

The Mason–Stothers theorem

Manuel Eberl

April 12, 2026

Abstract

This article provides a formalisation of Snyder’s simple and elegant proof of the Mason–Stothers theorem [2, 1], which is the polynomial analogue of the famous *abc* Conjecture for integers. Remarkably, Snyder found this very elegant proof when he was still a high-school student.

In short, the statement of the theorem is that three non-zero coprime polynomials A , B , C over a field which sum to 0 and do not all have vanishing derivatives fulfil $\max\{\deg(A), \deg(B), \deg(C)\} < \deg(\text{rad}(ABC))$ where $\text{rad}(P)$ denotes the *radical* of P , i. e. the product of all unique irreducible factors of P .

This theorem also implies a kind of polynomial analogue of Fermat’s Last Theorem for polynomials: except for trivial cases, $A^n + B^n + C^n = 0$ implies $n \leq 2$ for coprime polynomials A , B , C over a field.

Contents

1	The Mason–Stother’s Theorem	2
1.1	Auxiliary material	2
1.2	Definition of a radical	2
1.3	Main result	4

1 The Mason–Stother’s Theorem

theory *Mason-Stothers*

imports

HOL-Computational-Algebra.Computational-Algebra

HOL-Computational-Algebra.Polynomial-Factorial

begin

1.1 Auxiliary material

hide-const (open) *Formal-Power-Series.radical*

lemma *degree-div:*

assumes $a \text{ dvd } b$

shows $\text{degree } (b \text{ div } a) = \text{degree } b - \text{degree } a$

<proof>

lemma *degree-pderiv-le:*

shows $\text{degree } (\text{pderiv } p) \leq \text{degree } p - 1$

<proof>

lemma *degree-pderiv-less:*

assumes $\text{pderiv } p \neq 0$

shows $\text{degree } (\text{pderiv } p) < \text{degree } p$

<proof>

lemma *pderiv-eq-0:*

assumes $\text{degree } p = 0$

shows $\text{pderiv } p = 0$

<proof>

1.2 Definition of a radical

The following definition of a radical is generic for any factorial semiring.

context *factorial-semiring*

begin

definition *radical* :: $'a \Rightarrow 'a$ **where**

$\text{radical } x = (\text{if } x = 0 \text{ then } 0 \text{ else } \prod (\text{prime-factors } x))$

lemma *radical-0 [simp]: radical 0 = 0*

<proof>

lemma *radical-nonzero: $x \neq 0 \implies \text{radical } x = \prod (\text{prime-factors } x)$*

<proof>

lemma *radical-eq-0-iff [simp]: radical x = 0 \longleftrightarrow x = 0*

<proof>

lemma *prime-factorization-radical* [*simp*]:
assumes $x \neq 0$
shows $\text{prime-factorization } (\text{radical } x) = \text{mset-set } (\text{prime-factors } x)$
<proof>

lemma *prime-factors-radical* [*simp*]: $x \neq 0 \implies \text{prime-factors } (\text{radical } x) = \text{prime-factors } x$
<proof>

lemma *radical-dvd* [*simp, intro*]: $\text{radical } x \text{ dvd } x$
<proof>

lemma *multiplicity-radical-prime*:
assumes $\text{prime } p \ x \neq 0$
shows $\text{multiplicity } p \ (\text{radical } x) = (\text{if } p \text{ dvd } x \text{ then } 1 \text{ else } 0)$
<proof>

lemma *radical-1* [*simp*]: $\text{radical } 1 = 1$
<proof>

lemma *radical-unit* [*simp*]: $\text{is-unit } x \implies \text{radical } x = 1$
<proof>

lemma *prime-factors-power*:
assumes $n > 0$
shows $\text{prime-factors } (x \wedge^n) = \text{prime-factors } x$
<proof>

lemma *radical-power* [*simp*]: $n > 0 \implies \text{radical } (x \wedge^n) = \text{radical } x$
<proof>

end

context *factorial-semiring-gcd*
begin

lemma *radical-mult-coprime*:
assumes $\text{coprime } a \ b$
shows $\text{radical } (a * b) = \text{radical } a * \text{radical } b$
<proof>

lemma *multiplicity-le-imp-dvd'*:
assumes $x \neq 0 \ \wedge p. p \in \text{prime-factors } x \implies \text{multiplicity } p \ x \leq \text{multiplicity } p \ y$
shows $x \text{ dvd } y$
<proof>

end

1.3 Main result

The following proofs are basically a one-to-one translation of Franz Lemmermeyer's presentation [1] of Snyder's proof of the Mason–Stothers theorem.

