

The Chevalley–Warning Theorem

Arthur Freitas Ramos David Barros Hulak
Ruy J. G. B. de Queiroz

July 14, 2026

Abstract

This development formalizes the Chevalley–Warning theorem for finite fields: if finitely many multivariate polynomials over a finite field have total degree sum strictly smaller than the number of variables, then the number of their common zeros is divisible by the characteristic [1, 3]. The formalization reuses the concrete multivariate-polynomial representation and operations from the AFP *Polynomials* entry [2], and the proof follows the standard finite-field power-sum argument. AI assistance was used for proof engineering. The final definitions, statements, and proofs are checked by Isabelle.

Contents

1	The Chevalley–Warning theorem	1
1.1	Polynomial operations	3
1.2	Finite-field power sums	5
1.3	The theorem	7

```
theory Chevalley-Warning
  imports
    HOL-Number-Theory.Residues
    HOL-Computational-Algebra.Polynomial
    HOL-Library.FuncSet
    Polynomials.Polynomials
begin
```

1 The Chevalley–Warning theorem

We reuse the concrete multivariate-polynomial representation from the AFP entry *Polynomials.Polynomials*. Thus a polynomial has type $(\text{'v}, \text{'a}) \text{Polynomials.poly}$ and consists of AFP monomials paired with coefficients. The theorem takes an explicit finite set of variables, so it applies directly to the usual natural-number-indexed AFP polynomials.

definition *variables-poly* ::

$'v::\text{linorder set} \Rightarrow ('v, 'a) \text{ poly} \Rightarrow \text{bool}$ **where**
 $\text{variables-poly } V p \longleftrightarrow \text{poly-vars } p \subseteq V$

definition $\text{total-degree-poly-le} :: ('v::\text{linorder}, 'a) \text{ poly} \Rightarrow \text{nat} \Rightarrow \text{bool}$ **where**
 $\text{total-degree-poly-le } p d \longleftrightarrow \text{poly-degree } p \leq d$

definition $\text{total-degree-poly-less} :: ('v::\text{linorder}, 'a) \text{ poly} \Rightarrow \text{nat} \Rightarrow \text{bool}$ **where**
 $\text{total-degree-poly-less } p d \longleftrightarrow \text{poly-degree } p < d$

definition $\text{common-zeros} ::$
 $'v::\text{linorder set} \Rightarrow$
 $('v, 'a::\text{comm-semiring-1}) \text{ poly list} \Rightarrow ('v \Rightarrow 'a) \text{ set}$ **where**
 $\text{common-zeros } V ps =$
 $\{\alpha \in \text{PiE } V (\lambda-. \text{UNIV}). \text{list-all } (\lambda p. \text{eval-poly } \alpha p = 0) ps\}$

lemma $\text{variables-poly-UNIV [simp]: variables-poly UNIV } p$
 $\langle \text{proof} \rangle$

lemma $\text{monom-vars-subset-poly-vars:}$
assumes $(m, c) \in \text{set } p$
shows $\text{monom-vars } m \subseteq \text{poly-vars } p$
 $\langle \text{proof} \rangle$

lemma poly-degree-leI:
assumes $\bigwedge m c. (m, c) \in \text{set } p \implies \text{monom-degree } m \leq d$
shows $\text{poly-degree } p \leq d$
 $\langle \text{proof} \rangle$

lemma $\text{total-degree-poly-leD:}$
assumes $\text{total-degree-poly-le } p d (m, c) \in \text{set } p$
shows $\text{monom-degree } m \leq d$
 $\langle \text{proof} \rangle$

lemma $\text{total-degree-poly-lessD:}$
assumes $\text{total-degree-poly-less } p d (m, c) \in \text{set } p$
shows $\text{monom-degree } m < d$
 $\langle \text{proof} \rangle$

lemma $\text{total-degree-poly-le-mono:}$
assumes $\text{total-degree-poly-le } p d d \leq e$
shows $\text{total-degree-poly-le } p e$
 $\langle \text{proof} \rangle$

lemma $\text{total-degree-poly-less-of-le:}$
assumes $\text{total-degree-poly-le } p d d < e$
shows $\text{total-degree-poly-less } p e$
 $\langle \text{proof} \rangle$

