NUMBER THEORY III – WINTERSEMESTER 2016/17

PROBLEM SET 9

HÉLÈNE ESNAULT, LARS KINDLER

Exercise 1. Let k be a field of characteristic $\neq 2$ and let A be a central simple algebra over k such that $\dim_k(A) = 4$. This exercise shows that there are $a, b \in k^\times$, such that A is isomorphic to the generalized quarternion algebra $H(a, b; k)$. By Wedderburn's theorem there exists a division algebra over k, such that $A \cong M_n(D)$ for some $n \geq 1$. Thus either $A \cong M_2(k) = H(1, 1; k)$ or $A \cong D$ is a division algebra. From now on we assume that $A = D$ is a division algebra.

(a) Pick $x \in D \setminus k$ and let $k[x] \subseteq D$ be the sub-k-algebra generated by x. Show that $k[x]$ is a field and that $[k[x] : k] = 2$.
(b) Show that $C_D(k[x]) = k[x]$ where $C_D(k[x])$ is the centralizer of $k[x]$ in D.
(c) Let σ be the unique nontrivial k-automorphism of $k[x]$ and show that there exists $J \in D^\times$ such that $\sigma(y) = JyJ^{-1}$ for all $y \in k[x]$. Show that $J^2 \in k^\times$, and define $b := J^2$.
(d) Pick $I \in k[x]$ and $a \in k^\times$ such that $I^2 = a$. Prove that $D \cong H(a, b; k)$.

Solution. (a) The k-algebra $k[x] \subseteq D$ is commutative and for any $y \in k[x] \setminus \{0\}$ multiplication by y induces an endomorphism of k-vector spaces $m_y : k[x] \to k[x]$. Since left-multiplication by y is an isomorphism on D, m_y is injective. As $\dim_k k[x] < \infty$, m_y is also surjective, that is, there exist $y' \in k[x]$ such that $yy' = 1$. Thus $k[x]$ is a field. If $x \in D \setminus k$, then $k \subsetneq k[x]$, so $[k[x] : k] \geq 2$. But D is a 4-dimensional divison algebra with center k, so any subfield has dimension $\leq \sqrt{4} = 2$. Thus $[k[x] : k] = 2$.

(b) Since $k[x]$ is a maximal subfield of D, you know from the lecture that $C_D(k[x]) = k[x]$.

(c) For $\sigma \in \mathrm{Gal}(k[x]/k) \setminus \{\mathrm{id}\}$ we know that $\sigma^2 = \mathrm{id}$. By the Noether-Skolem theorem, there exists $J \in D^\times$ such that $\sigma(y) = JyJ^{-1}$ for every $y \in k[x]$. It follows that

$$y = \sigma^2(y) = J^2 y (J^{-1})^2$$

for every $y \in k[x]$, so $J^2 \in C_D(k[x]) = k[x]$. Since $\sigma \neq \mathrm{id}$, $J \notin k[x]$. Thus $[k[J] : k] = 2$. It follows that $k[J]$ is a quadratic extension of k with $k[J] \cap k[x] = k$. But $J^2 \in k[J] \cap k[x]$, so $J^2 \in k$. Write $b := J^2$.

(d) As $k[x]$ is a quadratic extension of k there exists $I \in k[x]$ such that $I^2 \in k$. Indeed, if $T^2 + \lambda T + \mu \in k[T]$ is the minimal polynomial of x over k, then

$$\left(x + \frac{\lambda}{2}\right)^2 = x^2 + \lambda x + \frac{\lambda^2}{4} = (-\lambda x - \mu) + \lambda x + \frac{\lambda^2}{4} \in k$$

Write $a := I^2$. Then $\sigma(I) = -I$ and hence $-I = JIJ^{-1}$, so $IJ = -JI$.

It remains to see that $1, I, J, IJ$ is a basis of D. Let V be the k-subvector space of D spanned by $1, I, J, IJ$. We show that $\dim_k V = 4$.

