

Seminar on Semisimple Algebras

The topic of the seminar is semisimple algebras, more precisely, semisimple finite-dimensional associative algebras over a field K . We do not assume that the algebras are commutative. Interesting examples are division algebras over K , i.e., algebras in which every non-zero element is invertible. A concrete example is the \mathbb{R} -algebra of quaternions constructed by Hamilton. We will see many other examples in the seminar.

This is a classical topic with many connections to other areas, and is a core part of “modern mathematics”. Towards the end of the seminar, we will make the connection with local class field theory, the main topic of the course Algebraic Number Theory 2. (So you get most out of it if you do both. It is possible, however, to take part in the seminar without attending the course, or vice versa.)

Credit points: The seminar is a combined Bachelor/Master seminar. If you successfully give one of the talks marked (Ba), you get 6 Credit Points. If you successfully give one of the talks marked (Ma), you obtain 9 CP (Master seminar) or 6 CP (Bachelor Seminar) at your choice. The talks marked (BaTh) are particularly suitable as the basis of a Bachelor’s thesis. Please contact me as soon as possible if you would like to write your Bachelor’s (or Master’s) thesis with me.

Prerequisites: Linear Algebra, Algebra. If you want to give a talk in the second half, some knowledge on local fields (e.g., finite extensions of \mathbb{Q}_p) is needed; in this case, it is strongly recommended that you attend the course Algebraic Number Theory 2.

Talks can be given in German or English upon the choice of the speaker.

How to give a successful seminar talk.

- Your first and most important goal should be to thoroughly understand the mathematics behind your talk. This will typically take quite a lot of time, so start preparing the talk early! Ask many questions: Be disciplined in asking yourself why (whether) claims made in the references are true. What can be simplified? When you hit things you do not understand, ask other participants of the seminar (those who will give the talks before/after your one might very well have had the same questions, and you might be able to answer them together). If you need assistance beyond that, feel free to ask.
- After digesting the mathematics, you should consciously (re-)arrange things for your talk. Especially in [Lo], the theory is cut into very many small portions, something which is (sometimes) useful in a text book, but usually not in a seminar talk. Ask yourself in advance, which are the main points of your talk that every participant must learn, and highlight them appropriately. You may skip some things if necessary (e.g., technical computations which you do not find enlightening); but think in advance about your choice what to skip, instead of letting time pressure force this choice upon you. Do

not skip things that you yourself had difficulties in understanding; others will probably have the same difficulties, so discussing these things is particularly valuable.

Notes on the references. We will in the beginning mostly follow Milne's [Mi] Ch. IV (which starts out completely independently of the earlier chapters). Later we will follow the book [Lo] by Lorenz (which contains the material of the first talks as well, and in greater generality). The book [GS] by Gille and Szamuely takes a more modern (but also more advanced) point of view. Bourbaki's [B] is an encyclopedic reference.

Note that Lorenz does not make the assumption that A be finite-dimensional as a K -vector space, so many parts of his discussion simplify in our setting.

The page numbers for [Lo] given below refer to the English edition of the book.

If you have difficulties finding any of the references, please contact me.

1. Semisimple algebras: Basic notions (Ba)

We start by introducing the language of K -algebras (K a field) and modules over them. All K -algebras will be assumed to be associative with 1 and *finite-dimensional as K -vector spaces*. Define (left) modules, simple and semisimple modules, ideals, simple and semisimple algebras, the opposite algebra A^{op} of an algebra A , the notion of division algebra.

Give examples of K -algebras:

- The endomorphism algebra of a module. Explain that the endomorphism algebra of A as a left- A -module is A^{op} and generalize this to finite free A -modules. Explain that for a division algebra D and $n \geq 1$, the algebra $\text{End}_D(D^n)$ is simple and semisimple.
- The group algebra of a finite group (we will come back to this in a later talk).
- Quaternion algebras. See e.g. [GS] 1.1; cf. also [Sch] 2.11, 8.11.
- What are examples of algebras which are not semisimple?

