Proofscape: Argument Mapping for Mathematics

Steve Kieffer, Monash University, Caulfield, Australia

Diagrams 2014

This talk has 2 parts:

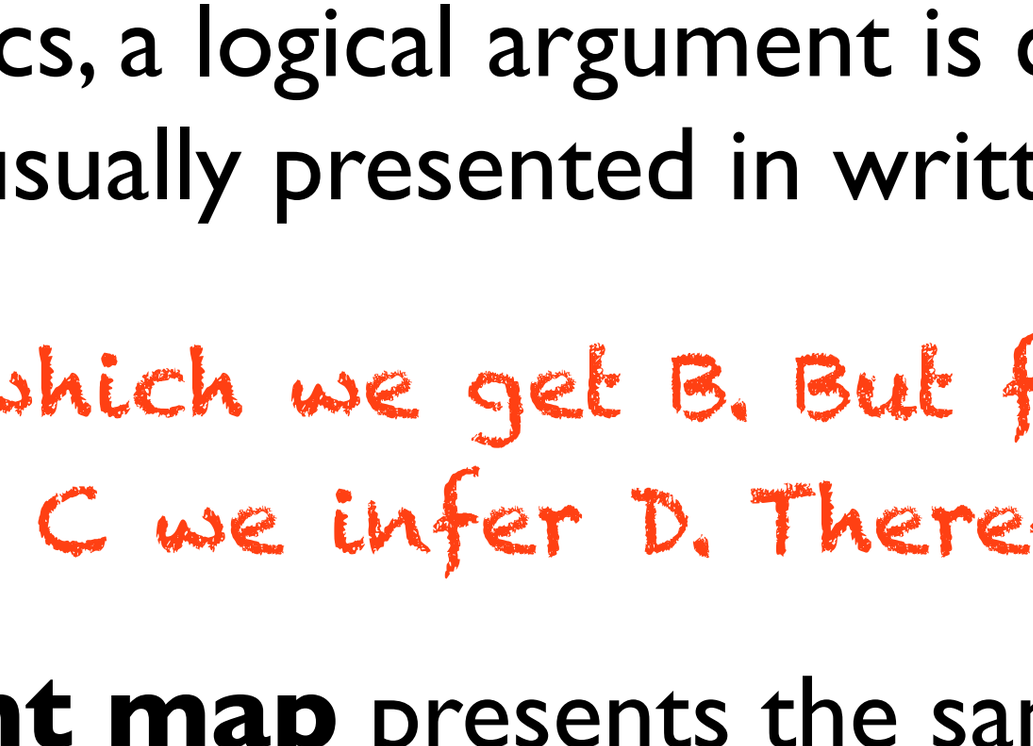
- 1. Proofscape: a simple argument mapping system for mathematics
- 2. What do argument maps *do for us* when we study mathematical proofs?

Part 1: Proofscape: a simple argument mapping system for mathematics

In mathematics, a logical argument is called a proof, and it is usually presented in written prose:

...from which we get B. But from A, B, and C we infer D. Therefore...

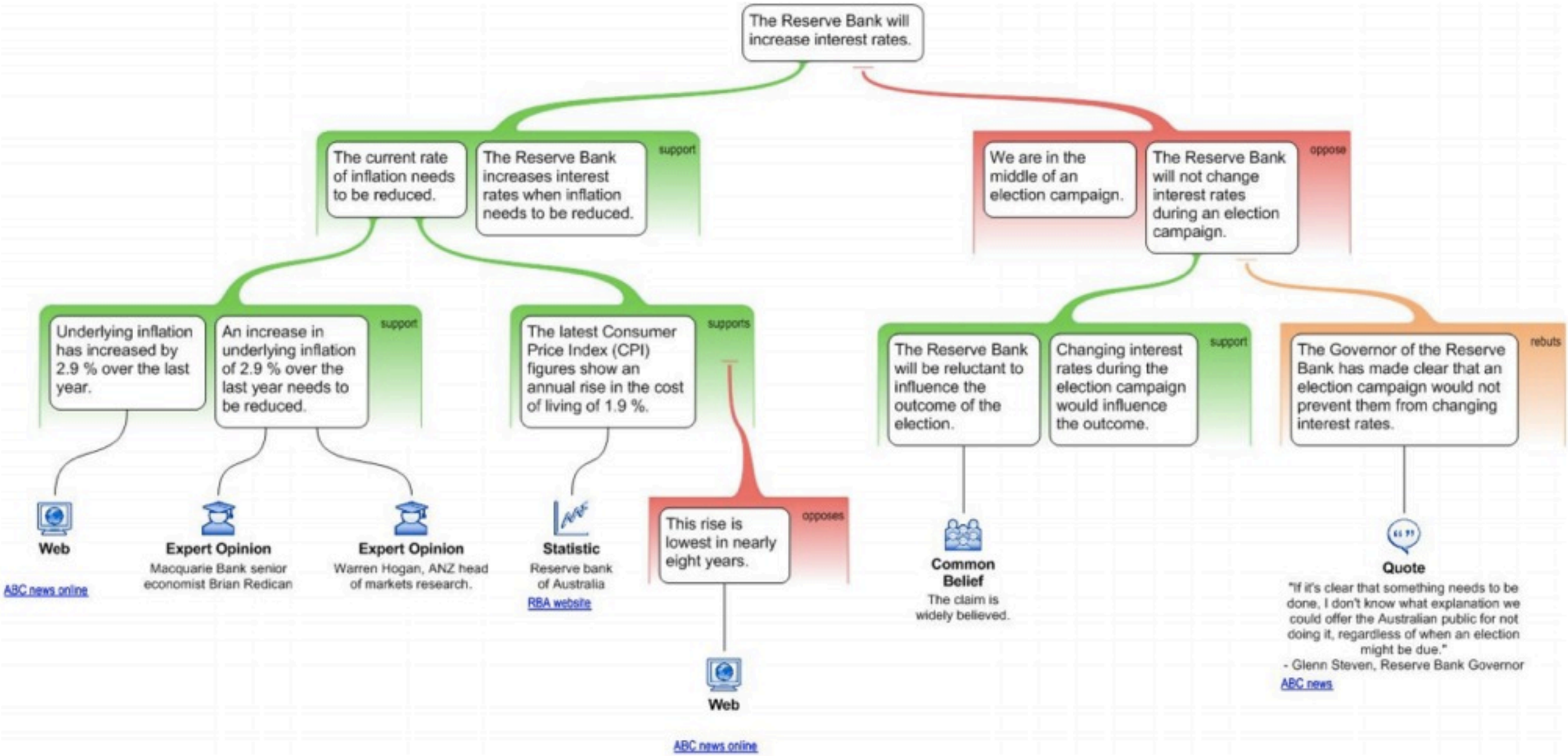
An **argument map** presents the same argument with a picture:



Argument Mapping

- Long used in Law, Politics, Business, Econ
  - Usually uses the *Toulmin model* (1969), which accommodates:
    - objections
    - rebuttals
    - citations of factual evidence

Example: decision to increase interest rates



Credit: Sbarski, Peter, Tim van Gelder, Kim Marriott, Daniel Prager, and Andy Bulka. *Visualizing argument structure*. Springer Berlin Heidelberg, 2008.

The Toulmin model is not really appropriate for mathematics, where claims are either true or false, never debatable.

Mathematical arguments have different requirements, starting with ways to introduce:

Definitions and **Assumptions**

Let g be the gradient of f...

Let E be a number field...

Suppose f has a zero in the interval I...

Suppose G is an Abelian group...

In Proofscape, assertions go on plain boxes:

$p = q^2$

f is continuous

$[\, E : F \,] = 3$

while definitions go on bold boxes:

Let $ef = n - 1$

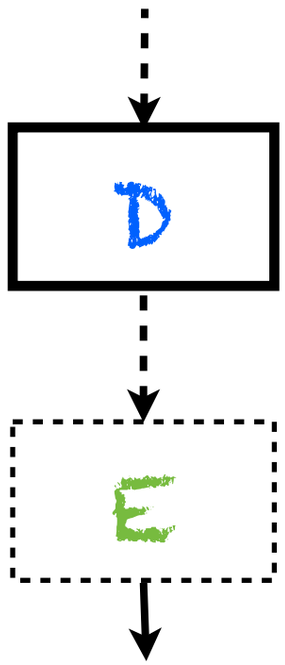
Let S be an elementary symmetric function

and assumptions go on dashed boxes:

Suppose f is strictly increasing

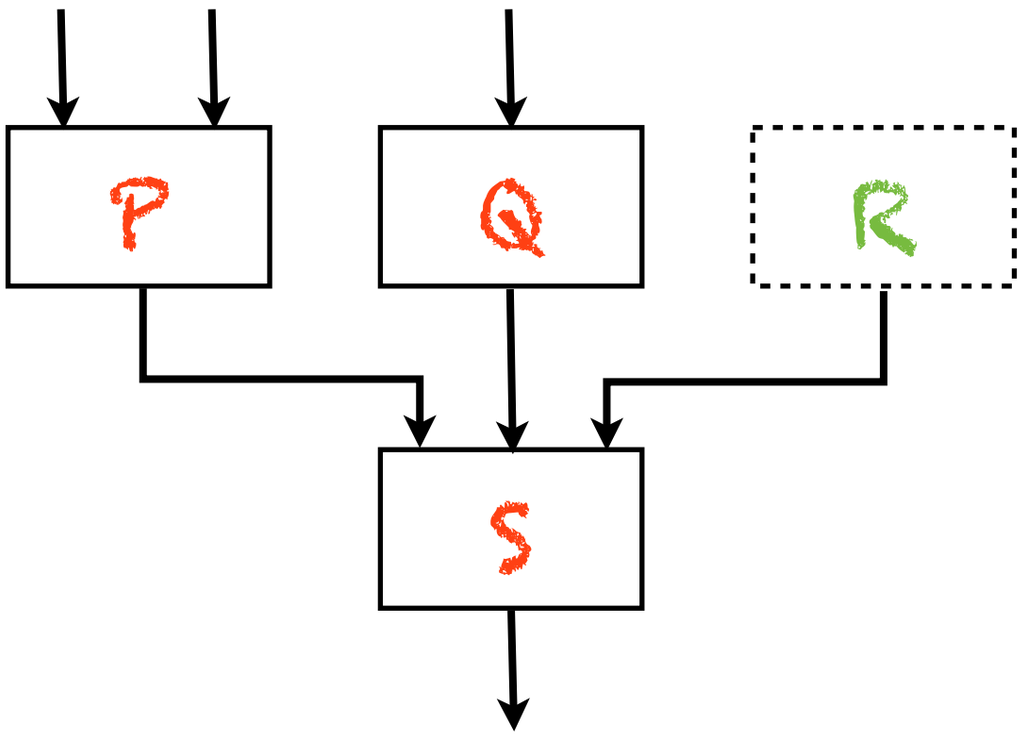
p is prime

Since it is important that definitions and assumptions be introduced before they are used, Proofscape features a dashed arrow called a **flow** arrow:



