LOGIC

HIDDEN IN

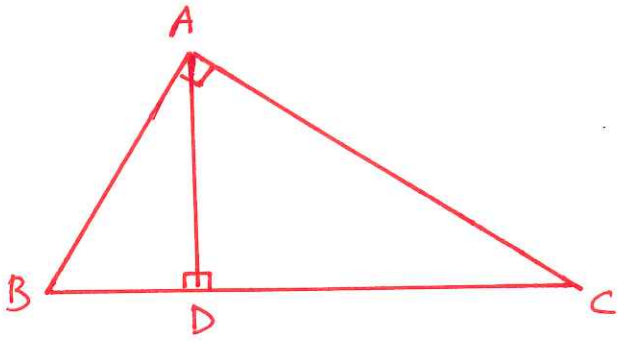
MATHEMATICS

Martin Hyland

GENOVA JULY 2017

PYTHAGORAS' THEOREM

EUCLID ELEMENTS BOOK 6 PROP 31



ABD, CAD and CAB are similar

$\therefore \quad (AB)^2 : (AC)^2 : (BC)^2 = ABD : CAD : CAB$

BUT $\quad ABD + CAD = CAB$

$\therefore \quad (AB)^2 + (AC)^2 = (BC)^2$

EUCLID AS LOGICIAN

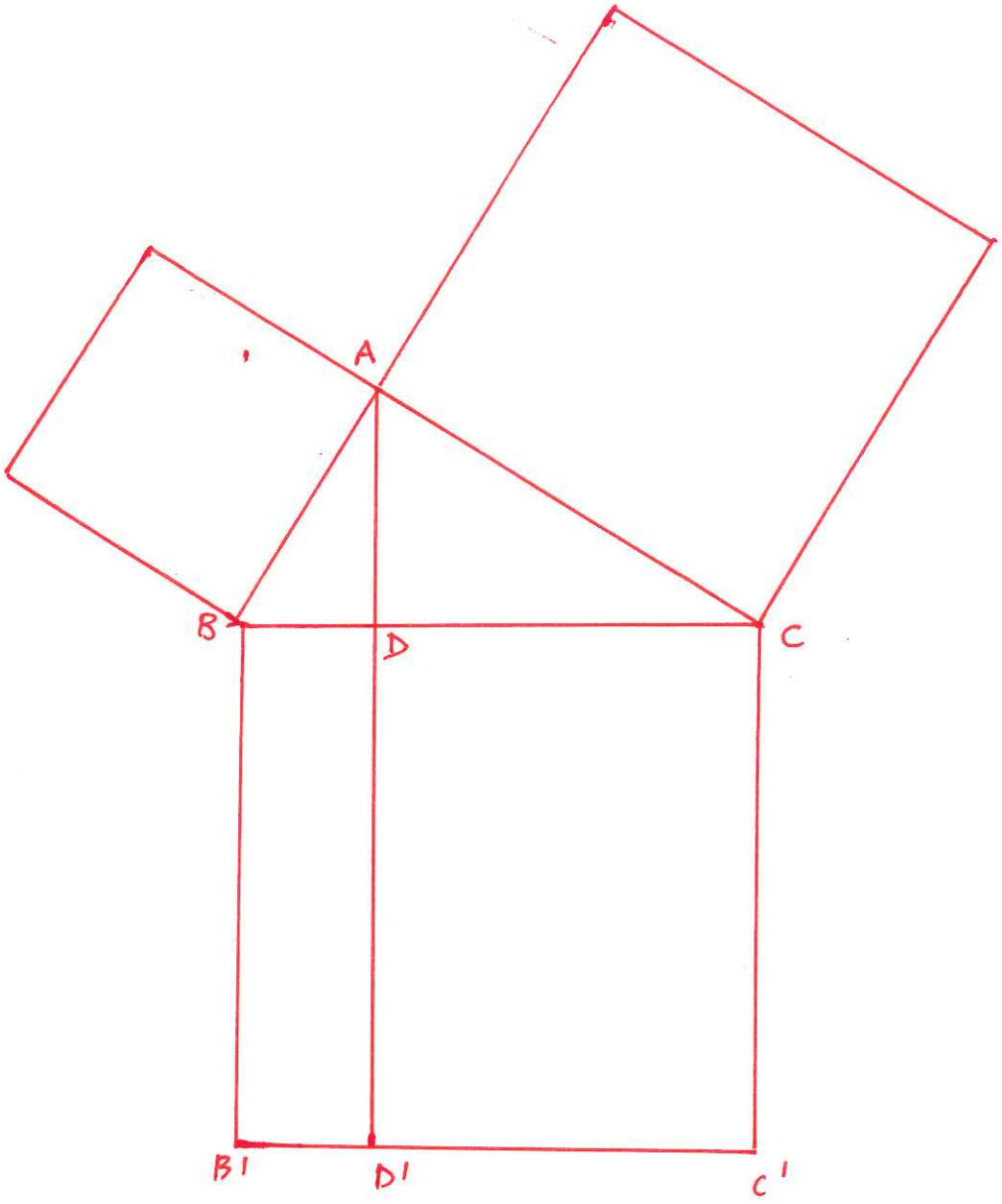
Proof uses the theory of proportion (Book 5)

