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

\[ \pi(x) \approx \frac{x}{\log x} \]

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 ≠ e have order 2 is abelian.

Groups
\[ + \]
\[ x^2 = e \]

(ii) A non-empty herd is a group.

Associative multiplication plus
for all \( x \), there is unique \( x \) \( x \bar{x}x = x \)

Associativity
\[ + \]
\[ x \bar{x}x = x \]
\[ = x \bar{x} = y \bar{y} \]
\[ + \]
\[ xyx = x \rightarrow y = \bar{x} \]
EXAMPLE
(Related to Computer Science)

A Conway Rig has
0, + commutative monoid
1, . monoid

Distributive laws

Operation \((\cdot)^*\) with
\[(ab)^* = 1 + a (ba)^* b\]
\[(a + b)^* = (a \cdot b)^* a^*\]

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

\[
\begin{pmatrix}
A & B \\
C & D
\end{pmatrix}
\]

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:

\[
\begin{pmatrix}
I & 0 \\
0 & 0
\end{pmatrix}
\]
EQUATIONAL REASONING

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

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

$$F(X;E) \rightarrow M$$

$$x_i \mapsto m_i$$
Soundness & Completeness

\[ F(x;E) \text{ determined by equalational reasoning.} \]

**Soundness** Anything deduced by equalational 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 equalational reasoning.
Example 1

Assume \( G \) is a group with \( x^2 = e \).

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:
  \[ x \bar{x} x = x \]
  \[ x \bar{y} x = x \rightarrow y = \bar{x} \]

(This is an essentially algebraic theory.)

Deduce

\[ x \bar{x} x \bar{x} x = x \bar{x} x = x \]

so by uniqueness

\[ \bar{x} \bar{x} = x \]

Now consider

\[ y \bar{x} y \bar{x} y \]

\[ y \bar{x} y \bar{x} y \bar{x} y = y \bar{x} y \bar{x} y \bar{x} y = y \bar{x} y \]

\[ y \bar{x} y \bar{x} y \bar{x} y \bar{x} y = y \bar{x} y \bar{x} y \bar{x} y = y \bar{x} y \]

so by uniqueness

\[ \bar{x} \bar{x} = y \bar{y} \]

so using

\[ \bar{x} = x \]

\[ x \bar{x} = y \bar{y} \]
Example 3

Assume

Conway rig

Deduce

$1^* = 1 + 1^*$

$\therefore \quad 1^* = (1 + 1)^* = 1^{**} 1^{**}$

$\therefore \quad 1^{**} = 1 + 1^{**} 1^{**} = 1 + 1^{**}$

Also

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

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

$\quad = 1 + 1^* + 1^{**} 1^{**}$

$\quad = 1^* + 1^{**} 1^{**}$

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

$\quad = 1^* 1^{**}$

So

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

Whence

$1^{***} = 1 + 1^{**} = 1^{**}$
**Fake Matrix Example 1**

In a non-commutative ring

Ex. \((1-ab)x = 1\) + Ex. \((1-ba)y = 1\)

Suppose

\[(1-ab)x = 1\]

Then

\[(1-ba)(1 + bxa)\]
\[= 1-ba + bxa - babxa\]
\[= 1-b(1-x+abx)\]
\[= 1-b(1-(1-ab)x)\]
\[= 1-b(1-1) = 1\]
FAKE MATRIX EXAMPLE 2

Given \((a, b)\) in a non-commutative ring.

Suppose \(d\) has a left inverse
\[ d^{-1} \cdot d = 1 \]

Then \((a, b)\) has a right inverse
if and only if
\((a - bd^{-1}c)\) has a right inverse \(u\) say.

