Algebra and Logic

Martin Hyland

Modern algebra and logic emerged at about the same time and were met with equal suspicion by many mathematicians. Hilbert, himself responsible for new forms of mathematical argument, later proposed to justify abstract mathematics in logical terms. This is known as the Hilbert programme - to establish the consistency of higher order mathematics in finitary terms. Gödel's celebrated Incompleteness Theorem shows that this idea cannot succeed generally; but there is a profound intuition behind it. Results in logic show that in many instances abstract ideas can be eliminated in favour of concrete ones. This has an interesting manifestation in the case of abstract algebra.

From a modern perspective, the concrete aspects of abstract algebra can be explained via the notion of classifying topos which arose in categorical logic. Typically the concrete algebraic manipulations reflect elementary properties of a classifying topos which can be presented in a completely explicit fashion. Then the seemingly problematic modern abstract formulation reflects a use of some form of the axiom of choice to establish the existence of enough points of the classifying topos, that is, enough models of the theory classified.

The basic ideas are best understood in terms of properties of very simple logical theories, which are easily appreciated. This talk will use these to explain arguments in abstract algebra with hidden computational content. It will be illustrated by leading examples derived from familiar Linear Algebra and elementary Commutative Algebra. Just at the end there will be a brief outline of the perspective of categorical logic.

ALGEBRA AND LOGIC

Hilbert: Concrete truths should have concrete proofs.

Not correct : Gödel

Question When are higher level concepts – necessary – just useful?

What can we tell in advance about how to prove something?

When we prove something what more do we know?

BACKGROUND CONTEXT

The Prime Number Theorem

$$\pi(x) \sim \frac{x}{\log x}$$

First proved by complex analysis.

Later an 'elementary' proof found.

LOGIC (= Cut Elimination for Analysis with Arithmetic Comprehension)

implies

Analysis proof $\Rightarrow$ Elementary proof

(Not necessarily interesting)

EXAMPLES
(Elementary Group Theory)

(i) A group in which all elements $\neq e$ have order 2 is abelian

$$\begin{array}{c} \text{Groups} \\ + \\ x^2 = e \end{array} \models \quad xy = yx$$

(ii) A non-empty herd is a group

associative multiplication plus
for all x there is unique $\bar{x}$
$$x \bar{x} x = x$$

$$\begin{array}{l} \text{Associativity} \\ + \\ x\bar{x}x = x \\ + \\ xyx = x \to y = \bar{x} \end{array} \models \quad x\bar{x} = y\bar{y}$$

EXAMPLE

(Related to Computer Science)

A Conway Rig has

$0\ ,\ +$ commutative monoid

$1\ ,\ \cdot$ monoid

Distributive laws

Operation $(\ )^*$ with

$$(ab)^* = 1 + a(ba)^* b$$

$$(a+b)^* = (a^* b)^* a^*$$

In a Conway Rig we have

$$1^{**} = 1^{***}$$

More generally $a^{***} = a^{****}$

EXAMPLES
on Matrices

(i) If $AB = I$ then $BA = I$.

(ii) If $(I - AB)$ invertible then $(I - BA)$ is invertible.

(iii) Suppose D is invertible.

Then

$$\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$$

is invertible

if and only if $A - BD^{-1}C$ is invertible.

Which is subtle?

EXAMPLE

From Commutative Algebra

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

Concretely: suppose E is an $n \times n$ matrix over R with

$$E^2 = E$$

Then we can find coordinates with respect to which E has the form
$$\left(\begin{array}{c|c} I & 0 \\ \hline 0 & 0 \end{array}\right).$$

Equational Reasoning

Given generators $X = \{x_1, \ldots x_n\}$ and some equations $E(\underline{x})$ in them there is a free model

$$F(X;E).$$

Whenever we have $m_1, \ldots, m_n \in M$

with $M \models E(\underline{m})$

then there is a unique algebra homomorphism

$$\begin{aligned} F(X;E) &\longrightarrow M \\ x_i &\longmapsto m_i \end{aligned}$$

SOUNDNESS & COMPLETENESS

$F(X;E)$ determined by equational reasoning.

Soundness Anything deduced by equational reasoning is true.