1.1 Polynomial operations

fun *poly-prod* :: ('v::linorder, 'a::comm-semiring-1) *poly list* $\Rightarrow$ ('v, 'a) *poly* **where**
poly-prod [] = *one-poly*
| *poly-prod* (p # ps) = *poly-mult* p (*poly-prod* ps)

definition *indicator-factor* ::

nat $\Rightarrow$ ('v::linorder, 'a::comm-ring-1) *poly* $\Rightarrow$ ('v, 'a) *poly* **where**
indicator-factor q p = *poly-minus* (*poly-const* 1) (*poly-power* p (q - 1))

definition *indicator-poly* ::

nat $\Rightarrow$ ('v::linorder, 'a::comm-ring-1) *poly list* $\Rightarrow$ ('v, 'a) *poly* **where**
indicator-poly q ps = *poly-prod* (map (*indicator-factor* q) ps)

lemma *monom-list-degree-mult*:

monom-list-degree (*monom-mult-list* m n) =
monom-list-degree m + *monom-list-degree* n
⟨*proof*⟩

lemma *monom-degree-mult* [*simp*]:

monom-degree (m * n) = *monom-degree* m + *monom-degree* n
⟨*proof*⟩

lemma *monom-degree-one* [*simp*]:

monom-degree (1::'v::linorder *monom*) = 0
⟨*proof*⟩

lemma *monom-vars-mult* [*simp*]:

monom-vars (m * n) = *monom-vars* m $\cup$ *monom-vars* n
⟨*proof*⟩

lemma *monom-mult-poly-monom*:

poly-monom (*monom-mult-poly* (m, c) p) $\subseteq$ (*) m ' *poly-monom* p
⟨*proof*⟩

lemma *variables-poly-const* [*simp*]:

variables-poly V (*poly-const* c :: ('v::linorder, 'a::zero) *poly*)
⟨*proof*⟩

lemma *total-degree-poly-le-const* [*simp*]:

total-degree-poly-le (*poly-const* c :: ('v::linorder, 'a::zero) *poly*) 0
⟨*proof*⟩

lemma *variables-poly-add*:

assumes p: *variables-poly* V p **and** q: *variables-poly* V q
shows *variables-poly* V (*poly-add* p q)
⟨*proof*⟩

lemma *total-degree-poly-le-add*:

assumes p: *total-degree-poly-le* p d **and** q: *total-degree-poly-le* q d

shows *total-degree-poly-le* (*poly-add* p q) d
 $\langle \text{proof} \rangle$

lemma *total-degree-monom-mult-poly*:
assumes m : *monom-degree* $m \leq d$ **and** p : *total-degree-poly-le* p e
shows *total-degree-poly-le* (*monom-mult-poly* (m , c) p) ($d + e$)
 $\langle \text{proof} \rangle$

lemma *variables-monom-mult-poly*:
assumes m : *monom-vars* $m \subseteq V$ **and** p : *variables-poly* V p
shows *variables-poly* V (*monom-mult-poly* (m , c) p)
 $\langle \text{proof} \rangle$

lemma *variables-poly-mult*:
assumes p : *variables-poly* V p **and** q : *variables-poly* V q
shows *variables-poly* V (*poly-mult* p q)
 $\langle \text{proof} \rangle$

lemma *total-degree-poly-le-mult*:
assumes p : *total-degree-poly-le* p d **and** q : *total-degree-poly-le* q e
shows *total-degree-poly-le* (*poly-mult* p q) ($d + e$)
 $\langle \text{proof} \rangle$

lemma *variables-poly-minus*:
assumes p : *variables-poly* V p **and** q : *variables-poly* V q
shows *variables-poly* V (*poly-minus* p q)
 $\langle \text{proof} \rangle$

lemma *total-degree-poly-le-minus*:
assumes p : *total-degree-poly-le* p d **and** q : *total-degree-poly-le* q d
shows *total-degree-poly-le* (*poly-minus* p q) d
 $\langle \text{proof} \rangle$

lemma *variables-poly-power*:
assumes p : *variables-poly* V p
shows *variables-poly* V (*poly-power* p k)
 $\langle \text{proof} \rangle$

lemma *total-degree-poly-le-power*:
assumes p : *total-degree-poly-le* p d
shows *total-degree-poly-le* (*poly-power* p k) ($k * d$)
 $\langle \text{proof} \rangle$

lemma *eval-poly-prod*:
 $\text{eval-poly } \alpha \text{ (poly-prod } ps) = \text{prod-list (map (eval-poly } \alpha) ps)$
 $\langle \text{proof} \rangle$

lemma *variables-poly-prod*:
assumes $\text{list-all (variables-poly } V) ps$

shows *variables-poly* V (*poly-prod* ps)
 $\langle proof \rangle$

lemma *total-degree-poly-prod*:
assumes *list-all2* *total-degree-poly-le* ps ds
shows *total-degree-poly-le* (*poly-prod* ps) (*sum-list* ds)
 $\langle proof \rangle$