Consider
\[
\begin{pmatrix}
  u & -ubd^{-1} \\
  -d'cu & d' - d'cubd^{-1}
\end{pmatrix}
\]
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
\[
au + bv = 1 \\
au + by = 0 \\
cu + dv = 0 \\
cv + dy = 1
\]

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
\[
au + cv = 1 \\
bv + dv = 0 \\
au + cy = 0 \\
bx + dy = 1
\]

Not an easy exercise!
Matrix Example
over fields \( F \)

We start with
\[
\begin{array}{c}
F^n & B \rightarrow & F^n & A \rightarrow & F^n \\
\end{array}
\]

Now
\[
AB = I \text{ implies } \ker B = \{0\}
\]
so \( B \) injective

Also by rank-nullity theorem
\[
dim \, \text{Im} \, B = n - \dim \ker B = n
\]
so \( B \) surjective

Thus
\( B \) is bijective (linear) with inverse \( A \)

So (property of maps)
\[
BA = I
\]
Matrix Example
over integral domain $R$

$R$ embeds

$\mathbb{R} \to \mathbb{F}$

in its field of fractions $\mathbb{F}$

An embedding (preserves and) reflects equalities: no result for $R$

follows from result for $F$

WARNING: An arbitrary ring is a quotient of an integral domain; no above not enough.
**Matrix Example**

over an arbitrary ring (commutative)

We use the determinant $\det A$ and adjugate matrix $\adj A$; and the algebraic identities

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

($\text{They hold in fields, so in integral domains, so in arbitrary rings}$.)

Assume $AB = I$

Deduce

$$\adj A = (\adj A) \, AB = (\det A) \, B$$

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

So

$$\det B \, \adj A = (\det B) (\det A) B = B$$

So

$$BA = \det B (\adj A) A = \det B \, \det A \, I = I.$$
Logic Question

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

\[
\begin{array}{ccc}
\text{integral domain} & \xrightarrow{D} & \text{field} \\
\text{ring} & \xrightarrow{R} & \text{field} \\
\end{array}
\]

Hilbert's Nullstellensatz says:

If $\forall i: f_i = 0 \rightarrow g = 0$ holds in all fields, then for some $i$,

$\exists f_i = 0 \rightarrow g^r = 0$ holds in all commutative rings.
Usual definition

An integral domain R is a valuation ring if in its field of fractions
\[ x + R = x^{-1} + R \]

Formally, we have as follows:

- Take \( I, J \subset R \) and suppose \( J \neq 0 \).
- For \( y \neq 0 \in J \), we have \( x/y \in R \) (else \( x \in I \)).
- \( y/x \in R \) \( \iff y \in I \). Thus \( J \subset I \).

This means ideals are totally ordered, so \( \exists \) unique maximal ideal \( \mathfrak{m} \) in \( R \).

Elementary char.: if \( x, y \in R \neq 0 \)

- if \( x/y, y/x \in k + \mathfrak{m} \) must be in \( \mathfrak{m} \), so either \( x | y \) or \( y | x \).

Thus \( R \) is valuation ring iff

- \( 0 \neq 1 \)
- \( ab = 0 \iff a = 0 \vee b = 0 \)
- \( -a = 0 \vee b = 0 \vee a/b \in k \)

Take \( a \in R \)

- \( a = 0 \vee (1-a) = 0 \) or \( a | 1-a \)
- \( a = 0 \vee 1-a = 1 \wedge \text{invertible} \)
- \( a = 0 \vee 1-a = 1 \wedge \text{invertible} \)
- \( (1-a) = 0 \vee a = 1 \wedge \text{invertible} \)
- \( a | (1-a) + 3k, xa = 1-a \vee \exists a(x+1) = 1 + a \text{ invertible} \)
- \( (1-a) | x \)
TESTING FOR ZERO

Let \( R \) be an integral domain.

- By the Remainder Theorem
  \[ f(x) \in R[x] \text{ has } \leq \deg f \text{ roots.} \]

- Hence
  \[ f(x) \in R[x] \text{ has } f(a) = 0 \text{ for only many a } \text{ then } f(x) \equiv 0. \]

- Hence inductively
  \[ f(x) \in R[x] = R[x_1, \ldots, x_n] \text{ has } \infty \text{ sets } A_1, \ldots, A_n \text{ with } f(a_i) = 0 \text{ for } a_i \in A_i
  \]
  \[ \text{then} \quad f(x) \equiv 0. \]
IRRELEVANCE OF ALGEBRAIC INEQUALITIES

Suppose $R$ is an infinite integral domain and $f(x), g_1(x), \ldots, g_r(x) \in R[x]$ $g_i(x) \neq 0$ such that $f(a) = 0$ whenever $g_1(a), \ldots, g_r(a) \neq 0$; then $f(x) \equiv 0$.