See [Mi] IV.1, [Lo] §28 (note that Lorenz does not make the assumption that A be finite-dimensional as a K -vector space, so many parts of his discussion simplify in our setting).

2. Decomposition of a semisimple algebras as a product of simple algebras (Ba)

Discuss the Jordan-Hölder Theorem [Mi] IV.1.2.

Prove the key proposition [Mi] IV.1.4 = [Lo] §28, Lemma (p. 135), and explain its consequences (e.g. [Mi] IV.1.6). Derive that A is semisimple if and only if every A -module is semisimple.

Discuss the decomposition of a semisimple A into isotypical components (the term *isogenous component* used in [Lo] is uncommon and should be avoided), and conclude that if A is semisimple, then it is isomorphic to a finite product of simple algebras ([Lo] §29, Theorem 1).

3. Wedderburn's Theorem (Ba) (BaTh)

Define the notion of centralizer and prove the double centralizer theorem, [Mi] IV.1, Thm. 1.13.

Prove **Wedderburn's Theorem**. Let A be a semisimple K -algebra. Then A is isomorphic to a product $M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$, where $n_i \geq 1$ and the D_i are division algebras.

Also discuss in which sense the decomposition is unique, and give some consequences. See [Mi] IV.1 (Theorem 1.15 – Corollary 1.20). See also [Lo] §29.

4. Representations of finite groups (Ma) (BaTh)

Discuss the basics of the representation theory of a finite group G over an algebraically closed field K of characteristic 0: Let $A = K[G]$ be the group algebra. Explain the notion of representation of G and relate it to the notion of A -module.

Show that A is semisimple (e.g., use that every finite A -module can be equipped with an G -invariant scalar product and hence can be decomposed as a finite direct sum of simple modules). Hence by Wedderburn's Theorem, $A \cong \prod_{i=1}^r M_{n_i}(K)$ for some $r \geq 1$, $n_i \geq 1$. Show that r equals the number of conjugacy classes in G by looking at the center $Z(A)$ of A . (*But note that there is no canonical bijection between the set of simple A -modules and the set of conjugacy classes in G .*)

In the language of representation theory, we get that G has precisely r irreducible representations, of dimensions n_1, \dots, n_r (up to isomorphism), and that $\#G = \sum n_i^2$.

Define the *character* of a representation (or equivalently, of an A -module). Let $e_i \in A$ denote the idempotent element given by the unit matrix in $M_{n_i}(K)$ in the decomposition above, compute it as an element of the group algebra, and derive the *orthogonality relations for characters*. Give some consequences of those, for example:

- Representations V, V' are isomorphic if they have the same character.
- If χ is the character of a representation, then $\langle \chi, \chi \rangle$ is a positive integer, and $\langle \chi, \chi \rangle = 1$ if and only if the underlying representation is irreducible. (See [Lo] §33 Def. 8 for the notation.)

See for instance [Lo] §33, Sections 1 and 2; but restrict to the case of K algebraically closed and of characteristic 0 right away to simplify the discussion.

Give some examples: G abelian; G a symmetric group S_n (at least for $n = 3$).

5. Tensor products and central simple algebras (Ba)

Define the notion of tensor product of two modules over a commutative ring R in terms of the universal property. Show its existence and discuss its properties in the case that R is a field. Explain that the tensor products of K -algebras (finite-dimensional or not) is a K -algebra. Give examples (e.g., of a tensor product of two division algebra which is not a division algebra). Discuss the notion of base change: If A is a K -algebra, and L/K a field extension, then $A \otimes_K L$ is an L -algebra. See e.g., Lang, *Algebra*, Ch. XVI, §1, §2; Jantzen, Schwermer, *Algebra* VII.10, IX.2; Bosch, *Algebra*, 7.2.

Define the notion of central K -algebra and prove that the product of two central K -algebras is central.