It is easy to see that V is actually a subalgebra of D, as $I^2, J^2 \in k$, $JI = -IJ \in V$. Moreover, V is a division algebra: For any $y \in V \setminus \{0\}$, multiplication by y induces an injective, k-linear morphism $V \to V$, as multiplication by y is injective on D. Thus multiplication by y induces a bijective endomorphism $V \to V$, so V is a division algebra.

If you want your solutions to be corrected, please hand them in just before the lecture on January 3, 2017. If you have any questions concerning these exercises you can contact Lars Kindler via `kindler@math.fu-berlin.de` or come to Arnimallee 3, Office 109.

We know that $k \subseteq Z(V)$ and that $[V : Z(V)] \leq [V : k] \leq [D : k] = 4$. Moreover $[V : Z(V)]$ is a square, thus either $= 1$ or $= 4$. But we know that V is not commutative: $IJ - JI = 2IJ \neq 0$ as $\mathrm{char}(k) \neq 2$. Thus $V \neq Z(V)$, so $Z(V) = k$ and $[V : k] = 4$. It follows that $D = V$ and that $\{1, I, J, IJ\}$ is a basis of D over k, and hence, as we proved in previous exercises, $D \cong H(a, b; k)$.

Exercise 2. Let D be a finite division algebra and let k denote its center (a finite field).

(a) Remark that $\dim_k(D) = n^2$ for some $n \in \mathbb{N}$.
(b) Use the Noether-Skolem theorem to show that if $L \subseteq D$ is a maximal subfield then $D^\times = \bigcup_{\alpha \in D^\times} \alpha L^\times \alpha^{-1}$ as abelian groups.
(c) Conclude that $L = D$.
(d) Conclude that the Brauer group of a finite field is trivial.

Solution. (a) From the lecture we know that $\dim_k D$ is a square, say $\dim_k D = n^2$.

(b) If $L \subseteq D$ is a maximal subfield, then $[L : k] = n$. As k is a finite field, every extension of k of degree exactly n is k-isomorphic to L. Thus, by the theorem of Noether-Skolem, the set of maximal subfields of D is $\{\alpha L \alpha^{-1} \subseteq D | \alpha \in D^\times\}$. As we saw before, every element of D is contained in a maximal subfield, so $D = \bigcup_{\alpha \in D} \alpha L \alpha^{-1}$ and$D^\times = \bigcup_{\alpha \in D^\times} \alpha L^\times \alpha^{-1}$

(c) If $L^\times \subsetneqq D^\times$, then $D^\times \neq \bigcup_{\alpha \in D^\times} \alpha L^\times \alpha^{-1}$, as the following lemma shows:

Lemma. *Let G be a* finite *group and $H \subsetneqq G$ a proper subgroup. Then $\bigcup_{g \in G} gHg^{-1} \subsetneqq G$.*

Proof. Write $n = |G|$, $m = |H|$ and $r = [G : H] = n/m$. Then

$$\left| \bigcup_{g \in G} gHg^{-1} \right| \leq r \cdot \underbrace{(m-1)}_{|H \setminus \{1\}|} + \underbrace{1}_{<r} < r \cdot m = n = |G|$$

□

Thus $D^\times = L^\times$ and hence $D = L$.

(d) We have just proved: Every division algebra with finite center is commutative. Now let k be a finite field and A a central simple algebra over k. Wedderburn's theorem states that $A \cong M_n(D)$ for some division algebra D. From the lecture you know that $k = Z(A) \cong Z(M_n(D)) \cong Z(M_n(k) \otimes_k D) \cong Z(M_n(k)) \otimes_k Z(D) \cong Z(D)$. Thus D is central and commutative, so $D = k$. Thus element of $\mathrm{Br}(k)$ is trivial.

Exercise 3. Let K be a nonarchimedean local field, i.e. a complete discretely valued field with finite residue field k. We assume that $\mathrm{char}(K) = 0$ and as usual write $\mathcal{O}_K$ for the valuation ring of K, and $\mathfrak{m}_K$ for its maximal ideal.