Completeness If $s=t$ holds whenever equations E hold then $s=t$ holds in $F(X;E)$ and hence can be derived by equational reasoning.

EXAMPLE 1

Assume $\quad$ Groups + $x^2 = e$

Deduce $\quad (xy)(xy) = e$

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

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 $y\,\overline{xy}\,x$

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

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

so by uniqueness

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

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

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

EXAMPLE 3

Assume Conway rig

Deduce $1^* = 1 + 1^*$

so $1^{**} = (1^* + 1)^* = 1^{***}1^{**}$

so $1^{***} = 1 + 1^{***}1^{**} = 1 + 1^{**}$

Also $1^{**} = 1 + 1^*1^{**}$

$= 1 + 1^*(1 + 1^*1^{**})$

$= 1 + 1^* + 1^{*2}1^{**}$

$= 1^* + 1^{*2}1^{**}$

$= 1^*(1 + 1^*1^{**})$

$= 1^* 1^{**}$

So $1 + 1^{**} = 1 + 1^*1^{**} = 1^{**}$

Whence $1^{***} = 1 + 1^{**} = 1^{**}$

FAKE MATRIX 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

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

FAKE MATRIX EXAMPLE 2

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

Suppose d has a left inverse

$$d^{-1} \cdot d = 1$$

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

MATRIX EXAMPLE

In 2 dimensions

Assume

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

that is

$$\begin{aligned} au + bx &= 1 \\ av + by &= 0 \\ cu + dx &= 0 \\ cv + dy &= 1 \end{aligned}$$

Deduce

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

that is

$$\begin{aligned} au + cv &= 1 \\ bu + dv &= 0 \\ ax + cy &= 0 \\ bx + dy &= 1 \end{aligned}$$

Not an easy exercise!

MATRIX EXAMPLE

over fields F

We start with

$$F^n \xrightarrow{B} F^n \xrightarrow{A} F^n$$

Now

$AB = I$ implies $\ker B = \{0\}$

so B injective

Also by rank-nullity theorem

$\dim \operatorname{Im} B = n - \dim \ker B = n$

so B surjective

Thus

B is bijective (linear) with inverse A

So (property of maps)

$$BA = I.$$

Matrix Example

over integral domains R

R embeds

$$R \hookrightarrow F$$

in its field of fractions F

An embedding (preserves and) reflects equalities : so

result for R

follows from

result for F

WARNING An arbitrary ring is a quotient of an integral domain ; so above not enough.

MATRIX EXAMPLE

over an arbitrary ring (<u>commutative</u>)

We use the determinant $\det A$ and adjugate matrix $\operatorname{adj} A$: and the

algebraic identities

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

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

(They hold in fields, so in integral domains, so in arbitrary rings.)

Assume $\quad AB = I$

Deduce

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

But $\quad \det A \, \det B = \det I = 1$

So

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

So

$$BA = \det B (\operatorname{adj} A) A = \det B \det A \, I = I.$$

LOGIC QUESTION

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

$$\begin{tikzcd} \text{integral domain } D \arrow[r, hook] \arrow[d] & E \text{ field} \\ \text{ring } R & \end{tikzcd}$$

shows its OK for equations

Hilbert's Nullstellensatz says

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

then for some r,

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

Usual definition

An integral domain R is a valuation ring

if in its field F of fractions

$$x \notin R \Rightarrow x^{-1} \in R$$

Usually argue as follows:

take $I, J \trianglelefteq R$ and suppose

$\exists x \in I \quad x \notin J$: then for $y \neq 0 \in J$

we have $x/y \notin R$ (else $x \in J$)

so $y/x \in R$ so $y \in I$. Thus $J \subseteq I$

This shows ideals are totally ordered

so $\exists$ unique maximal ideal m & m = $\{$non-invertibles$\}$

which R is a local ring.

Elementary char: if $x, y \in R \quad \neq 0$

then x/y, $y/x \in K$ + one must be in R

so either $x|y$ or $y|x$.