Proof: Consider $h(x) = f(x) \prod g_i(x)$.

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

But $g_i(x) \not\equiv 0$ in the integral domain $R[x]$. Hence $f(x) \equiv 0$. 
APPLICATION

The characteristic polynomial of $AB$ is the same as 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

$$\det(AB - tI)$$

$$= \det A \det (B - tA^{-1})$$

$$= \det (B - tA^{-1}) \det A$$

$$= \det (BA - tI).$$
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 in some space. Then the ring of germs of functions at $p$ is a local ring; and the quotient field is $R$.

[local behaviors of continuous real-valued functions.]
Elementary Notion
of local ring

Take $R$ local with maximal ideal $M$. If $a \notin M$ then $\langle a \rangle \neq M$ and so $\langle a \rangle = R$ i.e. $\exists a \in R$ such that $a \cdot a = 1$.

Since we can't have both $a, (1-a) \in M$,

$\exists x. a \cdot x = 1$ or $\exists y. (1-a) \cdot y = 1$ (and $0 \neq 1$)

Conversely if $\exists x. a \cdot x = 1$ holds then the non-invertible elements form the unique maximal ideal.

Now using coherent logic
Example of use of logic

Theorem (Kaplansky) Let \( R \) be a local ring.

Take \( E : R^n \to R^n \) an \( n \times n \) matrix with \( E^2 = E \).

Then for some \( 0 \leq r \leq n \) there is invertible \( P \) with

\[
P^{-1}EP = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}
\]

From logic (\( \Rightarrow \) completeness of coherent logic) we deduce that for each \( n \) there is a proof in coherent logic of \( \square \).

(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 $C(X)$
$\cong$ projective $\mathbb{R}$-modules in $\mathcal{S}h(X)$
and by internal Kaplansky the
latter
$\cong$ (locally) free $\mathbb{R}$-modules in $\mathcal{S}h(X)$

$\cong$ Vector bundles over $X$.

Thus
Theorem (Swan)

Projective $C(X)$ modules
$\cong$ Vector bundles/$X$. 
Let \( A \) be a local ring \( A^n \rightarrow A^n \) such that \( P = P^2 \). Then for some change of basis for \( A^n \), \( P \) has matrix \( \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \) and \( \begin{pmatrix} 0 & 0 \\ 0 & I_r \end{pmatrix} \).

Either \( p_{ii} \) invertible or \( 1 - p_{ii} \) invertible.

In case \( p_{ii} \) invertible we see that \( p^{(1)}, e_2, \ldots, e_n \) is a basis and w.r.t. \( \frac{\partial}{\partial P} \) \( P \) has matrix

\[
\begin{pmatrix}
1 & \cdots & 0 \\
0 & \ddots & \vdots \\
0 & \cdots & 1
\end{pmatrix}
\]

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

\[
\begin{pmatrix}
1 & \cdots & 0 \\
0 & I & 0 \\
0 & 0 & 0
\end{pmatrix}
\]

Here we have \( f_i \rightarrow f_i \)

\( 2 \leq i \leq r \)

\( f_i \rightarrow \lambda_i f_i + f_i \)

\( i > r \)

\( f_i \rightarrow \lambda_i f_i \)

so it follows that \( \lambda_i f_i = 0 \) and so \( \lambda_i = 0 \) \( 2 \leq i \leq r \).

Now replace with basis

\( f_1, \ldots, f_1, f_{n+1} - \lambda_i f_i, \ldots, f_n - \lambda_i f_i, \)

and we have the matrix

\[
\begin{pmatrix}
1 & 0 & 0 \\
0 & I & 0 \\
0 & 0 & 0
\end{pmatrix}
\]
In case $(1 - p_{11})$ is not 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

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

Let $a_1 = (1 - p_{11})^{-1} p_{11} a_1 + \cdots + (1 - p_{11})^{-1} p_{n1} a_n$

is a linear combination of $a_1, \ldots, a_n$ (independently of how $a_1, \ldots, a_n \in \{ \text{rows of } P \}$ is chosen.

It follows that the left column is a linear combination

$$p_{11} = \frac{\sum a_j p_{1j}}{2} \quad (\lambda_{ij} = (1 - p_{11})^{-1} p_{ij})$$

of the other columns.

