Induction in Algebra: First Steps

Peter Schuster

(Department of Pure Mathematics, University of Leeds)

Mathematisches Institut, Universität München

Based on joint work with Ulrich Berger and a lecture by Thierry Coquand

Supported by a Feodor Lynen Research Fellowship, Humboldt Foundation

Mathematics, Algorithms, Proofs 2010 (MAP 2010)

Universidad de La Rioja, Logroño, Spain, 8–12 November 2010

Zorn's Lemma and Open Induction

A *chain* in a poset X is an inhabited, totally ordered subset Y of X

For any property P of elements of X, understand $P(\bigvee Y)$ as

"the chain Y has a supremum in X, and this has property P"

If every chain Y in X has a supremum in X, then X is *chain complete*

In algebraic structures one often has $\bigvee Y = \bigcup Y$ for chains Y

Write $\mathsf{Chns}(X)$ for the class of chains Y in X

A subset B of X is *closed* (Zorn) if

$$\forall Y \in \mathsf{Chns}(X) \,.\, Y \subseteq B \to \bigvee Y \in B$$

A variant of the *Kuratowski-Zorn Lemma* reads as

If $B \subseteq X$ is closed and $B \neq \emptyset$, then B has a maximal element

or, equivalently with classical logic,

ZL *If $B \subseteq X$ is closed and unbounded, then $B = \emptyset$*

where B is *unbounded* if

$$\forall x \in X \,.\, x \in B \to \exists y > x \,(y \in B)$$

A subset A of X is *open* if

$$\forall Y \in \mathsf{Chns}(X) \,.\, \bigvee Y \in A \to Y \between A$$

where $S \between T$ denotes (Sambin) that the sets S and T meet each other

Raoult's *Open Induction* can be put as

OI *If $A \subseteq X$ is open and progressive, then $A = X$*

where A is *progressive* if

$$\forall x \in X \,.\, \forall y > x \,(y \in A) \to x \in A$$

With classical logic, OI implies ZL:

$$A \cup B = X\,, \quad A \cap B = \emptyset\,,$$

then clearly $A = X$ iff $B = \emptyset$ but also
— A is progressive iff B is unbounded
— A is open whenever B is closed

Is OI too strong classically? Not if restricted to chain complete posets X, for which A is open iff B is closed; whence $\mathsf{OI}_{X,A}$ is equivalent to $\mathsf{ZL}_{X,B}$

So OI for chain complete posets X is a classical equivalent of AC
Note that Raoult put OI only for chain complete posets X

Objective

Distinguish a class of "good" theorems for which

$$\mathsf{\Gamma} + \mathsf{ZL} \vdash_c G \;\Rightarrow\; \mathsf{\Gamma} + \mathsf{OI} \vdash_i G$$

whenever $\mathsf{\Gamma}$ is a good theory and G a good theorem

Desired solution: a transformation algorithm

Compare the Berger-Coquand variant OI_0 as a substitute for DC:

$$\vdash_c \mathsf{OI}_0 \leftrightarrow \mathsf{DC}\,, \qquad \mathsf{DC} \vdash_c B \;\Rightarrow\; \mathsf{OI}_0 \vdash_i B$$

where B is a $\mathbf{\Sigma}$-formula, i.e. $\vdash_i B \leftrightarrow \exists \vec{x} A$ with certain q.f. A

Contrast this with *Barr's Theorem*

$$\mathsf{\Gamma} + \mathsf{AC} \vdash_c G \;\Rightarrow\; \mathsf{\Gamma} \vdash_i G$$

where $\mathsf{\Gamma}$ is a geometric theory and G a geometric theorem

In general, however, there is no transformation algorithm

A *geometric formula* is of the form

$$\forall \vec{x}.E \to F$$

where E, F are built from atomic formulas by $\wedge$, $\vee$, $\exists$, and maybe $\bigvee$

