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. □

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, Spec $\prod$ = $\coprod$ 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. □