"after D, please consider E next"

while solid arrows are called **deduction** arrows, and indicate the logic of the argument:



"from P, Q, R, we deduce S logically"

Proofscape featrues a few other node types...

For citing results:

Theorem 33

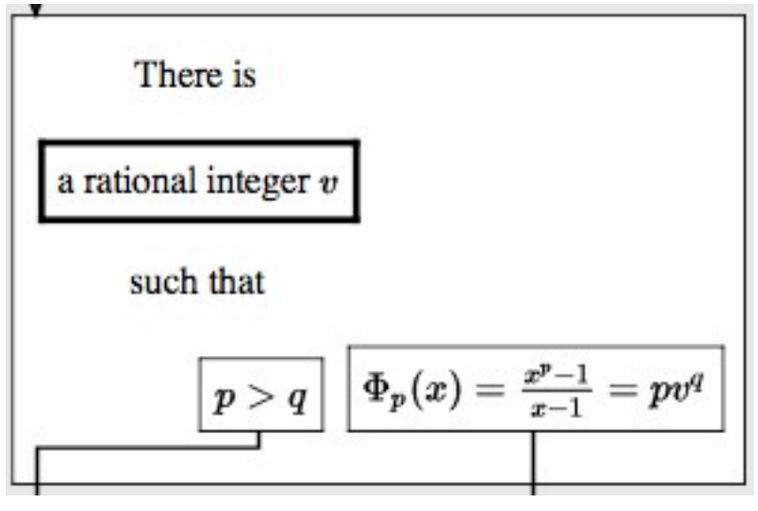
Lemma 8

For indicating methods of inference:

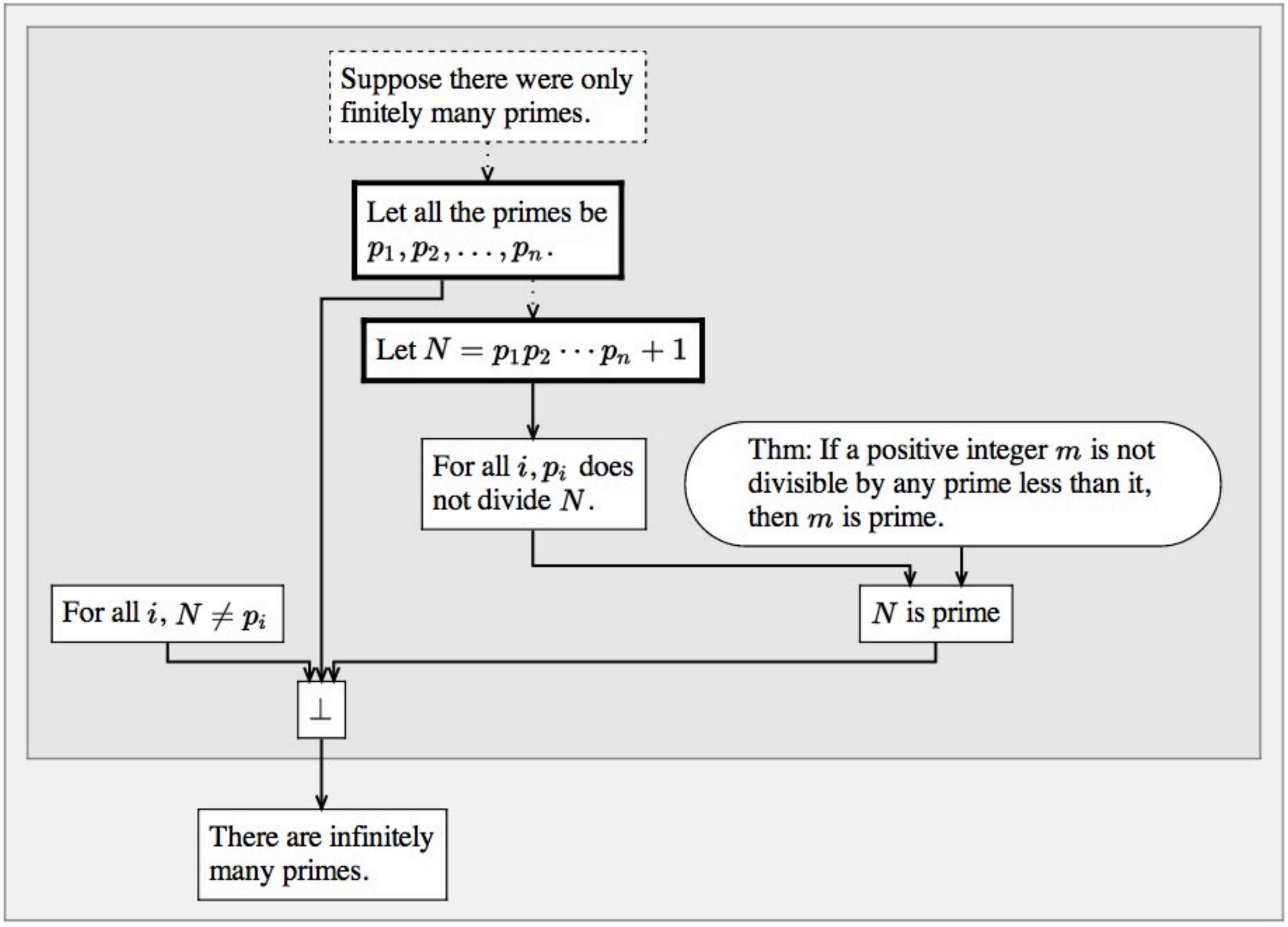
by induction

substituting c for x

And compound nodes
e.g. for existential
statements:



Example: proof that there are infinitely many primes

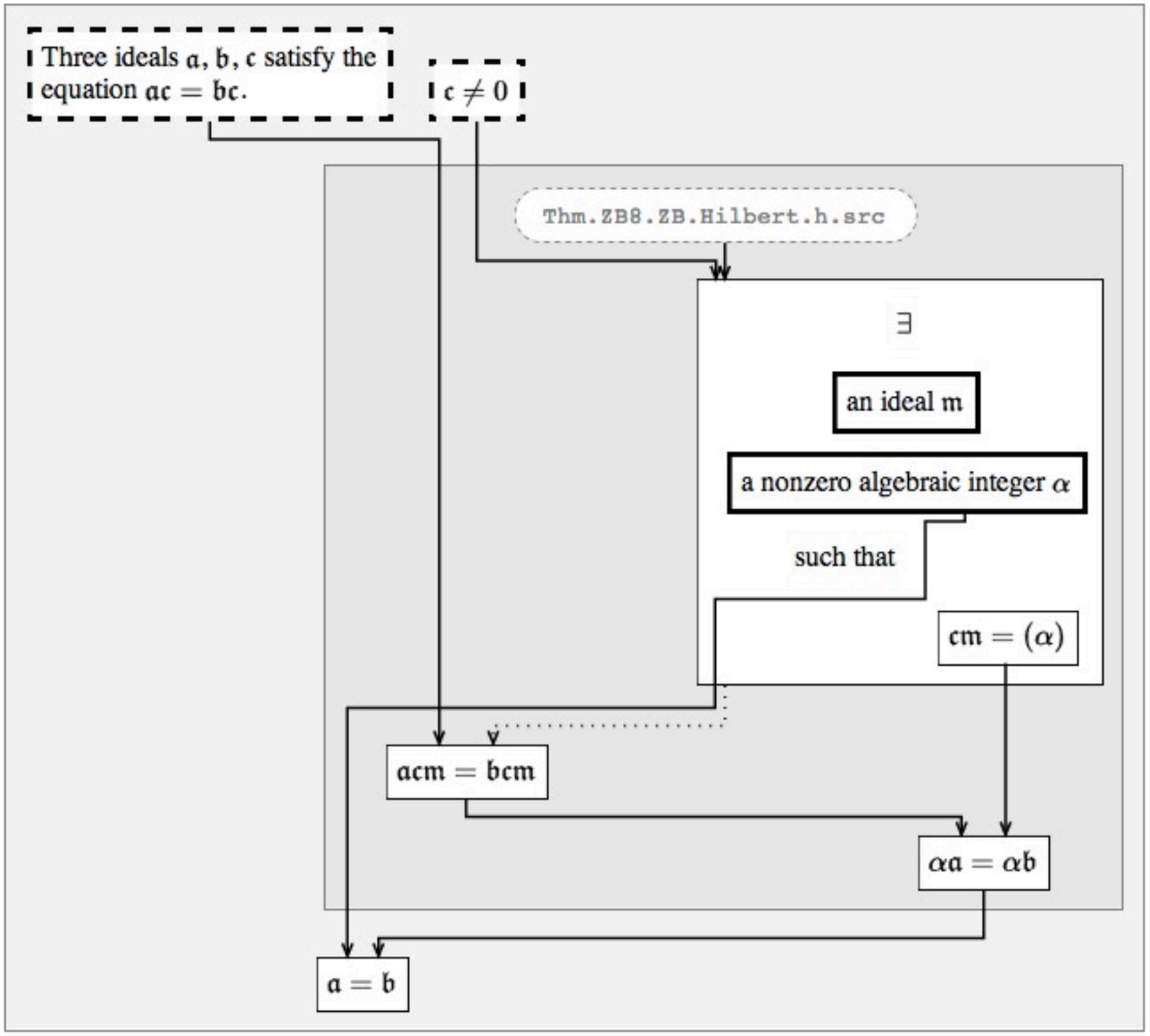


Part 2: What do argument maps *do for us* when we study mathematical proofs?