Motivations

— Proofs with OI tend to be direct and elementary
— Ideal objects—as output by ZL—are eliminated
— OI may be better behaved proof-theoretically
— Proofs with OI may be turned into dynamical proofs
— Proofs with OI may be suited for program extraction

There are a few case studies in algebra; for one see below
Case studies in logic, analysis, topology, ... are to follow

A Case Study in Algebra: Gauß's Lemma, here called "Theorem P"

Let R be a ring, commutative and with 1. In the polynomial ring $R[X]$,

$$f = \sum_{i=0}^{n} a_i X^i\,,\ g = \sum_{j=0}^{m} b_j X^j \ \Rightarrow\ fg = \sum_{k=0}^{n+m} c_k X^k\,,\ c_k = \sum_{i+j=k} a_i b_j$$

The *content* $\mathsf{cont}(f)$ of f is the ideal generated by $a_0, \ldots, a_n$

A polynomial f is *primitive* if $\mathsf{cont}(f) = R$: that is, $1 \in \mathsf{cont}(f)$

Theorem P *If f and g are primitive, then fg is primitive*

Note that hypotheses and conclusion of Theorem P are *concrete statements*

Of course there already are direct and elementary proofs, without ZL/OI
(For a short and elegant one see Banaschewski-Vermeulen)

There also is a proof with formal methods (Coquand), using Gauß-Joyal

We will first review the customary classical proof with ZL

Next, we will turn this into a constructive proof with OI

A Classical Proof of Theorem P from ZL

Let $\mathfrak{p}$ stand for the *prime ideals* of R: if $a \notin \mathfrak{p}$ and $b \notin \mathfrak{p}$, then $ab \notin \mathfrak{p}$

Let $\mathfrak{q}$ be a finitely generated ideal of R

Form of ZL $\mathfrak{q} \neq R \Rightarrow \exists \mathfrak{p}.\mathfrak{q} \subseteq \mathfrak{p}$ [$\Leftarrow$ anyway]

With ZL there is a maximal ideal above I, which is prime

Contrapositive $\mathfrak{q} = R \Leftarrow \forall \mathfrak{p}.\mathfrak{q} \not\subseteq \mathfrak{p}$ [$\Rightarrow$ anyway]

To arrive at Theorem P it now suffices to prove

Lemma *If* $\mathrm{cont}(f) \not\subseteq \mathfrak{p}$ *and* $\mathrm{cont}(g) \not\subseteq \mathfrak{p}$, *then* $\mathrm{cont}(fg) \not\subseteq \mathfrak{p}$

In other words, one has to verify

Lemma *If* $f \not\equiv 0 \bmod \mathfrak{p}$ *and* $g \not\equiv 0 \bmod \mathfrak{p}$, *then* $fg \not\equiv 0 \bmod \mathfrak{p}$

[$\mathrm{cont}(f) \not\subseteq \mathfrak{p}$ iff $\exists i\,(a_i \notin \mathfrak{p})$ iff $\exists i\,(a_i \not\equiv 0 \bmod \mathfrak{p})$ iff $f \not\equiv 0 \bmod \mathfrak{p}$]

Modulo $\mathfrak{p}$ we work in an *integral domain*: if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$

Lemma (Gauß) *If R is an integral domain, then so is $R[X]$*

To show this is to show that if $f \neq 0$ and $g \neq 0$, then $fg \neq 0$

To this end, take maximal i, j with $a_i \neq 0$ and $b_j \neq 0$. Now

$$c_{i+j} = \underbrace{a_0 b_{i+j} + \ldots + a_{i-1} b_{j+1}}_{=0} + a_i b_j + \underbrace{a_{i+1} b_{j-1} + \ldots + a_{i+j} b_0}_{=0}$$

and thus $c_{i+j} = a_i b_j$, which is $\neq 0$ for R is an integral domain

A Constructive Proof of Theorem P from OI

Surprisingly often in commutative algebra one invokes

Concrete Lemma *If S is a multiplicative subset of the commutative ring R, and I an ideal of R, then for all $a, b \in R$*

$$I + (a) \not\subset S,\ I + (b) \not\subset S \ \Rightarrow\ I + (ab) \not\subset S$$