Prove that the product of a central simple K -algebra with a simple K -algebra is simple.

See [Mi] IV.2 up to and including Cor. 2.9.

6. The theorem of Skolem and Noether and the Brauer group of a field (Ba) (BaTh)

State and prove the **Theorem of Skolem and Noether**, and its important Corollary: Every K -algebra automorphism of a central simple K -algebra is of the form $x \mapsto axa^{-1}$ for some $a \in A^\times$.

Define the Brauer group $\text{Br}(K)$ of the field K , including the group structure. Define the notion of splitting field. Show that the Brauer group of an algebraically closed field is trivial, and that the Brauer group of \mathbb{R} consists of 2 elements (see e.g. [Hu] IX, Cor. 6.8).

7. Existence of splitting fields (Ba) (BaTh)

Using the Theorem of Skolem and Noether, prove that every central simple K -algebra contains a field L such that $[L : K]^2 = [A : K]$ (in particular, L is finite over K), and that such an L is a splitting field of A . Also show that there always exists a splitting field which is separable over K . ([Mi], IV.3 up to and including Cor. 3.10.)

Give some examples! One possibility would be discussing the Brauer group of a finite field (which is trivial by what is usually called *Wedderburn's Theorem*, not to be confused with Wedderburn's Theorem of Talk 3), see [Lo] §29 Theorem 21. You could also look at quaternion algebras again (depending on what has been covered in Talk 1). Another interesting thing would be to see some explicit division algebras (together with splitting fields) over a non-archimedean local field such as \mathbb{Q}_p .

8. Cohomological description of the Brauer group (Ma)

Explain the standard approach via “Galois descent” to the classification of central simple algebras: For a central simple K -algebra A with splitting field L , assumed to be Galois over K , fixing an isomorphism $h: A \otimes_K L \xrightarrow{\sim} M_n(L)$ the action of $G := \text{Gal}(L/K)$ on $A \otimes_K L$ (obtained from the Galois action on L) gives rise to a “twisted” action of G on $M_n(L)$ which will usually be different from the “standard” action given by the G -action on the individual entries of the matrices in $M_n(L)$. With respect to this action, $A = M_n(L)^G$: A is the subalgebra of elements in $M_n(L)$ fixed by all Galois automorphisms.

For $\sigma \in G$, write $\rho_{\text{std}}(\sigma)$ for the K -algebra automorphism $M_n(L) \rightarrow M_n(L)$ given by applying σ to all matrix entries, and write $\rho_A(\sigma) := h^{-1}(\text{id} \otimes \sigma)h$ for the K -algebra automorphism $M_n(L) \rightarrow M_n(L)$ obtained as described above.¹ Then $\Phi_\sigma := \rho_{\text{std}}(\sigma)^{-1}\rho_A(\sigma)$ is an L -algebra automorphism, i.e., an element $\Phi_\sigma \in \text{Aut}_L(M_n(L))$, and the collection of Φ_σ satisfies the “1-cocycle condition”

$$\Phi_{\sigma\tau} = \Phi_\sigma^\tau \Phi_\tau,$$

¹Note that one can choose different normalizations at this point. Since [Lo] is the most comprehensive source for the remainder of the seminar, here we follow the conventions of [Lo] §30. In particular, maps are applied on the right, e.g., $x^{\rho_A(\sigma)} = ((x^{h^{-1}})^{\text{id} \otimes \sigma})^h$ and $x^{\Phi_\sigma} = (x^{\rho_{\text{std}}(\sigma)^{-1}})^{\rho_A(\sigma)}$. This is different from the normalization in [Se].

where for $\Phi \in \text{Aut}_L(M_n(L))$, $\tau \in G$, we write $\Phi^\tau := \rho_{\text{std}}(\tau)^{-1}\Phi\rho_{\text{std}}(\tau)$. One can now go on and show that every 1-cocycle $(\Phi_\sigma)_\sigma$ comes from some K -algebra A , and nail down precisely when two 1-cocycles $(\Phi_\sigma)_\sigma$ and $(\Psi_\sigma)_\sigma$ give rise to isomorphic K -algebras.

