Partial Fraction Decomposition

Why Your School Teachers Were(n't) Wrong

Sidharth Hariharan sidharth.hariharan21@imperial.ac.uk

How would you simplify the following?

$$\sum_{x=2}^{n} \frac{1}{x-x^2}$$

How would you simplify the following?

$$\sum_{x=2}^{n} \frac{1}{x - x^2} = \sum_{x=2}^{n} \left(\frac{1}{x} - \frac{1}{x - 1} \right)$$

Motivations

How would you simplify the following?

Let's decompose the following:

$$\frac{x^3 + 2x^2 + x + 7}{x^3 + 2x^2 + x + 2}$$

Let's decompose the following:

$$\frac{x^3 + 2x^2 + x + 7}{x^3 + 2x^2 + x + 2} = \frac{x^3 + 2x^2 + x + 2}{x^3 + 2x^2 + x + 2} + \frac{5}{x^3 + 2x^2 + x + 2}$$

Let's decompose the following:

$$\frac{x^3 + 2x^2 + x + 7}{x^3 + 2x^2 + x + 2} = \frac{x^3 + 2x^2 + x + 2}{x^3 + 2x^2 + x + 2} + \frac{5}{x^3 + 2x^2 + x + 2}$$
$$= 1 + \frac{5}{(x+2)(x^2+1)}$$

Let's decompose the following:

$$\frac{x^3 + 2x^2 + x + 7}{x^3 + 2x^2 + x + 2} = \frac{x^3 + 2x^2 + x + 2}{x^3 + 2x^2 + x + 2} + \frac{5}{x^3 + 2x^2 + x + 2}$$
$$= 1 + \frac{5}{(x+2)(x^2+1)}$$

It's not obvious how to proceed from here.

Motivations

Let's decompose the following:

$$\frac{x^3 + 2x^2 + x + 7}{x^3 + 2x^2 + x + 2} = \frac{x^3 + 2x^2 + x + 2}{x^3 + 2x^2 + x + 2} + \frac{5}{x^3 + 2x^2 + x + 2}$$
$$= 1 + \frac{5}{(x+2)(x^2+1)}$$

The "High School method" was to write

$$\frac{5}{(x+2)(x^2+1)} = \frac{a}{x+2} + \frac{bx+c}{x^2+1}$$

and solve for $a, b, c \in \mathbb{R}$.

Motivations

Let's decompose the following:

$$\frac{x^3 + 2x^2 + x + 7}{x^3 + 2x^2 + x + 2} = \frac{x^3 + 2x^2 + x + 2}{x^3 + 2x^2 + x + 2} + \frac{5}{x^3 + 2x^2 + x + 2}$$
$$= 1 + \frac{5}{(x+2)(x^2+1)}$$

The "High School method" was to write

$$\frac{5}{(x+2)(x^2+1)} = \frac{a}{x+2} + \frac{bx+c}{x^2+1}$$

and solve for $a, b, c \in \mathbb{R}$. Doing this gives us a = 1, b = -1, c = 2.

Motivations

Let's decompose the following:

$$\frac{x^3 + 2x^2 + x + 7}{x^3 + 2x^2 + x + 2} = \frac{x^3 + 2x^2 + x + 2}{x^3 + 2x^2 + x + 2} + \frac{5}{x^3 + 2x^2 + x + 2}$$
$$= 1 + \frac{5}{(x+2)(x^2+1)}$$

The "High School method" was to write

$$\frac{5}{(x+2)(x^2+1)} = \frac{a}{x+2} + \frac{bx+c}{x^2+1}$$

and solve for $a, b, c \in \mathbb{R}$. Doing this gives us a = 1, b = -1, c = 2.

But how do we know a, b, c exist?

Motivations

One more example.

Let $(x+1), (x-1) \in \mathbb{R}[X]^1$. We can write

$$\frac{1}{(x+1)(x-1)} = \frac{(-1/2)}{x+1} + \frac{(1/2)}{x-1}$$

But, if we think of (x+1), (x-1) as elements of $\mathbb{Z}[X]$ instead, then this decomposition ceases to be valid, as -1/2 and 1/2 (the numerators on the RHS) are not integers.