It can be used, with $S = R \setminus \mathfrak{m}$, to prove that a maximal ideal $\mathfrak{m}$ is prime

In particular it occurs in the proof of the aforementioned form of ZL

As is usually proved instance-by-instance, a set of the form

$$B = \{I \in X : I \subseteq T\}$$

is closed (in the sense of Zorn), and downwards closed

General Fact *If R is any set, $S \subseteq R$, and X a set of subsets of R, then*

$$A = \{I \in X : I \between S\}$$

is open and upwards closed where X is ordered by inclusion

Proof If Y is a chain in X with $\bigcup Y \in X$, then
$\bigcup Y \in A \Leftrightarrow \bigcup Y \between S \Leftrightarrow \exists I \in Y.I \between S \Leftrightarrow \exists I \in Y.I \in A \Leftrightarrow Y \between A$

Order the ideals of a commutative ring by inclusion
For every chain Y of ideals, $\bigvee Y = \sum Y = \bigcup Y$

A ring R is *discrete* if equality is decidable on R
An ideal I of R is *detachable* if membership to I is decidable

Note that R is discrete if and only if 0 is detachable

Let R be a discrete ring, and X the set (!) of the detachable ideals of R
We have supposed that R be discrete to achieve that $0 \in X$

It is a classical tautology that R is discrete, and every ideal I detachable
In particular, X is chain complete with classical logic

Again let $f, g \in R[X]$ and fg have coefficients a_i, b_j and c_k; set

$$\mathfrak{a} = \mathsf{cont}(f) = (a_0, \ldots, a_n) \qquad \mathfrak{b} = \mathsf{cont}(g) = (b_0, \ldots, b_m)$$

$$\mathfrak{c} = \mathsf{cont}(fg) = (c_0, \ldots, c_{n+m})$$

Assume that $1 \in \mathfrak{a}$ and $1 \in \mathfrak{b}$; we want to show $1 \in \mathfrak{c}$

Let A be as in the general fact with $S = 1 + \mathfrak{c}$:

$$A = \{I \in X : I \not\subset 1 + \mathfrak{c}\}$$

To show $1 \in \mathfrak{c}$ is tantamount to show $0 \in A$, i.e. $A = X$

With OI at hand it remains to show that A is progressive

Fix $I \in X$ and suppose that $J \in A$ for every $J \in X$ with $I \subsetneq J$

To show $I \in A$ we distinguish two case
(Recall that every $I \in X$ is detachable)

Case 1 $\forall i\,(a_i \in I)$ or $\forall j\,(b_j \in I)$

In this case $1 \in I$ for $1 \in \mathfrak{a} \cap \mathfrak{b}$; whence $I \in A$

Case 2 $\exists i\,(a_i \notin I)$ and $\exists j\,(b_j \notin I)$

Take maximal i, j with $a_i \notin I$ and $b_j \notin I$

First, we have $I \subsetneqq I + (a_i)$ and $I \subsetneqq I + (b_j)$
Hence $I + (a_i) \in A$ and $I + (b_j) \in A$ by induction hypothesis
By the concrete lemma also $I + (a_i b_j) \in A$, i.e. $I + (a_i b_j) \not\subset 1 + \mathfrak{c}$

Next, $c_{i+j} \equiv a_i b_j \bmod I$ as in the classical proof:

$$c_{i+j} = \underbrace{a_0 b_{i+j} + \ldots + a_{i-1} b_{j+1}}_{\equiv 0 \bmod I} + a_i b_j + \underbrace{a_{i+1} b_{j-1} + \ldots + a_{i+j} b_0}_{\equiv 0 \bmod I}$$