The theorem is elementary (in particular no mention of proportion in the statement.)

So Is there an elementary proof?

Does the abstract proof offer a clue?

EUCLID'S INSPIRATION



$$(AB)^2 : (AC)^2 = ABD : CAD$$

$$= BD : DC$$

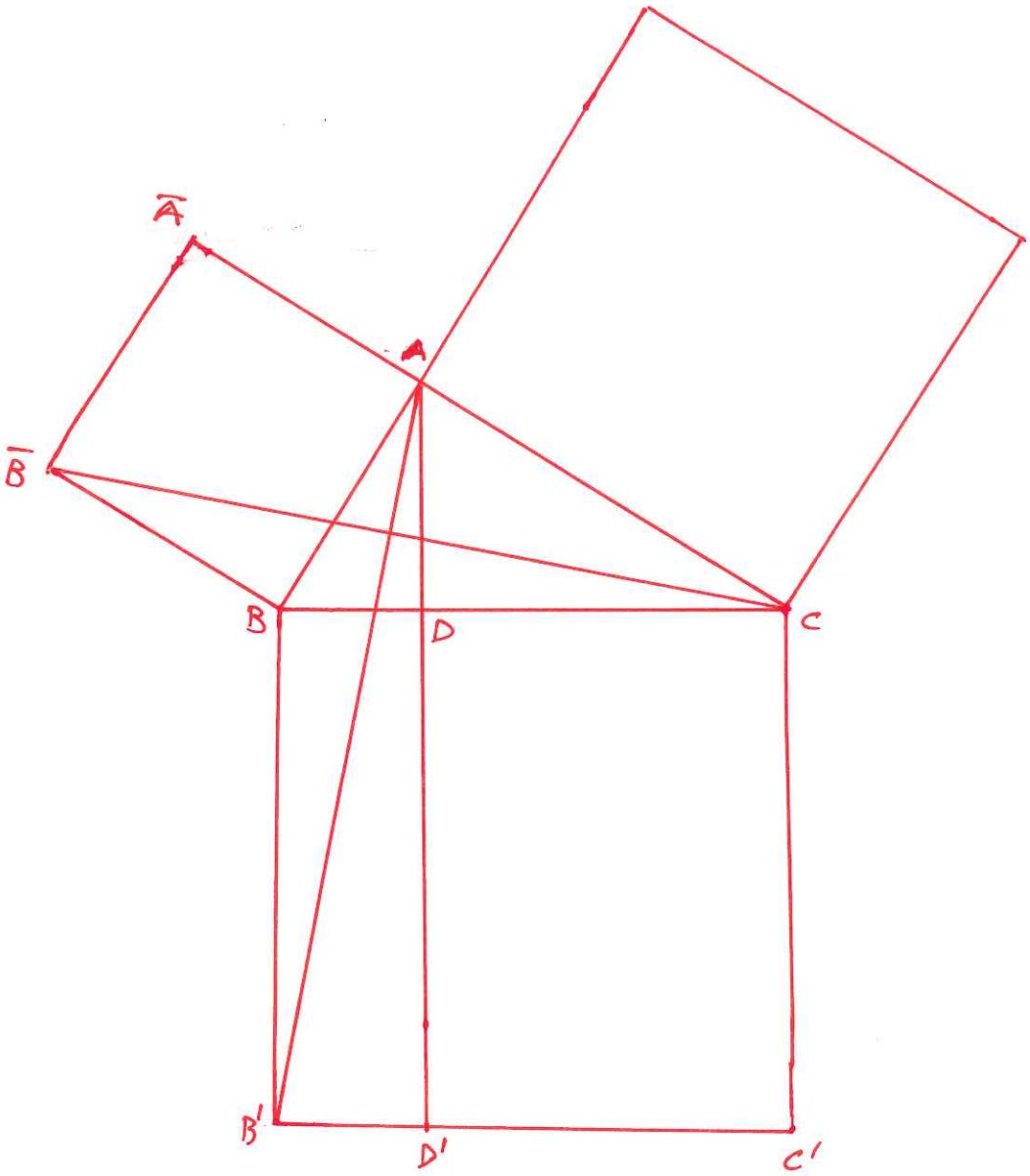
$$= BB'D'D : DD'C'C$$

$\therefore (AB)^2 = BB'D'D$ AND $(AC)^2 = DD'C'C$

Can we prove that?

PYTHAGORAS' THEOREM

EUCLID ELEMENTS BOOK 1 PROP 47



$BC\bar{B}$ and $BB'A$ are congruent

$BC\bar{B} = \frac{1}{2}(AB)^2$ $\quad BB'A = \frac{1}{2} BB'D'D$

$\therefore \quad (AB)^2 = BB'D'D$.

GROUP THEORY

① A group in which all elements $\neq e$ have order 2 is abelian.

$$\text{Groups} + \forall x.\ x^2 = e \quad \models \quad \forall xy \quad xy = yx .$$

② A <u>herd</u> has an associative multiplication plus for all x there is a unique $\bar{x}$ with

$$x\bar{x}x = x .$$

A non-empty herd is a group.

$$\begin{array}{l} \text{Associativity} \\ + \\ \forall x.\ x\bar{x}x = x \\ + \end{array} \quad \models \quad \forall xy \quad x\bar{x} = y\bar{y} .$$

$$\forall xy \quad xyx = x \longrightarrow y = \bar{x}$$

NON-COMMUTATIVE ALGEBRA

(1) Suppose that in a non-commutative ring R, $(1-ab)$ has a right inverse. Then so does $(1-ba)$

$$\text{Rings} + \exists x.\ (1-ab)x = 1 \vdash \exists x.\ (1-ba)x = 1.$$

(2) Suppose that in a non-commutative ring R d has a left inverse $\bar{d}$. Then a matrix

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has a right inverse

if and only if

$(a - b\bar{d}c)$ has a right inverse.

