Mathematical insights from using Lean

Damiano Testa

University of Warwick

Lean Together 2021, January 7th, 2021

For those who do not know me, I consider myself an algebraic geometer, with a strong interest in number theory.

My computer experience prior to this summer was

- browsing the internet,
- typing in $\mathbb{A}T_{\mathbb{E}}X$,
- using the computational algebra system called MAGMA.

However, I know Kevin Buzzard and I was aware of his efforts in formalization of mathematics.

I started using Lean over the summer and I am still a beginner.

I feel confident in the mathematical side of my presentation.

The Lean side is quite a bit shakier: I welcome all sorts of comments!

I am going to present my personal experience with my first, serious, ongoing formalization project.

In these slides, what is trivial, is formalized; what is interesting is in progress.

The ideas expressed in this presentation are mostly reflection of my limited understanding of how mathematics can be formalized.

My long-term, yet unreached, goal is to formalize Chevalley's Theorem.

Theorem (Chevalley)

Let $\pi: X \to Y$ be a morphism of schemes [more assumptions]. The image of a constructible subset of X is constructible.

Do not worry if you do not understand the meaning of most of the words in this statement: we will reduce to polynomials very quickly!

As an algebraic geometer, I view this statement as an important and useful result.

Theorem (Chevalley)

Let $\pi: X \to Y$ be a morphism of schemes [more assumptions]. The image of a constructible subset of X is constructible.

Constructible means a finite union of intersections of open and a closed set.

I also thought that it was relatively easy to prove... on paper!

Reduction steps: it suffices to consider the case

| Geometry side | Algebra side | | | | | |
|--|---|--|--|--|--|--|
| $X = Y \times \mathbb{A}^r$ and | $R 	ext{ is a comm_ring} (\leftrightarrow Y)$ | | | | | |
| $\pi\colon Y\times \mathbb{A}^r\to Y$ is the | study the inclusion $R \to R[x_1, \ldots, x_r]$ | | | | | |
| projection | | | | | | |
| r = 1 | {R : Type*} [comm_ring R] | | | | | |
| $\pi\colon Y\times \mathbb{A}^1\to Y$ | C : R \rightarrow polynomial R | | | | | |

Lemma (Simplified Chevalley's Theorem, version 1)

Let $\pi: Y \times \mathbb{A}^1 \to Y$ be the projection onto the first factor.

Given U, V open subsets of $Y \times \mathbb{A}^1$, the set $\pi(U \cap V^c)$ is constructible.

Recall: constructible is a finite union of intersections of open and a closed set.

It turns out that the projection map $Y \times \mathbb{A}^1 \to Y$ is *open*, and we can break our goal further:

• if $U \subset Y \times \mathbb{A}^1$ is open, then show that $\pi(U) \subset Y$ is open (instead of just constructible).

2 if $C \subset Y \times \mathbb{A}^1$ is closed, then show that $\pi(C) \subset Y$ is constructible.

Lemma (Simplified Chevalley's Theorem, version 2)

Let $\pi: Y \times \mathbb{A}^1 \to Y$ be the projection onto the first factor.

- **1** The morphism π is open.
- \bigcirc if $C \subset Y \times \mathbb{A}^1$ is closed, then $\pi(C) \subset Y$ is constructible.

Item (1) is fully formalized! (More on this below.)

Item (2) is still in progress.

