Some remarks about Skolem-Noether Theorem

Dagsthul, November 24, 2021

This talk

A discussion of a (constructive) proof of *Skolem-Noether Theorem*

Let F be a discrete field.

Let A be a finite algebra over F which is a *division* algebra of center F and $\sigma : A \to A$ a F-automorphism.

Theorem: (Skolem-Noether) *We can find* a *invertible such that* $\sigma(x) = axa^{-1}$, *i.e. any automorphism is an* inner *automorphism*

Skolem-Noether

F discrete field

A is given by generators e_i and multiplication table $e_i e_j = \Sigma_k \Gamma_{ij}^k e_k$

Example: Quaternion algebra e_1, e_2, e_3 with

$e_1^2 = e_2^2 = e_3^2 = -1 \qquad e_1 e_2 = e_3 = -e_2 e_1$

This is a division algebra if $F = \mathbb{Q}$

This talk

Hurwitz 1896 "Über die Zahlentheorie der Quaternionen"

Skolem 1927 "Zur Theorie der assoziativen Zahlensysteme"

Noether 1933 "Nichtkommutative Algebra"

Different proofs

The simplest proof is probably the one of Baer 1940 in his review of Albert's book *Structure of algebras*

This talk

Cohomological proof in Gilles-Szamuely
Central simple algebras and Galois cohomology, 2006

Both Skolem's proof and this proof starts by proving the result, not for division algebras, but for a *matrix algebras* (*weak* form of Skolem-Noether).

(The proof is direct and we assume this weak form in the rest of the talk.)

They then use that a division algebra of center F becomes a matrix algebra after scalar extension by a *separable* finite extension of F

Central simple algebra: a F-algebra which becomes a matrix algebra by a separable extension

Classifying topos

Essential use of the *coherent* theory of separably closed field over F

$1 \neq 0$

$x = 0 \vee \exists_y (xy = 1)$

$S(x_1, \ldots, x_n) \to \exists_x \ (x^n + x_1 x^{n-1} + \cdots + x_n = 0)$

where $S(x_1, \ldots, x_n)$ expresses that $X^n + x_1 X^{n-1} + \cdots + x_n$ is separable

Classifying topos

We can build a *sheaf* model of this theory

This model is built in an effective meta theory

No need of classical logic and Zorn's Lemma

Site model: (opposite of) the category of finitely presented F-algebras R

We "force" the separable closure condition by taking as covering

$R \to R[X]/(P)$

for P separable

Classifying topos

J. Della Dora, C. Dicrescenzo, D. Duval
About a new method for computing in algebraic number fields, 1985

D5 method in *computer algebra*

M. Coste, H. Lombardi, M.-F. Roy
Dynamical method in algebra: effective Nullstellensätze, 2001

A. Joyal
Les théoremes de Chevalley–Tarski et remarques sur l'algèbre constructive, 1976

This talk

Part of a research program

Constructive development of the theory of central simple algebras

j.w.w. Henri Lombardi and Stefan Neuwirtz

We present most basic results of this theory in a constructive setting

One application: analysis of a simple classical proof by Karim Becher (2016), which uses the axiom of choice, of a corollary of Merkurjev's Theorem

The bounds are not primitive recursive!

History

Historical interest of the topic

(1) early use of *classical logic* in algebra, maybe as important as (or even more than) Hilbert's basis theorem

(2) to understand the origin of the notion of *site*

Vast generalisation by Grothendieck of the notion of topological space, where we replace the poset of basic open subsets by a category. I believe one important historical source comes from works on central simple algebras, in particular the work of François Châtelet and his attempt to develop a "Géométrie Galoisienne"

History

(1) early use of *classical logic*

The basic theorem Wedderburn's 1907 result states that a central simple algebra A can be written as a matrix algebra $M_n(D)$ over a division algebra

This result is *not* constructively valid!

The situation is typical: it is valid in a *dynamical* sense, and most other important results of the theory that we built from it are *constructively valid*

History

Played an important role in the development of abstract algebra

See e.g.

"The influence of J.H.M. Wedderburn on the development of modern algebra", E. Artin, 1950

"Hyperkomplexe Größen und Darstellungstheorie", E. Noether, 1927

Noetherian and Artinian rings

History: Gémétrie Galoisienne

(2) to understand the origin of the notion of *site*

Thesis of F. Châtelet

Difference between *algebraic* study of a polynomial system (is there a solution in the algebraic closure of $\mathbb{Q}$) and *arithmetic* study (is there a rational solution?)