(I understand that this is a somewhat pedantic distinction, but the point I'm making is that the existence of the decomposition isn't always guaranteed.)

¹This means they're polynomials with coefficients in \mathbb{R} . More on this shortly.

Imperial College London Discussion

At this point, we may make the following interesting observation:

At this point, we may make the following interesting observation:

The properties of our base structure influence the properties of the polynomials over that structure.

Imperial College London Discussion

At this point, we may make the following interesting observation:

The properties of our base structure influence the properties of the polynomials over that structure.

To determine when we can viably decompose, and to prove that we can in those cases, we need a bit of theory.

Imperial College London On Rings

Typically, the coefficients of a polynomial belong to a kind of algebraic structure known as a **ring**.

On Rings

A **Ring** is a set R with two binary operations + and \cdot such that

- $\forall a, b, c \in R$, (a + b) + c = a + (b + c)
- $\forall a, b \in R$, a + b = b + a
- $\exists 0 \in R \text{ s.t. } \forall x \in R, \ 0 + x = x$
- $\forall x \in R, \ \exists (-x) \in R \text{ s.t. } x + (-x) = 0$
- $\forall a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- $\exists 1 \in R \text{ s.t. } \forall x \in R, 1 \cdot x = x \cdot 1 = x$
- $\forall a, x, y \in R$, $a \cdot (x + y) = a \cdot x + a \cdot y$ and $(x + y) \cdot a = x \cdot a + y \cdot a$

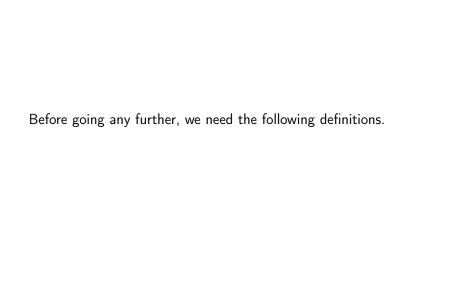
Note that if a ring is nontrivial, then $1 \neq 0$ in that ring. [2]

Imperial College London On Rings

There are many common examples of rings, some of which we're all quite familiar with:

- Z, with normal addition and multiplication
- $\mathbb{Z}/n\mathbb{Z}$, with addition and multiplication modulo n
- Any Field
- $M_n(\mathbb{R})$, with standard matrix addition and multiplication

The rings we'll primarily be dealing with are called **Polynomial** Rings.



Imperial College London Polynomial Rings

Definition (Commutative Ring)

A Commutative Ring is a Ring in which the multiplication operation is commutative.

Imperial College London Polynomial Rings

Before talking about Polynomial Rings, we need the following definitions.

Definition (Commutative Ring)

A Commutative Ring is a Ring in which the multiplication operation is commutative.

Definition (Integral Domain)

An Integral Domain is a Commutative Ring R with $\forall a, b \in R \setminus \{0\}$, we have $ab \neq 0$.

Imperial College London Polynomial Rings

Before talking about Polynomial Rings, we need the following definitions.

Definition (Commutative Ring)

A Commutative Ring is a Ring in which the multiplication operation is commutative.

Definition (Integral Domain)

An Integral Domain is a Commutative Ring R with $\forall a, b \in R \setminus \{0\}$, we have $ab \neq 0$.

Polynomial Rings

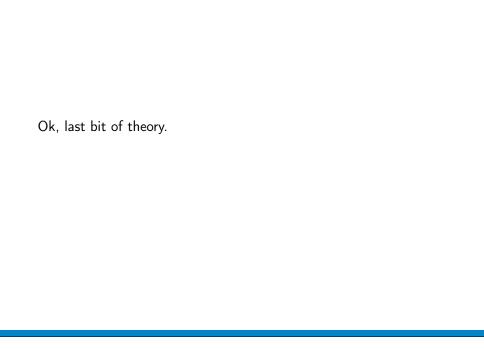
We're now ready for the following:

Definition (Polynomial Ring over an Integral Domain)

If R is an Integral Domain, the set R[X] of polynomials with coefficients in R forms a ring under addition (p+q)(X)=p(X)+q(X) and multiplication (pq)(X)=p(X)q(X).