$$\text{Rings} + \bar{d}d = 1$$
$$+ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \vdash \exists X \quad AX = I$$
$$\longleftrightarrow \exists x \ (a - b\bar{d}c)x = 1.$$

WHAT DOES LOGIC SAY?

Group Theory examples involve algebraic or essentially algebraic theories.

There are enough free models (and the Completeness Theorem is trivial).

Non-commutative algebra examples involve regular theories (i.e. simple existence statements).

Completeness and nature of proofs still simple.

EQUATIONAL REASONING

Given generators $X = \{x_1, \ldots, x_n\}$ and equations $E(\underline{x})$ in them, there is a free model $F(X; E)$ determined by equational reasoning.

SOUNDNESS Anything deduced by equational reasoning is true.

Whenever we have $m_1, \ldots, m_n \in M$ with $M \models E(\underline{m})$, there is a unique algebra homomorphism

$$F(X, E) \longrightarrow M \;;\; x_i \longmapsto m_i.$$

COMPLETENESS If $s(\underline{x}) = t(\underline{x})$ holds whenever $E(\underline{x})$ holds then $s = t$ holds in $F(X; E)$ and hence can be derived by equational reasoning from the equations $\underline{E}$

EXAMPLE 1

Assume Groups + $x^2 = e$

Deduce $(xy)(xy) = e$

$$(yx)(xy) = y(xx)y = yey = y^2 = e$$

so by cancellation

$$xy = yx$$

Here

$F(x, y \mid t^2 = e)$ is the

4-group

$$\{e, x, y, xy\} \cong C_2 \times C_2$$

EXAMPLE 2

Assume Associative law

$$x\bar{x}x = x$$

$$xyx = x \longrightarrow y = \bar{x}$$

(This is an essentially algebraic theory.)