This leads to a description in terms of the “cohomology group $H^1(G, \text{Aut}_L(M_n(L)))$ ” (you need not introduce this group in the talk, but see [Se] VII Annexe and X.2; [Lo] §30 Appendix), and is a very general formalism which applies to many analogous situations where one wants to classify objects “over a field K ” which attain a standard form after “base change” to some Galois extension L of K . See [Se] Ch. X, in particular §2, §5. Cf. also Bosch, *Algebra*, 4.11.

Now using Skolem-Noether, $\text{Aut}_L(M_n(L)) = \text{PGL}_n(L) := \text{GL}_n(L)/L^\times$. Given a 1-cocycle $(\Phi_\sigma)_\sigma$, choose a representative $\dot{\Phi}_\sigma \in \text{GL}_n(L)$ for each Φ_σ . The cocycle condition implies that $\Phi_{\sigma\tau}^{-1}\Phi_\sigma^\tau\Phi_\tau = 1$, hence we obtain

$$c_{\sigma,\tau} := \dot{\Phi}_{\sigma\tau}^{-1}\dot{\Phi}_\sigma^\tau\dot{\Phi}_\tau \in L^\times.$$

Although the index set is now $G \times G$ instead of G , the families $(c_{\sigma,\tau})$ are much easier to handle, since the $c_{\sigma,\tau}$ are just elements of L^\times rather than $\text{Aut}_L(M_n(L))$; in particular, there is no dependence on n anymore. The situation at hand is particularly favorable in the sense that the family $(c_{\sigma,\tau})_{\sigma,\tau}$ still determines the K -algebra A . Show that these families satisfy the 2-cocycle condition, and prove that we obtain an isomorphism between the group $\text{Br}(L/K)$ of central simple K -algebras for which L (Galois $/K$ with Galois group G) is a splitting field and the “cohomology group” $H^2(L/K)(= H^2(G, L^\times))$ (give an ad hoc definition of this group in terms of cocycles).

For the latter, you can follow [Lo] §30.1 (the end result is Theorem 2). Some translations have to be done, since Lorenz works with the $\rho_A(\sigma)$ directly (p_σ in his notation) rather than with the Φ_σ , and applies Skolem-Noether to those elements (which lie in $\text{Aut}_K(M_n(L))$, but not in $\text{Aut}_L(M_n(L))$). You could also follow [Se] X.5 (see Exercises 1, 2), but the end result should be stated using the normalizations of [Lo]. See also [Mi] IV.3, second part (starting after Cor. 3.10, up to and including Lemma 3.15).

9. $\text{Br}(L/K)$ for a cyclic extension L/K (Ma)

Discuss compatibility with field extensions, [Lo] §30 F1 (= [Mi] IV Cor. 3.16). [Lo] §30 F2. Since there is a lot of material to be covered in this talk, you probably have to be sketchy in this part.

Next prove that the Brauer group of a field is a torsion group, [Lo] §30 Theorem 3 (the statement is a more precise version of [Mi] IV Cor. 3.17, but of course we cannot use Milne’s proof). Explain how the proof goes, but do not spend too much time on the technical computations.

The most important part of the talk is a detailed study of the case of a cyclic extension L/K . When the Galois group G is cyclic, show that there is a particularly simple description of $H^2(L/K)$: [Lo] §30.4, in particular Theorem 4:

$$\text{Br}(L/K) \cong H^2(L/K) \cong K^\times / N_{L/K}L^\times \quad \text{for } L/K \text{ cyclic.}$$

We immediately obtain a new proof that the Brauer group of \mathbb{R} consists of 2 elements. Furthermore, use it to prove that the Brauer group of a finite field is trivial.

