$ab = \frac{1}{4}\left[(a+b)^2 - (a-b)^2\right]$

Toby Lam

October 21, 2022

Motivation

- Title identity comes from $a^2 - b^2 = (a+b)(a-b)$
- The main idea is that we can express an arbitrary product as a difference of squares
- Similar to Cauchy-Schwarz

$$ab = \frac{1}{4}\left[(a+b)^2 - (a-b)^2\right]$$

$$\langle u, v\rangle \leq \langle u, u\rangle \cdot \langle v, v\rangle$$

Basic Structure

We're going to try to prove theorems using this structure
We would generalise this later on

Theorem

Suppose $P \subseteq V$. Show that $\forall x, y \in V$, if $x, y \in P$, then $xy \in P$

Proof.

1. Prove that linear combinations of elements in P are in P
2. Prove that if $x \in P$, then $x^2 \in P$
3. Use the identity to deduce that $xy = \frac{1}{4}\left[(x+y)^2 - (x-y)^2\right] \in P$

□

Integrability

Theorem

If f, g are integrable then fg is integrable.

Proof.

1. Prove that linear combinations of integrable functions are integrable
2. Prove that if f is integrable then f^2 is integrable
3. Use the identity to deduce that $fg = \frac{1}{4}\left[(f+g)^2 - (f-g)^2\right]$ is integrable

□

Algebra of Limits

Theorem

If $(a_n) \to L, (b_n) \to M$ *then* $(a_n b_n) \to LM$

Proof.

1. Show that linear combinations of convergent sequences converges to the linear combinations of the limits.
2. Prove $(a_n^2) \to L^2$ if $(a_n) \to L$
3. Use the identity $a_n b_n = \frac{1}{4}\left[(a_n + b_n)^2 - (a_n - b_n)^2\right] \in P$ to show $a_n b_n \to LM$

□

Algebra of Limits

Lemma

If (a_n) converges to L, (a_n^2) converges to L^2

Proof.

Take $\epsilon > 0$. We may assume that $\epsilon < 1$. Suppose $a_n \to L$, then by definition $\exists\, N \in \mathbb{Z}$ such that if $n \geq N$ then $\|a_n - L\| < \epsilon$. We have,

$$\begin{aligned} \|a_n^2 - L^2\| &= \|a_n + L\| \cdot \|a_n - L\| \\ &\leq (\|a_n\| + \|L\|) \cdot \|a_n - L\| \\ &\leq (2\|L\| + \epsilon) \cdot \epsilon \leq (2\|L\| + 1) \cdot \epsilon \end{aligned}$$

As $(2\|L\| + 1)$ is constant, this is enough to show that (a_n^2) is convergent.

□

Product Rule

Theorem

If f, g is differentiable then fg is differentiable and $(fg)' = f'g + fg'$

Proof.

1. Show that linear combinations of differentiable functions are differentiable
2. Prove that if f differentiable then f^2 differentiable and $(f^2)' = 2f \cdot f'$
3. Use the identity to deduce that $fg = \frac{1}{4}\left[(f+g)^2 - (f-g)^2\right]$ is differentiable and its formula is $fg' + f'g$

□

Product Rule

Lemma

If f differentiable then f^2 is differentiable and $(f^2)' = 2f \cdot f'$

Proof.

$$\lim_{x \to x_0} \frac{f(x)^2 - f(x_0)^2}{x - x_0} = \lim_{x \to x_0} \left[\left(f(x) + f(x_0)\right) \frac{f(x) - f(x_0)}{x - x_0} \right]$$
$$= 2f(x_0) \cdot f'(x_0)$$

□

Product Rule

Theorem

If f, g is differentiable then fg is differentiable and $(fg)' = f'g + fg'$

Proof.

First proving that $(\lambda f)' = \lambda f', (f+g)' = f' + g'$,

$$\begin{aligned}(fg)' &= \frac{1}{4}\left\{\left[(f+g)^2\right]' - \left[(f-g)^2\right]'\right\} \\ &= \frac{1}{2}\left[(f+g)(f'+g') - (f-g)(f'-g')\right] \\ &= f'g + fg'\end{aligned}$$

□

Gradient

Theorem

$\nabla(fg) = f\,\nabla g + g\,\nabla f$

Proof.