Note that X does **not** have to belong to R. It is called an "indeterminate" or a "variable" and is treated somewhat like a constant when one manipulates polynomials.

Can you think of an example where one can apply a polynomial to an object not in the base ring?



Imperial College London Fields of Fractions

Roughly speaking, the Field of Fractions K over an Integral Domain R is

"
$$\{p/q: p \in R, q \in R \setminus 0\}$$
" (1)

But, this is a pretty terrible definition... can anyone see why?

Imperial College London Fields of Fractions

To fix the problem, we make use of the following two observations:

- Each element "p/q" consists of two ring elements: p and q
- Each "p/q" would also be expected to be the same as "px/qx" for some $x \in R \setminus 0$. So, each element is not represented by a *unique* pair (p,q).

Field of Fractions

Let R be an ID. Consider the set $J := R \times (R \setminus \{0\})$. Define an equivalence relation \sim on J by $(a,b) \sim (c,d)$ iff ad = bc. This loosely models what we would intuitively expect:

"
$$\frac{a}{b} = \frac{c}{d} \iff ad = bc$$
"

Definition (Field of Fractions)

Given an ID R, we construct a set J as above. Then, the Field of Fractions K of R is the set of Equivalence Classes on J given by \sim , which forms a field under the operations

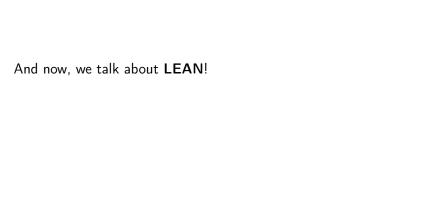
$$[(a,b)] + [(c,d)] = [(ad + bc,bd)]$$
$$[(a,b)] \cdot [(c,d)] = [(ac,bd)]$$

Field of Fractions

At this point, we note the following things:

- The construction of the Field of Fractions mirrors identically the construction of $\mathbb Q$ from $\mathbb Z$ (go back to your IUM notes if you forgot!)
- The reason we need R to be an ID is so that we don't get 0 in the denominator when we multiply two "fractions".
- It is improper to say that $R \subseteq K$ (even though we were taught in school that $\mathbb{Z} \subseteq \mathbb{Q}$). What is true, however, is that there is an injective "inclusion map" going from R to K. In fact, one can even show it to be a ring homomorphism. [1]

(Note: we usually drop the [(p,q)] notation and just use normal fraction notation p/q.)



Imperial College London Introduction to Lean

Lean is a dependent type theory-based programming language that's being used to formalise and verify proofs.

Imperial College London Introduction to Lean

Lean is a dependent type theory-based programming language that's being used to formalise and verify proofs.

In Lean, one can have objects, definitions, theorems and proofs.

Imperial College London Introduction to Lean

Lean is a dependent type theory-based programming language that's being used to formalise and verify proofs.

In Lean, one can have objects, definitions, theorems and proofs.

Every object has a Type and is a term of that Type.

Introduction to Lean

Lean is a dependent type theory-based programming language that's being used to formalise and verify proofs.

In Lean, one can have objects, definitions, theorems and proofs.

Every object has a Type and is a term of that Type.

```
variables (R S : Type) (f : R \rightarrow S) (hf : f.injective)
```

Introduction to Lean

The way theorems work in Lean is that they're maps that take as input the hypotheses and give as output the desired result.

```
theorem my_transitivity (P Q R : Prop) (hPQ : P \rightarrow Q) (hQR : Q \rightarrow R) : P \rightarrow R := begin sorry end
```

Introduction to Lean

The way theorems work in Lean is that they're maps that take as input the hypotheses and give as output the desired result.

```
theorem my_transitivity (P Q R : Prop) (hPQ : P \rightarrow Q) (hQR : Q \rightarrow R) : P \rightarrow R := begin intro hP, sorry end
```

Introduction to Lean

The way theorems work in Lean is that they're maps that take as input the hypotheses and give as output the desired result.

```
theorem my_transitivity (P Q R : Prop) (hPQ : P \rightarrow Q) (hQR : Q \rightarrow R) : P \rightarrow R := begin intro hP, apply hQR, sorry end
```