lemma *prime-power-dvd-pderiv*:

fixes $f p :: 'a :: \text{field-gcd poly}$
assumes *prime-elem* p
defines $n \equiv \text{multiplicity } p f - 1$
shows $p \wedge n \text{ dvd } p \text{deriv } f$

<proof>

lemma *poly-div-radical-dvd-pderiv*:

fixes $p :: 'a :: \text{field-gcd poly}$
shows $p \text{ div radical } p \text{ dvd } p \text{deriv } p$

<proof>

lemma *degree-pderiv-mult-less*:

assumes $p \text{deriv } C \neq 0$
shows $\text{degree } (p \text{deriv } C * B) < \text{degree } B + \text{degree } C$

<proof>

lemma *Mason-Stothers-aux*:

fixes $A B C :: 'a :: \text{field-gcd poly}$
assumes $\text{nz}: A \neq 0 B \neq 0 C \neq 0$ **and** $\text{sum}: A + B + C = 0$ **and** $\text{coprime}: \text{Gcd } \{A, B, C\} = 1$
and $\text{deg-ge}: \text{degree } A \geq \text{degree } (\text{radical } (A * B * C))$
shows $p \text{deriv } A = 0 \text{ pderiv } B = 0 \text{ pderiv } C = 0$

<proof>

theorem *Mason-Stothers*:

fixes $A B C :: 'a :: \text{field-gcd poly}$
assumes $\text{nz}: A \neq 0 B \neq 0 C \neq 0 \exists p \in \{A, B, C\}. p \text{deriv } p \neq 0$
and $\text{sum}: A + B + C = 0$ **and** $\text{coprime}: \text{Gcd } \{A, B, C\} = 1$
shows $\text{Max } \{\text{degree } A, \text{degree } B, \text{degree } C\} < \text{degree } (\text{radical } (A * B * C))$

<proof>

The result can be simplified a bit more in fields of characteristic 0:

corollary *Mason-Stothers-char-0*:

fixes $A B C :: 'a :: \{\text{field-gcd}, \text{field-char-0}\} \text{ poly}$
assumes $\text{nz}: A \neq 0 B \neq 0 C \neq 0$ **and** $\text{deg}: \exists p \in \{A, B, C\}. \text{degree } p \neq 0$
and $\text{sum}: A + B + C = 0$ **and** $\text{coprime}: \text{Gcd } \{A, B, C\} = 1$
shows $\text{Max } \{\text{degree } A, \text{degree } B, \text{degree } C\} < \text{degree } (\text{radical } (A * B * C))$

<proof>

As a nice corollary, we get a kind of analogue of Fermat's last theorem for polynomials: Given non-zero polynomials A, B, C with $A^n + B^n + C^n = 0$ on lowest terms, we must either have $n \leq 2$ or $(A^n)' = (B^n)' = (C^n)' = 0$.

In the case of a field with characteristic 0, this last possibility is equivalent to $A, B,$ and C all being constant.

corollary *fermat-poly*:

fixes $A B C :: 'a :: \text{field-gcd poly}$

assumes $\text{sum}: A^n + B^n + C^n = 0$ **and** $\text{cop}: \text{Gcd } \{A, B, C\} = 1$

assumes $\text{nz}: A \neq 0 B \neq 0 C \neq 0$ **and** $\text{deg}: \exists p \in \{A, B, C\}. \text{pderiv } (p^n) \neq 0$

shows $n \leq 2$

<proof>

corollary *fermat-poly-char-0*:

fixes $A B C :: 'a :: \{\text{field-gcd, field-char-0}\} \text{ poly}$

assumes $\text{sum}: A^n + B^n + C^n = 0$ **and** $\text{cop}: \text{Gcd } \{A, B, C\} = 1$

assumes $\text{nz}: A \neq 0 B \neq 0 C \neq 0$ **and** $\text{deg}: \exists p \in \{A, B, C\}. \text{degree } p > 0$

shows $n \leq 2$

<proof>

end

References

- [1] F. Lemmermeyer. Algebraic Geometry (lecture notes). <http://www.fen.bilkent.edu.tr/~franz/ag05/ag-02.pdf>, 2005.
- [2] N. Snyder. An alternate proof of Mason's theorem. *Elemente der Mathematik*, 55(3):93–94, Aug 2000.