(a) Let D be a central division algebra over K, with $[D : K] = n^2$. Prove the following statements.
  (i) The absolute value $|\cdot|$ on K extends uniquely to an absolute value on D, i.e., to a map $D \to \mathbb{R}_{\geq 0}$ such that $|x| = 0$ iff $x = 0$, and such that for all $x, y \in D$ we have $|xy| = |x||y|$ and $|x + y| \leq \max\{|x|, |y|\}$.
  (ii) If $q = \#k$, define the "valuation v_D" such that $|x| = (1/q)^{v_D(x)}$ for all $x \in D$. Define

$$\mathcal{O}_D := \{x \in D | v_D(x) \geq 0\}, \quad \mathfrak{m}_D := \{x \in D | v_D(x) > 0\}.$$

  Show that $\mathcal{O}_D$ consists of the elements of D which are integral over $\mathcal{O}_K$.
  (iii) $\mathfrak{m}_D$ is a two-sided ideal in $\mathcal{O}_D$ and $\mathfrak{m}_K \mathcal{O}_D = \mathfrak{m}_D^e$ for some $0 < e \leq n$.
  (iv) $d := \mathcal{O}_D / \mathfrak{m}_D$ is a field and $f := [d : k] \leq n$.

(v) $\mathcal{O}_D$ is a free $\mathcal{O}_K$-module of rank

$$n^2 = \dim_k(\mathcal{O}_D/\mathfrak{m}_K\mathcal{O}_D) = ef.$$

(vi) Conclude that $e = f = n$.

(vii) Write $d = \mathcal{O}_D/\mathfrak{m}_D\mathcal{O}_D = k[a]$ and let $\alpha \in D$ be a lift of a. Then $K[\alpha]$ is a maximal subfield of D and splits D. Show that $K[\alpha]/K$ is unramified.

(b) If D/K is a central division algebra, and $L \subseteq D$ a maximal subfield unramified over K, then L/K is Galois with Galois group $\mathrm{Gal}(d/k)$. Let $\sigma \in \mathrm{Gal}(L/K)$ be the lift of the Frobenius automorphism of d/k. Show that there exists $\alpha \in D$ such that $\sigma(x) = \alpha x \alpha^{-1}$ for all $x \in L$. Show that $v_D(\alpha) \mod \mathbb{Z}$ is independent of the choice of α.

(c) Show that the above construction gives a well-defined map $\mathrm{inv}_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$, $[D] \mapsto \alpha \mod \mathbb{Z}$. We will prove next year that inv_K is in fact an isomorphism.

Solution.

(a) (i) I gave a complete proof in the exercises. For $x \in D$ define $|x|_D := |x|_{K[x]}$, where $K[x]$ is the subfield of D spanned by x. We know that the absolute value of K extends uniquely to $K[x]$, so this defines a map $|\cdot|_D : D \to \mathbb{R}_{\geq 0}$ which is unique as an extension of the absolute value on K. To see that this is in fact a norm, we showed that if $n^2 = \dim_K D$, then $|x|_D = |\det(m_x)|^{1/n^2}$, where $m_x \in \mathrm{End}_K(D)$ is left-multiplication by x. This formula immediately implies that $|\cdot|_D$ is multiplicative, so that it suffices to check that $|1+x|_D \leq 1$ if whenever $|x| \leq 1$ for $x \in D$. But this is clear, as $1 + x \in K[x]$.

(ii) As usual we can write $\mathcal{O}_D = \{x \in D || x|_D \leq 1\}$ and $\mathfrak{m}_D = \{x \in D || x|_D < 1\}$. Then $x \in \mathcal{O}_D$ if and only if $x \in \mathcal{O}_{K[x]}$ if and only if x is integral over $\mathcal{O}_K$.