A proof that $\pi: Y \times \mathbb{A}^1 \to Y$ is open

| <pre>1 provide ring there perpendicular state: 1 provide ring there</pre> | | import algebraic geometry prime spectrum | Stramo. | | Tab Black of the constant membrane B 1 T 4 or M . constit d 4 d as 1 1 | Elburro. |
|--|-------|--|--|-----|--|---|
| <pre>pressure for the provide state of the provide</pre> | | There a denote a denote a beer an | | 30 | ter otor := {p : prime_spectrum K 3 1 : N ; coerr i 1 e p.1 ;; | |
| <pre>1 Horitatisti 1 Horizattisti 1 Horizatt</pre> | - 2 | import ring_theory.polynomial.basic | NAME AND ADDRESS OF TAXABLE PARTY. | 56 | <pre>let Uis := {Ui : set (prime_spectrum R) 3 i : N , Ui = {p : prime_spectrum R coeff f i € p.1 }},</pre> | CONTRACTOR OF |
| <pre> function provide pro</pre> | - 3 - | import tactic | 1704Chammer | 57 | have upion : Utot = He Uis. | 1705240 |
| <pre>gene link (proved) (provide) (p</pre> | | | CARL STREET AND AND AND AND AND AND | 50 | (with | party house of |
| <pre>space and public processing of the space and procesing of the space and processing of the space and processin</pre> | - 2 | and ideal adjusted adde another add | Jubijester. | | (units) | Julipine. |
| <pre>Status in the provide status pr</pre> | 2 | open ibeat potynomiat prime_spectrum set | The statistic state prove | 59 | split, | 200 000 000.00 |
| <pre>1 List introde (List case) (f = set (f</pre> | 6 | | | 68 | { intro xh, | |
| <pre>starts the start is the start is been in backed by the starts is backed b</pre> | 7 | local attribute [instance] classical.prop decidable | All lines | 61 | simp at *. | Sec. and |
| <pre></pre> | 8 | | Statement of the second | 62 | care vb with 1 th | Tex.meners |
| <pre>A The second secon</pre> | 12 | | | | | 1000 |
| <pre>A Provide the optimal provide by the statust by -> optimal provide by -> optimal p</pre> | | universe a | Sec | 63 | use {p : prime_spectrum H coeff f 1 @ p.1 }, | - Anno - |
| <pre>11 / . Provide the (1) - be (1) for a prior of a start (1) for a star</pre> | 10 | | 30 | 64 | use 1, | -01 |
| <pre>2 set:10 balance 3 set:10 balance 4 set:20 s</pre> | 11 | /- The morphism Spec Rixl> Spec R induced by the natural inclusion R> Rixl is an open map -/ | | 65 | refl.). | |
| <pre>image spatial states is the spatial state is t</pre> | 12 | section Ry2Romen | SAL. | 66 | / intro xh | 80 |
| <pre>A relationships have the f f is f is a f is the fight (main fight f is is f is f is f is f is f is f is</pre> | | | Records. | | 1 And a ship | Reason. |
| <pre>3 / Intermediation (* 1) / (*)</pre> | 13 | | 289 | 67 | simp at ", | 209- |
| <pre>10 immediate (in (i) (i) (i) (i) (i) (i) (i)</pre> | 14 | 7- quoisintoomain shows that if P is a prime ideal of K, then K[x]/(P) satisfies is integral_domain -/ | 0.00.0 | 68 | rcases xh with (Ui , 1 , xui) , | 0.01.0.000.00 |
| <pre>(eptic use (p = (p = (a = (p + (p</pre> | 15 | lemma quoisintdomain {R : Type u} [comm ring R] {P : ideal R} (H : is prime P) : is integral domain | all and a second | 69 | cases 1 with 1 ih. | No. |
| <pre>1 main and a second secon</pre> | | (quotient (man C P : ideal (polynomial B))) := | and the second s | 70 | ure 1 | and the second second |
| <pre>1 The set of the</pre> | | Constant Company of Constant | Contraction and and and and a | 70 | use a, | CONCERN- |
