MATH 8, SECTION 1, WEEK 1 - RECITATION NOTES

TA: PADRAIC BARTLETT

Abstract. These are the notes from Friday, Oct. 1st's lecture. In this talk, we study one last example of induction, discuss proofs by contrapositive, and examine the field axioms of $\mathbb{R}$ (specifically, we look for other objects that satisfy these rules, and ask when such things can exist.)

1. Random Question

Question 1.1. *Can you cover the plane $\mathbb{R}^2$ with closed disks[1] of positive radius, so that no two disks intersect at more than one point?*

2. Proofs by Induction: One More Example

In our last lecture, we discussed proofs by induction. Just to make sure that the concept of an inductive proof is solid, we offer one more example here:

Claim 2.1. *(Bernoulli) $(1+a)^n \geq 1+na$, for any $a \in \mathbb{R}, n \in \mathbb{N}$.*

Proof. We proceed by induction.

Base case: $n = 1$. In this case, our claim is trivial, as $(1+a)^1 = 1+a = 1+1\cdot a$, for any a.

Inductive step: Assuming that $(1+a)^k \geq 1+ka$, for k between 1 and n, we want to prove that

$$(1+a)^{n+1} \geq 1+(n+1)a.$$

How do we do this?

Well: if we factor out a copy of $(1+a)$ from the left hand side, we have that

$$(1+a)^{n+1} = (1+a)\cdot(1+a)^n.$$

Why would we do this? Well, the nice thing about our factoring is that it breaks our left hand side into two parts, one of which is really simple [i.e. $(1+a)$] and one of which we can apply our inductive hypothesis to [i.e. $(1+a)^n$]. Having done this, we can then apply our inductive hypothesis, which gives us

$$\begin{aligned}(1+a)^{n+1} &= (1+a)\cdot(1+a)^n \\ &\geq (1+a)(1+na) \\ &= 1+a+na+na^2 \\ &= 1+(n+1)a+na^2.\end{aligned}$$

[1] A **closed disk** is just a filled-in circle in $\mathbb{R}^2$; explicitly, it's a collection of points $\{(x,y) : (x-a)^2+(y-b)^2 \leq r\}$ for some $a, b, r \in \mathbb{R}$.

Because na^2 is positive, we can discard this term (as it is only making the right-hand side larger,) to get

$$(1+a)^{n+1} \geq 1 + (n+1)a$$

as claimed. □

3. Proofs by Contrapositive

The last proof method we have to introduce is, conveniently, one of the easiest – the concept of "proof by contrapositive." The structure of a proof by contrapositive is remarkably simple:

(1) Suppose we want to prove some statement of the form $P \Rightarrow Q$.
(2) By our earlier work in class, we know that $\neg Q \Rightarrow \neg P$ being true is equivalent to $P \Rightarrow Q$ being true.
(3) So: if we want to prove $P \Rightarrow Q$, we can just prove $\neg Q \Rightarrow \neg P$ instead!

Basically, proofs by contrapositive are just proofs that . . . use the contrapositive. Their structure is accordingly easy; the interesting thing to think about with them is *when* to use them, which the two following examples will hopefully illustrate:

Claim 3.1. *If n^2 is odd, then n is odd, for any $n \in \mathbb{N}$.*

Proof. Forgetting about which section of the notes we're in at the moment, let's try to prove this directly for a second: i.e. given that $n^2 = 2k+1$ for some k, can we deduce that n is odd? Looking at this, it seems not particularly obvious why this might be true at all; that n^2 is odd only tells us things about the factorization of n^2, which we'd then have to turn into arguments about the factors of n and do a number of somewhat mildly-tricky things (like proving that $1/2$ isn't an integer, depending on how pedantic you feel.)

Presented with such a situation – where our assumed condition, $n^2 = 2k+1$, is something that looks easy to check but difficult to prove – we are *strongly* motivated to try a proof by contrapositive! In other words, instead of proving

$$\text{If } n^2 \text{ is odd, then } n \text{ is odd, for any } n \in \mathbb{N},$$

let's prove

$$\text{If n is even, then } n^2 \text{ is even, for any } n \in \mathbb{N}.$$

But this is now incredibly trivial! – if $n = 2k$ for some k, $n^2 = 2(2k^2)$, so we're done. □

This is the power of the contrapositive: instead of starting from a relatively difficult-to-use condition, we got to start from a really nice one! In essence, it turns tricky proofs into easier ones, as the next example also illustrates:

Claim 3.2. *If $n \equiv 2 \mod 3$[2], n is not a square.*

Proof. Again, a direct approach looks hard; in other words, suppose that we know $n \equiv 2 \mod 3$. Relating this to whether n is not a square seems. . . hard. How can we tell if something isn't a square? Check all of the powers of the prime factors? Difficult, right?

Instead, let's work with the contrapositive of our claim: i.e. let's try to prove

[2]We write that $a \equiv b \mod c$ iff $a - b$ is a multiple of c: in other words, that a and b are the "same" up to some number of copies of c.

Claim 3.3. *If n is a square, then $n \not\equiv 2 \mod 3$.*

Equivalently, because every number is equivalent to either $0, 1$, or $2 \mod 3$, we're trying to prove the following:

Claim 3.4. *k^2 is $\equiv 0$ or $1 \mod 3$, for every $k \in \mathbb{N}$.*

This is now a much easier claim! – the initial condition is really easy to work with, and the later condition is rather easy to check. So, now that we have some confidence in our ability to prove this, let's try it!