1. Show $\nabla(f^2) = 2f\,\nabla f$ directly
2. $$\begin{aligned}\nabla(fg) &= \frac{1}{2}\Big[(f+g)(\nabla f + \nabla g) - (f-g)(\nabla f - \nabla g)\Big]\\ &= f\,\nabla g + g\,\nabla f\end{aligned}$$

□

Generalisation preliminaries

Definition

Characteristic of a field

The smallest number of times one must use the ring's multiplicative identity (1) in a sum to get the additive identity (0)

Example

- $\mathbb{R}$ has characteristic 0
- $\mathbb{Z}/p\mathbb{Z}$ for prime p has characteristic p

Generalisation Goal

We want to generalise the following

Theorem

Suppose $P \subseteq V$. Show that $\forall x, y \in V$, if $x, y \in P$, then $xy \in P$

Proof.

1. Prove that linear combinations of elements in P are in P
2. Prove that if $x \in P$, then $x^2 \in P$
3. Use the identity to deduce that $xy = \frac{1}{2}\left[x^2 + y^2 - (x-y)^2\right] \in P$

$\square$

Generalisation

Theorem

Let V be a vector space over some field F with characteristic 0 or greater than 2. Let there be a symmetric bilinear product $V \times V \to V$ denoted by $\times$. Let P be a subspace of V.

Then $v \times v \in P \, \forall v \in P$ is equivalent to $v \times w \in P \, \forall v, w \in P$

Proof

Proof.

$\Longrightarrow$: Suppose $v, w \in P$, then $v + w, v - w \in P$ so $(v + w) \times (v + w) - v \times v - w \times w \in P$ by linearity and assumption of P. By commutativity of $\times$ we deduce that $(1_F + 1_F)v \times w \in P$. As the characteristic of F is greater than 2, $(1_F + 1_F)^{-1}$ exists and is in F so $v \times w \in P$.

$\Longleftarrow$: Immediate $\square$

Generalisation

- Why use $vw = \frac{1}{2}\left[(v+w)^2 - v^2 - w^2\right]$?
  - So that we avoid stating the invertbility of 4. Although it is actually equivalent as fields can only have 0, 1 or prime characteristics.
- Why require the characteristic to be 0 or greater than 2?
  - So that $1_F + 1_F \neq 0_F$ and hence invertible
- Why does P need to be a subspace?
  - For the proof in its current state to work you'd need $p_1 + p_2, p_1 - p_2, \frac{1}{2}p_1 \in P \; \forall p_1, p_2 \in P$
  - It might as well be one
- Why does the bilinear product need to be symmetric?
  - So that $v \times w + w \times v = (1_F + 1_F) v \times w$
  - Alternatively, consider the cross product as a counterexample

Summary

We can retroactively use the theorem for the three examples.

	AOL	Product Rule	Integrability
V	Sequences	$\mathbb{R} \to \mathbb{R}$ func.	$\mathbb{R} \to \mathbb{R}$ func.
P	Conv. seq.	diff. func.	int. func.
$+$	Term-by-term addition	addition	addition
$\times$	Term-by-term mult.	mult.	mult.

Theorem

Let V be a vector space over some field F with characteristic 0 or greater than 2. Let there be a symmetric bilinear product $V \times V \to V$ denoted by $\times$. Let P be a subspace of V.

Then $v \times v \in P \, \forall v \in P$ is equivalent to $v \times w \in P \, \forall v, w \in P$

Related ideas

- Isometries in Geometry
  - A map T from $\mathbb{R}^n$ to $\mathbb{R}^n$ is called an isometry if $\|T(u) - T(v)\| = \|u - v\| \; \forall u, v \in \mathbb{R}^n$
  - Show $T(u) \cdot T(u) = u \cdot u$ by definition
  - Use $u \cdot v = \frac{1}{4}(u + v) \cdot (u + v) - \frac{1}{4}(u - v) \cdot (u - v)$ to show $T(u) \cdot T(v) = u \cdot v$

Related ideas

- Young's inequality for products
  - If $a, b \geq 0$ and $p, q > 1$ such that $p^{-1} + q^{-1} = 1$, then

$$ab \leq \frac{a^p}{p} + \frac{b^q}{q}$$

with equality if and only if $a^p = b^q$

- Hölder's inequality for integrals
  - If $p, q > 1$ such that $p^{-1} + q^{-1} = 1$, then

$$\int_a^b |fg| \leq \left[\int_a^b |f|^p\right]^{1/q} \left[\int_a^b |g|^q\right]^{1/p}$$

Conclusion

Control products by controlling squares

The End

Any Questions?