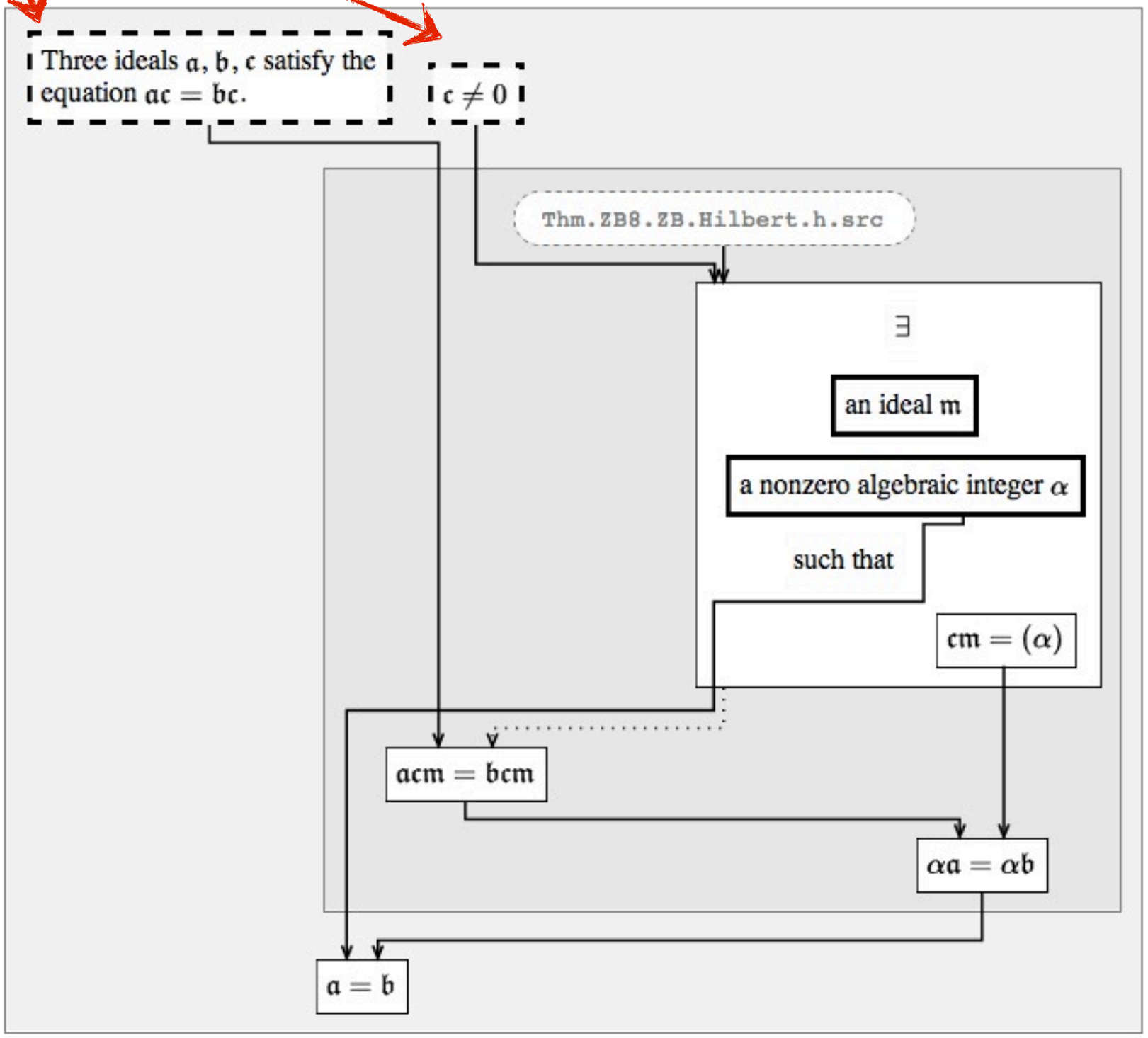
Answer: argument maps...

- ...show where all the hypotheses are used
- ...show the role of each intermediate conclusion
- ...exhibit "pivots"
- ...facilitate switching between details and the big picture
- Many more.

Seeing where the hypotheses are used

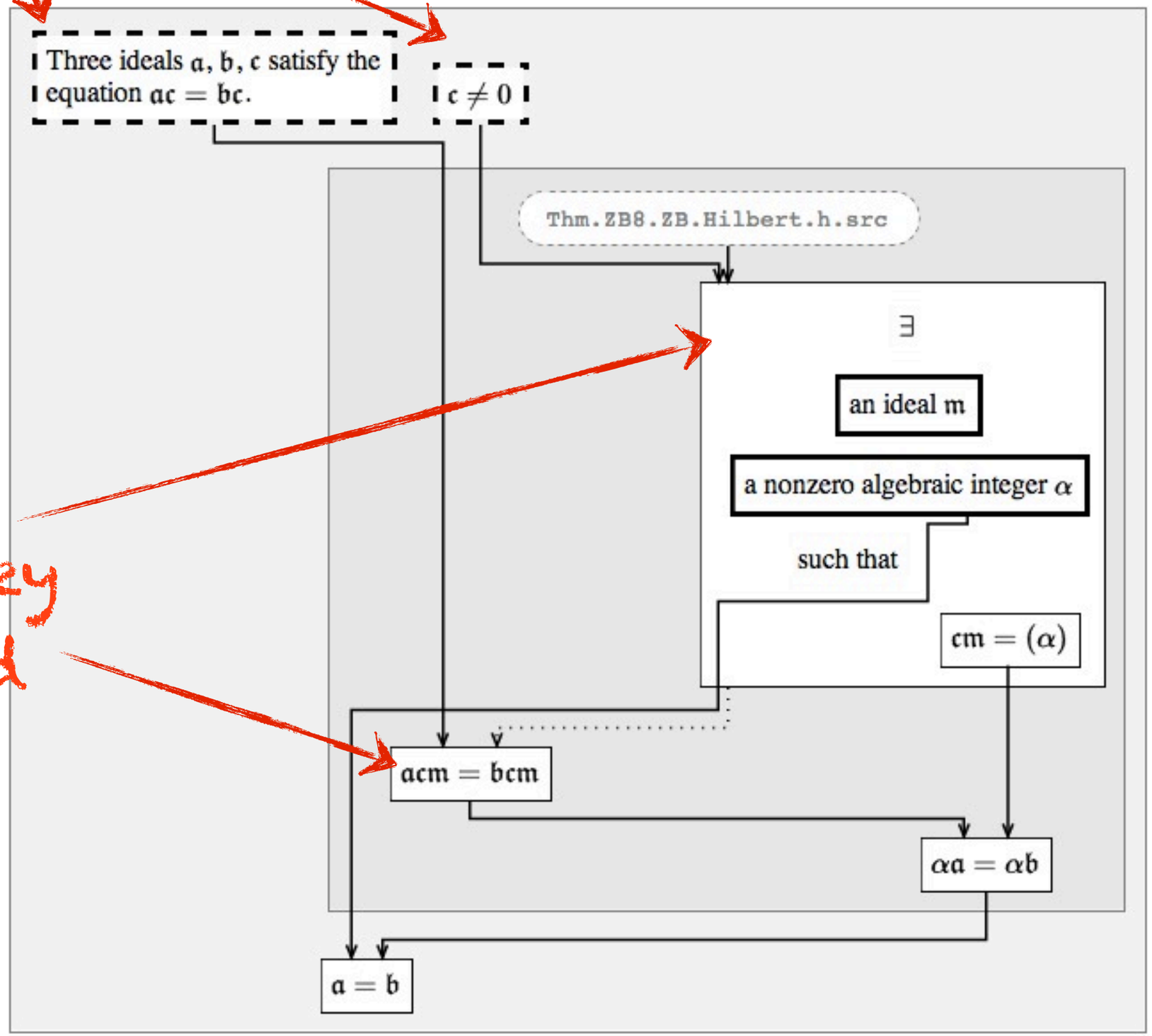

Three ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ satisfy the equation $\mathfrak{ac} = \mathfrak{bc}$.
$\mathfrak{c} \neq 0$
Thm.ZB8.ZB.Hilbert.h.src
∃
an ideal $\mathfrak{m}$
a nonzero algebraic integer α
such that
$\mathfrak{cm} = (\alpha)$
$\mathfrak{acm} = \mathfrak{bcm}$
$\alpha\mathfrak{a} = \alpha\mathfrak{b}$
$\mathfrak{a} = \mathfrak{b}$

