Constructive semantics for classical theories

Example of Galois theory of a separable polynomial

Constructive Mathematics: Proofs and Computation

Chiemsee, 7-11 June 2010

H. Lombardi, Besançon

henri.lombardi@univ-fcomte.fr, http://hlombardi.free.fr

if you want to print these slides:

http://hlombardi.free.fr/publis/Chiemsee2010Doc.pdf

Classical Galois Theory

Let $\mathbf{K}$ be a field and $f \in \mathbf{K}[T]$ a *separable polynomial* of degree n (this means that $\exists u, v \in \mathbf{K}[T]$, $uf + v\frac{\partial f}{\partial T} = 1$).

1. (splitting field) There exists a field $\mathbf{L} \supseteq \mathbf{K}$ and $x_1, \ldots, x_n \in \mathbf{L}$ such that $x_i - x_j \in \mathbf{L}^\times$ if $i \neq j$ and

   (a) in $\mathbf{L}[T]$ we have $f(T) = \prod_{i=1}^{n}(T - x_i)$

   (b) $\mathbf{L} = \mathbf{K}[x_1, \ldots, x_n]$, i.e., any element of $\mathbf{L}$ can be written as $Q(x_1, \ldots, x_n)$ for some $Q \in \mathbf{K}[X_1, \ldots, X_n]$

2. $\mathbf{L}$ is a finite dimensional $\mathbf{K}$-vector space (notation for the dimension $[\mathbf{L} : \mathbf{K}]$)

Classical Galois Theory (2)

3. (unicity theorem) Let $\mathbf{L}'$ be another overfield of $\mathbf{K}$ with elements $y_1, \ldots, y_n$ satisfying 1a) and 1b).
   Then there exists a $\mathbf{K}$-isomorphism $\varphi : \mathbf{L} \to \mathbf{L}'$ and a permuation σ of $[\![1..n]\!]$ such that $\varphi(x_k) = y_{\sigma(k)}$ for all $k \in [\![1..n]\!]$.

4. (Galois group) Let us denote $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ the group of $\mathbf{K}$-automorphisms of $\mathbf{L}$ (such an automorphism ψ is characterised by the permutation σ it induces over $x_1, \ldots, x_n$, so $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ can be viewed as a subgroup of S_n). Then $|\mathrm{Gal}(\mathbf{L}/\mathbf{K})| = [\mathbf{L} : \mathbf{K}]$

Galois correspondance

For a subgroup H of $G = \mathrm{Gal}(\mathbf{L}/\mathbf{K})$ let us denote $\mathrm{Fix}_{\mathbf{L}}(H)$, or $\mathbf{L}^H$ the sub-$\mathbf{K}$-algebra of $\mathbf{L}$ defined as

$$\mathbf{L}^H = \{\, y \in \mathbf{L} \,|\, \forall \psi \in H,\, \psi(y) = y \,\}$$

For a field $\mathbf{M}$ with $\mathbf{K} \subseteq \mathbf{M} \subseteq \mathbf{L}$ tel us denote $\mathrm{Stp}_G(\mathbf{M})$ the subgroup H of G defined as

$$H = \{\, \psi \in G \,|\, \forall y \in \mathbf{M},\, \psi(y) = y \,\}\,.$$

5. $\mathrm{Fix}_{\mathbf{L}}$ and Stp_G are decreasing one to one correspondances between

   $$\{\text{subgroups of } G\} \text{ and } \{\text{fields } \mathbf{M} \text{ s.t. } \mathbf{K} \subseteq \mathbf{M} \subseteq \mathbf{L}\}$$

   with $\mathrm{Stp} \circ \mathrm{Fix} = \mathrm{Id}_{\text{subgroups}}$ and $\mathrm{Fix} \circ \mathrm{Stp} = \mathrm{Id}_{\text{subfields}}$

Galois correspondance, continued

6. If $\mathbf{L}^H = \mathbf{M}$, then $\mathbf{L}$ is a splitting field for f over $\mathbf{M}$.
   Moreover $\mathrm{Gal}(\mathbf{L}/\mathbf{M}) = H$.

7. For $\psi \in G$, $\psi(\mathbf{L}^H) = \mathbf{L}^{\psi H \psi^{-1}}$.

8. $\mathbf{L}^H = \mathbf{M}$ is a splitting field for some polynomial $g \in \mathbf{K}[T]$ if and only if H is a normal subgroup of G.
   In this case $\mathrm{Gal}(\mathbf{M}/\mathbf{K}) \simeq G/H$.

9. In characteristic 0 the equation $f(x) = 0$ is solvable by extractions of m-th roots if and only if G is resoluble.

Bases over $\mathbf{K}$

10. (resolvent) For $z \in \mathbf{L}$,

    – let $z_1, \ldots, z_r$ be the orbit $G.z$,

    – $H = \mathsf{Stab}_G(z) = \mathsf{Stp}_G(\mathbf{K}[z])$ (so $r \cdot |H| = |G|$)

    – and $R_z(T) = \prod_{i=1}^{r}(T - z_i)$.

    Then $R_z(T)$ is the minimal polynomial of z over $\mathbf{K}$.

    As a particular case $\mathsf{Stab}_G(z) = \{\mathrm{Id}\}$ if and only if $\mathbf{L} = \mathbf{K}[z]$ (primitive elements).

11. (normal basis) There exists a basis of $\mathbf{L}$ as $\mathbf{K}$-vector space made of $\psi(y)'s$ for some y in $\mathbf{L}$ and all $\psi \in \mathsf{Gal}(\mathbf{L}/\mathbf{K})$.

Richman semantics

There is a possible description of classical mathematics as

"constructive mathematics when allowing TEM (and often Choice)" (see Fred Richman).

Let us see what is the issue for Galois theory with this semantics

An intriguing example

What about the splitting field of $T^2 - a$, $a \neq 0$ (in characteristic $\neq 2$)

Dynamical semantics

It is often possible to understand "too abstract objects in classical mathematics" (too abstract means that TEM and Choice are too much used) as "nonstatic constructive objects, dynamical ones"

Let us see what is the issue for Galois theory with this semantics.

What Model Theory says about Galois theory

The theory of a splitting field $\mathbf{L}$ for f over $\mathbf{K}$ is coherent. More precisely . . . (constructive version)

With Gödel's Completeness Axiom (a mixture of TEM and Zorn), which is constructively equivalent to Gödel's Completeness Theorem, the splitting field $\mathbf{L}$ does "exist".

When allowing classical logic (i.e., TEM), the theory of $\mathbf{L}$ (and variants of this theory allowing us to speak of $\mathbf{L}'$ and $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$) proves all theorems of classical Galois theory.

Constructive understanding of these "classical" facts leads to . . . .

Thank you