Now let $f_1 = e_1 - \sum a_j e_j$, for $i = 2, \ldots, n$ and write it

$P$ has matrix

$$\begin{pmatrix}
\lambda_{11} & 0 \\
0 & Q
\end{pmatrix}$$

$Q^{2k_{ij}} = 0$ and so by induction hypothesis we can find a good basis for $(e_2 \ldots e_n)$. Then we get a basis

$f_1 \ldots f_n$ for which $P$ has matrix

$$\begin{pmatrix}
\text{diag}(m, m) & 0 \\
0 & 0 & 0 & \text{I}
\end{pmatrix}$$

Then we have $f_i \rightarrow 0$

$2 < i \leq k$ $f_i \rightarrow \lambda_i f_i \rightarrow 0$

$i > k$ $f_i \rightarrow \lambda_i f_i + f_i \rightarrow \lambda_i f_i + f_i$

So $\lambda_i f_i = 0$ $2 < i \leq k$ and so $\lambda_i = 0$ $2 < i \leq k$

Now replace with basis $f_1 \ldots f_n$, then $+ \lambda_1 f_1 \ldots \lambda_n f_n$, and we have matrix

$$\begin{pmatrix}
\lambda_{11} & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0
\end{pmatrix} .$$
\[ \begin{align*}
\text{ASIDE} \\
r &: \mathbb{Z} \to \mathbb{Z} \\
s &: \mathbb{Z} \to \mathbb{Z} \\
u &: \mathbb{Z} \to \mathbb{Z} \\
v &: \mathbb{Z} \to \mathbb{Z} \\
&\text{in } \text{End}(\mathbb{Z}^2) \\
(r \cdot s)(u) &= (ru + sv) = (1) \\
(u)(r \cdot s) &= (uvus) = (1 \ 0) \\
&\text{or } (v \ 0) \\
&\left( \begin{array}{cc}
ru & sv \\
v & u
\end{array} \right) = (1 \ 0)
\end{align*} \]
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 ≠ e have order 2 is abelian

\[
\begin{align*}
\text{Groups} & \\
+ & = xy = yx \\
x^2 & = e
\end{align*}
\]

(ii) A non-empty herd is a group

associative multiplication plus
for all x, there is unique \( \bar{x} \)

\[
x \bar{x} x = x
\]

Associativity

\[
\begin{align*}
+ & \\
x \bar{x} x & = x \\
\bar{x} & = y \bar{y} \\
x \bar{x} \bar{x} & = x \\
y & = \bar{x}
\end{align*}
\]
EXAMPLE
(Related to Computer Science)

A Conway Rig has
0, +  commutative monoid
1, .  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 $(I-AB)$ is invertible then $(I-BA)$ is invertible.

(iii) Suppose $D$ is invertible.

Then

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

is invertible

if and only if

$A-BC^{-1}D$ 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

$$\begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}.$$
EQUATIONAL REASONING

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

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

$$F(X; E) \longrightarrow M$$

$$x_i \longrightarrow m_i$$
Soundness & Completeness

\[ F(x;E) \text{ determined by equational reasoning.} \]

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 \( G \) is a group and \( x^2 = e \).

Deduce

\[
(xy)(xy) = e
\]

\[
(yx)(xy) = y(xyx) = yey = y^2 = e
\]

So by cancellation

\[ xy = yx \]

Here

\[ F(x,y | t^2 = e) \] is the 4-group

\[ \{ e, x, y, xy \} \cong C_2 \times C_2 \]
Example 2

Assume

Associate law

$x \overline{x} x = x$

$x y x = x \rightarrow y = \overline{x}$

(This is an essentially algebraic theory.)