Introduction to Lean

```
theorem my_transitivity (P Q R : Prop) (hPQ : P \rightarrow Q) (hQR : Q \rightarrow R) : P \rightarrow R := begin intro hP, apply hQR, apply hPQ, sorry end
```

Introduction to Lean

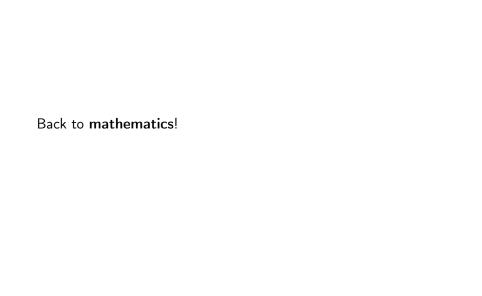
```
theorem my_transitivity (P Q R : Prop) (hPQ : P \rightarrow Q) (hQR : Q \rightarrow R) : P \rightarrow R := begin intro hP, apply hQR, apply hPQ, exact hP end
```

Introduction to Lean

```
theorem my_transitivity (P Q R : Prop) (hPQ : P \rightarrow Q) (hQR : Q \rightarrow R) : P \rightarrow R := begin intro hP, exact hQR (hPQ hP), end
```

Imperial College London Introduction to Lean

```
theorem my_transitivity (P Q R : Prop) (hPQ : P \rightarrow Q) (hQR : Q \rightarrow R) : P \rightarrow R := \lambda hP, hQR (hPQ hP)
```



Preliminary Definitions

Definition (Monic)

Let R be an ID. $f \in R[X]$ is monic if its leading coefficient is 1, ie, if f is of the form

$$f(X) = a_0 + a_1 X + a_2 X^2 + \dots + a_{n-1} X^{n-1} + X^n$$

where $n = \deg(f)$ and $a_i \in R$ for all i.

Definition (Coprime)

Let R be an ID. Then, $f, g \in R[X]$ are coprime if $\exists a, b \in R[X]$ s.t.

$$af + bg = 1$$

Useful Results

Theorem

Let R be an ID. For $f, g \in R[X]$ with g monic, $\exists Q, R \in R[X]$ s.t. R + Qg = f.

In mathlib, this is polynomial.mod_by_monic_add_div. Note also that Q and R are respectively denoted f $/_m$ g and f $%_m$ g in Lean. We also have polynomial.degree_mod_by_monic_lt, which states that $\deg(R) < \deg(g)$.

Lemma

Let R be an ID. Fix $f, g, h \in R[X]$ and let f, g and f, h be coprime. Then, f and gh are coprime.

In mathlib, this exists (more generally) as is_coprime.mul_right.

Imperial College London Main Result

Theorem (Partial Fraction Decomposition)

Let R be an Integral Domain. Fix $f, g_1, g_2, \dots, g_n \in R[X]$ and let the g_i s be *monic* and *pairwise coprime*. Then, $\exists q, r_1, r_2, \dots, r_n \in R[X]$ such that $\deg(r_i) < \deg(g_i)$ for all i, and

$$\frac{f}{\prod_{i=1}^{n} g_i} = q + \sum_{i=1}^{n} \frac{r_i}{g_i}$$

Imperial College London Proof Sketch

We start by proving the n=2 case and then proceed by induction.

Proof Sketch: n = 2

By coprimality of g_1 and g_2 , we know $\exists c, d \in R[X]$ s.t. $cg_1 + dg_2 = 1$. Then, we write $f = f \cdot 1$, and then get

$$\frac{f}{g_1g_2} = \frac{f(cg_1 + dg_2)}{g_1g_2}$$
$$= \frac{cf}{g_2} + \frac{df}{g_1}$$

We know that $\exists q_1, q_2, r_1, r_2 \in R[X]$ s.t.

$$rac{cf}{g_2} + rac{df}{g_1} = \left(q_2 + rac{r_2}{g_2}\right) + \left(q_1 + rac{r_1}{g_1}\right)$$

$$= \left(q_1 + q_2\right) + rac{r_1}{g_1} + rac{r_2}{g_2}$$

Proof Sketch: General *n*

We proceed by induction on n. The n=1 base case follows directly from the quotient-remainder result².