hypotheses

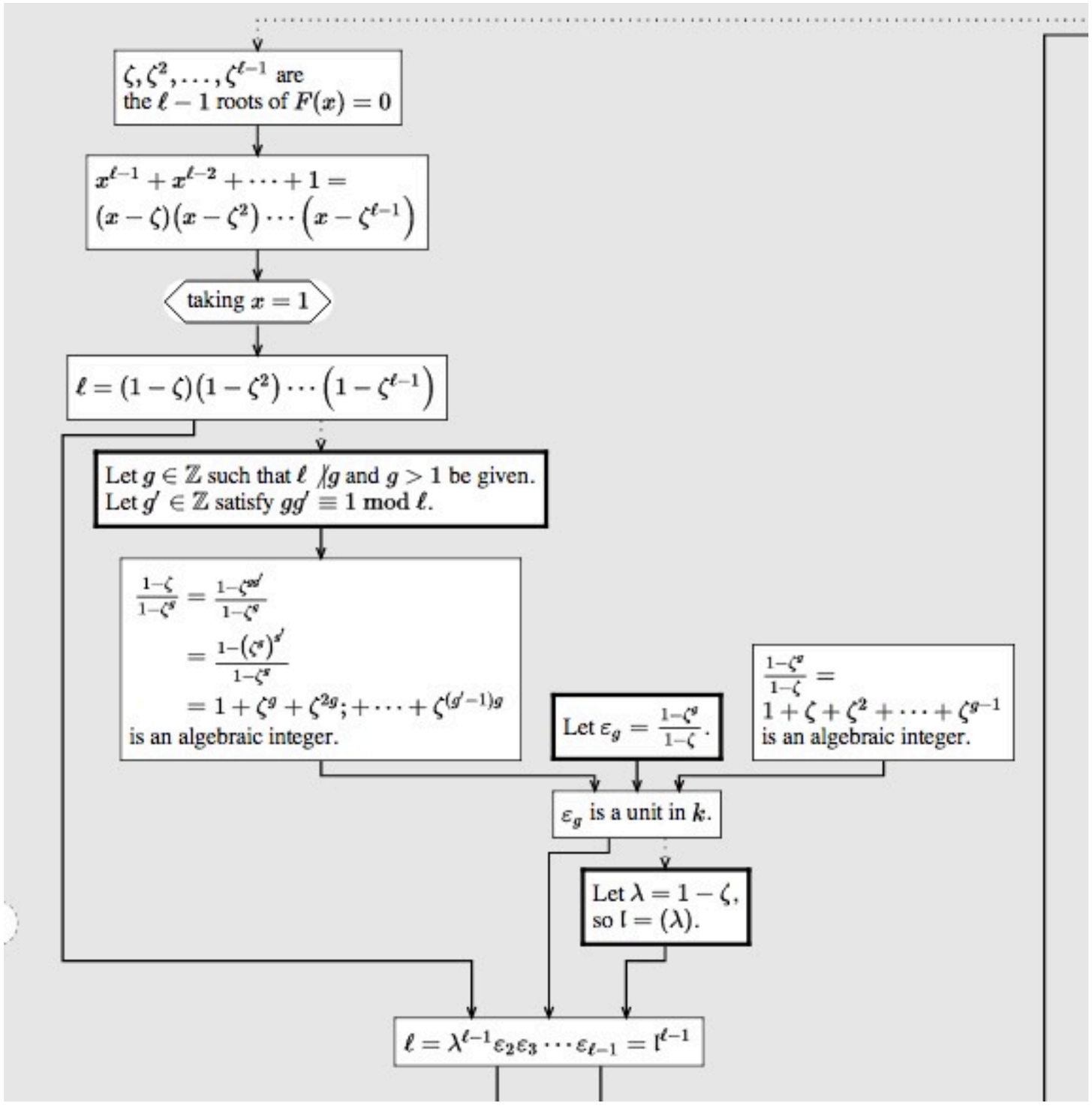

Three ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ satisfy the equation $\mathfrak{ac} = \mathfrak{bc}$.
$\mathfrak{c} \neq 0$
Thm.ZB8.ZB.Hilbert.h.src
∃
an ideal $\mathfrak{m}$
a nonzero algebraic integer α
such that
$\mathfrak{cm} = (\alpha)$
$\mathfrak{acm} = \mathfrak{bcm}$
$\alpha\mathfrak{a} = \alpha\mathfrak{b}$
$\mathfrak{a} = \mathfrak{b}$