Thus R is valuation ring iff

$$0 \neq 1$$

$$ab = 0 \vdash a = 0 \vee b = 0$$

$$\vdash a = 0 \vee b = 0 \vee a|b \vee b|a$$

Take $a \in R \qquad a = 0 \vee (1-a) = 0$ or $a|1-a$

or $1-a|a$

so
- $a = 0 \vdash 1-a = 1$ is invertible
- $(1-a) = 0 \vdash a = 1$ is invertible
- $a|(1-a) \vdash \exists x.\ xa = 1-a \vdash a(1+x) = 1 \vdash a$ invertible
- $(1-a)|a \qquad \vdash (1-a)$ invertible

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 $f(\underline{x}) \in R[\underline{x}] = R[x_1, \dots, x_n]$ has

  ∞ sets $A_1, \dots, A_n$ 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

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

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

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

then $\quad f(x) \equiv 0$.

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

The characteristic polynomial of AB
= the characteristic polynomial of BA

Proof: We show this set of algebraic identities subject to $\det A \neq 0$ in the free ring (integral domain)

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

Embed in the field of fractions and we have

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

LOCAL RINGS

A commutative ring R is a local ring just when it has a unique maximal ideal $\mathfrak{m}$.

Then $R/\mathfrak{m}$ is the unique quotient field.

Example Take $p \in M$ a point in some space. Then the

ring of germs of functions

is a local ring; and the quotient field is $\mathbb{R}$.

[local behaviours of continuous real-valued functions.]

ELEMENTARY NOTION
of local ring

Take R local with maximal ideal $\mathfrak{m}$.

If $a \notin \mathfrak{m}$ then $\langle a \rangle \nsubseteq \mathfrak{m}$ and so

$$\langle a \rangle = R \quad \text{i.e} \quad \exists \bar{a} \quad a\bar{a} = 1$$

Since we can't have both $a, (1-a)$
$\in \mathfrak{m}$,

$$\boxed{\begin{array}{l} \models \exists x.\ ax = 1 \vee \exists y.\ (1-a)y = 1 \\ \quad (\text{and } \ 0 \neq 1) \end{array}}$$

Conversely if $\boxed{\quad\quad}$ holds then the non-invertible elements form the unique maximal ideal.

NOW using $\boxed{\text{coherent logic}}$

EXAMPLE

of use of logic

Theorem (Kaplansky) Let R be a local ring.

Take $E : R^n \longrightarrow R^n$ an $n \times n$ matrix with $E^2 = E$.
Then for some $0 \leq r \leq n$ there is invertible P with

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

From logic (= completeness of coherent logic)
we deduce that for each n
there is a proof in coherent logic of $\boxed{}$.

(Actually an exercise in row/column operations.)

APPLICATION

via Categorical Logic

We deduce:

Kaplansky 'holds in (sheaf) toposes'

Now

By general topology

If X is a compact space then

projective modules over $C(X)$

$\simeq$ projective $\mathbb{R}$-modules in $Sh(X)$

and by internal Kaplansky the latter

$\simeq$ (locally) free $\mathbb{R}$-modules in $Sh(X)$

$=$ Vector bundles over X.

Thus

Theorem (Swan)

Projective $C(X)$ modules $\simeq$ Vector bundles$/X$.

Let A be a local ring $A^n \xrightarrow{P} A^n$ such that $P^2 = P$. Then for some choice of basis for A^n, P has matrix
$$\left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right) \text{ or } \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & I_r \end{array}\right).$$

EITHER p_{11} invertible or $(1-p_{11})$ invertible

In case p_{11} invertible we see that $p^{(1)}, e_2, \dots e_n$ is a basis and w.r.t. it P has matrix
$$\left(\begin{array}{c|c} 1 & \ast\ast\ast \\ \hline 0 & \\ \vdots & Q \\ 0 & \end{array}\right)$$

$Q^2 = Q$ and so by induc hypothesis we can find a good basis of $\langle e_2, \dots e_n\rangle$. Thus we get basis $f_1 = p^{(1)}, f_2, \dots f_n$ w.r.t. which P has matrix
$$\left(\begin{array}{c|c|c} 1 & \ast\ast & \ast\ast \\ \hline & I & 0 \\ 0 & & \\ \hline & 0 & 0 \end{array}\right)$$

Here we have $f_1 \longmapsto f_1$

$2 \le i \le r \quad f_i \longmapsto \lambda_i f_1 + f_i \longmapsto 2\lambda_i f_1 + f_i$

$i > r \quad f_i \longmapsto \lambda_i f_1 \longmapsto \lambda_i f_1$

so it follows that $\lambda_i f_1 = 0$ and so $\lambda_i = 0$ $2 \le i \le r$.