(iii) Since $|\cdot|_D$ is is multiplicative, $\mathfrak{m}_D$ is a two-sided ideal. Observe that $|\cdot|_D$ is discrete. Indeed, if for any field $L \subseteq D$ contained in D we define v_L via the relation $|x|_K = 1/q^{v_L(x)}$, $x \in L^\times$, then for any $x \in D^\times$ we have $v_D(x) \in \frac{1}{n}\mathbb{Z}$. Indeed, $v_D(x) = v_{K[x]}(x)$ and as $K[x]$ is contained in a maximal subfield of D, $[K[x] : K] | n$. If $e_{K[x]}$ is the ramification index of $K[x]$, then $e_{K[x]} | n$ and $\mathrm{im}(v_{K[x]}) = \frac{1}{e_{K[x]}}\mathbb{Z} \subseteq \frac{1}{n}\mathbb{Z}$.
Now let $\pi_D \in \mathfrak{m}_D$ be an element such that $|\pi_D|$ is maximal, i.e., π_D is an element of $\mathcal{O}_D$ with maximal absolute value < 1. We show that for any $e \geq 1$, $\mathfrak{m}_D^e$ can be written as $\pi_L^e\mathcal{O}_D$. Clearly $\pi_L^e\mathcal{O}_D \subseteq \mathfrak{m}_D^e$. Conversely, if $x_1, \ldots, x_e \in \mathfrak{m}_D$, then $|\pi_D^{-e} x_1 \cdot \ldots \cdot x_e|_D = |\pi_D|_D^{-e} \prod_i |x_i|_D \leq 1$, so $\pi_D^{-e} x_1 \cdot \ldots \cdot x_e \in \mathcal{O}_D$ which implies that $x_1 \cdot \ldots \cdot x_e \in \pi_D^e\mathcal{O}_D$. Since any element of $\mathfrak{m}_D^e$ is a sum of products of e elements of $\mathfrak{m}_D$, it follows that $\mathfrak{m}_D^e = \pi_D^e\mathcal{O}_D$.[1]
As π_D has maximal absolute value < 1, the same is true for $\pi_D \in K[\pi_D]$. Thus π_D is a uniformizer in $\mathcal{O}_{K[\pi_D]}$. Thus, if we fix a uniformizer π_K of $\mathcal{O}_K$, then there exists $1 \leq e \leq n$ and a unit $u \in \mathcal{O}_{K[\pi_D]}^\times$, such that $\pi_K u = \pi_D^e$. This shows that $\mathfrak{m}_D^e = \pi_D^e\mathcal{O}_D = \pi_K\mathcal{O}_D$ with $1 \leq e \leq n$.

(iv) Note that $\mathcal{O}_D^\times = \mathcal{O}_D \setminus \mathfrak{m}_D$, so $d = \mathcal{O}_D/\mathfrak{m}_D$ is a division algebra over k. But k is a finite field, so d is a field. Write $f := [d : k]$ and $d = k(a)$. If $\alpha \in \mathcal{O}_D$ is a lift of a, then $K[\alpha] \subseteq D$ is a subfield with residue field containing d. Thus $f = [d : k] \leq [K[\alpha] : K] \leq n$.

(v) Note that $\mathcal{O}_K \subseteq Z(D)$, so we do not have to worry about distinguishing left- or right-$\mathcal{O}_K$-structures on $\mathcal{O}_D$. As D is a division algebra, $\mathcal{O}_D$ is a domain containing $\mathcal{O}_K$ as a subring, so $\mathcal{O}_D$ is a torsion free $\mathcal{O}_K$-module.
Let $\bar{e}_1, \ldots, \bar{e}_r$ be a k-basis of d and let $e_1, \ldots, e_r \in \mathcal{O}_D$ be lifts. The elements $e_1, \ldots, e_r$ are linearly independent over $\mathcal{O}_K$. Otherwise there would exist a relation

[1] This might look a little bit strange, as we are dealing with two-sided ideals. But note that $|x\pi_D| = |\pi_D x|$, so there always is a way to write $x\pi_D$ as an element of $\pi_D\mathcal{O}_D$: $u := (\pi_D x)^{-1} x\pi_D \in \mathcal{O}_D^\times$, so $\pi_D x \cdot u = x\pi_D$.