Deduce

$x \overline{x} x \overline{x} x = x \overline{x} x = x$

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

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

Now consider $y \overline{x} y x$

$y \overline{x} y x \overline{x} y x = y \overline{x} y x \overline{x} y x = y \overline{x} y x$

$y \overline{x} y y x \overline{x} y x = y \overline{x} y x \overline{x} y x = y \overline{x} y x$

so by uniqueness

$\overline{x} x = y \overline{y}$

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

$x \overline{x} = y \overline{y}$
Example 3

Assume Conway rig

Deduce

\[ 1^* = 1 + 1^* \]

\[ 1^{**} = (1^*1^*)^* = 1^{***}1^{*2} \]

\[ 1^{***} = 1 + 1^{****}1^{*2} = 1 + 1^{*2} \]

Also

\[ 1^{**} = 1 + 1^*1^{*2} \]

\[ = 1 + 1^*(1 + 1^*1^{*2}) \]

\[ = 1 + 1^{*2} 1^{*2} \]

\[ = 1^* (1 + 1^*1^{*2}) \]

\[ = 1^* 1^{*2} \]

So

\[ 1 + 1^{*2} = 1 + 1^*1^{*2} = 1^{*2} \]

Whence

\[ 1^{****} = 1 + 1^{***} = 1^{*2} \]
Fake Matrix Example 1

In a non-commutative ring

Ex. \((1-ab)x = 1\) + Ex. \((1-ba)y = 1\)

Suppose

\((1-ab)x = 1\)

Then

\[
(1-ba)(1+bxa) = 1-ba+bxa-baba
\]

\[
= 1-b(1-x+abx)
\]

\[
= 1-b(1-(1-ab)x)
\]

\[
= 1-b(1-1) = 1
\]
FAKE MATRIX EXAMPLE 2

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

Suppose \( d \) has a left inverse \( d^{-l} \).

Then \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) has a right inverse if and only if

\( (a - bd^{-l}c) \) has a right inverse \( u \) say.

Consider

\[
\begin{pmatrix}
   u & -ucd^{-l} \\
   -d'^{-1}cu & d'^{-1} - d'^{-1}ucbd^{-l}
\end{pmatrix}
\]
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
\[
au + bv = 1 \\
au + by = 0 \\
cv + dx = 0 \\
cv + dy = 1
\]

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
\[
au + cv = 1 \\
bv + dv = 0 \\
ax + cy = 0 \\
bx + dy = 1
\]

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

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

so $B$ surjective

Thus

$B$ is bijective (linear) with inverse $A$

So (property of maps)

$$ BA = I $$
Matrix Example

over integral domain $\mathbb{R}$

$\mathbb{R}$ embeds $\mathbb{R} \hookrightarrow \mathbb{F}$
in its field of fractions $\mathbb{F}$

An embedding (preserves and) reflects equalities: no
result for $\mathbb{R}$
follows from
result for $\mathbb{F}$

WARNING: An arbitrary ring is a quotient of an integral domain; as above not enough.
Matrix Example
over an arbitrary ring (commutative)

We use the determinant \( \det A \)
and adjugate matrix \( \text{adj} A \); and the
algebraic identities
\[
\det(AB) = \det A \det B
\]
\( A \cdot \text{adj} A = \det A \cdot I = \text{adj} A \cdot A \)
(They hold in fields, so in integral domains, so in arbitrary rings.)

Assume \( AB = I \)

Deduce
\[
\text{adj} A = (\text{adj} A) AB = (\det A) B
\]
But \( \det A \cdot \det B = \det I = 1 \)
So \( \det B \cdot \text{adj} A = (\det B)(\det A)B = B \)
So \( BA = \det B (\text{adj} A)A = \det B \det A I = I \).
**Logic Question**

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

- Integral domain $D \rightarrow$ Field $E$
- Ring $R$  

It's OK for equations.

Hilbert's Nullstellensatz says:

If $\sum f_i = 0 \rightarrow g = 0$ holds in all fields,

then for some $r$,

$\sum f_i = 0 \rightarrow g^r = 0$ holds in all commutative rings.
A valued domain \( R \) is a valuation ring if its field of fractions 
\[
x \overline{\mathbb{Q}} = \frac{x}{\mathbb{Z}} \in \mathbb{Q}
\]

Uniquely argue as follows:

Take \( I, J \subset \mathbb{R} \) and suppose \( \exists x \in I \cap J : 1 \notin \mathbb{Q} \Rightarrow x \notin I \cap J \)

we have \( \frac{x}{y} \notin \mathbb{R} \). Suppose \( x \in I \)

\( y \in J \Rightarrow x \notin I \cap J \).