Now replace with basis

$f_1, \dots, f_r, f_{r+1} - \lambda_{r+1} f_1, \dots, f_n - \lambda_n f_1$, and

we have the matrix
$$\left(\begin{array}{c|c|c} 1 & 0 & 0 \\ \hline 0 & I & 0 \\ \hline 0 & 0 & 0 \end{array}\right)$$

In case $(1-p_{11})$ invertible, take any row $(a_1, \ldots a_n)$ of the matrix P and observe that

$$(a_1 \ldots a_n) P = (a_1 \ldots a_n)$$

so in particular

$$a_1 . p_{11} + a_2 p_{21} + \cdots a_n p_{n1} = a_1$$

and so $a_1 = (1-p_{11})^{-1} p_{21} a_2 + \cdots + (1-p_{11})^{-1} p_{n1} a_n$ is a linear combination of $a_2 \ldots a_n$ (independently of how $a_1 \ldots a_n \in \langle \text{rows } P \rangle$ is chosen.

It follows then that the 1st column is a linear combination $p^{(1)} = \sum_2^n \lambda_j p^{(j)}$ $\quad (\lambda_j = (1-p_{11})^{-1} p_{j1})$ of the other columns.

Now $f_1 = e_1 - \sum \lambda_j e_j$, ~~$f_2$~~ $e_2 \ldots$ ~~f_n~~ e_n is a basis and w.r.t. it P has matrix

$$\left(\begin{array}{c|c} 0 & \text{---} \\ \hline 0 & Q \end{array}\right)$$

$Q^2 = Q$ and so by induction hypothesis we can find a good basis for $\langle e_2 \ldots e_n \rangle$. Then we get a basis $f_1 \ldots f_n$ w.r.t. which P has matrix

$$\left(\begin{array}{c|c|c} 0 & \sim & \sim \\ \hline 0 & O & O \\ \hline 0 & O & I \end{array}\right)$$

Then we have $f_1 \longmapsto 0$

$$2 \le i \le k \quad f_i \longmapsto \lambda_i f_1 \longmapsto 0$$

$$i > k \quad f_i \longmapsto \lambda_i f_1 + f_i \longmapsto \lambda_i f_1 + f_i$$

So $\lambda_i f_1 = 0 \quad 2 \le i \le k$ and so $\lambda_i = 0 \quad 2 \le i \le k$

Now replace with basis $f_1 \ldots f_k, f_{k+1} + \lambda_{k+1} f_1, \ldots, f_n + \lambda_n f_1$.
and we have matrix
$$\left(\begin{array}{c|c|c} 0 & 0 & 0 \\ \hline 0 & O & 0 \\ \hline 0 & 0 & I \end{array}\right).$$

ASIDE

$$r : e_k \mapsto e_{2k}$$
$$s : e_k \mapsto e_{2k+1} \qquad \text{in } \mathrm{End}\left(\bigoplus_{\mathbb{N}} \mathbb{Z}\right)$$
$$u : e_{2k} \mapsto e_k \qquad e_{2k+1} \mapsto 0$$
$$v : e_{2k+1} \mapsto e_k \qquad e_{2k} \mapsto 0$$

$$(r\ s)\begin{pmatrix} u \\ v \end{pmatrix} = (ru + sv) = (1) \qquad \begin{pmatrix} u \\ v \end{pmatrix}(r\ s) = \begin{pmatrix} ur & us \\ vr & vs \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Algebra and Logic

Martin Hyland

Modern algebra and logic emerged at about the same time and were met with equal suspicion by many mathematicians. Hilbert, himself responsible for new forms of mathematical argument, later proposed to justify abstract mathematics in logical terms. This is known as the Hilbert programme - to establish the consistency of higher order mathematics in finitary terms. Gödel's celebrated Incompleteness Theorem shows that this idea cannot succeed generally; but there is a profound intuition behind it. Results in logic show that in many instances abstract ideas can be eliminated in favour of concrete ones. This has an interesting manifestation in the case of abstract algebra.

