Let me just finish off Chapter 3. Recall last time we proved

Theorem 3.23. If $n \in \mathbb{Z}_{\geq 1}$ then there exactly n complex numbers ζ satisfying $\zeta^n = 1$.

A fancy way of saying this is that there are n nth roots of unity. The proof showed that the n solutions are $\text{cis}(2\pi/n)^j$ for $0 \leq j \leq n-1$.

We can go one better though – we can prove that *every* non-zero complex number has n nth roots!

However we will have to *assume* that for every $n \geq 1$, every positive real number r has a unique positive real nth root $r^{1/n}$.

This needs justification, and doesn't follow from all the things we assumed about real numbers so far.

I'll talk about this later on (when we revisit the reals).

Corollary 3.24. If w is a fixed non-zero complex number and $n \in \mathbb{Z}_{\geq 1}$, then there are exactly n solutions to the equation $z^n = w$.

Proof. Write $w = r\,\text{cis}(\theta)$. Then $z = r^{1/n}\,\text{cis}(\theta/n)$ is a solution, by de Moivre, so certainly at least one solution exists.

Let's fix a solution z_0 to $z_0^n = w$ (and let's note that $z_0 \neq 0$ because $w \neq 0$), and let's say z is any solution, so $z^n = w$.

Then $z_0^n = w = z^n$, so $(z/z_0)^n = 1$.

By 3.23, z/z_0 must be $\text{cis}(2\pi/n)^j$ for some $0 \leq j \leq n-1$.

By 3.23, z/z_0 must be $\operatorname{cis}(2\pi/n)^j$ for some $0 \leq j \leq n-1$.

Hence z must be $z_0 \operatorname{cis}(2\pi/n)^j$ for some $0 \leq j \leq n-1$. And conversely all of these solutions do work, and they're all different.

So indeed there are exactly n solutions to $z^n = w$.

□

Exercise: How many solutions to $z^n = 0$ are there?

We want there to be "n solutions, all of which are 0".

Jean-Pierre Serre, one of the greatest mathematicians of the 20th century, developed modern intersection theory, which enabled us to express this idea rigorously.

Alexandre Grothendieck, another one of the greatest mathematicians of the 20th century, developed a theory of modern algebraic geometry, which gave an even better way of working with such ideas.

[the scheme $\operatorname{Spec}(\mathbb{C}[x]/(x^n))$ is locally free of rank n]
This is non-examinable ;-)

We have seen that a certain equation of degree *n*, namely $X^n - w = 0$, has exactly *n* solutions (if you count them with multiplicities). But what about more general polynomials of degree *n*?

How many solutions are there to $X^5 - X - 1 = 0$ in the complex numbers? Can you prove it?

The *fundamental theorem of algebra* says that every polynomial of degree *n* with complex coefficients has *n* complex roots (when counted with multiplicity). The name of the theorem is bad – it was named in the days when “algebra” meant the same thing as “equations” – but it is an analytical fact about the complex numbers.

The first rigorous proof was published by Argand in 1806. You will see a proof in the 2nd year.

Chapter 4. Induction.

The *principle of mathematical induction* is a technique for proving infinitely many propositions at once.
Say $P(1)$, $P(2)$, $P(3)$, $\ldots$, $P(n), \ldots$ are all *propositions*. Note: $P(n)$ is not a number, or a polynomial – it is a *true-false statement*.

Assume that we know two things:
(1) $P(1)$ is true.
(2) For every positive integer d, we can deduce $P(d+1)$ from $P(d)$.

The principle of mathematical induction states that under these two hypotheses, $P(n)$ is true for every positive integer n.
Formally, the principle says that hypotheses (1) and (2) imply

$$\forall n \in \mathbb{Z}_{\geq 1}, P(n).$$

1) $P(1)$ is true.
2) For every positive integer d, we can deduce $P(d+1)$ from $P(d)$.

Here is an intuitive reason for believing the principle of mathematial induction. We know $P(1)$ is true by the first assumption. Applying the second assumption with $d = 1$, we know $P(1) \implies P(2)$. Hence $P(2)$ is true.

We've just seen that $P(2)$ is true. Applying the second assumption again, we see that $P(2)$ implies $P(3)$, hence $P(3)$ is true.

Continuing in this way, it looks like we can prove $P(n)$ for every n.

Happy?

I am not 100% happy with this intuitive proof. It seems to me that if we want to prove $P(100)$, our proof is 100 lines long, and looks something like this:
$P(1)$ is true
$P(1)$ implies $P(2)$ and hence $P(2)$ is true.
$P(2)$ implies $P(3)$ and hence $P(3)$ is true.
. . .
$P(99)$ inplies $P(100)$ and hence $P(100)$ is true.

The proof of $P(100)$ is hence 100 steps long.

So it seems to me that the proof of $\forall n \in \mathbb{Z}_{\geq 1}, P(n)$ must be infinitely long.

Are infinitely long proofs allowed? I'm not sure they are.

Here is another proof.

Let's assume $P(1)$, and $\forall d \in \mathbb{Z}_{\geq 1}, P(d) \implies P(d+1)$.

I claim that the proposition $\forall n \in \mathbb{Z}_{\geq 1}, P(n)$ is true.

Let's prove it by contradiction!

