Showing preservation of properties under multiplication via difference of squares

Toby Lam
University of Oxford

March 21, 2023

Summary

- Idea: Multiplication = Squaring + Linear Combination through the identity

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

- We'd start proving preservation of analytic properties under multiplication using the identity
  - Algebra of limits
  - Product Rule
  - Integrability
- Then we're going to generalise the method of proof and talk about similar ideas

Basic Structure

We're going to try to prove theorems using this structure
It usually produces an easier proof

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

□

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 $a_n b_n \to \frac{1}{4}\left[(L+M)^2 - (L-M)^2\right] = LM$

□

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.

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

□

Product Rule

Theorem

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

Proof.

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

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

□

Gradient

Theorem

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

Proof.

1. Show $\nabla(f^2) = 2f\nabla f$ directly
(Direction of gradient of f^2 is identical to that of f)
2. $$\begin{aligned}\nabla(fg) &= \frac{1}{2}\Big[(f+g)(\nabla f+\nabla g) - (f-g)(\nabla f-\nabla g)\Big] \\ &= f\nabla g + g\nabla f\end{aligned}$$

□

Riemann 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

□

Similarly for simple / piece-wise linear / Lebesgue measurable functions
(Chapter 1, Thm 8.4, Theory of the Integral, Stanislaw Saks)

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)

If such a number doesn't exist, the characteristic is 0

Example

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

Generalisation Goal

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 $xy = \frac{1}{2}\left[(x+y)^2 - x^2 - y^2\right] \in P$

□

Theorem

Generalisation Goal

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 $xy = \frac{1}{2}\left[(x+y)^2 - x^2 - y^2\right] \in P$

□

Theorem

Let V be a vector space

Let P be a subspace of V.

Generalisation Goal

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 $xy = \frac{1}{2}\left[(x+y)^2 - x^2 - y^2\right] \in P$

$\square$

Theorem

Let V be a vector space

Let there be a bilinear map $V \times V \to V$ denoted by $\times$. Let P be a subspace of V.

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

Generalisation Goal

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 $xy = \frac{1}{2}\left[(x+y)^2 - x^2 - y^2\right] \in P$

□

Theorem

Let V be a vector space over some field F with characteristic 0 or greater than 2. Let there be a symmetric bilinear map $V \times V \to V$ 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

Theorem

Let V be a vector space over some field F with characteristic 0 or greater than 2. Let there be a symmetric bilinear map $V \times V \to V$ 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.

$\implies$: 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 $v \times w \in P$.

$\impliedby$: Immediate $\square$

Application

Theorem

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

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

	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.

Remarks

Theorem

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

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

- Does the bilinear map 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. Set P to be a plane.
- 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

Further Remarks

Theorem

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

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

- Why require the characteristic to be 0 or greater than 2?
  - So that $2_F := 1_F + 1_F \neq 0_F$ and hence 2_F is invertible
- Why use $vw = \frac{1}{2}\left[(v+w)^2 - v^2 - w^2\right]$?
  - So that we avoid assuming the invertability of 4. Although in reality 2 is invertible if and only if 4 is invertible as fields can only have 0, 1 or prime characteristics.

Summary

Theorem

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

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

	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.

Related ideas - Dot product

- Isometries in Geometry
  - A map T from $\mathbb{R}^n$ to $\mathbb{R}^n$ is called an isometry if $\|T(\mathbf{u}) - T(\mathbf{v})\| = \|\mathbf{u} - \mathbf{v}\| \; \forall \mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, i.e. it preserves distance
  - Rotations, reflections and translations are all examples of isometries.
  - Claim: $T(\mathbf{u}) \cdot T(\mathbf{v}) = \mathbf{u} \cdot \mathbf{v}$ if $T(\mathbf{0}) = \mathbf{0}$
  - Proof: Show $T(\mathbf{u}) \cdot T(\mathbf{u}) = \mathbf{u} \cdot \mathbf{u}$ by definition. Then use $\mathbf{u} \cdot \mathbf{v} = \frac{1}{4}(\mathbf{u} + \mathbf{v}) \cdot (\mathbf{u} + \mathbf{v}) - \frac{1}{4}(\mathbf{u} - \mathbf{v}) \cdot (\mathbf{u} - \mathbf{v})$ to show $T(\mathbf{u}) \cdot T(\mathbf{v}) = \mathbf{u} \cdot \mathbf{v}$
- Multivariable calculus
  - You can prove $\nabla(\mathbf{u} \cdot \mathbf{v}) = (\mathbf{u} \cdot \nabla)\mathbf{v} + \mathbf{u} \times (\nabla \times \mathbf{v}) + (\mathbf{v} \cdot \nabla)\mathbf{u} + \mathbf{v} \times (\nabla \times \mathbf{u})$ from proving $\nabla(\mathbf{u} \cdot \mathbf{u}) = 2[(\mathbf{u} \cdot \nabla)\mathbf{u} + \mathbf{u} \times (\nabla \times \mathbf{u})]$
  - You can prove the above neatly using Levi-Cevita Symbols

Related ideas

- Cauchy–Schwarz inequality:

$$|\langle \mathbf{u}, \mathbf{v} \rangle|^2 \leq \langle \mathbf{u}, \mathbf{u} \rangle \langle \mathbf{v}, \mathbf{v} \rangle$$

- Idea: Bound products with squares
- Results:
  1. Triangle inequality
  2. If $\langle \mathbf{v}, \mathbf{v} \rangle$ bounded for all $\mathbf{v} \in V$, then $\langle \mathbf{u}, \mathbf{v} \rangle$ bounded for all $\mathbf{u}, \mathbf{v} \in V$
  3. $$\begin{aligned} \mathrm{Var}(X)\mathrm{Var}(Y) &= \mathrm{Cov}(X, X)\mathrm{Cov}(Y, Y) \\ &\geq \mathrm{Cov}(X, Y)^2 \end{aligned}$$

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

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

- Functional Analysis
  - Study of vector spaces endowed with some kind of limit-related (topological) structure

The End

- Takeaway: **Transform facts about powers (squares) into facts about products**
- Website: tobylam.xyz
- Email: toby.lam@balliol.ox.ac.uk
- Questions away!