Thus maximal ideals are totally ordered so \( \exists \) unique maximal ideal \( \mathfrak{m} \) and \( \mathbb{R} / \mathfrak{m} \) is a local ring.

Elementary char: \( \forall x, y \in \mathbb{R} \rightarrow \left( x \overline{\mathbb{Q}}, y \overline{\mathbb{Q}} \in \mathbb{Q} \right) \Rightarrow x/\mathbb{Z}, y/\mathbb{Z} \in \mathbb{Q} \Rightarrow x \overline{\mathbb{Q}} = y \overline{\mathbb{Q}} \Rightarrow x \in \mathbb{Z} \) so either \( x/\mathbb{Q} \notin \mathbb{Q} \).

Thus \( \mathbb{R} \) is valuation ring iff

\[
\begin{align*}
0 & \neq 1 \\
ab & = 0 \iff a = 0 \lor b = 0 \\
- a & = 0 \lor b = 0 \lor a/\mathbb{Q} \in \mathbb{Q}
\end{align*}
\]

Take \( a \in \mathbb{R} \) such \( a = 0 \lor (1-a) = 0 \) or \( a \mid 1-a \)

\[
\begin{align*}
a & = 0 \iff 1-a = 1 \text{ is in } \mathbb{Q} \\
(1-a) & = 0 \iff a = 1 \text{ is in } \mathbb{Q} \\
a & \mid (1-a) + 3x, xa = 1-a + 3x a(1+x) = 1 + a \text{ is in } \mathbb{Q} \iff (1-a) \mid a
\end{align*}
\]

\[ + (1-a) \text{ in } \mathbb{Q} \]
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 only many $a$ then $f(x) \equiv 0$.

- Hence inductively if $f(x) \in R[x] = R[x_1, \ldots, x_n]$ has $\infty$ sets $A_1, \ldots, A_n$ with $f(x) = 0$ for $a_i \in A_i$ then $f(x) \equiv 0$. 
IRRELEVANCE OF ALGEBRAIC INEQUALITIES

Suppose \( R \) is an infinite integral domain and 
\[ f(x), g_1(x), \ldots, g_r(x) \in R[x] \quad g_i(x) \neq 0 \]
such that 
\[ f(a) = 0 \quad \text{whenever} \quad g_1(a), \ldots, g_r(a) \neq 0; \]
then 
\[ f(x) \equiv 0. \]

Proof: Consider 
\[ h(x) = f(x) \prod g_i(x). \]
\[ h(a) = 0 \quad \text{all } a \quad \text{and so} \quad h(x) \equiv 0. \]
But 
\[ g_i(x) \neq 0 \quad \text{in the integral domain} \quad R[x]. \]
Hence 
\[ f(x) \equiv 0. \]
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

$$\det(AB - tI)$$

$$= \det A \det(B - tA^{-1})$$

$$= \det(B - tA^{-1}) \det A$$

$$= \det(BA - tI).$$
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 in some space. Then the ring of germs of functions
is a local ring; and the quotient field is $IR$.

[local behaviors of continuous real-valued functions.]
Elementary Notion
of local ring

Take $R$ local with maximal ideal $M$. If $a \notin M$ then $\langle a \rangle \neq M$ and so $\langle a \rangle = R$ i.e. $\exists \bar{a} \ a\bar{a} = 1$

Since we can't have both $a, (1-a) \in M$,

$$\exists x. \ ax = 1 \lor \exists y. \ (1-a)y = 1$$

(and $0 \neq 1$)

Conversely if $ax = 1$ holds then the non-invertible elements form the unique maximal ideal.

Now using coherent logic...
**Example**

of use of logic

Theorem (Kaplansky) Let $R$ be a local ring.

Take $E : R^n \to R^n$ an $n \times n$ matrix with $E^2 = E$.

Then for some $0 \leq r \leq n$ there is invertible $P$ with

$$P^{-1}EP = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

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

(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 \( C(X) \)
\( \cong \) projective \( \mathbb{R} \)-modules in \( \mathbb{S}h(X) \)
and by internal Kaplansky the
latter
\( \cong \) (locally) free \( \mathbb{R} \)-modules in \( \mathbb{S}h(X) \)

\( \cong \) Vector bundles over \( X \).