lemma *eval-indicator-factor*:
 $eval_poly\ \alpha\ (indicator_factor\ q\ p) = 1 - eval_poly\ \alpha\ p^{\wedge}(q - 1)$
 $\langle proof \rangle$

lemma *eval-indicator-poly*:
 $eval_poly\ \alpha\ (indicator_poly\ q\ ps) =$
 $prod_list\ (map\ (\lambda p.\ 1 - eval_poly\ \alpha\ p^{\wedge}(q - 1))\ ps)$
 $\langle proof \rangle$

lemma *variables-indicator-factor*:
assumes *variables-poly* V p
shows *variables-poly* V (*indicator-factor* q p)
 $\langle proof \rangle$

lemma *variables-indicator-poly*:
assumes *list-all* (*variables-poly* V) ps
shows *variables-poly* V (*indicator-poly* q ps)
 $\langle proof \rangle$

lemma *total-degree-indicator-factor*:
fixes $p :: ('v::linorder, 'a::comm-ring-1)\ poly$
assumes p : *total-degree-poly-le* p d
shows *total-degree-poly-le* (*indicator-factor* q p) $((q - 1) * d)$
 $\langle proof \rangle$

lemma *total-degree-indicator-poly*:
assumes *list-all2* *total-degree-poly-le* ps ds
shows *total-degree-poly-le* (*indicator-poly* q ps) $((q - 1) * sum_list\ ds)$
 $\langle proof \rangle$

1.2 Finite-field power sums

lemma *finite-field-card-gt-one*:
 $1 < card\ (UNIV :: 'a::finite-field\ set)$
 $\langle proof \rangle$

lemma *finite-field-power-card-minus-one*:
fixes $x :: 'a::finite-field$
assumes $x \neq 0$
shows $x^{\wedge}(card\ (UNIV :: 'a\ set) - 1) = 1$
 $\langle proof \rangle$

lemma *finite-field-exists-power-ne-one*:
fixes $k :: \text{nat}$
assumes $k\text{-pos}$: $0 < k$
assumes $k\text{-lt}$: $k < \text{card } (\text{UNIV} :: 'a::\text{finite-field set}) - 1$
shows $\exists a::'a. a \neq 0 \wedge a^k \neq 1$
 $\langle \text{proof} \rangle$

lemma *finite-field-power-sum-less*:
assumes $k\text{-lt}$: $k < \text{card } (\text{UNIV} :: 'a::\text{finite-field set}) - 1$
shows $(\sum_{x \in \text{UNIV}} x^k :: 'a) = 0$
 $\langle \text{proof} \rangle$

lemma *eval-monom-list-prod-sum-var*:
fixes $\alpha :: 'v::\text{linorder} \Rightarrow 'a::\text{comm-semiring-1}$
assumes finite : $\text{finite } V$ **and** vars : $\text{fst } ' \text{ set } m \subseteq V$
shows $\text{eval-monom-list } \alpha \ m =$
 $(\prod_{x \in V} \alpha \ x^{\text{sum-var-list } m \ x})$
 $\langle \text{proof} \rangle$

lemma *eval-monom-prod-sum-var*:
fixes $\alpha :: 'v::\text{linorder} \Rightarrow 'a::\text{comm-semiring-1}$
assumes $\text{finite } V$ $\text{monom-vars } m \subseteq V$
shows $\text{eval-monom } \alpha \ m = (\prod_{x \in V} \alpha \ x^{\text{sum-var } m \ x})$
 $\langle \text{proof} \rangle$

lemma *monom-list-degree-sum-var*:
fixes $m :: 'v::\text{linorder monom-list}$
assumes $\text{finite } V$ $\text{fst } ' \text{ set } m \subseteq V$
shows $\text{monom-list-degree } m = (\sum_{x \in V} \text{sum-var-list } m \ x)$
 $\langle \text{proof} \rangle$

lemma *monom-degree-sum-var*:
fixes $m :: 'v::\text{linorder monom}$
assumes $\text{finite } V$ $\text{monom-vars } m \subseteq V$
shows $\text{monom-degree } m = (\sum_{x \in V} \text{sum-var } m \ x)$
 $\langle \text{proof} \rangle$

lemma *sum-monom-assignments*:
fixes $m :: 'v::\text{linorder monom}$
assumes finite : $\text{finite } V$ **and** vars : $\text{monom-vars } m \subseteq V$
shows $(\sum_{\alpha \in \text{PiE } V} (\lambda-. \text{UNIV} :: 'a::\text{finite-field set}).$
 $\text{eval-monom } \alpha \ m) =$
 $(\prod_{x \in V} \sum_{y \in (\text{UNIV} :: 'a \text{ set}). y^{\text{sum-var } m \ x}})$
 $\langle \text{proof} \rangle$

