Constructive Remarks about the Theory of Central Simple Algebras

Oberwolfach, November 13, 2020

This talk

Work in progress, several discussions with Henri Lombardi and Stefan Neuwirth

A research program

Constructive development of the theory of central simple algebras

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

Division Algebra

F commutative discrete field

First, consider finite dimension algebra over F which forms a *division* algebra

Example: over the reals we consider $\mathbb{H}$ (Hamilton 1843)

$$i^2 = -1 \qquad j^2 = -1 \qquad ij = -ji$$

$\mathbb{H}$ is of dimension 4 with a basis $1, i, j, k = ij$

The *center* of $\mathbb{H}$ is $\mathbb{R}$

A is *central* and *simple* (no non trivial two-sided ideals)

Division Algebra

What are the division algebras over a given field?

Brauer group $Br(F)$: collection of all division algebras of center F

$Br(F) = 0$ if F is algebraically closed

$Br(F) = 0$ if F is *finite* (Wedderburn's Theorem)

$Br(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$

Direct product

If A and B algebras over F we can form $C = A \otimes_F B$

Solution of the following universal problem:

find C with $i : A \to C$ and $j : B \to C$ and such that $i(a)j(b) = j(b)i(a)$

Concretely we give A with a basis u_i and a multiplication table $u_i u_j = \Sigma \alpha_{ij}^k u_k$

B is given by v_p and $v_p v_q = \Sigma \beta_{pq}^r v_r$

Then C has formal basis $u_i v_p$ and $u_i v_p u_j v_q = \Sigma \alpha_{ij}^k \beta_{pq}^r u_k v_r$

Clearly $A \otimes_F B = B \otimes_F A$

Direct product

If A and B are *central simple* over F then so is $A \otimes_F B$

If A and B are division algebras then $A \otimes_F B$ may not be a *division* algebra

E.g. $\mathbb{H} \otimes \mathbb{H} = M_4(\mathbb{R})$

Theorem: (classical) *If A is central simple over F we can write $A = M_n(D)$ where D is a* division *algebra over F*

This is also due to Wedderburn 1907

The product of $\mathbb{H}$ with itself in $Br(\mathbb{R})$ is $\mathbb{R}$

Wedderburn's 1907 Theorem

This result with its proof is an early use of classical logic

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

Brauer equivalence

We say that A and B are *equivalent* if we have $A = M_m(D)$ and $B = M_n(D)$ with the same division algebra D

Modulo equivalences $Br(F)$ is now an abelian group associated to F, the *Brauer group* of F

To understand the structure of this group is a fundamental question in algebra and number theory

Number theory

$Br(F) = \mathbb{Q}/\mathbb{Z}$ if F is a p-adic field

$Br(\mathbb{Q})$ subgroup of $\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Q}/\mathbb{Z})^{\mathbb{N}}$

cf. P. Roquette *The Brauer-Hasse-Noether Theorem in Historical Perspective*

Algebra

What is also of interest for logic is that there are several remarkable results which hold for *arbitrary* fields

E.g. Merkuriev's Theorem which gives a complete description of the 2-torsion part of $Br(F)$

Milnor's conjecture (solved by Voevodsky 1996) is a generalisation which also holds for an arbitrary field

Constructive development?

Only one paper by F. Richman

Finite dimensional algebras over discrete fields, 1982

This is reproduced in the 1988 book

A Course in Constructive Algebra, R. Mines, F. Richman, W. Ruitenburg

Constructive development?

Main issue: Wedderburn's Theorem $A = M_n(D)$ *does not* hold constructively

Given A, we cannot decide if A is a division algebra or not in general

E.g. over F if we define A by

$$i^2 = -1 \qquad j^2 = -1 \qquad ij = -ji$$

then A is a division algebra iff $-1 = x^2 + y^2$ has no solution in F

Constructive development?