I hope that all of you can write down the negation of $\forall n \in \mathbb{Z}_{\geq 1}, P(n)$, so why don't I just pause for 30 seconds and let you all do that.

It's $\exists n \in \mathbb{Z}_{\geq 1}, \neg P(n)$, i.e. "there exists an n such that $P(n)$ is false".

So let's assume for a contradiction that $\exists n \in \mathbb{Z}_{\geq 1}, \neg P(n)$ is true.

Let's set $S = \{\, n \in \mathbb{Z}_{\geq 1} \mid \neg P(n) \,\}$, that is, let's let S be the set of n's for which $P(n)$ is false.

Our assumption is that S is non-empty.

Let's choose some positive integer $m \in S$.

Now let T be the elements of the set $\{1, 2, \ldots, m\}$ which are in S; then T is finite and $m \in T$. Let e be the smallest element of T.

Then e is the smallest element of S.

The story so far:
(1) We have infinitely many propositions $P(1)$, $P(2)$, $P(3)$ and so on.

(2) We know $P(1)$ is true, and that for all d we have $P(d) \implies P(d+1)$.

(3) We're assuming for a contradiction that $\forall n, P(n)$ is false.

(4) We hence have a non-empty set $S \subseteq \mathbb{Z}_{\geq 1}$ consisting of the positive integers n such that $P(n)$ is false, and e is its smallest element. In particular $P(e)$ is false.

So what is e?

It can't be 1, because we are assuming $P(1)$ is true, so $1 \notin S$.

So $e = d + 1$ for some $d \in \mathbb{Z}_{\geq 1}$, and $d < e$. Because e is the smallest element of S, this means $d \notin S$. So $P(d)$ is true. And $P(d) \implies P(d+1)$. So $P(d+1) = P(e)$ is true. Contradiction!

Happy?

I am slightly worried that the way to prove that a non-empty subset of $\{1, 2, \ldots, m\}$ has a smallest element is by induction on m...

Let's not worry about this technicality. If you're worried, maybe you should go to the logic course in your third year and learn about the axiom of foundation.

Let's do some induction!

Example 1. For all $n \in \mathbb{Z}_{\geq 1}$, the sum of the first n positive odd integers is n^2.

Test to see if it looks OK: $1 + 3 + 5 + 7 = 16 = 4^2$.

Proof. Let $P(n)$ be the proposition that the sum of the first n positive odd integers is n^2.

The i'th positive odd integer is $2i - 1$.

So $P(n)$ is the statement that $\sum_{i=1}^{n}(2i - 1) = n^2$.

Well $P(1)$ says $1 = 1$, so it is certainly true.

[Do you think $P(0)$ is true?]

$P(n)$ is the statement that $\sum_{i=1}^{n}(2i-1)=n^2$.

Note: anyone who writes that $P(n)=\sum_{i=1}^{n}(2i-1)$ *loses a mark.*

$P(n)$ is not a number, it is a *true-false statement* – a proposition.

Anyway, now say d is a fixed positive integer and let's assume that $P(d)$ is true.
Then $P(d+1)$ is the claim that $\sum_{i=1}^{d+1}(2i-1)=(d+1)^2$.

And $\sum_{i=1}^{d+1}(2i-1)=\sum_{i=1}^{d}(2i-1)+(2d+1)$ (by definition)
$=d^2+(2d+1)$ (by assumption $P(d)$)
$=(d+1)^2$ (by algebra)
and we have deduced the proposition $P(d+1)$.

Hence $P(n)$ is true for all n by induction.

Example 2. Fix $t \in \mathbb{R}$ with $t > -1$. Prove that if $n \in \mathbb{Z}_{\geq 1}$ then $(1+t)^n \geq 1 + nt$.

Proof. Exercise: write down the appropriate statement $P(n)$.

Let $P(n)$ be the statement that $(1+t)^n \geq 1 + nt$.
Then $P(1)$ is the statement that $1 + t \geq 1 + t$, which is certainly true.
And if $P(d)$ is true, then
$(1+t)^{d+1} = (1+t)^d(1+t)$ (by definition)
$\geq (1+dt)(1+t)$ (by induction. . . and the fact that $1+t > 0$)
$= 1 + (d+1)t + dt^2 \geq 1 + (d+1)t$.
So $P(d)$ implies $P(d+1)$, and hence $P(n)$ is true for all $n \geq 1$ by induction.

Example 3. Find all integers $n \geq 1$ such that $n^3 < 3^n$.

Solution. Let's do some experiments.

$n = 1: \ 1^3 = 1 < 3^1 = 3$? **Yes**

$n = 2: \ 2^3 = 8 < 3^2 = 9$? **Yes**

$n = 3: \ 3^3 = 27 < 3^3 = 27$? **No**

Aargh. How do we use induction on this one??

$n = 4: \ 4^3 = 64 < 3^4 = 81$? **Yes**

$n = 5$? $n = 6$? What is the story?

Modified principle of induction (different base). If $k \in \mathbb{Z}$ is a fixed “base”, and $Q(m)$ are true/false statements for $m = k, k+1, k+2, \ldots$, and if:
1) $Q(k)$ is true
2) $Q(e) \implies Q(e+1)$ for all $e \geq k$,
then $Q(m)$ is true for all $m \geq k$.

Do we need to prove this or did we already do it?

Find out next time, in “M1F lecture 13: the return of the Buzzard.”