Noncommutative Algebra, 4$^{\text{th}}$ homework

Benjamin Benčina, 27192018

18. december 2020

Ex. 1: Let Q_1 and Q_2 be quaternion F-algebras with $\operatorname{char} F \neq 2$. We will show the following statements are equivalent:

(a) There exist $a, b, b' \in F^{-1}$ such that $Q_1 \cong \left(\frac{a,b}{F}\right)$ and $Q_2 \cong \left(\frac{a,b'}{F}\right)$.

(b) Q_1 and Q_2 have a common subfield of dimension 2 over F.

(c) Q_1 and Q_2 have a common splitting field of dimension 2 over F.

Firstly, assume that F does indeed have an extension of degree 2 (e.g. F must not be algebraically closed). Such extensions must necessarily be algebraic, namely extended by a single element. Wherever an extension is given, it is given without loss of generality. Secondly, by "the theorem" we refer to a theorem from the lectures from Chapter 4.3, consisting of parts (a) and (b) and describing the relationships between splitting fields (and the relative Brauer group) and self-centralizing fields.

- <u>$(b) \implies (c)$</u>: Let K be such an extension of F with $[K : F] = 2$. Since $C(K)$ is a subalgebra in both Q_1 and Q_2, K must be a self-centralizing field in both Q_1 and Q_2. By part (a) of the theorem, K is a splitting field for both algebras.

- <u>$(a) \implies (b)$</u>: Recall we can always pick a to not be a square (from Homework 2). Consider $K = F(\sqrt{a})$. Since a is not a square, clearly $[K : F] = 2$ and K is a subfield of both Q_1 and Q_2 (we are really looking at $F + iF$).

- <u>$(c) \implies (a)$</u>: Let K be an extension of F with $[K : F] = \deg Q_1 = \deg Q_2 = 2$ that splits both algebras. By part (b) of the theorem, we get that K is a self-centralizing subfield in both Q_1 and Q_2 (incidentally proving (b) on the way). This means $C(K)$ is a subalgebra in both quaternion algebras of dimension 2, generated by $1, c$, where $c \in Q_1 \setminus F, Q_2 \setminus F$. But since $[K : F] = 2$, $c^2 \in F \setminus \{0\}$ (c will be our common basis element i). Denote $a = c^2$ and write $c = y_1 i_1 + z_1 j_1 + w_1 i_1 j_1 \in Q_1$ (without loss of generality we can omit the pure field term). Then clearly c anticommutes with j_1. If we write the analogue for $c \in Q_2$, we see also that c anticommutes with j_2. Hence, we get $Q_1 = \left(\frac{a,b_1}{F}\right)$ and $Q_2 = \left(\frac{a,b_2}{F}\right)$.

Ex. 2: Let A be a central simple k-algebra and $\operatorname{Nrd}\colon A \to k$ its reduced norm. For any $a \in A$ we define the left multiplication $L_a \in \operatorname{End}_k(A)$ by $L_a(x) = ax$ and the unreduced norm by $N(a) = \det(L_a)$. Let us show that $\mathrm{N}(a) = \operatorname{Nrd}(a)^{\deg(A)}$.

Since we are calculating the reduced norm in field extensions and the reduced norm does not depend on the extension we take, we might as well take a splitting extension. It is therefore enough to prove the case for $A \cong M_n(k)$. Now view $A \cong M_n(k)$ as a left $M_n(k)$-module via matrix multiplication. Furthermore, A is isomorphic to a direct sum of its columns, each of them isomorphic to k^n. Then L_a can be viewed as an $n^2 \times n^2$ block-diagonal matrix, each of the $n \times n$ diagonal blocks acting on one of the columns. By definition of L_a, each of these blocks is the matrix a and has determinant $\det(a)$, hence

$$\mathrm{N}(a) = \det L_a = \det(a)^n = \operatorname{Nrd}(a)^{\deg(A)}.$$

Ex. 3: Let A be a central simple F-algebra with $\operatorname{char} F \neq 2$. Let us show that $[A] = [Q] \in \operatorname{Br}(F)$ for some quaternion algebra $Q \iff A$ has a separable splitting field of degree 2.

- $(\Longrightarrow)$: Recall that there are only 2 possibilities for a quaternion algebra, either $Q \cong M_2(F)$ or Q is a central division algebra. In the first case, $[A] = [F] = 1$ in the Brauer group of F, so any extension of F is also splitting[1]. Of course separable extension over F of degree 2 exist, since $\operatorname{char} F \neq 2$ (the problem is that in general they do not split A). In the second case, $A \cong M_n(Q)$ by the Wedderburn Structure Theorem, but Q is a non-commutative central division algebra, so by the Jacobson-Noether Theorem there exists $c \in Q$ which is separable over F. Then $F(c)$ is separable and contained in Q, so by Koethe's Theorem there exists a separable maximal subfield of Q that contains $F(c)$ and splits Q (and hence A). By dimension count, it must have degree 2 over F.

- $(\Longleftarrow)$: Suppose there exists a separable field extension $[K : F] = 2$ that splits A. Suppose in addition that $[A] \neq 1$ in the Brauer group of F. By the Wedderburn Structure Theorem, $A \cong M_m(D)$ for a unique central division F-algebra D. We want to show that $D \cong Q$ for some quaternion division algebra Q, or equivalently, that $\dim_F D = 4$. Notice that by our additional assumption, we have $\dim_F D \geq 4$. Since K splits A and $A \cong M_m(D)$, K splits D as well. Without loss of generality we can view $K \subseteq D$. By the exercise from Tutorials about Koethe's theorem, K is in fact a maximal subfield in D (here we use the fact that K is separable). By the theorem we referenced in (1), since $[K : F] = 2$ and K is maximal in D, it must be the case that $\dim_F D = 4$.