From a modern perspective, the concrete aspects of abstract algebra can be explained via the notion of classifying topos which arose in categorical logic. Typically the concrete algebraic manipulations reflect elementary properties of a classifying topos which can be presented in a completely explicit fashion. Then the seemingly problematic modern abstract formulation reflects a use of some form of the axiom of choice to establish the existence of enough points of the classifying topos, that is, enough models of the theory classified.

The basic ideas are best understood in terms of properties of very simple logical theories, which are easily appreciated. This talk will use these to explain arguments in abstract algebra with hidden computational content. It will be illustrated by leading examples derived from familiar Linear Algebra and elementary Commutative Algebra. Just at the end there will be a brief outline of the perspective of categorical logic.

ALGEBRA AND LOGIC

Hilbert: Concrete truths should have concrete proofs.

Not correct : Gödel

Question When are higher level concepts – necessary
– just useful?

What can we tell in advance about how to prove something?

When we prove something what more do we know?

BACKGROUND CONTEXT

The Prime Number Theorem

$$\pi(x) \sim \frac{x}{\log x}$$

First proved by complex analysis.

Later an 'elementary' proof found.

LOGIC (= Cut Elimination for Analysis with Arithmetic Comprehension)

implies

Analysis proof $\Rightarrow$ Elementary proof

(Not necessarily interesting)

EXAMPLES
(Elementary Group Theory)

(i) A group in which all elements $\neq e$ have order 2 is abelian

$$\begin{array}{c}\text{Groups}\\ + \\ x^2 = e\end{array} \quad \models \quad xy = yx$$

(ii) A non-empty herd is a group

associative multiplication plus
for all x there is unique $\bar{x}$

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

$$\begin{array}{c}\text{Associativity}\\ + \\ x\bar{x}x = x \\ + \\ xyx = x \to y = \bar{x}\end{array} \quad \models \quad x\bar{x} = y\bar{y}$$

EXAMPLE

(Related to Computer Science)

A Conway Rig has

$0\ ,\ +$ commutative monoid

$1\ ,\ \cdot$ monoid

Distributive laws

Operation $(\ )^*$ with

$$(ab)^* = 1 + a(ba)^* b$$

$$(a+b)^* = (a^* b)^* a^*$$

In a Conway Rig we have

$$1^{**} = 1^{***}$$

More generally $a^{***} = a^{****}$

EXAMPLES
on Matrices

(i) If $AB = I$ then $BA = I$.

(ii) If $(I - AB)$ invertible then $(I - BA)$ is invertible.

(iii) Suppose D is invertible.

Then

$$\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$$ is invertible

if and only if
$A - BD^{-1}C$ is invertible.

Which is subtle?

EXAMPLE

From Commutative Algebra

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

Concretely: suppose E is an $n \times n$ matrix over R with

$$E^2 = E$$

Then we can find coordinates with respect to which E has the form $\left(\begin{array}{c|c} I & 0 \\ \hline 0 & 0 \end{array}\right)$.

EQUATIONAL REASONING

Given generators $X = \{x_1, \dots x_n\}$ and some equations $E(\underline{x})$ in them there is a free model

$$F(X; E).$$

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

$$\begin{aligned} F(X;E) &\longrightarrow M \\ x_i &\longmapsto m_i \end{aligned}$$

SOUNDNESS & COMPLETENESS

$F(X;E)$ determined by equational reasoning.

Soundness Anything deduced by equational reasoning is true.

Completeness If $s=t$ holds whenever equations E hold then $s=t$ holds in $F(X;E)$ and hence can be derived by equational reasoning.

