divides $\phi(a^k - 1)$.