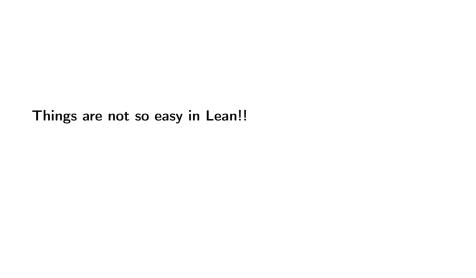
We assume the result for general n. Then, we write

$$\frac{f}{\prod_{i=1}^{n+1} g_i} = \frac{f}{(\prod_{i=1}^n g_i) \cdot g_{n+1}}$$

$$= q' + \frac{r_{n+1}}{g_{n+1}} + \frac{f}{\prod_{i=1}^n g_i}$$

$$= (q' + Q) + \frac{r_{n+1}}{g_{n+1}} + \sum_{i=1}^n \frac{r_i}{g_i}$$

²In informal mathematics, yes; in Lean, not quite!



Things are not so easy in Lean!!
In informal mathematics, we tend to gloss over a lot of details!

Things are not so easy in Lean!!	
In informal mathematics, we tend to gloss over a lot of details	į

In Lean, another complication is that we want maximum generality!

The Use of Finsets

In Lean, rather than indexing over \mathbb{N} , we index over an arbitrary type ι and look at an arbitrary finite subset s of ι . This allows for more generality.

Induction therefore looks a bit different:

- Base Case: True over $(\emptyset : finset \ \iota)$
- Inductive Case: True over (b : finset ι) \Longrightarrow true over (insert a b : finset ι), where (a : ι) and (a \notin b).

Example: the missing product coprimality lemma in the general n proof.

Imperial College London The Lean Proof

Let's see the proof in VS Code!

Imperial College London Some Discussion

One question that you might have is, "Why did we need all that theory at the beginning?"

Imperial College London Some Discussion

One question that you might have is, "Why did we need all that theory at the beginning?"

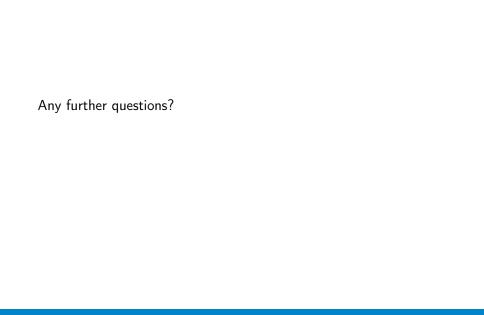
Let's revisit our
$$\frac{1}{(x+1)(x-1)}$$
 example.

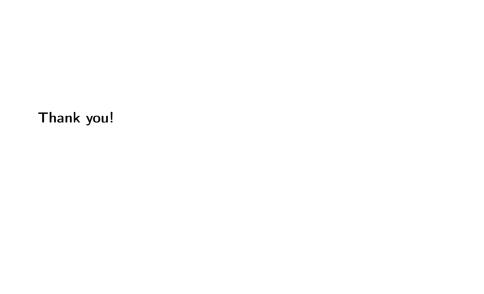
Imperial College London Some Discussion

One question that you might have is, "Why did we need all that theory at the beginning?"

Let's revisit our
$$\frac{1}{(x+1)(x-1)}$$
 example.

The reason we could decompose in the FoF of $\mathbb{R}[x]$ but not $\mathbb{Z}[x]$ is that x+1 and x-1 are coprime in $\mathbb{R}[x]$ but not in $\mathbb{Z}[x]$.





Imperial College London References

- [1] James McKernan. MATH 103B. Field of Fractions. University of California San Diego, 2016. URL: https://mathweb.ucsd.edu/~jmckerna/Teaching/15-16/Spring/103B/1_14.pdf.
- [2] Alexei N. Skorobogatov. *MATH50005. Groups and Rings: Rings.* Imperial College London, 2022.

Imperial College London Further Resources

Click on the item to visit the linked page.

- Mathlib documentation
- Lean code for this project, written in collaboration with Dr. Kevin Buzzard (WIP)
- Imperial College MathWiki: Links to notes and resources from our second-year course MATH50005 Groups and Rings