hypotheses

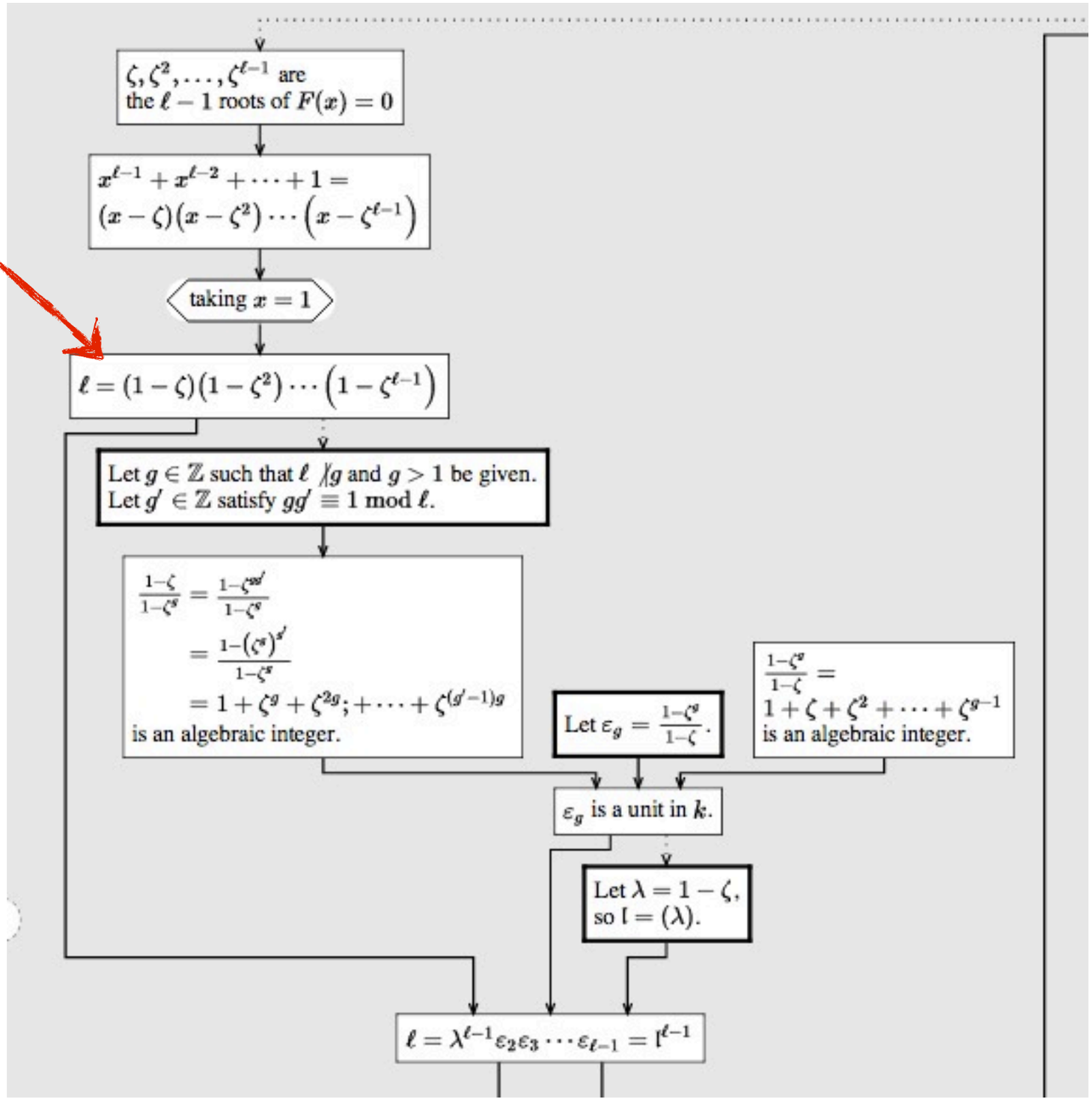
steps where they are used



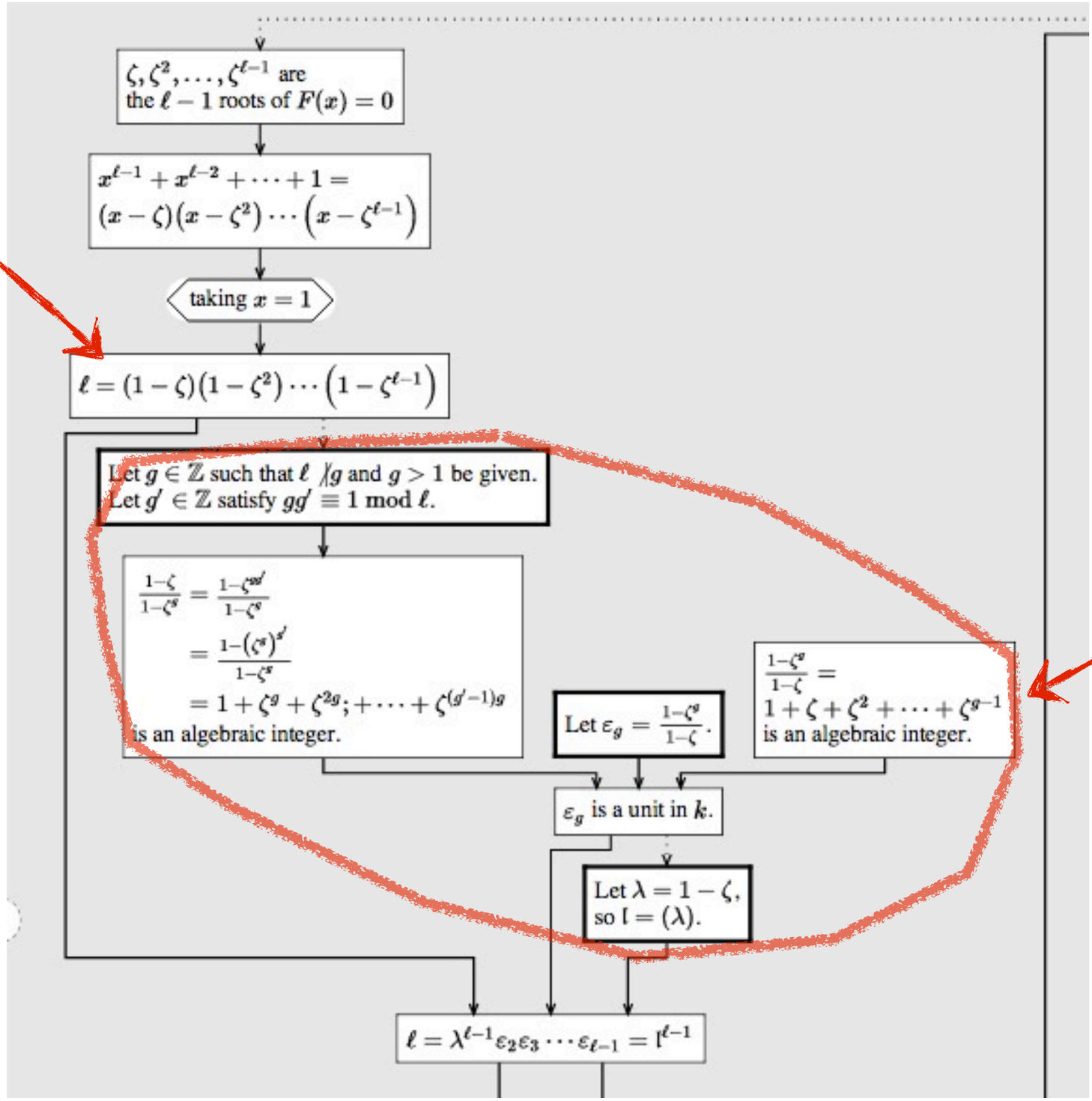
Understanding the role of intermediate steps


$\zeta, \zeta^2, \ldots, \zeta^{\ell-1}$ are the $\ell - 1$ roots of $F(x) = 0$
$x^{\ell-1} + x^{\ell-2} + \cdots + 1 = (x-\zeta)(x-\zeta^2)\cdots\left(x-\zeta^{\ell-1}\right)$
taking $x = 1$
$\ell = (1-\zeta)(1-\zeta^2)\cdots\left(1-\zeta^{\ell-1}\right)$
Let $g \in \mathbb{Z}$ such that $\ell \not| g$ and $g > 1$ be given. Let $g' \in \mathbb{Z}$ satisfy $gg' \equiv 1 \bmod \ell$.
$\frac{1-\zeta}{1-\zeta^s} = \frac{1-\zeta^{sg'}}{1-\zeta^s}$
$= \frac{1-(\zeta^s)^{g'}}{1-\zeta^s}$
$= 1 + \zeta^g + \zeta^{2g}; + \cdots + \zeta^{(g'-1)g}$
is an algebraic integer.
Let $\varepsilon_g = \frac{1-\zeta^g}{1-\zeta}$.
$\frac{1-\zeta^g}{1-\zeta} =$
$1 + \zeta + \zeta^2 + \cdots + \zeta^{g-1}$
is an algebraic integer.
ε_g is a unit in k.
Let $\lambda = 1 - \zeta$, so $\mathfrak{l} = (\lambda)$.
$\ell = \lambda^{\ell-1}\varepsilon_2\varepsilon_3\cdots\varepsilon_{\ell-1} = \mathfrak{l}^{\ell-1}$

We reach conclusion Q, but don't immediately use it.

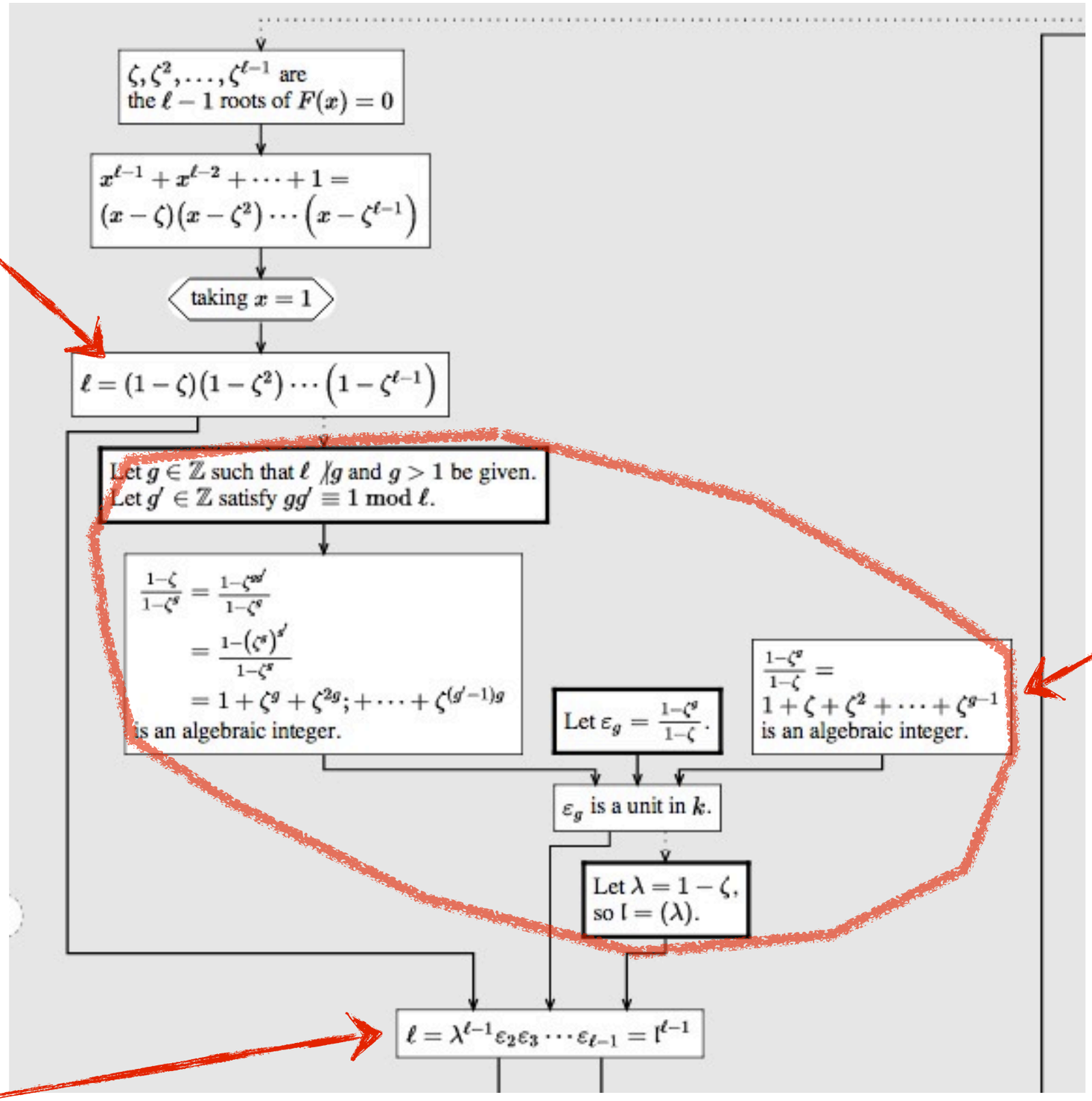


We reach conclusion Q, but don't immediately use it.



The argument carries on for quite a while...

We reach conclusion Q, but don't immediately use it.



The argument carries on for quite a while...

...before Q is finally used.

Pivots

The truth of a theorem is in no way obvious.

$x^3 + y^3 = z^3$ has no nontrivial solutions in the integers!

Really?

But a proof confirms a theorem by a sequence of small inferences, each of which *is* obviously true.

Well we know A and B.

Of course.

And from A and B, C follows.

That is clear.

But from C and D we get E.

Nothing could be plainer.

How can this be possible?

How can

obvious + obvious + ... + obvious = not at all obvious

?????

Answer: Often the cleverness in a proof comes in the form of what are called

“pivot objects”

or simply

“pivots”

What is a pivot?

A pivot is an **object** which the author of the proof asks you to consider -- it could be a certain *polynomial*, or *matrix*, or *summation*, etc.

And this object always has at least **two** important properties, germane to the theorem being proved.

The existence of a single object possessing these two properties (whatever they are) is often the key to proving the theorem.

Example:

"Fermat's Last Theorem" states that $a^n + b^n = c^n$ has no nontrivial integer solutions when $n > 2$.