| <pre>1</pre> | 10 | Dig 11 | and the second second | /1 | rw in at xui, | Ginema |
| <pre>1 transition (transition (transitio</pre> | 17 | let quo := polynomial (quotient P), | and the second | 72 | exact xui, }, }, | Revenue |
| <pre>1</pre> | 18 | <pre>let quot := quotient (map C P : ideal (polynomial R)),</pre> | A DESCRIPTION OF A DESC | 73 | have allopen : V i : N , is open (p : prime spectrum R coeff f i € p.1). | A STRANTS |
| <pre>bit is give "wide "> wide "> wide</pre> | 19 | have ide : is integral domain dup := integral domain to is integral domain dup. | 200 | 7.4 | / intro i | ,220, |
| <pre>prefrom the provide provide provide provide provide the provide the provide provide the provide t</pre> | 20 | but iss : sup set out :- solutestal sutient equiv sutient solutestal P | CARL & TO ALL AND A COMPANY OF | | and and and an annual and an a | Cash Livers |
| <pre>1</pre> | 20 | and the state of the become destant destant destant bechanges it | Jan- | /5 | exact std_arr_is_open (r.coerr i), j, | COLUMN AT A |
| <pre>1</pre> | 21 | symmetry' at 150, | Mart . | 76 | refine (is_open_iff {p : prime_spectrum R 3 (i : N), f.coeff i # p.val}).mpr _, | - Contraction |
| <pre>/ If the provide role of the provide role</pre> | | exact ring equiv.is integral domain quo idg iso, | (Channel of Channel of | 77 | use (r : R 3 1 : N , r = coeff f 1). | |
| <pre>1</pre> | 23 | end | | 78 | extl | CORRECT OF COLUMN |
| <pre>3 - /:Iffiture show that (if is a prime show of is a prime show o</pre> | 2.4 | | 1 A 4 4 7 10 10 10 10 10 10 10 10 10 10 10 10 10 | 20 | | Second and |
| <pre>So const trypes () (cons, risk () () = risk () (() : risk () (() : risk () risk () (() : risk () risk () (() : risk () : risk () (() : risk () (() : risk () : risk () (() : risk () : risk (</pre> | | | - Barrow | 79 | spir, | - Andrews |
| <pre>spliture (spliture) (splitur</pre> | 25 | 7- circiprime shows that if P is a prime ideal of R, then P.N[X] is a prime ideal of R[X] -7 | 18m | 80 | (intro xn, | Tilla |
| <pre>(private N):= (private N)</pre> | 26 | lemma liftprime {R : Type u} [comm_ring R] {P : ideal R} (H : is_prime P) : is_prime (map C P : ideal | DROARTA WELWINGT | 81 | simp at *, | 281.800244 |
| <pre>27 Bail 28 Bail 29 Bail 29 Bail 29 Bail 29 Bail 29 Bail 20 Bail 2</pre> | | (polynomial R)) := | Street and the second second | 82 | intres co.cob | |
| <pre>3</pre> | 22 | bento | 311 | | have an i 2 (1 : h) an - f coeff 1 | -237 |
| <pre>bit ref: (perturbative perturbative per</pre> | 20 | | A CONTRACTOR OF A CONTRACTOR O | | | Te reasonante |
| <pre>3 Prime (application), being (application), be</pre> | 20 | tet 1 : Ideat (polynomiat k) := map C P, | | 84 | { exact con, }, | APRIL 1 |
| <pre>set set set set set set set set set set</pre> | 29 | retine (quotient.is_integral_domain_itt_prime_i).mp, | 8 | 85 | cases ox with 11, | 10.7 million |