In all, $I + (c_{i+j}) \not\subset 1 + \mathfrak{c}$, and thus $I \not\subset 1 + \mathfrak{c}$, which is to say that $I \in A$

Strategy

— Notice the concrete lemma(s) in the proof of the form of ZL
— Deduce from OI first the form's contrapositive,* and then the theorem
— To this end, take suitable X, A (almost) as X, B in the form's proof
— Observe that A is open, which usually follows from the general fact
— Prove that A is progressive using the concrete lemma(s) from above

The ideal objects output by ZL are replaced by (parts of) their incomplete specifications, as in dynamical algebra; these are just the elements of X

*See the appendix below

Appendix: A Deduction from OI of the Contrapositive of ZL

Let X be the set of the ideals I of R that admit a *strong primality test*: that is, it is decidable whether I is a prime ideal, and if not, then the test produces a certificate for this: that is, witnesses $a, b \in R \setminus I$ with $ab \in I$

To ensure that $0 \in X$ suppose that 0 admits a strong primality test: i.e, either R is an integral domain or else there are $a, b \in R \setminus \{0\}$ with $ab = 0$

Classically, every ideal admits a strong primality test
In particular, X is chain complete with classical logic

Let $\mathfrak{q}$ be a finitely generated ideal of R

Assume that $\mathfrak{q} \nsubseteq \mathfrak{p}$ for all prime ideals $\mathfrak{p}$

To prove $1 \in \mathfrak{q}$ we prove again $0 \in A$ or, equivalently, $A = X$ where

$$A = \{I \in X : I \not\subset 1 + \mathfrak{q}\}$$

As before it suffices to verify that A is progressive

Fix $I \in X$ and suppose that $J \in A$ for every $J \in X$ with $I \subsetneq J$

To show $I \in A$ we once more distinguish two cases

Case 1 I is a prime ideal

In this case $\mathfrak{q} \nsubseteq I$ by assumption
Now $I \subsetneqq I + \mathfrak{q}$ and thus $I + \mathfrak{q} \in A$ by induction hypothesis
In other words, $I + \mathfrak{q} \not\subset 1 + \mathfrak{q}$; whence $I \not\subset 1 + \mathfrak{q}$, i.e. $I \in A$

Case 2 I is not a prime ideal, and $ab \in I$ for some $a, b \in R \setminus I$

In this case $I \subsetneqq I + (a)$ and $I \subsetneqq I + (b)$
Hence $I + (a) \in A$ and $I + (b) \in A$ by induction hypothesis
By the concrete lemma also $I = I + (ab) \in A$

Kuratowski, C., Une méthode d'élimination des nombres transfinis des raisonnements mathématiques. *Fund. Math.* 3 (1922) 76–108

Zorn, M., A remark on method in transfinite algebra.
Bull. Amer. Math. Soc. 41 (1935) 667–670

Raoult, J.-C., Proving open properties by induction.
Inform. Process. Lett. 29 (1988) 19–23

Coquand, T., Constructive topology and combinatorics. In: J. Myers and M. O'Donnell, eds., *Constructivity in Computer Science*. Springer *Lecture Notes in Computer Science* 613 (1992), 28–32

Coquand, T., A note on the open induction principle.
Chalmers Institute of Technology and Göteborg University (1997)

Coste, M., H. Lombardi, and M.-F. Roy, Dynamical method in algebra: Effective Nullstellensätze. *Ann. Pure Appl. Logic* 111 (2001), 203–256

Berger, U., A computational interpretation of open induction. In: F. Titsworth, ed., *Proceedings of the Nineteenth Annual IEEE Symposium on Logic in Computer Science (LICS), Turku, Finland, July 2004.* IEEE Computer Society Press (2004) 326–334

Coquand, T. and H. Lombardi, A logical approach to abstract algebra.
Math. Struct. in Comput. Science 16 (2006), 885–900