10. The Brauer group of a local field 1 (Ma)

Our next task is to compute the Brauer group of a non-archimedean local field K (i.e., K is a finite extension field of \mathbb{Q}_p for some prime p , or $K = \mathbb{F}_q((t))$, a Laurent series field over a finite field). See [Lo] §31, cf. also [Mi] IV.4.

Discuss valuations on division algebras and use this occasion to also give a quick reminder on the structure of local fields.

The crucial observation is that every central simple algebra over K has an unramified splitting field, [Lo] §31.3.

Finally compute $K^\times/N_{L/K}L^\times$ for an unramified extension L/K of local fields ([Lo] §31 Theorem 2/Theorem 2') which by the previous talk is isomorphic to $\text{Br}(L/K)$.

11. The Brauer group of a local field 2 (Ma)

Prove that by passing to the union running over all unramified extensions L/K , we obtain an isomorphism

$$\text{Br}(K) \cong \mathbb{Q}/\mathbb{Z} \quad \text{for } K \text{ a non-archimedean local field.}$$

and discuss the more precise results in [Lo] §31.4.

12. Connection with Local Class Field Theory 1 (Ma)

The final topic of the seminar is the relation between the Brauer group of a local field and local class field theory. To get started, note that for a finite group G , we obtain a duality theory by defining the dual group

$$G^\vee := \text{Hom}_{\text{gp}}(G, \mathbb{Q}/\mathbb{Z}) = \text{Hom}_{\text{gp}}(G, \mathbb{C}^\times),$$

the abelian group of group homomorphisms from G to the additive group \mathbb{Q}/\mathbb{Z} , or equivalently to the multiplicative group \mathbb{C}^\times , i.e., we obtain a natural isomorphism $(G^\vee)^\vee = G$ for *abelian* G , and

$$(G^\vee)^\vee \cong G^{\text{ab}} \quad \text{for general finite } G.$$

Here G^{ab} denotes the largest abelian quotient of G , i.e., the quotient of G by its commutator subgroup.

Now let L/K be a Galois extension with Galois group G . Using our description of $\text{Br}(E/K)$ for cyclic E/K , one defines a pairing ([Lo] §32, Def. 1)

$$K^\times \times G^\vee \rightarrow \text{Br}(L/K) \subset \text{Br}(K) \cong \mathbb{Q}/\mathbb{Z}.$$

We obtain a homomorphism

$$(\cdot, L/K): K^\times/N_{L/K}L^\times \rightarrow \text{Gal}(L/K)^{\text{ab}},$$

the *reciprocity map*. Prove that this map is an isomorphism ([Lo] §32, Theorem 1). This statement is one of the key results of local class field theory.

13. Connection with Local Class Field Theory 2 (Ma)

Discuss the local existence theorem (at least if $\text{char } K = 0$) which describes precisely which subgroups in K^\times have the form $N_{L/K}L^\times$ for a finite extension L/K ([Lo] §32 Theorem 2).

Finally, derive the **Local Kronecker-Weber Theorem** from this ([Lo] §32 Theorem 3): The maximal abelian extension \mathbb{Q}_p^{ab} of \mathbb{Q}_p is the extension generated by all roots of unity.

References

- [B] N. Bourbaki, *Algèbre*, Ch. 8, Springer.
- [GS] P. Gille, T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge University Press
- [Hu] T. Hungerford, *Algebra*, Springer Graduate Texts in Mathematics.
- [Lo] F. Lorenz, *Einführung in die Algebra II*, Spektrum Akad. Verlag (in English: *Algebra. Volume II: Fields with structure, algebras, and advanced topics*, Springer Universitext 2008).
- [Mi] J. Milne, *Class Field Theory*, see <http://www.jmilne.org/math/>
- [Sch] W. Scharlau, *Quadratic and Hermitian Forms*, Grundlehren der math. Wiss. **270**, Springer
- [Se] J.-P. Serre, *Corps locaux*, Hermann (in English: *Local Fields*, Springer Graduate Texts in Mathematics)