| <pre>11 def 11 def 12 def lags of f(1 - fps a) [com_ring R] (f : prime_spectrum R a f p.1)):> 13 def lags of f(1 - fps a) [com_ring R] (f : prime_spectrum (phymetal R)) 14 def lags of f(1 - fps a) [com_ring R] (f : prime_spectrum (phymetal R)) 15 def lags of f(1 - fps a) [com_ring R] (f : prime_spectrum (R) = f fp.1)):> 15 def lags of f(1 - fps a) [com_ring R] (f : prime_spectrum R a f p.1)):> 15 def lags of f(1 - fps a) [com_ring R] (f : prime_spectrum R a f p.1)):> 15 def lags of f(1 - fps a) [com_ring R] (f : prime_spectrum R a f p.1)):> 15 def lags of f(1 - fps a) [com_ring R] (f : prime_spectrum R a f p.1)):> 15 def lags of f(1 - fps a) [com_ring R] (f : h) (so f(1 - frime_s f(1 - fprime_s f(1 -</pre> | 30 | exact quoisintdomain H, | PL- | 86 | DV 9X h. | Pare |
| <pre>7 rest (0, Type () (Desr, Tell ()) () () () () () () () () () () () ()</pre> | 33 | ent | | | overft vik 51 | 1000 |
| <pre>S variable (k : Type d) (cmm.ring N) (c</pre> | - | | Decemponence. | | the contract of the contract o | |
| <pre>3 social prior [f = [f = []] [social [f = []]] [social [f = [</pre> | 32 | | and the second s | 00 | De la construcción de la | Down. |
| <pre>3 monopuls of Chir : prime spectra comp (pipponal)(: 1 + * pipponal)</pre> | 33 | variables (R : Type u) [comm_ring R] | 100 | 89 | { intro xh, | - Dan |
| 1 antic [1: yew] (com.res [1] (1: yew] spectrum (ph)mail [1]) 1 antic [1: yew] (com.res [1] (1: yew] spectrum (ph)mail [1]) 1 antic [1: yw] (com.res [1] (1: yew] spectrum (ph)mail [1]) 1 antic [1: yw] (com.res [1] (1: yw] (spectrum (ph)mail [1]) 1 antic [1: yw] (com.res [1] (1: yw] (spectrum (ph)mail [1]) 1 antic [1: yw] (com.res [1] (1: yw] (spectrum (ph)mail [1]) 2 antic [1: yw] (com.res [1] (1: ph)mail [1]) (spectrum [1] [1] (spectrum [1] (1]) 1 1 3 antic [1: yw] (com.res [1] (1: ph)mail [1]) (spectrum [1] [1] (spectrum [1] (1]) 1 1 4 antic [1: yw] (com.res [1] (1: ph)mail [1] (spectrum [1] [1] (spectrum [1] (1] (spectrum [1] (spectrum | 34 | noncomputable def Cstar := prime spectrum.comap (polynomial.C : R -+* polynomial R) | Janes. | 90 | simp at *. | 30000- |
| <pre>5 town def (R : Type u) (cmm.ring N (I : prom.spectrum (h))meant N) 5 town def (R : Type u) (cmm.ring N (I : prom.spectrum (h))meant N) 5 town def (R : Type u) (cmm.ring N (I : prom.spectrum (h))meant N) 5 town def (R : Type u) (cmm.ring N (I : prom.spectrum (h) = 1 : N , 5 town def (R : Type u) (cmm.ring N (I : prom.spectrum (h) = 1 : N , 5 town def (R : Type u) (cmm.ring N (I : prom.spectrum (h) = 1 : N , 5 town def (R : Type u) (cmm.ring N (I : prom.spectrum (h) = 1 : N , 5 town def (R : Type u) (cmm.ring N (I : prom.spectrum (h) = 1 : N , 5 town def (R : Type u) (cmm.ring N (I : prom.spectrum (h) = 1 : N , 5 town def (R : Type u) (cmm.ring N (I : h) : h, per (h) = prom.spectrum (h = 1 : f, p)) 5 town def (R : Type u) (cmm.ring N (I : h) : h, per (h) = prom.spectrum (h = 1 : f, p)) 5 town def (R : Type u) (cmm.ring N (I : h) : h, per (h) = prom.spectrum (h = 1 : f, p)) 5 town def (R : Type u) (cmm.ring N (I : h) : h, per (h) = prom.spectrum (h = 1 : f, p)) 5 town def (R : Type u) (cmm.ring N (I : h) : h, per (h) = prom.spectrum (h = 1 : h, p)) 5 town def (R : Type u) (cmm.ring N (I : h) : h, per (h) = prom.spectrum (h = 1 : h, p)) 5 town def (R : Type u) (cmm.ring N (I : h) : h, per (h) = prom.spectrum (h = 1 : h, p)) 5 town def (R : Type u) (cmm.ring N (I : h) : h, per (h) = prom.spectrum (h = 1 : h, p)) 5 town def (R : Type u) (cmm.ring N (I : h) : h, per (h) = prom.spectrum (h = 1 : h, p)) 5 town def (R : Type u) (cmm.ring N (I : h) : h, per (h) = prom.spectrum (h = 1 : h, p)) 5 town def (R : Type u) (cmm.ring N (I : h) : h, per (h) = prom.spectrum (h = 1 : h, p)) 5 town def (R : Type u) (cmm.ring N (I : h) : h, per (h) = prom.spectrum (h = 1 : h, p)) 5 town def (R : Type u) (cmm.ring N (I : h) : h, per (h) = prom.spectrum (h = 1 : h, p)) 5 town def (R : Type u) (cmm.ring N (I : h) : h, per (h) = prom.spectrum (h = 1 : h, p)) 5 town def (R : Type u) (cmm.ring N (I : h)) 5 town def (R : Type u) (cmm.ring N (I : h, prom.spectrum (h = 1 : h, p)) 5 town def (R : Type u) (cmm.ring N (I</pre> | 35 | | | 91 | intro 1 | 1.00 |
| y: | 24 | losso incl (R : Turo u) (coss ring R) (T : prime spectrum (polynomial R)) | | | | |
| 1 | | and the first of the state of t | | 92 | NAVE BOTT F I TN , LOUPIT I C X.1, | |
| <pre>31 Depin</pre> | 37 | : * p e (cstar 1).as_ideat , potynomiatic p e 1.as_ideat := | | 93 | { 18Tr0 111, | |
| <pre>3</pre> | 38 | begin | | 94 | refine mem def.mpr , | |
| 6 0 (ritize seq. et al.) (ritize seq. et al.) (ritize seq. et al.) 6 (ritize seq. et al.) (ritize seq. et al.) (ritize seq. et al.) (ritize seq. et al.) 6 (ritize seq. et al.) (ritize seq. et al.) (ritize seq. et al.) (ritize seq. et al.) 6 (ritize seq. et al.) (ritize seq. et al.) (ritize seq. et al.) (ritize seq. et al.) 6 (ritize seq. et al.) (ritize seq. et al.) (ritize seq. et al.) (ritize seq. et al.) 6 (ritize seq. et al.) (ritize seq. et al.) (ritize seq. et al.) (ritize seq. et al.) 6 (ritize seq. et al.) (ritize seq. et al.) (ritize seq. et al.) (ritize seq. et al.) 6 (ritize seq. et al.) (ritize seq. et al.) (ritize seq. et al.) (ritize seq. et al.) 6 (ritize seq. et al.) (ritize seq. et al.) (ritize seq. et al.) (ritize seq. et al.) | 19 | intros p hp. exact hp. | | 95 | have : f.coeff iii $\in \{r : R \mid \exists (i : N), r = f.coeff i\}$. | |
| 1 2 cell lange of βf (β: Type u) (cene, ring β] (f: polynostik β) := (p: prime_spectrum R B 1: N , (cell f 1) f = j.) 2 cell cell cell cell cell cell cell cel | 40 | and the second se | | 06 | I refine man def mar | |
| 21 get page of # (# : Type u) [com_ring #] (f : physetal #) := (p : prime_spectrum # [3 : N , [| 11 | | | 90 | 1 for any one of the set of the set | |
| <pre>2. sectempt of ent types 0 (cong, top at (1 + products at (2 + products at (1 + 1)), (2 + produc</pre> | 75 | | | 97 | retime sec_ot_app_int.mpr _, | |
| (cost f i f p.). 6 (cost f i f p.). 6 (cost d this,). 6 (cost d this,). 6 (cost d this,). 7 (cost d this,). 8 (cost | 42 | <pre>oet image_ot_bt {H : type u} [comm_ring H] (T : polynomial R) := {p : prime_spectrum R B i : N ,</pre> | | 98 | use iii, }, | |
| 33 44 54 55 55 57 57 57 57 57 57 57 57 | | (coeff f i) ¢ p.1) | | 99 | exact xh this,). | |
| | 43 | | | 160 | most och 11 | |
| 101 emo 102 emo 103 emo 103 emo 104 emo 104 emo 104 emo 105 | 22 | | | 100 | ware and 1 h | |
| 3 Insert d_s ff_1sepse (it : type i) (com_ring R) (a : B) : is_spen ((p : prime_spectrum R a (p.1)) := 102 | - | | | 101 | C19 | |
| 46 begin 103 104 1 refine (a),), | 45 | <pre>lemma std_aff_is_open {R : Type u} [comm_ring R] (a : R) : is_open ({p : prime_spectrum R a @ p.1 }) :=</pre> | | 102 | | |
| 47 refine ({a} ,), 100 | 46 | begin | | 103 | | |
| | 47 | refine ({a} ,), | | 104 | | |