Deduce

$$x\bar{x}x\bar{x}x = x\bar{x}x = x$$

so by uniqueness $\bar{x}x\bar{x} = \bar{x}$

so by uniqueness $\bar{\bar{x}} = x$

Now consider $y\,\bar{x}\bar{y}\,x$

$$y\,\bar{x}\bar{y}\,x\,\bar{x}x\,y\bar{x}\bar{y}\,x = y\,\bar{x}\bar{y}\,xy\,\bar{x}\bar{y}\,x = y\,\bar{x}\bar{y}\,x$$

$$y\,\bar{x}\bar{y}\,x\;y\bar{y}\;y\,\bar{x}\bar{y}\,x = y\,\bar{x}\bar{y}\,xy\,\bar{x}\bar{y}\,x = y\,\bar{x}\bar{y}\,x$$

so by uniqueness

$$\bar{x}x = y\bar{y}$$

so using $\bar{\bar{x}} = x$

$$x\bar{x} = y\bar{y}$$

NON-COMMUTATIVE EXAMPLE 1

In a non-commutative ring

$$\exists x.\ (1-ab)x = 1 \vdash \exists y.\ (1-ba)y = 1$$

Suppose

$$(1-ab)x = 1$$

Then

$$\begin{aligned}(1-ba)(1+bxa) &= 1-ba+bxa-babxa \\ &= 1-b(1-x+abx) \\ &= 1-b(1-(1-ab)x) \\ &= 1-b(1-1) = 1\end{aligned}$$

NON-COMMUTATIVE EXAMPLE 2

Given $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in a non-commutative ring.

Suppose d has a left inverse

$$d^{-1}.d = 1$$

Then $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has a right inverse

if and only if

$(a - bd^{-1}c)$ has a right inverse u say.

Consider $\begin{pmatrix} u & -ubd^{-1} \\ -d^{-1}cu & d^{-1} - d^{-1}cubd^{-1} \end{pmatrix}$.

LINEAR ALGEBRA

Suppose $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} u & v \\ x & y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

that is $au + bx = 1 \quad av + by = 0$

$cu + dx = 0 \quad cv + dy = 1$.

Does it follow that

$$\begin{pmatrix} u & v \\ x & y \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

that is $au + cv = 1 \quad ax + cy = 0$

$bu + dv = 0 \quad bx + dy = 1$.

Try it!

More generally does $AB = I$

imply $BA = I$

for any commutative ring of coefficients?

First Attempt

(Integral Domains)

Any integral domain R embeds $R \hookrightarrow F$ in its field of fractions F.

An embedding preserves and reflects equalities. Hence

$$AB = I \implies BA = I \quad \text{for } F$$

implies

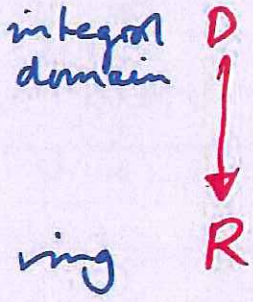
$$AB = I \implies BA = I \quad \text{for } R$$

An arbitrary commutative ring is a quotient of an integral domain.

Why does the above argument not extend?

Logic Question

Suppose we know ϕ holds in all fields: when do we know ϕ (or something like it) holds in all commutative rings?



means it's OK for equations

Hilbert's Nullstellensatz says

If $\forall_i f_i = 0 \to g = 0$ holds in all fields,

then for some r,

$\forall_i f_i = 0 \to g^r = 0$ holds in all commutative rings.

SECOND ATTEMPT

(MULTILINEAR ALGEBRA)

Consider the determinant $\det A$ and adjugate matrix $\operatorname{adj} A$. These satisfy the algebraic identities

$$\det AB = \det A \det B$$

$$A.\operatorname{adj} A = \det A . I = \operatorname{adj} A . A .$$

WHY? They hold in fields (basic linear algebra)

so in integral domains (reflection)

so in commutative rings (preservation)

Now assume $AB = I$ in a commutative ring.

Then $$\det A \det B = \det I = 1$$

Also $$\operatorname{adj} A = (\operatorname{adj} A) A B = (\det A) B$$

So $$\det B \operatorname{adj} A = (\det B)(\det A) B = B$$

So $$BA = \det B \operatorname{adj} A A = \det B \det A I = I .$$

TESTING FOR ZERO

Let R be an integral domain.

- By the Remainder Theorem

  $f(x) \in R[x]$ has $\leq \deg f$ roots

- Hence

  if $f(x) \in R[x]$ has $f(a) = 0$ for ∞ly many a then $f(x) \equiv 0$.