Gerhard Frey introduced the *Frey curve:*

$$y^2 = x(x - a^n)(x + b^n)$$

which has **two** important properties:

1. If $a^n + b^n$ *were* equal to c^n then this curve would not be modular (never mind what that means); and

2. This curve is semistable, which (as Wiles proved) implies that it *is* modular.

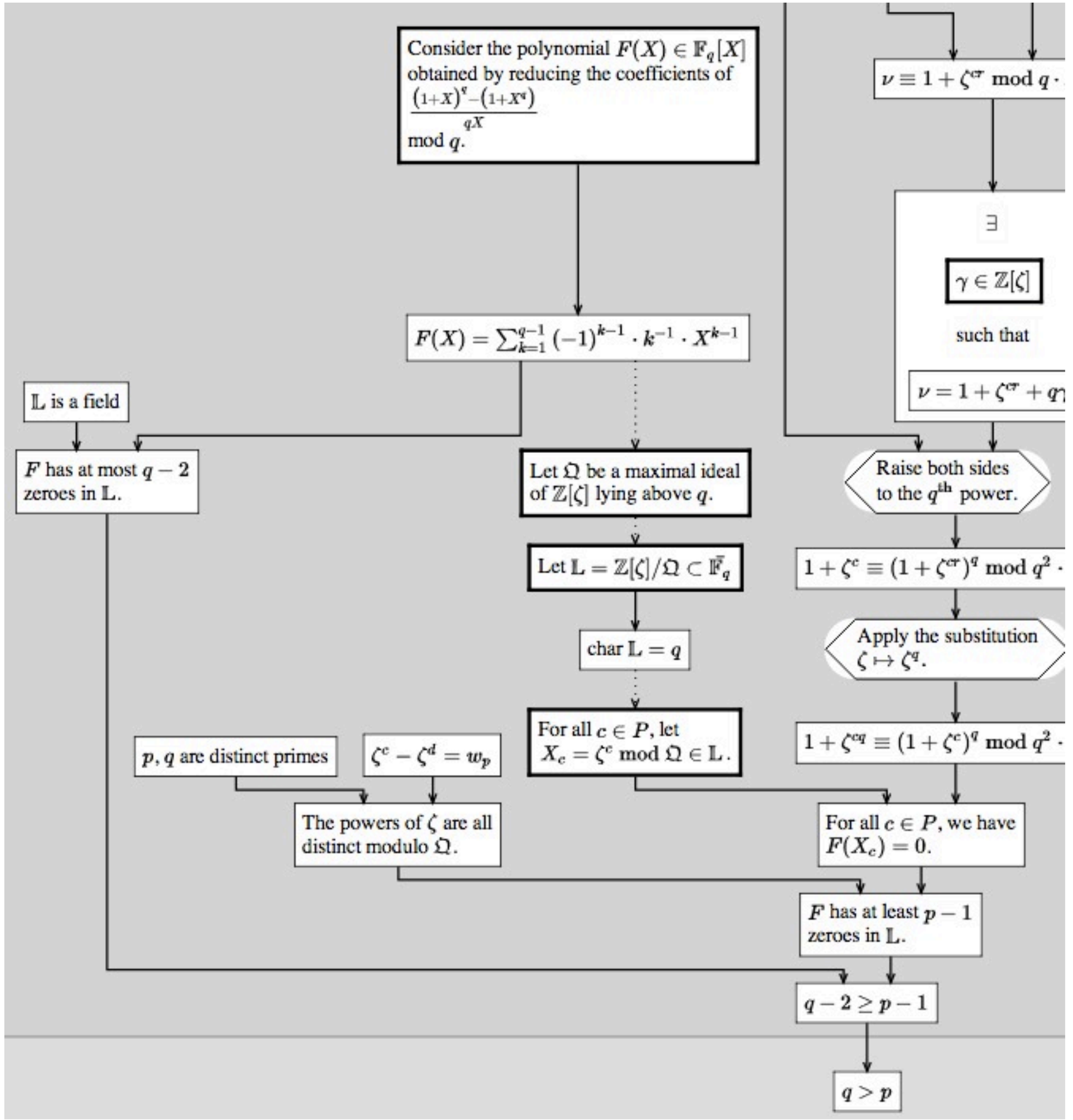
So the Frey curve was a **pivot** in the proof of FLT.

In general, the **non-obviousness** in a proof *often* lies largely in the decision to consider a certain pivot object.

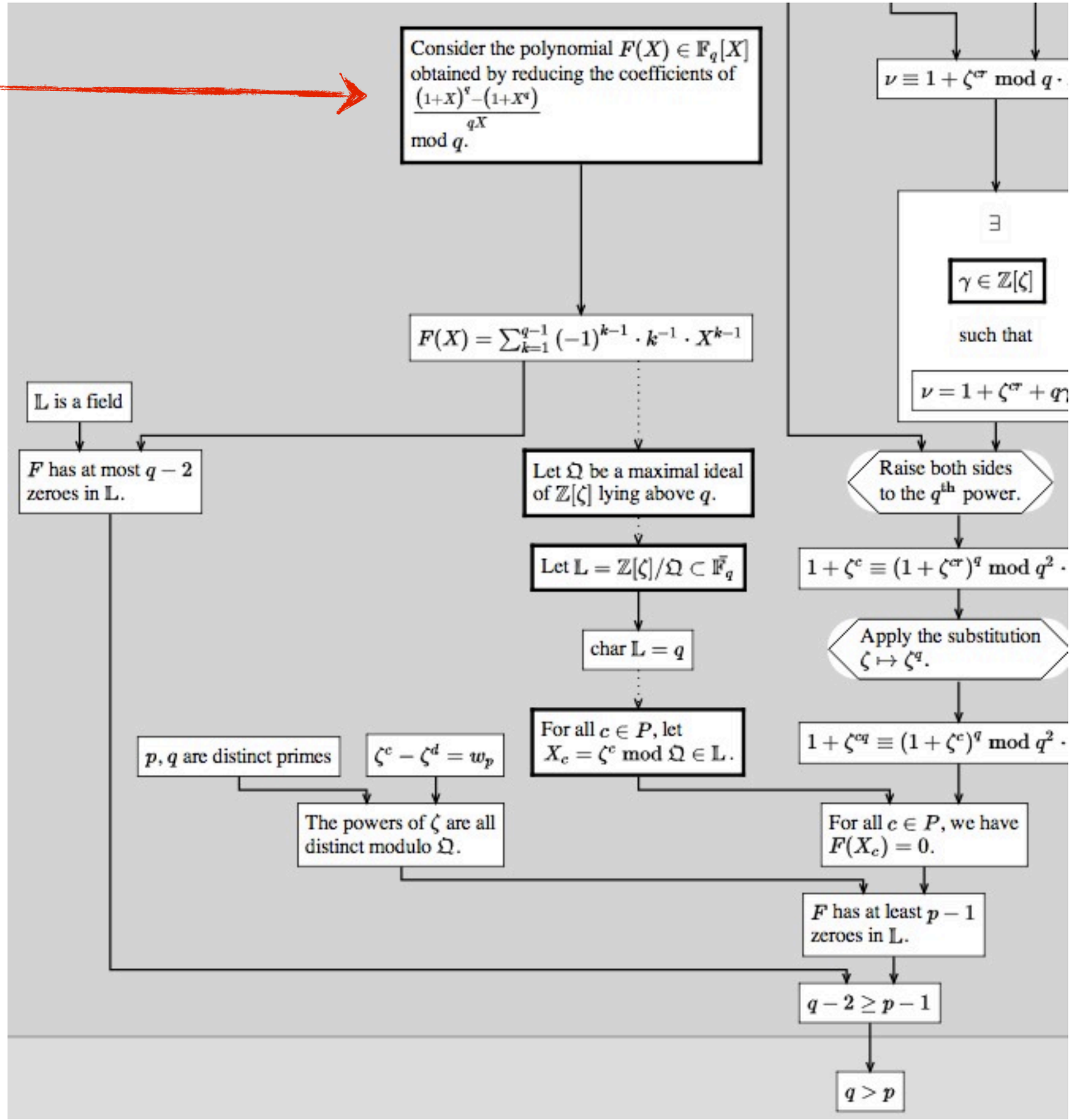
obvious + obvious + **pivot** + obvious = not at all obvious

Therefore: when we study a proof, the pivots are among the first things we should hope to identify!

How can an argument map help with this?