A proof that $\pi: Y \times \mathbb{A}^1 \to Y$ is open – frame 2

| | rw mul comm, | | 165 | apply n1, | | |
|-------|--|--|-------|--|-------|--|
| 113 | refine submodule.smul mem | Salar Printing and the rates | 167 | exact mem_map_C_iff.mp_a_i, | | PROPERTY AND |
| 114 | and a second sec | TERCONFERMENT. | 168 | rad | - 1 | A March Holeward |
| | appry additionate approx | and to see an else have been a | 100 | | | |
| 112 | use 1, J, | and the fifth of a same brand of | 100 | | | A4 74 844 |
| 116 | { have h2 : f.coeff 1 = 0, by simpa using h, | And the state of t | 170 | | | ALC: NOT THE OWNER OF THE OWNER |
| 117 | simp [h2], } | CONTRACTORS AND | | | | |
| 110 | and | J. Colorado | 172 | lenna updown (R : Type u) [conn ring R] (r : R) : r = coeff (C r) 0 := | | |
| | | SAMPLES FITTLESSES | 173 | hanin | - 1 | EASTERNATION. |
| 178 | | Parent and | | | | |
| 128 | | Sec. | 1/4 | exact coeri_L_zero.symm, | | |
| | | Partan | 175 | end | - 2 | (hereige- |
| 121 | lenna imma f2ind (R : Type u) (comm ring R) (f : polynomial R) (I : prime spectrum (polynomial R)) : f f | | 176 | | 1 | |
| | I 1 - 21 : N coeff f 1 6 (Catar I) 1 :- | | | | | 2017 82 |
| | | 2000 | 3 710 | losso undersBid (2 : Turo u) (come ring 2) (r : 2) (2 : prime reactrum 2) (2 : r = 2 1) : r = ((idea) co | | Critica |
| 122 | begin . | 100 | 110 | (C. D. A strain of the strain | | 100- |
| 123 | let P := Cstar I, | Second Second | | (c : R +++ potynomiat R)) ((map c +:1 : ineat (potynomiat R)))) := | - 1 | |
| 124 | by contradiction a, | View. | 179 | Degin | | |
| 125 | push neg at a. | APPA ANALY MALE AND | 189 | <pre>let liftP := ideal.map (polynomial.C : R -+* polynomial R) P.1,</pre> | | PROGRAMMENT |
| 1.74 | coror a with fet cial | 9/C | 101 | have req : $(r) = C^{(1)}(C^{(1)}(r))$ | 5 | 197 |
| 120 | sector ded | See | 197 | (with | | |
| 127 | appry mi, | 80000 | | 1 | | Correctores |
| 128 | have tins : T E ideal.span {Tt : polynomial R d 1 : N ,Tt = (C [coeff T 1)]}, by exact tinch T, | 20 | 10.3 | spece, | | 185 |
| 129 | have pas : V (i : N), f.coeff i c P.1, by exact cini, | AND A PRIMA PRAY | 184 | { intro hx, | | |
| 138 | have Mod P1 Cod I1 | 30- | 185 | have ; x=r, by exact hx, | | See. |
| 121 | (intro p hp | COLUMN STREET | 185 | ne this. | | ALCONGLUSS |
| | and the property of the second s | jan | 107 | finish 1 | | |
| 125 | exact inct i p np, p, | 5-mon | 407 | tataan, j, | 2 | |
| 133 | have anc : V (1 : N), C (f.coeff 1) ∈ I.val, | A WYAR | 188 | (intro hx, | | grane |
| 134 | (intro 1. | and the second s | 189 | refine mem_singleton_iff.mpr _, | | |
| 135 | exact this (f.coeff 1) (cini 1).). | Mar. | 199 | simp * at *, | 2 | Ma |