EXAMPLE 1

Assume $\quad$ Groups + $x^2 = e$

Deduce $\quad (xy)(xy) = e$

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

so by cancellation

$$xy = yx$$

Here

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

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 $y\,\overline{xy}\,x$

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

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

so by uniqueness

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

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

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

EXAMPLE 3

Assume Conway rig

Deduce $1^* = 1 + 1^*$

so $1^{**} = (1^* + 1)^* = 1^{***} 1^{**}$

so $1^{***} = 1 + 1^{***} 1^{**} = 1 + 1^{**}$

Also $1^{**} = 1 + 1^* 1^{**}$

$= 1 + 1^*(1 + 1^* 1^{**})$

$= 1 + 1^* + 1^{*2} 1^{**}$

$= 1^* + 1^{*2} 1^{**}$

$= 1^*(1 + 1^* 1^{**})$

$= 1^* 1^{**}$

So $1 + 1^{**} = 1 + 1^* 1^{**} = 1^{**}$

Whence $1^{***} = 1 + 1^{**} = 1^{**}$

FAKE MATRIX 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

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

FAKE MATRIX EXAMPLE 2

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

Suppose d has a left inverse

$$d^{-1} \cdot d = 1$$

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

MATRIX EXAMPLE

in 2 dimensions

Assume

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

that is

$$\begin{aligned} au + bx &= 1 \\ av + by &= 0 \\ cu + dx &= 0 \\ cv + dy &= 1 \end{aligned}$$

Deduce

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

that is

$$\begin{aligned} au + cv &= 1 \\ bu + dv &= 0 \\ ax + cy &= 0 \\ bx + dy &= 1 \end{aligned}$$

Not an easy exercise!

MATRIX EXAMPLE

over fields F

We start with

$$F^n \xrightarrow{B} F^n \xrightarrow{A} F^n$$

Now

$AB = I$ implies $\ker B = \{0\}$

so B injective

Also by rank-nullity theorem

$\dim \operatorname{Im} B = n - \dim \ker B = n$

so B surjective

Thus

B is bijective (linear) with inverse A

So (property of maps)

$BA = I$.

MATRIX EXAMPLE

over integral domains R

R embeds

$$R \hookrightarrow F$$

in its field of fractions F

An embedding (preserves and) reflects equalities: so

result for R

follows from

result for F

WARNING An arbitrary ring is a quotient of an integral domain; so above not enough.

MATRIX EXAMPLE

over an arbitrary ring (<u>commutative</u>)

We use the determinant $\det A$ and adjugate matrix $\operatorname{adj} A$: and the

algebraic identities

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

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

(They hold in fields, so in integral domains, so in arbitrary rings.)

Assume $AB = I$

Deduce

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

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

So

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

So

$$BA = \det B (\operatorname{adj} A) A = \det B \det A \; I = I.$$

LOGIC QUESTION

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

$$
\begin{tikzcd}
\text{integral domain } D \arrow[r, hook] \arrow[d] & E \text{ field} \\
\text{ring } R &
\end{tikzcd}
$$

shows its OK for equations

Hilbert's Nullstellensatz says

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

then for some r,

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

Usual definition

An integral domain R is a valuation ring if in its field F of fractions

$$x \notin R \Rightarrow x^{-1} \in R$$

Usually argue as follows:

take $I, J \trianglelefteq R$ and suppose

$\exists x \in I \quad x \notin J$: then for $y \neq 0 \in J$

we have $x/y \notin R$ (else $x \in J$)

so $y/x \in R$ so $y \in I$. Thus $J \subseteq I$

This shows ideals are totally ordered so $\exists$ unique maximal ideal m & so R is a local ring.

Elementary char: if $x, y \in R \neq 0$
then x/y, $y/x \in K$ & one must be in R
so either $x|y$ or $y|x$.

Thus R is valuation ring iff

$$0 \neq 1$$

$$ab = 0 \vdash a = 0 \vee b = 0$$

$$\vdash a = 0 \vee b = 0 \vee a|b \vee b|a$$

Take $a \in R$ $\quad a = 0 \vee (1-a) = 0$ or $a | 1-a$ or $1-a | a$

so
- $a = 0 \vdash 1 - a = 1$ is invertible
- $(1-a) = 0 \vdash a = 1$ is invertible
- $a | (1-a) \vdash \exists x.\ xa = 1 - a \vdash a(1+x) = 1 \vdash a$ invertible
- $(1-a) | a \vdash (1-a)$ invertible

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 $f(\underline{x}) \in R[\underline{x}] = R[x_1, \dots, x_n]$ has

  ∞ sets $A_1, \dots, A_n$ 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

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

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

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

then $\quad f(x) \equiv 0$.

