The Mason–Stothers theorem

Manuel Eberl

March 17, 2025

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

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 dvd b*
shows *degree* (*b div a*) = *degree b* − *degree a*
⟨*proof*⟩

lemma *degree-pderiv-le*:
shows *degree* (*pderiv p*) ≤ *degree p* − *1*
⟨*proof*⟩

lemma *degree-pderiv-less*:
assumes *pderiv p* ≠ *0*
shows *degree* (*pderiv p*) < *degree p*
⟨*proof*⟩

lemma *pderiv-eq-0*:
assumes *degree p* = *0*
shows *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* ⇒ *'a* **where**
radical x = (*if x* = *0 then 0 else* ∏ (*prime-factors x*))

lemma *radical-0* [*simp*]: *radical 0* = *0*
⟨*proof*⟩

lemma *radical-nonzero*: *x* ≠ *0* ⟹ *radical x* = ∏ (*prime-factors x*)
⟨*proof*⟩

lemma *radical-eq-0-iff* [*simp*]: *radical x* = *0* ⟷ *x* = *0*
⟨*proof*⟩

lemma *prime-factorization-radical* [*simp*]:
  assumes $x \neq 0$
  shows *prime-factorization* (*radical* x) = *mset-set* (*prime-factors* x)
⟨*proof*⟩

lemma *prime-factors-radical* [*simp*]: $x \neq 0 \Longrightarrow$ *prime-factors* (*radical* x) = *prime-factors* x
  ⟨*proof*⟩

lemma *radical-dvd* [*simp*, *intro*]: *radical* x *dvd* x
  ⟨*proof*⟩

lemma *multiplicity-radical-prime*:
  assumes *prime* p $x \neq 0$
  shows *multiplicity* p (*radical* x) = (*if* p *dvd* x *then* 1 *else* 0)
⟨*proof*⟩

lemma *radical-1* [*simp*]: *radical* 1 = 1
  ⟨*proof*⟩

lemma *radical-unit* [*simp*]: *is-unit* $x \Longrightarrow$ *radical* x = 1
  ⟨*proof*⟩

lemma *prime-factors-power*:
  assumes $n > 0$
  shows *prime-factors* ($x \hat{} n$) = *prime-factors* x
  ⟨*proof*⟩

lemma *radical-power* [*simp*]: $n > 0 \Longrightarrow$ *radical* ($x \hat{} n$) = *radical* x
  ⟨*proof*⟩

end

context *factorial-semiring-gcd*
begin

lemma *radical-mult-coprime*:
  assumes *coprime* a b
  shows *radical* ($a * b$) = *radical* a * *radical* b
⟨*proof*⟩

lemma *multiplicity-le-imp-dvd'*:
  assumes $x \neq 0$ $\bigwedge p.\ p \in$ *prime-factors* $x \Longrightarrow$ *multiplicity* p $x \leq$ *multiplicity* p y
  shows x *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* :: *field-gcd poly*
assumes *prime-elem p*
defines *n* ≡ *multiplicity p f* − *1*
shows *p* ^ *n dvd pderiv f*
⟨*proof*⟩

lemma *poly-div-radical-dvd-pderiv*:
fixes *p* :: *'a* :: *field-gcd poly*
shows *p div radical p dvd pderiv p*
⟨*proof*⟩

lemma *degree-pderiv-mult-less*:
assumes *pderiv C* ≠ *0*
shows *degree* (*pderiv C* ∗ *B*) < *degree B* + *degree C*
⟨*proof*⟩

lemma *Mason-Stothers-aux*:
fixes *A B C* :: *'a* :: *field-gcd poly*
assumes *nz*: *A* ≠ *0 B* ≠ *0 C* ≠ *0* **and** *sum*: *A* + *B* + *C* = *0* **and** *coprime*: *Gcd* {*A*, *B*, *C*} = *1*
and *deg-ge*: *degree A* ≥ *degree* (*radical* (*A* ∗ *B* ∗ *C*))
shows *pderiv A* = *0 pderiv B* = *0 pderiv C* = *0*
⟨*proof*⟩

theorem *Mason-Stothers*:
fixes *A B C* :: *'a* :: *field-gcd poly*
assumes *nz*: *A* ≠ *0 B* ≠ *0 C* ≠ *0* ∃ *p*∈{*A*,*B*,*C*}. *pderiv p* ≠ *0*
and *sum*: *A* + *B* + *C* = *0* **and** *coprime*: *Gcd* {*A*, *B*, *C*} = *1*
shows *Max* {*degree A*, *degree B*, *degree C*} < *degree* (*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* :: {*field-gcd*, *field-char-0*} *poly*
assumes *nz*: *A* ≠ *0 B* ≠ *0 C* ≠ *0* **and** *deg*: ∃ *p*∈{*A*,*B*,*C*}. *degree p* ≠ *0*
and *sum*: *A* + *B* + *C* = *0* **and** *coprime*: *Gcd* {*A*, *B*, *C*} = *1*
shows *Max* {*degree A*, *degree B*, *degree C*} < *degree* (*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* :: *field-gcd poly*
assumes *sum*: $A \hat{} n + B \hat{} n + C \hat{} n = 0$ **and** *cop*: $Gcd\ \{A, B, C\} = 1$
assumes *nz*: $A \neq 0\ B \neq 0\ C \neq 0$ **and** *deg*: $\exists p{\in}\{A,B,C\}.\ pderiv\ (p \hat{} n) \neq 0$
shows $n \leq 2$
⟨*proof*⟩

corollary *fermat-poly-char-0*:
fixes *A B C* :: *'a* :: {*field-gcd*,*field-char-0*} *poly*
assumes *sum*: $A \hat{} n + B \hat{} n + C \hat{} n = 0$ **and** *cop*: $Gcd\ \{A, B, C\} = 1$
assumes *nz*: $A \neq 0\ B \neq 0\ C \neq 0$ **and** *deg*: $\exists p{\in}\{A,B,C\}.\ degree\ p > 0$
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.