| 126 | have and : $(tt : nolumential R 2 (1 : b) tt = 0 (t coeff (b) < 1 val$ | SHALLING AND | 191 | exact hr.).). | | |
| | and more a fee a preprint of a fee of a contract of a struct | Provide and a second second | 103 | I unfold ideal man | | |
| 137 | f intros te tin, | Str. | 192 | 1 unoto iveat.may, | - 3 | div |
| 138 | cases tth with 1 hi, | and a second sec | 193 | apply submodule.subset_span, | | |
| 139 | ne hi, | and the second s | 194 | exact mem_image_of_mem C.to_fun H, }, | | |
| 148 | exact (submodule.mem.com L.val).mor (this (coeff f i) (cini i)). }. | Street, Street | 195 | exact ring to semiring, | | |
| 1.4.5 | have seed a dense the a seturement of a 1 7 dd a bit at a fild another distance from | What have no | 105 | evant set has simpleton | | |
| 141 | note and a topan fire pergenerate a b (1 - n), cc = c (1.0001 1)), 1 5 1.9ac, | Sectors | 107 | and | | |
| 142 | <pre>{ have : (span {tt : polynomial K 3 (1 : n), tt = C (T.COETT 1)}).1 S (span +(1.Val)).1,</pre> | Constanting of | 197 | | | |
| 143 | { apply span_mono, | and the second s | 198 | | | |
| 144 | exact ancl, }, | Dave and | 199 | | | |
| 145 | evact binter subset of mem and) | 2 Martin Contraction of the Cont | 288 | lemma liftproi (R : Type u) [comm ring R] (P : prime spectrum R) : (prime spectrum.comap (polynomial.C : | R → 2 | |
| 140 | (what sould find) | | | +* polynomial R)) ((ideal.map C.P.1 : ideal (polynomial R)) , by exact (quotient, | | |
| 140 | tweet and this, p. | | | is integral demain iff orige (ideal man (P val - ideal (columnais) P))) an (qualitationate P 2) 1 - P - | | |
| 147 | e10 | | | The state of the s | | |
| 148 | | | 281 | begin | | |
| 149 | | | 282 | <pre>let lift : prime_spectrum (polynomial R) := ((ideal.map C P.1 : ideal (polynomial R)) , by exact</pre> | | |
| 150 | /- imma spec shows that if a point of Spec Rixi is not contained in the vanishing set of f. | | | (quotient.is_integral_domain_iff_prime (ideal.map C P.val : ideal (polynomial R))).mp (quoisintdomain | Ρ. | |
| 161 | . then its impose in Spec R is contained in the open where at least one of the coefficients | | | 21.1. | | |
| 100 | | | 202 | av 21 | | |
| 125 | | | 203 | Contract of the second s | | |
| 153 | <pre>lemma imma_spec {R : Type u} [comm_ring R] {f : polynomial R) {I : prime_spectrum (polynomial R)} (H : I</pre> | | 284 | ext, | | |
| | E (orime spectrum.zero locus (f) : set (prime spectrum (polynomial R)))*) : Cstar I E image of Df f := | | 285 | split, | | |
| 154 | beats | | 285 | { intro hx, | | |
| 155 | simp 5 at 5 | | 287 | ny undown x. | | |
| | and a second sec | | 207 | and an an C iff as he C 1 | | |
| 156 | apply imma_tzing, | | 208 | CARLS HER HOP CLITTER IN 0, J. | | |
| 157 | exact H. | | 209 | f Inclo Inc. | | |