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

The characteristic polynomial of AB = the characteristic polynomial of BA

Proof: We show this set of algebraic identities subject to $\det A \neq 0$ in the free ring (integral domain)

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

Embed in the field of fractions and we have

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

LOCAL RINGS

A commutative ring R is a local ring just when it has a unique maximal ideal $\mathfrak{m}$.

Then $R/\mathfrak{m}$ is the unique quotient field.

Example Take $p \in M$ a point in some space. Then the

ring of germs of functions

is a local ring; and the quotient field is $\mathbb{R}$.

[local behaviour of continuous real-valued functions.]

Elementary Notion

of local ring

Take R local with maximal ideal $\mathfrak{m}$.

If $a \notin \mathfrak{m}$ then $\langle a \rangle \nsubseteq \mathfrak{m}$ and so

$$\langle a \rangle = R \text{ i.e } \exists \bar{a} \quad a\bar{a} = 1$$

Since we can't have both $a, (1-a)$ $\in \mathfrak{m}$,

$$\boxed{\begin{array}{l} \models \exists x.\ ax = 1 \vee \exists y.\ (1-a)y = 1 \\ \quad (\text{and} \quad 0 \neq 1) \end{array}}$$

Conversely if $\boxed{}$ holds then the non-invertible elements form the unique maximal ideal.

NOW using $\boxed{\text{coherent logic}}$

EXAMPLE

of use of logic

Theorem (Kaplansky) Let R be a local ring.

Take $E : R^n \longrightarrow R^n$ an $n \times n$ matrix with $E^2 = E$.
Then for some $0 \leq r \leq n$ there is invertible P with

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

From logic (= completeness of coherent logic)
we deduce that for each n
there is a proof in coherent logic
of $\boxed{}$.

(Actually an exercise in row/column operations.)

APPLICATION

via Categorical Logic

We deduce:

Kaplansky 'holds in (sheaf) toposes'

Now

By general topology

If X is a compact space then

projective modules over $C(X)$

$\simeq$ projective $\mathbb{R}$-modules in $Sh(X)$

and by internal Kaplansky the latter

$\simeq$ (locally) free $\mathbb{R}$-modules in $Sh(X)$

$=$ Vector bundles over X.

Thus

Theorem (Swan)

Projective $C(X)$ modules $\simeq$ Vector bundles$/X$.

Let A be a local ring $A^n \xrightarrow{P} A^n$ such that $P^2 = P$. Then for some choice of basis for A^n, P has matrix $\left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$. or $\left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & I_r \end{array}\right)$.

EITHER p_{11} invertible or $(1-p_{11})$ invertible

In case p_{11} invertible we see that $p^{(1)}, e_2, \dots e_n$ is a basis and w.r.t. it P has matrix

$$\left(\begin{array}{c|c} 1 & \sim\sim\sim \\ \hline 0 & \\ \vdots & Q \\ 0 & \end{array}\right)$$

$Q^2 = Q$ and so by induc hypothesis we can find a good basis of $\langle e_2, \dots e_n \rangle$. Thus we get basis $f_1 = p^{(1)}, f_2, \dots f_n$ w.r.t. which P has matrix

$$\left(\begin{array}{c|c|c} 1 & \sim\sim & \sim\sim \\ \hline & I & 0 \\ 0 & & \\ \cline{2-3} & 0 & 0 \end{array}\right)$$

Here we have $f_1 \longmapsto f_1$

$2 \leq i \leq r \quad f_i \longmapsto \lambda_i f_1 + f_i \longmapsto 2\lambda_i f_1 + f_i$

$i > r \quad f_i \longmapsto \lambda_i f_1 \longmapsto \lambda_i f_1$

so it follows that $\lambda_i f_1 = 0$ and so $\lambda_i = 0 \quad 2 \leq i \leq r$.