The first question is decidable, while the second question is very difficult

Under what conditions can one "descend" an algebraic solution to an arithmetic solution?

Géométrie Galoisienne

With sheaves over a topological space, we have a notion of *local* existence: there is a covering U_i and an inhabitant of each $A(U_i)$

Maybe these inhabitants are not compatible and we don't have *global* existence

F. Châtelet: we have a presheaf A on finite separable field extension of a given field F and local existence now means that $A(L)$ is inhabited for an *extension* L

$$A(L) = \{(x, y) \in L^2 \mid x^2 + y^2 = a\}$$

Global existence corresponds to: *rational* solution

Sheaves

When does $A(L)$ define a "geometrical object"?

If L Galois extension and u in $A(L)$ is invariant under the Galois group of L/F then there is a *unique* a in $A(F)$ such that $a|L = u$.

Example of sheaves/geometrical objects:

$A(L) = Hom(F[X], L)$ separable extension of F

$\mathbb{G}_m(L) = Hom(F[X, 1/X], L) = L^\times$

Géométrie Galoisienne

Another example of a sheaf

Let A division algebra of center F, and σ automorphism of A

$U(L) = \{a \in A_L^\times \mid \forall_x\ \sigma_L(x) = axa^{-1}\ \}$

where A_L is $A \otimes_F L$

U is a $\mathbb{G}_m$-torsor!

A $\mathbb{G}_m$ action, and as soon as $U(L)$ is inhabited, it is isomorphic to $\mathbb{G}_m$

Géométrie Galoisienne

$U(L) = \{a \in A_L^\times \mid \forall_x\ \sigma_L(x) = axa^{-1}\ \}$

If a in $U(L)$ and c in $L^\times$ then ca in $U(L)$

If we have a and b in $U(L)$ then ab^{-1} is in the center of A_L, hence in L

It is *locally* inhabited: we can find a finite separable extension such that A_L is a matrix algebra, and then U is inhabited (by the *weak* form of Skolem-Noether)

Galoisian descent

We have $a(x)$ in $U(F[x])$ with $P(x) = 0$ and P separable

Can we "descend" this solution to a an element in $U(F)$?

Let L be the splitting field of P of roots $x_1, \ldots, x_n$

Try $\Sigma a(x_i),\ \Sigma x_i a(x_i),\ \ldots,\ \Sigma x_i^{n-1} a(x_i)$

They are all elements of A_F, being symmetric, and one of them is $\neq 0$

Uses Vandermonde matrix (or Lagrange interpolation) and P separable

Galoisian descent

There is *another* constructive argument but less explicit

The condition $\forall_x(\sigma(x) = axa^{-1})$ can be written as a *linear* system

$\sigma(e_1)a = ae_1 \quad \dots \quad \sigma(e_n)a = ae_n$

This linear system should be of rank 1 in F if it is of rank 1 in L!

The computation of the rank of a matrix is independent of the ambiant field

This other argument however does not explain *how* to find a solution in F from the given solution in L

Site

Sheaf model for the theory of separable algebraic closure of F

Objects: separable triangular extensions of F

Covering: $R = R_1 \times \cdots \times R_n$

Covering: $R \to R[x]$ separable extension

Sheaf condition

$A(R)$ with restriction maps $A(R) \to A(S)$ given $R \to S$

$A(R) = A(R_1) \times \cdots \times A(R_n)$

If $u(a)$ in $A(R[a])$ and $u(a) = u(b)$ in $A(R[a,b])$ then there is a unique u in $A(R)$ which restricts to $u(a)$

Sheaf condition

This is *equivalent* to a Galoisian condition

Let $L = R[x_1, \ldots, x_n]$ universal decomposition algebra of P

-If $u(x_1) = \cdots = u(x_n)$ in $A(L)$ then $u(x_i) = u$ for a unique u in $A(R)$

-If $v(\vec{x})$ in $A(L)$ is symmetric then $v(\vec{x}) = v$ for a unique v in $A(R)$

Sheaves

Theorem: $C = Hom(F[X], \_)$ *and* $\mathbb{G}_m = Hom(F[X, 1/X], \_)$ *are sheaves and* C *is the separable closure of* F*. Furthermore, any* $\mathbb{G}_m$ *torsor is trivial.*

This last statement is known as Hilbert's Theorem 90

Theorem: *If* A *is a finite algebra over* F*, then* A *is central simple if, and only if,* A *becomes a matrix algebra if we extend the scalar to* C*.*

Corollary (Skolem-Noether): *Any automorphism of a central division algebra is an inner automorphism.*