This is similar to the problem of existence of algebraic closure of a field: we cannot decide if a polynomial is irreducible or not

This difficulty is reminiscent of the problem Brouwer addressed when introducing choice sequences

1918 Second Act of Intuitionism

Intuitionism should be more general than “separable” mathematics

Dynamic Algebra

Cf. *Commutative algebra: constructive methods*, H. Lombardi, C. Quitté

D5 method in *computer algebra*

J. Della Dora, C. Dicrescenzo, D. Duval

About a new method for computing in algebraic number fields, 1985

Dynamic Algebra

“Lazy” computation

We proceed *as if* A had no non trivial idempotent

If ever during a computation/proof we discover a non trivial idempotent in A we go back and write $A = M_n(B)$ with $n > 1$ and B a simpler algebra

We proceed replacing A by B

Application

While Wedderburn's Theorem does not hold constructively we can prove

Theorem: $[A : F]$ *is always a square*

Theorem: (Skolem-Noether) *If* $u : A \to A$ *automorphism we can find* a *regular such that* $u(x) = axa^{-1}$*, i.e. any automorphism is an* inner *automorphism*

We also redefine equivalence as: we can find C such that $A = M_m(C)$ and $B = M_n(C)$ for some C, *without* requiring C to be a division algebra

Application

For L is an algebra over F say L *splits* A iff $A \otimes_F L$ is a matrix algebra $M_n(L)$

Theorem: *A is central simple over F iff it can be split by a separable extension of F*

Separable extension: we add formally a root x of a separable polynomial

This polynomial may not be irreducible, $F[x]$ may not be a field

A central simple algebra is a *twisted* form of a matrix algebra

It becomes a matrix algebra after scalar extension

Application

If $[A:F] = n^2$ and a in A then a is a root of a polynomial of degree n

A priori, seeing a as a linear map $A \to A$ one would expect (Cayley-Hamilton) a polynomial of degree n^2

This uses the previous result and constructive Galois theory!

(This is a nice basic example of Galois descent)

An example

Splitting fields of central simple algebra of exponent two, Karim Becher 2016

Theorem: (classical) *If A is of exponent 2 then A can be split by a sequence of quadratic extensions of F*

This is a consequence of Merkurjev's Theorem (1982) but Becher provides a short proof, which uses the Axiom of Choice however

An example

We have reformulated Becher's argument so that it becomes constructive

We assume $car\ F \neq 2$

Theorem: *If A is of exponent 2 then A can be split by a sequence of* formal *quadratic extensions of F*

We cannot decide in general if a given element is a square

The argument proceeds then as follows

Definition: A sequence of natural number $n_1, \ldots, n_l$ is *admissible* if we can split A by a sequence of formal root extensions of degrees $n_1, \ldots, n_l$

We want to show that we have an admissible sequence of the form $2, \ldots, 2$

An example

Main Lemma: *If* $\sigma, N, 2, \ldots, 2$ *is admissible with* $N > 2$ *then we can find an admissible sequence of the form* $\sigma, m_1, \ldots, m_p$ *with* $m_1, \ldots, m_p$ *all* $< N$

In this way we get a constructive proof of Becher's application

The proof uses a well-founded induction over ω^ω

What next?

Severi-Brauer variety, Chatelet's Theorem on rational points

Formulation of Milnor's conjecture

Brauer's group can be formulated as a cohomology group $H^2(F, \mathbb{G}_m)$

The 2-torsion subgroup is $H^2(F, \mathbb{Z}/2\mathbb{Z})$

Using constructive (sheaf) models of univalent type theory, we have a constructive description of $H^p(F, \mathbb{G}_m)$ and $H^p(F, \mathbb{Z}/2\mathbb{Z})$

We use the site of finite étale algebras over F

Merkurjev's Theorem

Let (a, b) the element of $Br(F)$ defined by

$$i^2 = a \qquad j^2 = b \qquad ij = -ji$$

for a and b in $F^\times$

Note that we have $(a, 1 - a) = 1$

Also $(aa', b) = (a, b)(a', b)$ and $(a, b) = (b, a)$

Merkurjev's Theorem states that the 2-torsion part of $Br(F)$ is presented by these symbols and relations!