Now replace with basis

$f_1, \dots, f_r, f_{r+1} - \lambda_{r+1} f_1, \dots \dots f_n - \lambda_n f_1$, and

we have the matrix
$$\left(\begin{array}{c|c|c} 1 & 0 & 0 \\ \hline 0 & I & 0 \\ \hline 0 & 0 & 0 \end{array}\right)$$

In case $(1-p_{11})$ invertible, take any row $(a_1, \dots a_n)$ of the matrix P and observe that

$$(a_1 \dots a_n) P = (a_1 \dots a_n)$$

so in particular

$$a_1 p_{11} + a_2 p_{21} + \dots a_n p_{n1} = a_1$$

and so $a_1 = (1-p_{11})^{-1} p_{21} a_2 + \dots + (1-p_{11})^{-1} p_{n1} a_n$ is a linear combination of $a_2 \dots a_n$ (independently of how $a_1 \dots a_n \in \langle \text{rows } P \rangle$ is chosen.

It follows then that the 1st column is a linear combination $p^{(1)} = \sum_2^n \lambda_j p^{(j)}$ $\quad (\lambda_j = (1-p_{11})^{-1} p_{j1})$ of the other columns.

Now $f_1 = e_1 - \sum \lambda_j e_j$, $e_2 \dots e_n$ is a basis and w.r.t. it P has matrix

$$\left(\begin{array}{c|c} 0 & \text{---} \\ \hline 0 & Q \end{array}\right)$$

$Q^2 = Q$ and so by induction hypothesis we can find a good basis for $\langle e_2 \dots e_n \rangle$. Then we get a basis $f_1 \dots f_n$ w.r.t. which P has matrix

$$\left(\begin{array}{c|c|c} 0 & \sim & \sim \\ \hline 0 & 0 & 0 \\ \hline 0 & 0 & I \end{array}\right)$$

Then we have $f_1 \longmapsto 0$

$$2 \le i \le k \quad f_i \longmapsto \lambda_i f_1 \longmapsto 0$$

$$i > k \quad f_i \longmapsto \lambda_i f_1 + f_i \longmapsto \lambda_i f_1 + f_i$$

So $\lambda_i f_1 = 0 \quad 2 \le i \le k$ and so $\lambda_i = 0 \quad 2 \le i \le k$

Now replace with basis $f_1 \dots f_k, f_{k+1} + \lambda_{k+1} f_1, \dots, f_n + \lambda_n f_1$.

and we have matrix $\left(\begin{array}{c|c|c} 0 & 0 & 0 \\ \hline 0 & 0 & 0 \\ \hline 0 & 0 & I \end{array}\right)$.

ASIDE

$r : e_k \mapsto e_{2k}$

$s : e_k \mapsto e_{2k+1}$ in $\mathrm{End}(\bigoplus_n \mathbb{Z})$

$u : e_{2k} \mapsto e_k \quad e_{2k+1} \mapsto 0$

$v : e_{2k+1} \mapsto e_k \quad e_{2k} \mapsto 0$

$$(r \ s)\begin{pmatrix} u \\ v \end{pmatrix} = (ru + sv) = (1) \qquad \begin{pmatrix} u \\ v \end{pmatrix}(r \ s) = \begin{pmatrix} ur & us \\ vr & vs \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Algebra and Logic

Martin Hyland

Modern algebra and logic emerged at about the same time and were met with equal suspicion by many mathematicians. Hilbert, himself responsible for new forms of mathematical argument, later proposed to justify abstract mathematics in logical terms. This is known as the Hilbert programme - to establish the consistency of higher order mathematics in finitary terms. Gödel's celebrated Incompleteness Theorem shows that this idea cannot succeed generally; but there is a profound intuition behind it. Results in logic show that in many instances abstract ideas can be eliminated in favour of concrete ones. This has an interesting manifestation in the case of abstract algebra.

From a modern perspective, the concrete aspects of abstract algebra can be explained via the notion of classifying topos which arose in categorical logic. Typically the concrete algebraic manipulations reflect elementary properties of a classifying topos which can be presented in a completely explicit fashion. Then the seemingly problematic modern abstract formulation reflects a use of some form of the axiom of choice to establish the existence of enough points of the classifying topos, that is, enough models of the theory classified.

The basic ideas are best understood in terms of properties of very simple logical theories, which are easily appreciated. This talk will use these to explain arguments in abstract algebra with hidden computational content. It will be illustrated by leading examples derived from familiar Linear Algebra and elementary Commutative Algebra. Just at the end there will be a brief outline of the perspective of categorical logic.