Take any number k. We can break k into three cases:

(1) $k \equiv 0 \mod 3$.
(2) $k \equiv 1 \mod 3$.
(3) $k \equiv 2 \mod 3$.

(any natural number k has one of these three remainders when divided by 3, so these three cases cover all of the possibilities for k.)

In case 1, $k \equiv 0 \mod 3$ means that k is a multiple of 3, which means that k^2 is also a multiple of 3 and thus that $k^2 \equiv 0 \mod 3$.

In case 2, $k \equiv 1 \mod 3$ means that $k = 3m + 1$, for some m; squaring this gives us $k^2 = 9m^2 + 6m + 1 = 3(3m^2 + 2m) + 1$, and thus that $k^2 \equiv 1 \mod 3$.

Finally, in case 2, $k \equiv 2 \mod 3$ means that $k = 3m + 2$, for some m; squaring this gives us $k^2 = 9m^2 + 12m + 4 = 3(3m^2 + 4m + 1) + 1$, and thus that $k^2 \equiv 1 \mod 3$.

Thus, for any value of k, we have that k^2 isn't congruent to 2 mod 3; so we've proven our claim! □

4. Field Axioms

The real numbers $\mathbb{R}$ satisfy a number of curious properties and rules: one set of these rules, which you may be familar with, are called the **field axioms**. We list them below:

(1) **Closure**: For any x, y in $\mathbb{R}$, $x + y$ and $x \cdot y$ are also in $\mathbb{R}$.
(2) **Identity**: There are elements $0, 1$ in $\mathbb{R}$, $0 \neq 1$, such that $0 + x = x$ and $1 \cdot x = x$, for any $x \in \mathbb{R}$.
(3) **Inverse**: For any $x \in \mathbb{R}, x \neq 0$, there are elements $-x, x^{-1}$ in $\mathbb{R}$ such that $x + (-x) = 0$ and $x \cdot x^{-1} = 1$.
(4) **Associativity**: For any $x, y, z \in \mathbb{R}$, $x+(y+z) = (x+y)+z$ and $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
(5) **Commutativity**: For any $x, y \in \mathbb{R}$, $x + y = y + x$ and $x \cdot y = y \cdot x$.
(6) **Distributivity**: For any $x, y, z \in \mathbb{R}$, $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

Here's a question: are there other mathematical structures that also satisfy all of these rules? The answer, as it turns out, is yes! – examples you're probably familiar with are the rational numbers, $\mathbb{Q}$, and the complex numbers, $\mathbb{C}$. We are also familiar with structures that are *not* fields: the integers with their usual operations of $+$ and $\cdot$, for example, are not a field because 2 doesn't have a multiplicative inverse.

So: one property all three of our fields have in common is that they are all infinte. Does this have to be the case?

Perhaps surprisingly enough, the answer is the following:

Theorem 4.1. *There are finite fields.*

Proof. We need to start somewhere: so, let's try to make the *smallest* field possible. How many elements do we need? Well, we know (by the axioms of identity) that our field must contain at least two elements: 0 and 1, with $0 \neq 1$. Do we need any more elements?

Well, let's try to make multiplication and addition tables with just these two:

$+$	0	1
0	0	1
1	1	$\square$

$\cdot$	0	1
0	$\Diamond$	0
1	0	1

The axioms of identity force all of the filled-in entries, with the exception of $1+1$ and $0 \cdot 0$. In class on Wednesday, however, we proved that $0 \cdot x = 0$ for any x using just the field axioms: so we know that $\Diamond$ must be 0. This just leaves $1+1$: so what should this be?

Well: if we don't introduce any other symbols, we only have two choices: 0 and 1. But wait! – we know, by the axiom of additive inverse, that there has to be some element to add to 1 to get 0. As $0 + 1 = 1 \neq 0$, we know that 0 is not that element – so 1 must be its own additive inverse! In other words, $1 + 1 = 0$: so we have the addition and multiplication tables given by

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Check the axioms: this is a field!

Specifically, as the eagle-eyed among you pointed out in class, this is the field acquired by using addition mod 2: in other words, this is the field you get by taking the numbers 0 and 1, adding/multiplying them, and then looking at the remainders after multiplying by 2. Inspired in some sense by this observation, we call this field $\mathbb{Z}/2\mathbb{Z}$, and ask ourselves the following natural question: was there something special about 2, or can this work for general n?

Well: let's look at $n = 3$. In this case, our set would be the three possible remainders after dividing an integer by 3 – $\{0, 1, 2\}$ – and our addition/multiplication tables would come from using our normal operations and then taking everything mod 3:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Checking the axioms, this is again a field!

That's encouraging: what about $n = 4$? As before, our set is just $\{0, 1, 2, 3\}$, and our tables are

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

However, in this case, we don't satisfy all of our axioms: specifically, there is no multiplicative inverse for 2.

So: what cases does our construction work for? Which ones does it fail for? Does its failure mean that there isn't a finite field of that size? Is there a finite field of order 4?

We may (hopefully, will!) return to these questions later; in the meantime, try to resolve some of these for yourselves, and see what you can prove! □