Ex. 4: We will determine the Brauer group of $\mathbb{C}(t)$ and $\mathbb{R}(t)$.

- For the first part we will prove that $\mathbb{C}(t)$ is a C_1-algebra. By an exercise from Tutorials, any central simple algebra over $\mathbb{C}(t)$ will then just be isomorphic to $\mathbb{C}(t)$, so $\operatorname{Br}(\mathbb{C}(t)) = 1$.

  Let F be a homogeneous polynomial of degree d in $\mathbb{C}(t)[f_1, \ldots, f_n]$, where $n > d$. Since we are considering the equation $F \equiv 0$, we can clearly just rid ourselves of the denominators of all coefficients, so $F \in \mathbb{C}[t][f_1, \ldots, f_n]$. Take a natural number $N > 0$ and consider the change of variables
  $$f_i := \Sigma_{j=0}^{N} a_{ij} t^j$$
  for new variables a_{ij}. Now substitute this into F and group by powers of t to obtain the following equation
  $$0 = F(f_1, \ldots, f_n) = \Sigma_{l=0}^{dN+r} F_l(a_{1,0}, \ldots, a_{n,N}) t^l$$
  where r is the maximal degree of all the coefficients of F and F_l are homogeneous polynomials over $\mathbb{C}$ in the variables a_{ij}. This equation has a solution precisely when there exist elements $a_{ij} \in \mathbb{C}$ such that $F_l(a_{1,0}, \ldots, a_{nN}) = 0$ for all $l = 0, \ldots, dN + r$. We now have $dN + r + 1$ equations in $n(N + 1)$ variables, which need to have a common solution in $\mathbb{C}$. Since r is a constant and $d < n$, for a large enough N we have $dN + r + 1 < n(N + 1)$. Since $\mathbb{C}$ is algebraically closed (in particular, it is also infinite and C_1) and we have more variables than (homogeneous) equations in $\mathbb{C}$, we have non-trivial solutions. Hence $\mathbb{C}(t)$ is a C_1-algebra.

- We can immediately see how the above approach fails for $\mathbb{R}(t)$. Indeed, $\mathbb{R}$ is of course not algebraically closed and, say, $F(x, y, z) = x^2 + y^2 + z^2$ has no non-trivial zero, so $\mathbb{R}$ is not a C_1-algebra. Then of course $\mathbb{R}(t)$ cannot be a C_1-algebra as well, since we can view $\mathbb{R}$ as its subalgebra.

  The problem we are facing is by the system of equations in the previous point analogous to the problem of $x^2 = -1$ not having a solution in $\mathbb{R}$. We thus use the proof of Frobenius' Theorem to

[1] Beware that similar considerations as in (1) mush be made, namely, F must allow algebraic extensions. If F is, say, algebraically closed, then no such extensions exist, yet $\operatorname{Br}(F) = 1$.

obtain that $\mathrm{Br}(\mathbb{R}(t)) = \{[\mathbb{R}(t)], [\mathbb{H}(t)]\}$, since $\mathbb{H}(t) \otimes \mathbb{H}(t) \cong (\mathbb{H} \otimes \mathbb{H})(t) \cong M_n(\mathbb{R})(t) \cong M_n(\mathbb{R}(t))$ by examining coefficients[2].

<u>Ex. 5:</u> Let A be a central simple k-algebra. Let $f\colon A \to A$ be an involution of A. We will do the following:

(a) Describe all involutions of A using f.

(b) Show that $M_n(A)$ admits an involution.

(a) By the immediate corollary to the Skolem-Noether Theorem, we have that every $\sigma \in \operatorname{Aut} A$ is inner, so there exists $\alpha \in A$ such that $\sigma(z) = \alpha z \alpha^{-1}$. Then

$$\sigma \circ f(xy) = \alpha f(y) f(x) \alpha^{-1} = \alpha f(y) \alpha^{-1} \alpha f(x) \alpha^{-1} = (\sigma \circ f(y))(\sigma \circ f(x))$$

so $\sigma \circ f$ is again an involution. Also note that since $f\colon A \to A^{\mathrm{op}}$ is a homomorphism (indeed, f is an antihomomorphism), by Skolem-Noether Theorem, these are the only involutions.

(b) We already know that $M_n(k)$ admits an involution, namely the transposition map T. Since $M_n(k) \otimes A \cong M_n(A)$, the map $F = T \otimes f$ is a good candidate. Indeed, by definition of the tensor product, it is clearly both k-linear and $F^2 = id$. To verify it is an involution, calculate

$$F(X \otimes y \cdot Z \otimes w) = F(XZ \otimes yw) = Z^T X^T \otimes f(w) f(y) = Z^T \otimes f(w) \cdot X^T \otimes f(x) = F(Z \otimes w) F(X \otimes y)$$

Here we relied on the lectures that the product of simple tensors is indeed well-defined. Since F is k-linear, extend this calculation to the entire tensor product.

[2] Note that the solution of both points is somewhat motivated by the observation that any finite-dimensional division algebra over $k(t)$ yields a finite-dimensional division algebra over k through coefficients. E.g. any rational function over $\mathbb{H}$ can be seen as a sum of rational functions over $\mathbb{R}$ grouped by the basis of $\mathbb{H}$. Likewise, for the $\mathbb{R}(t)$-algebra $\mathbb{H}(t)$ (still grouped by the basis of $\mathbb{H}$).

Index of comments

3.1 Tu enak dokazne deluje. Br(R(t)) je neštevno neskončna direktna vsota kopij Z/2.

3.2 ali je (\sigma f)^2 = id za vsak sigma.

Zakaj so vse take oblike.