- Hence inductively

  if $f(\underline{x}) \in R[\underline{x}] = R[x_1, \ldots, x_n]$ has ∞ sets $A_1, \ldots, A_n$ with $f(\underline{a}) = 0$ for $a_i \in A_i$

  then $f(\underline{x}) \equiv 0$.

Irrelevance of Algebraic Inequalities

Suppose R is an infinite integral domain and

$f(\underline{x}), g_1(\underline{x}), \ldots g_r(\underline{x}) \in R[\underline{x}]$ $g_i(x) \not\equiv 0$

such that $f(\underline{a}) = 0$ whenever

$g_1(\underline{a}), \ldots, g_r(\underline{a}) \neq 0$;

then $f(x) \equiv 0$.

Proof:- Consider $h(\underline{x}) = f(\underline{x}) \prod g_i(\underline{x})$.

$h(\underline{a}) = 0$ all $\underline{a}$ and so $h(\underline{x}) \equiv 0$.

But $g_i(\underline{x}) \not\equiv 0$ in the integral domain $R[\underline{x}]$. Hence

$f(\underline{x}) \equiv 0$.

APPLICATION

For square matrices A and B,

the characteristic polynomial of AB

equals that of BA.

WHY? This is a collection of algebraic identities in the free ring

$$\mathbb{Z}[a_{ij}, b_{ij}]$$

First we prove them subject to the inequality $\det A \neq 0$: we embed in the field of fractions and have

$$\begin{aligned} \det(AB - tI) &= \det A \det(B - tA^{-1}) \\ &= \det(B - tA^{-1}) \det A \\ &= \det(BA - tI). \end{aligned}$$

Then

$$\det(AB - tI) = \det(BA - tI)$$

reflects back into free ring.

But the inequality is irrelevant so

$$\det(AB - tI) = \det(BA - tI)$$

holds outright.

Local Rings

A commutative ring R is a local ring just when it has a unique maximal ideal m. Then R/m is the unique quotient field.

Example Take $p \in M$ a point of a manifold (space). Then the ring of germs of functions at p is local with quotient $\mathbb{R}$.

Local rings pervade algebraic geometry because of an analogous phenomenon at points of varieties. That corresponds to

Further example If p is a prime ideal in a commutative ring R then the localisation R_p is a local ring.

ELEMENTARY NOTION OF LOCAL RING

Suppose R local with maximal ideal m.

- Certainly R is non-trivial $(0 \neq 1)$
- Also if $a \notin m$, $\langle a \rangle \not\subseteq m$ so $\langle a \rangle = R$; so a is invertible.

Since we cannot have both $a, (1-a) \in m$ one of them must be invertible.

THUS

$$\vdash \exists x\ ax = 1 \vee \exists y\ (1-a)y = 1$$

$$0 = 1 \vdash \bot$$

Conversely if ▭ holds then the non-invertible elements form a unique maximal ideal in a ring R.

So ▭ is an elementary and in fact coherent notion of local ring

SOME COMMUTATIVE ALGEBRA

Let R be a local ring. Then any finitely generated projective module over R is free.

Concretely: suppose E is a square matrix over R with $E^2 = E$; then there is an invertible matrix P with

$$P^{-1} E P = \left(\begin{array}{c|c} I & 0 \\ \hline 0 & 0 \end{array}\right).$$

Moreover that is provable in coherent logic from the coherent axioms for local rings.

Hence that holds for local rings in sheaf toposes.

SOME GENERAL TOPOLOGY

Let X be a compact Hausdorff space

$Sh(X)$ the category of sheaves on X

$\mathbb{R}_X$ the sheaf of sections of $\mathbb{R} \times X \longrightarrow X$

$C(X)$ the algebra of continuous $\mathbb{R}$-valued functions on X

[$C(X)$ is the global sections of $\mathbb{R}_X$]

There is an equivalence of categories

Finitely generated projective modules / $C(X)$

$\simeq$ Finitely generated projective modules in $Sh(X)$.

CATEGORICAL LOGIC

AN APPLICATION

- $\mathbb{R}_X$ is a local ring in $Sh(X)$
- $Sh(X) \models$ finitely generated projective $\mathbb{R}_X$-modules are free.
- Existence is local in the logic of $Sh(X)$
- So (locally) free $\mathbb{R}_X$-modules are $\mathbb{R}$-vector bundles
- So

THEOREM (Swan) There is an equivalence of categories

Finitely generated $C(X)$-modules

$\simeq$ Vector bundles $/X$