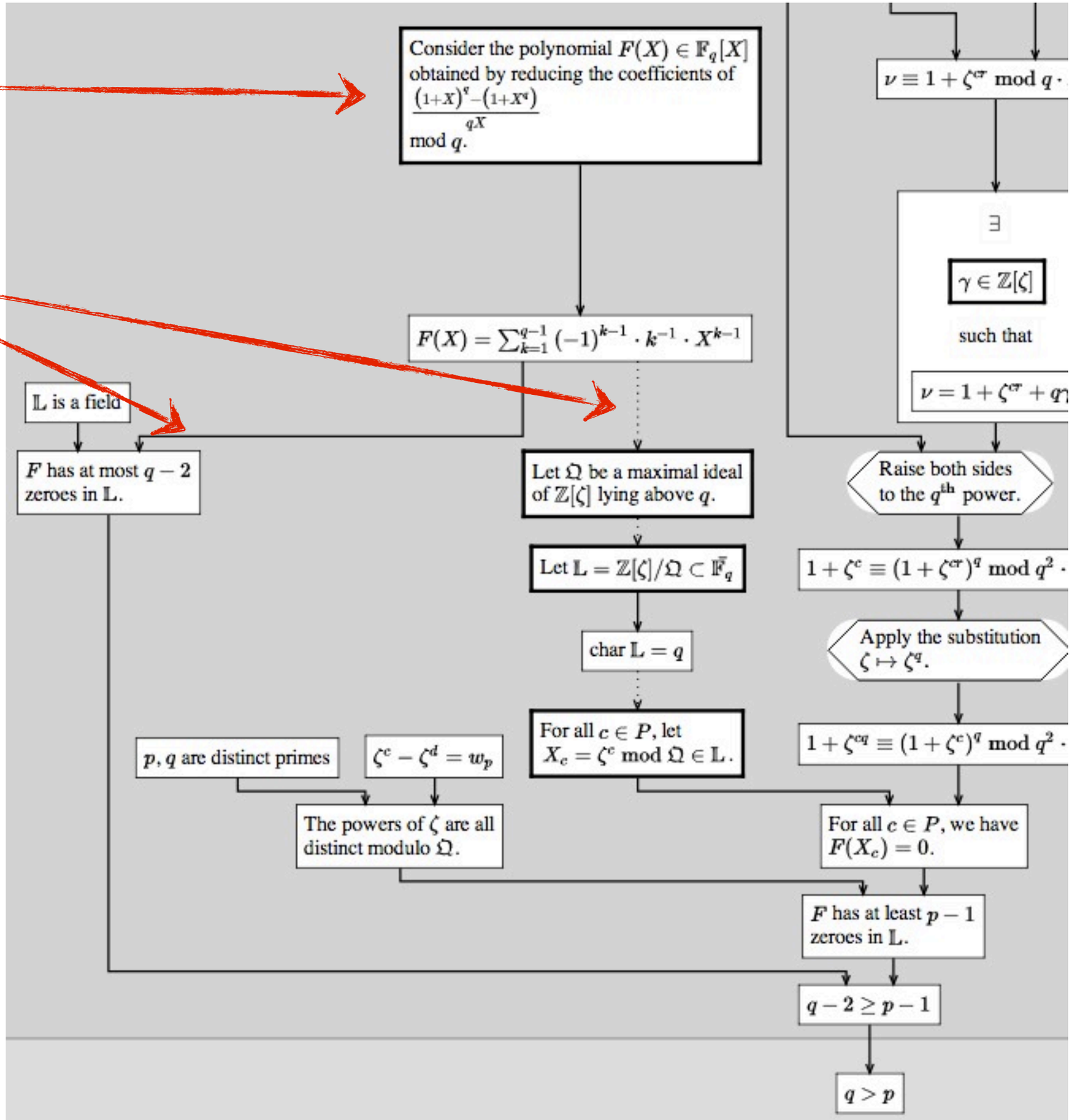

Consider the polynomial $F(X) \in \mathbb{F}_q[X]$ obtained by reducing the coefficients of $\frac{(1+X)^q-(1+X^q)}{qX}$ mod q.
$F(X) = \sum_{k=1}^{q-1} (-1)^{k-1} \cdot k^{-1} \cdot X^{k-1}$
$\mathbb{L}$ is a field
F has at most $q-2$ zeroes in $\mathbb{L}$.
Let Ω be a maximal ideal of $\mathbb{Z}[\zeta]$ lying above q.
Let $\mathbb{L} = \mathbb{Z}[\zeta]/\Omega \subset \bar{\mathbb{F}}_q$
char $\mathbb{L} = q$
For all $c \in P$, let $X_c = \zeta^c \bmod \Omega \in \mathbb{L}$.
p, q are distinct primes
$\zeta^c - \zeta^d = w_p$
The powers of ζ are all distinct modulo Ω.
$\nu \equiv 1 + \zeta^{cr} \bmod q \cdot$
$\exists$
$\gamma \in \mathbb{Z}[\zeta]$
such that
$\nu = 1 + \zeta^{cr} + q\gamma$
Raise both sides to the q^{th} power.
$1 + \zeta^c \equiv (1 + \zeta^{cr})^q \bmod q^2 \cdot$
Apply the substitution $\zeta \mapsto \zeta^q$.
$1 + \zeta^{cq} \equiv (1 + \zeta^c)^q \bmod q^2 \cdot$
For all $c \in P$, we have $F(X_c) = 0$.
F has at least $p-1$ zeroes in $\mathbb{L}$.
$q - 2 \geq p - 1$
$q > p$

An object is introduced.



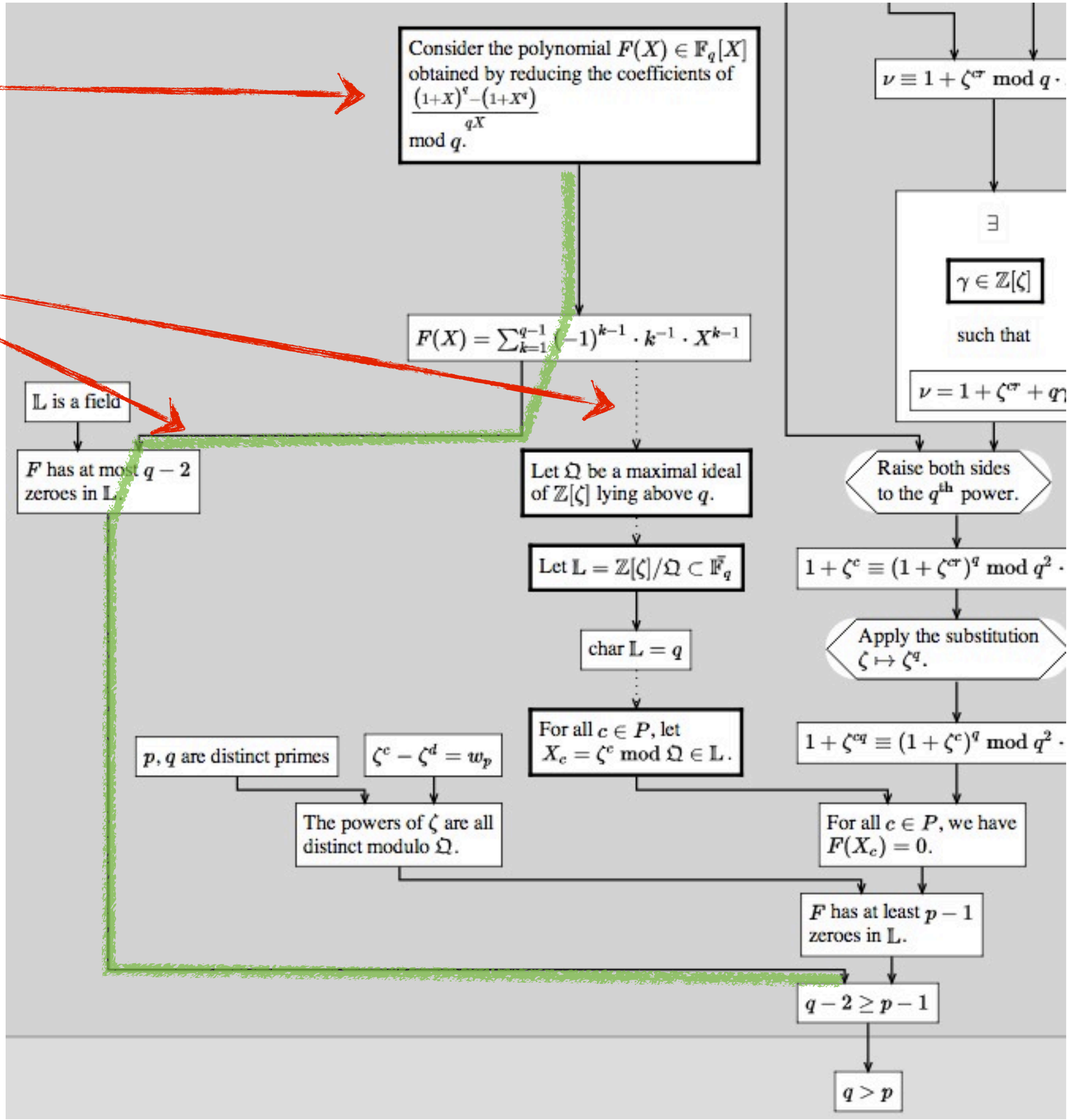
An object is introduced.

Two lines of reasoning branch off from this object



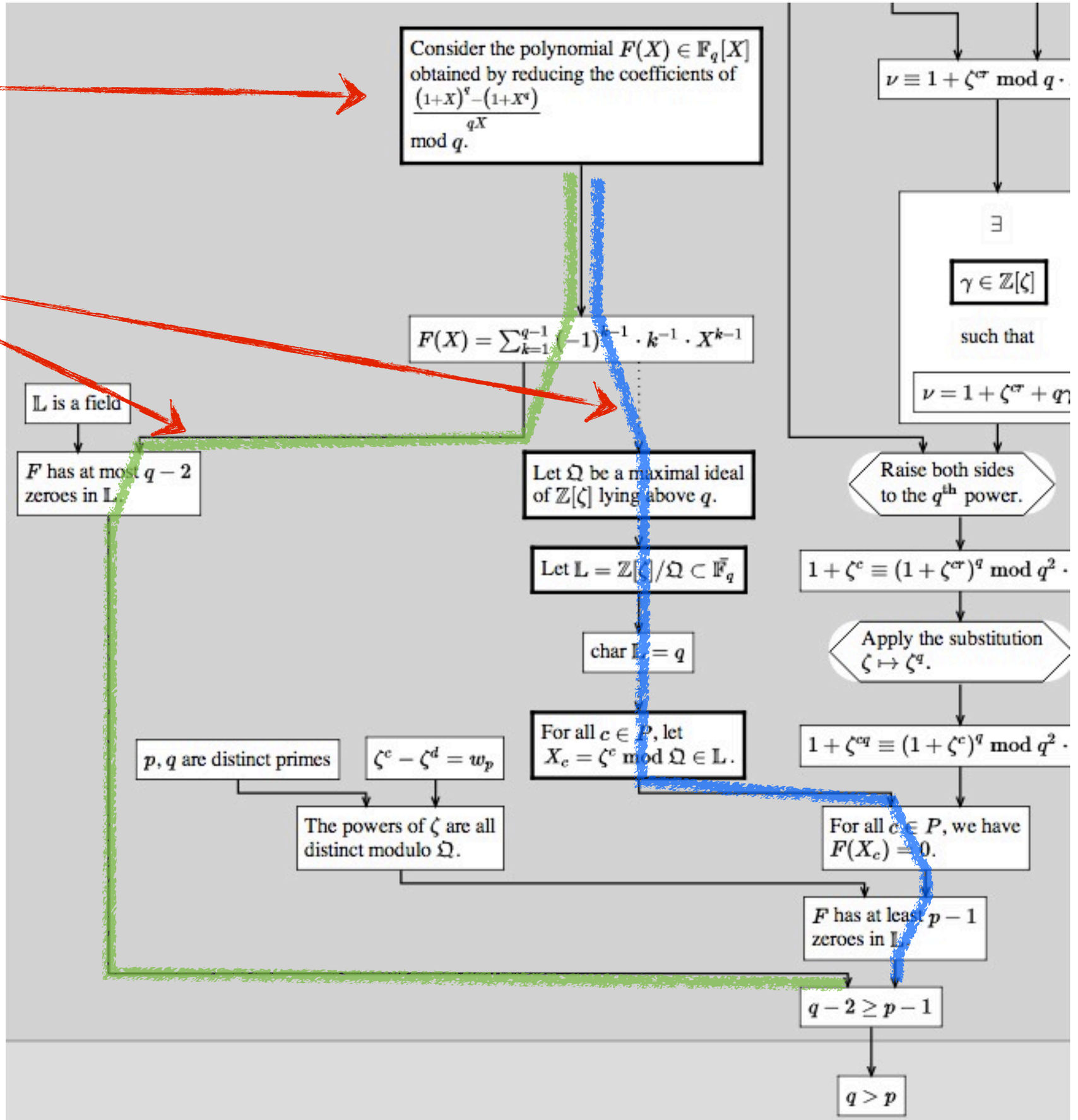
An object is introduced.