lemma *exists-variable-degree-lt*:
assumes finite : $\text{finite } V$
assumes $(\sum_{x \in V} f \ x) < \text{card } V * k$

shows $\exists x \in V. f\ x < k$
 $\langle proof \rangle$

lemma *monomial-sum-zero-if-degree-lt*:
fixes $m :: 'v::linorder\ monom$
assumes *finite*: $finite\ V$ **and** *vars*: $monom-vars\ m \subseteq V$
assumes *deg*:
 $monom-degree\ m <$
 $card\ V * (card\ (UNIV :: 'a::finite-field\ set) - 1)$
shows $(\sum \alpha \in PiE\ V\ (\lambda-. UNIV :: 'a\ set). eval-monom\ \alpha\ m) = 0$
 $\langle proof \rangle$

lemma *finite-field-sum-poly-zero*:
assumes *finite*: $finite\ V$ **and** *vars*: $variables-poly\ V\ p$
assumes *deg*:
 $total-degree-poly-less\ p$
 $(card\ V * (card\ (UNIV :: 'a::finite-field\ set) - 1))$
shows $(\sum \alpha \in PiE\ V\ (\lambda-. UNIV :: 'a\ set). eval-poly\ \alpha\ p) = 0$
 $\langle proof \rangle$

1.3 The theorem

lemma *finite-field-indicator-factor-value*:
fixes $y :: 'a::finite-field$
shows $1 - y \wedge (card\ (UNIV :: 'a\ set) - 1) = of_bool\ (y = 0)$
 $\langle proof \rangle$

lemma *prod-list-of-bool-list-all*:
 $prod-list\ (map\ (\lambda x. of_bool\ (P\ x)) :: 'a::comm-semiring-1)\ xs) =$
 $of_bool\ (list-all\ P\ xs)$
 $\langle proof \rangle$

lemma *eval-indicator-poly-value*:
fixes $ps :: ('v::linorder, 'a::finite-field)\ poly\ list$
shows $eval-poly\ \alpha\ (indicator-poly\ (card\ (UNIV :: 'a\ set))\ ps) =$
 $of_bool\ (list-all\ (\lambda p. eval-poly\ \alpha\ p = 0)\ ps)$
 $\langle proof \rangle$

lemma *list-all2-variables*:
assumes
 $list-all2\ (\lambda p\ d. variables-poly\ V\ p \wedge total-degree-poly-le\ p\ d)\ ps\ ds$
shows $list-all\ (variables-poly\ V)\ ps$
 $\langle proof \rangle$

lemma *list-all2-degrees*:
assumes
 $list-all2\ (\lambda p\ d. variables-poly\ V\ p \wedge total-degree-poly-le\ p\ d)\ ps\ ds$
shows $list-all2\ total-degree-poly-le\ ps\ ds$
 $\langle proof \rangle$

theorem *chevalley-warning*:
fixes $V :: 'v::\text{linorder set}$
and $ps :: ('v, 'a::\text{finite-field}) \text{ poly list}$
assumes *finite*: $\text{finite } V$
assumes *polys*:
 $\text{list-all2 } (\lambda p d. \text{variables-poly } V p \wedge \text{total-degree-poly-le } p d) ps ds$
assumes *degree-sum*: $\text{sum-list } ds < \text{card } V$
shows $\text{CHAR}('a) \text{ dvd card } (\text{common-zeros } V ps)$
 $\langle \text{proof} \rangle$

corollary *chevalley-warning-finite-type*:
fixes $ps :: ('v::\{\text{finite}, \text{linorder}\}, 'a::\text{finite-field}) \text{ poly list}$
assumes *polys*: $\text{list-all2 total-degree-poly-le } ps ds$
assumes *degree-sum*: $\text{sum-list } ds < \text{card } (UNIV :: 'v \text{ set})$
shows $\text{CHAR}('a) \text{ dvd card } (\text{common-zeros } UNIV ps)$
 $\langle \text{proof} \rangle$

end

References

- [1] C. Chevalley. Démonstration d’une hypothèse de M. Artin. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 11(1):73–75, 1935. DOI: <https://doi.org/10.1007/BF02940714>.
- [2] C. Sternagel, R. Thiemann, A. Maletzky, F. Immler, F. Haftmann, A. Lochbihler, and A. Bentkamp. Executable multivariate polynomials. *Archive of Formal Proofs*, August 2010. <https://isa-afp.org/entries/Polynomials.html>, Formal proof development.
- [3] E. Warning. Bemerkung zur vorstehenden Arbeit von Herrn Chevalley. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 11(1):76–83, 1935. DOI: <https://doi.org/10.1007/BF02940715>.