Thus
Theorem (Swan)
Projective \( C(X) \) modules
\( \cong \) Vector bundles over \( X \).
Let $A$ be a local ring $A^n \to A^n$ such that $P^2 = P$. Then for some choice of basis for $A^n$, $P$ has matrix

$$
\begin{pmatrix}
I_r & 0 \\
0 & 0
\end{pmatrix} \cdot
\begin{pmatrix}
0 & 0 \\
0 & I_r
\end{pmatrix}
$$

Either $p_{ii}$ invertible or $(1 - p_{ii})$ invertible.

In case $p_{ii}$ invertible we see that $p^{(i)}$, $e_2$, $\ldots$, $e_n$ is a basis and w.r.t. to $P$ has matrix

$$
\begin{pmatrix}
1 \\
0 \\
\vdots \\
0
\end{pmatrix}
\begin{pmatrix}
Q
\end{pmatrix}
$$

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

$$
\begin{pmatrix}
1 & 0 & 0 \\
0 & I & 0 \\
0 & 0 & 0
\end{pmatrix}
$$

Here we have $f_i \to f_i$

$2 \leq i \leq r$ $f_i \to \lambda_i f_i + f_i$ $1 \to 2\lambda_i f_i + f_i$

$0 \to f_i \to 0 \to \lambda_i f_i$ $\lambda_i f_i$ so it follows that $\lambda_i f_i = 0$ and so $\lambda_i = 0$ $2 \leq i \leq r$.

Now replace with basis $f_1$, $f_1 - \lambda_1 f_i$, $\ldots$, $f_r - \lambda_r f_i$, and we have the matrix

$$
\begin{pmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 0
\end{pmatrix}
$$
In case \((1 - p_{ii})\) is 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
\[ a_1P_{11} + a_2P_{21} + \cdots + a_nP_{n1} = a_1. \]

If \(a_1 = (1 - p_{ii})^{-1} p_{21} a_2 + \cdots + (1 - p_{ii})^{-1} p_{n1} a_n\) is a linear combination of \(a_2, \ldots, a_n\) (independently of how \(a_1, \ldots, a_n \in \{\text{rows of } P\}\) is chosen), it follows that the last column is a linear combination
\[ P^{(i')} = \sum_{j=2}^{n} \lambda_j P^{(i)} \quad (\lambda_i = (1 - p_{ii})^{-1} p_{i1}) \]
of the other columns.

Now \(f_i = e_i - \sum_{j \neq i} e_j\), and we are done and write it
\[ P \quad \text{has matrix} \quad \begin{pmatrix} \lambda & 0 \\ 0 & Q \end{pmatrix} \]
and \(Q^2 = 0\) and so by induction hypothesis we can find a good basis for \((e_2, \ldots, e_n)\). Then we get a basis \(f_1, \ldots, f_n\) with which \(P\) has matrix
\[ \begin{pmatrix} \lambda & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & I \end{pmatrix} \]
Then we have
\[ f_i \rightarrow \begin{cases} 0 & \text{if } i \neq 1 \\ 2 \varepsilon_i \in \mathbb{R} & \text{if } i = 1 \end{cases} \quad f_i \rightarrow \lambda f_i \quad f_i \rightarrow \lambda f_i + f_i \quad f_i \rightarrow \lambda f_i + f_i \]
So \(f_i = 0\) \(2 \varepsilon_i \in \mathbb{R}\) and so \(\lambda_i = 0\) \(2 \varepsilon_i \in \mathbb{R}\) and we have matrix
\[ \begin{pmatrix} \lambda & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & I \end{pmatrix} \].
Aside:

$r : \mathbb{Z}^k \rightarrow \mathbb{Z}^k$

$s : \mathbb{Z}^k \rightarrow \mathbb{Z}^{k+1}$

$u : \mathbb{Z}^{k+1} \rightarrow \mathbb{Z}^{k+1} \rightarrow \mathbb{Z}^{k+1} \rightarrow 0$

$v : \mathbb{Z}^{k+1} \rightarrow \mathbb{Z}^{k+1} \rightarrow \mathbb{Z}^{k+1} \rightarrow 0$

$(rs)(u) = (ru + sv) = 0$

$(u)(rs) = (uv, us) = (0, v)$
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.