Two lines of reasoning branch off from this object



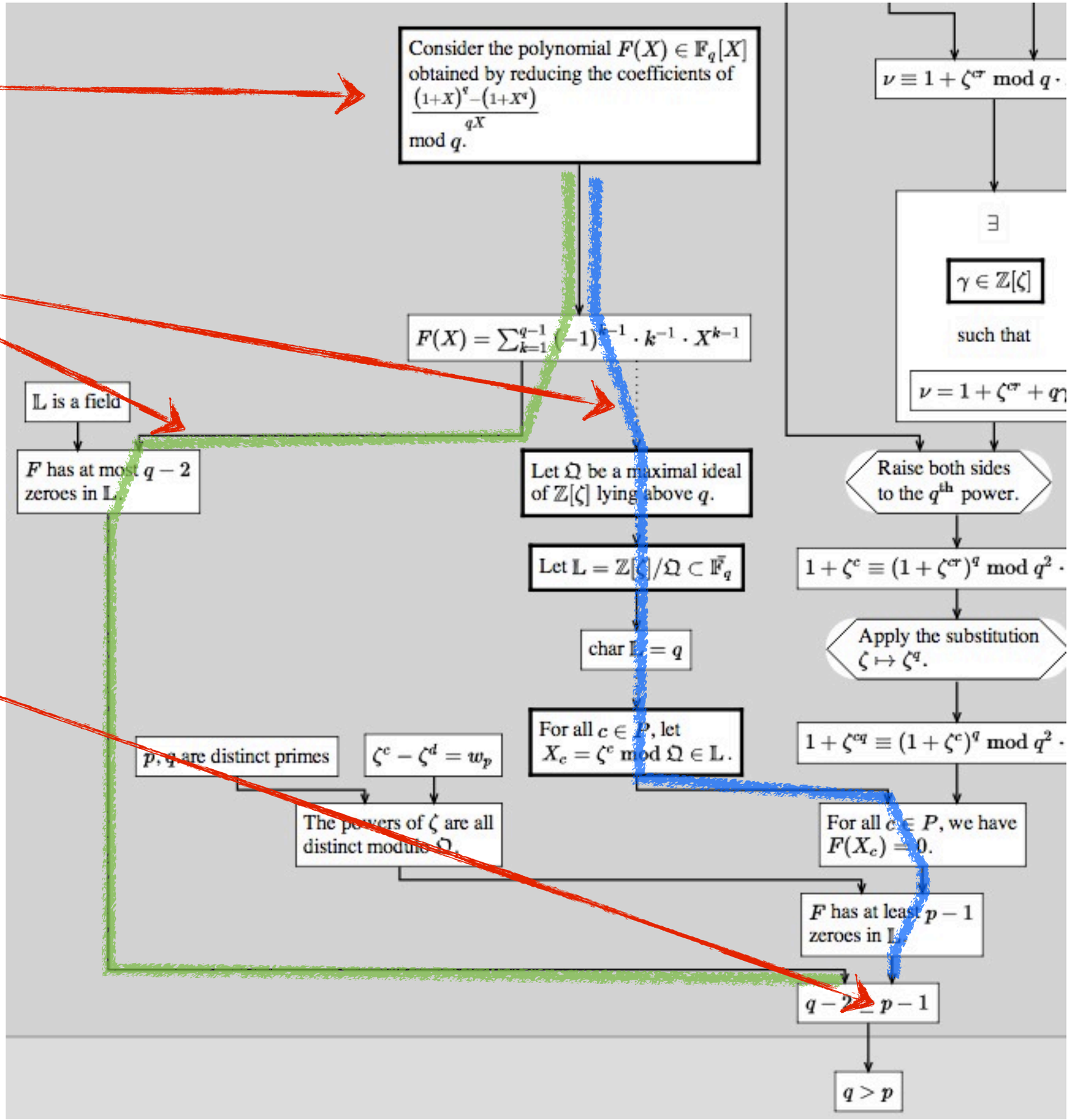
An object is introduced.

Two lines of reasoning branch off from this object



An object is introduced.

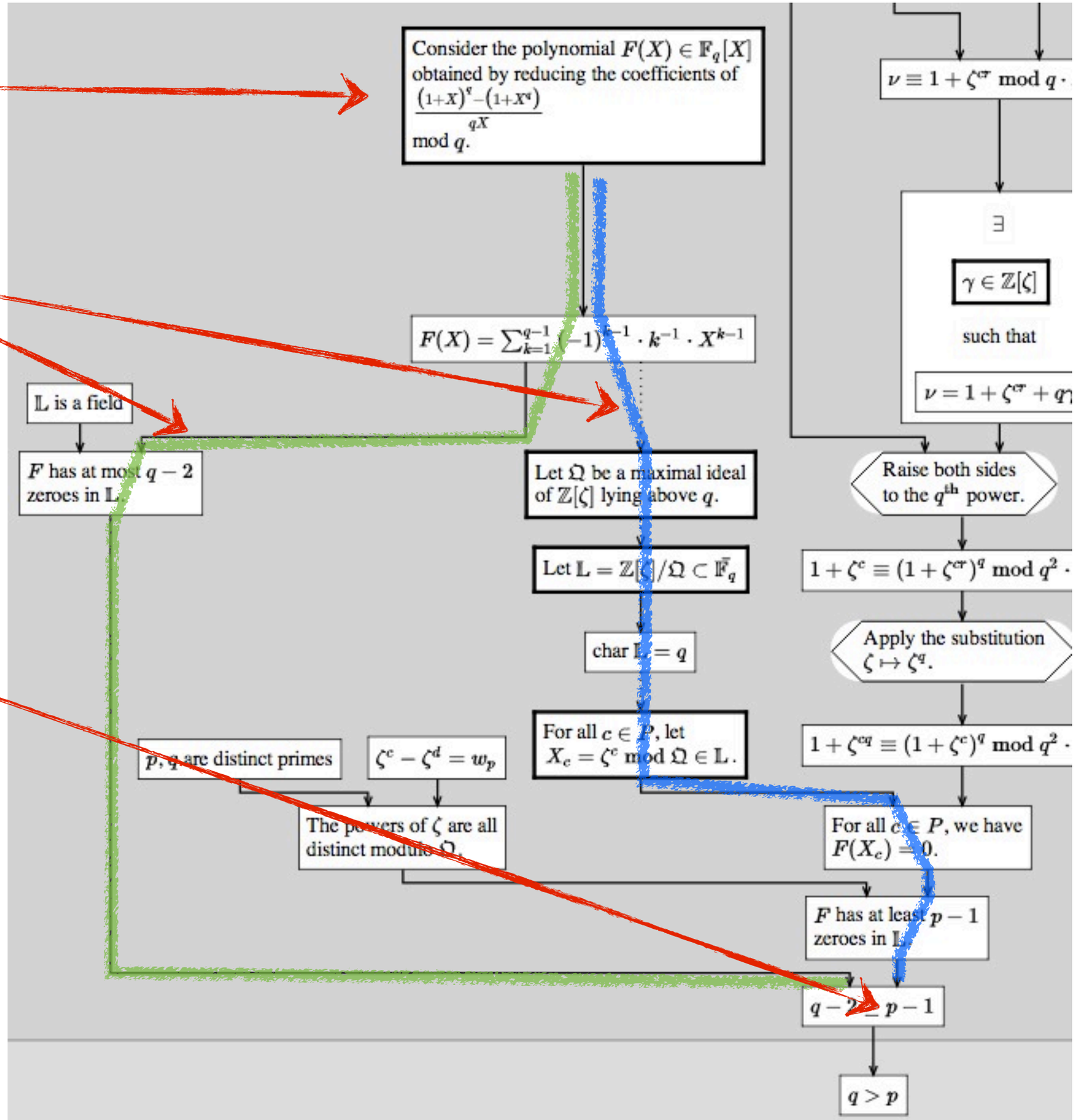
Two lines of reasoning branch off from this object, and reconverge at the end of the proof.



An object is introduced.

Two lines of reasoning branch off from this object, and reconverge at the end of the proof.

This is a clear indication that the object is a pivot.



Conclusions

- Argument maps have great potential to aid in the study of mathematical proofs.
- User studies should be conducted, to test which features work best, and which might need improvement.
- Please visit proofscape.org and send feedback!