$\pi \colon Y \times \mathbb{A}^1 \to Y$ is open

goals accomplished

219 intros U hU. rw is open iff at hU. cases hU with fs cl. 224 225 have funi : fs = ([] 1 : fs , {1.1}), fext1. split;finish}, rw funi at cl, 238 rw zero locus Union at cl. have uuni : $U = (\Pi (i : rfs), zero locus {i,val})^c$. 234 {rw + cl, 235 symmetry. 236 exact compl_compl U.}. 238 rw compl Inter at uuni. 239 rw uuni. 242 rw image Union, 244 apply is open Union, 245 246 intro f. 247 have image : (Cstar) '' (zero locus {f.val})' = image of Df f.1, 251 { ext1. split, { intro hx. cases hx with xli. cases hx h with complement img, 256 symmetry' at img. rw img, 258 apply imma spec. exact complement, }, 260 { intro hx, simp * at *. use (ideal.map C x.val : ideal (polynomial R)), 262 263 { exact liftprime x.2. }. { split, { exact sur1 +f x hx, }. 266 { exact liftproj x, }, }, }, }, 267 rw image, exact total image f.1, 270 end 272 end Rx2Ropen

 Tartic state goals accomplished 🔏 All Messages (0) 1 Karn Sharm.

Damiano Testa (Warwick)

Maths in Lear

January 7th, 2021

After that, I became better at golfing!

I am learning golfing tricks thanks to the combined efforts of the many users of the Zulip chat.

I am incredibly grateful for the time that everyone on Zulip devotes to answering the questions that appear there!

Shortened version



The proof went from approx 250 to approx 90 lines. Of course, there is room for further compression.

However, I have not inspected the proof with the idea of formalizing it.

I simply took *some* mathematical proof and converted it step by step.

The proofs above are based on Lemma 10.28.7 of the Stacks project and its dependencies.

The arguments in the Stacks project are very easy to read for a human.

For me, though, they were hard to formalize directly. The end result is the initial long argument.

Golfing provided a layer of compression, basically navigating inside the same proof, but taking fewer detours.

Revising the proof with the idea of formalizing



Image credit: Robert Hodgin.



Image credit: Aubrey Jaffer.

Writing a mathematical paper gives a chance to revise proofs:

- many arguments are dead-ends,
- several lemmas go around in circles,
- some steps required a more details.

Revising the proof with the idea of formalizing



Image credit: Robert Hodgin.



Image credit: Aubrey Jaffer.

For me, the initial plane-filling proof is almost a necessity.

I make sure that what I am saying is **true** by

- working out representative cases,
- thinking about extreme cases and pushing boundaries,
- removing hypotheses to see what fails,
- proving related, but unnecessary statements.

Damiano Testa (Warwick)

Maths in Lear

- I believe that the carpet of lemmas around a definition is related to what is called an API by the Lean community!
- In the long run, the vast amount of auxiliary results, unneeded corollary, trivial implications, barely off-target proofs is what convinces me that what I want to prove is actually true.
- After that, I write a proof.

I am confident that I am proving something true, **because** of the carpet of auxiliary results.

I am also confident that I may make mistakes in writing it down.

The meanderings around my arguments are the reason that I am confident that my mistakes are fixable.

What I am still getting used to, is that now **Lean** is making sure of the soundness of the arguments!

Of course, there is still the need of the carpet of lemmas of the API, but it now plays a somewhat different role, at least in my mind!

Chevalley's Theorem – formalization revised

Back to the projection map

$$\pi \colon \operatorname{Spec} R[x] \longrightarrow \operatorname{Spec} R$$

or, in Lean,

```
prime_spectrum.comap (C : R \rightarrow^{+*} polynomial R)
```

Going deeper into the proof, besides inductions, open covers, restrictions and tautologies, the main lemma is the following.

Lemma

Let R be a commutative ring and let $I \subset R$ be an ideal. A polynomial $f \in R[x]$ belongs to the ideal generated by I if and only if all the coefficients of f belong in I.

Lemma

Let R be a commutative ring and let $I \subset R$ be an ideal. A polynomial $f \in R[x]$ belongs to the ideal generated by I if and only if all the coefficients of f belong in I.

This lemma appears in ring_theory/polynomial/basic.lean under the name mem_map_C_iff.

Theorem (mem_map_C_iff)

Also, I understand better the mathematical proof!

I think that I can further substantially shorten the proof.

In the golfed proof above, lemma mem_map_C_iff only appears at the very end of the final proof.

I need to go back and rethink all the proofs with the aim of extending the application of mem_map_C_iff.

In fact, I might even discover that this is already developed in mathlib! If someone knows that this is the case, then I would be extremely happy to learn this!

Thank you!

Questions?

Damiano Testa (Warwick)

Maths in Lean

January 7th, 2021