$0 = \sum_{i=1}^r a_i e_r$ with some $a_j \in \mathcal{O}_K^\times$ (take any relation with nonzero coefficients from $\mathcal{O}_K$ and devide by a suitable power of the uniformizer). But this would imply that the $\bar{e}_1, \ldots, \bar{e}_r$ are not linearly independent over k.

Consider the free $\mathcal{O}_K$-submodule $E := \bigoplus_{i=1}^r e_i \mathcal{O}_K \subseteq \mathcal{O}_D$. For $b \in \mathcal{O}_D$ we can write $b = c_0 + \pi_K b_1$, with $c_0 \in E$, $b_1 \in \mathcal{O}_D$. The same is true for b_1, etc. Thus $b = c_0 + c_1\pi_K + c_2\pi_K^2 + \ldots + c_n\pi_K^n + b_{n+1}\pi_K^{n+1}$, for any n with $c_i \in E$ and $b_{n+1} \in \mathcal{O}_D$. In other words, $b \mod \mathfrak{m}_K^{n+1} \in E/\mathfrak{m}_K^{n+1}E$ for every n. But as $\mathcal{O}_K$ is complete, so is the free, finite rank $\mathcal{O}_K$-submodule E of $\mathcal{O}_D$. Thus $b \in E \cong \varprojlim_n E/\mathfrak{m}_K^n E$ and $\mathcal{O}_D = E \cong \mathcal{O}_K^r$, where $r = \dim_k \mathcal{O}_D/\mathfrak{m}_K\mathcal{O}_D$.

Finally, as in the commutative case, one sees that $K \otimes_{\mathcal{O}_K} \mathcal{O}_D \to D$, $a \otimes b \mapsto ab$, is an isomorphism of K-vector spaces.

Thus

$$\operatorname{rank}_{\mathcal{O}_K} \mathcal{O}_D = \dim_K(K \otimes_{\mathcal{O}_K} \mathcal{O}_D) = \dim_K D = n^2.$$

On the other hand $\operatorname{rank}_{\mathcal{O}_K} \mathcal{O}_D = \dim_k \mathcal{O}_D/\mathfrak{m}_K\mathcal{O}_D = ef$. Indeed, we saw that $\mathfrak{m}_K\mathcal{O}_D = \mathfrak{m}_D^e$, and $\mathfrak{m}_D^n/\mathfrak{m}_D^{n+1}$ is a 1-dimensional k-vector space spanned by π_D^n, and for every n there is a short exact sequence

$$0 \to \mathfrak{m}_D^n/\mathfrak{m}_D^{n+1} \to \mathcal{O}_D/\mathfrak{m}_D^{n+1} \to \mathcal{O}_D/\mathfrak{m}_D^n \to 0.$$

By induction it follows that $\dim_k \mathcal{O}_D/\mathfrak{m}_D^e = e \cdot \dim_k \mathcal{O}_D/\mathfrak{m}_D = e \cdot f$.

(vi) We know that $e \leq n$, $f \leq n$ and $ef = n^2$, so $e = f = n$.

(vii) Write $d = k(a)$ and let $\alpha \in \mathcal{O}_D$ be a lift of a. Then $K[\alpha]$ is a subfield of D with $[K[\alpha] : K] \geq [k(a) : k] = f = n$. But subfields of D have degree $\leq n$, so $[K[\alpha] : K] = n$ and $K[\alpha]$ is a maximal subfield of D. Thus it splits D. Moreover, as $\alpha \in \mathcal{O}_D$, α is integral over $\mathcal{O}_K$ and thus the residue field of $K[\alpha]$ contains d and for degree reasons it is precisely d. This means that $K[\alpha]/K$ has the same degree as its residue extension, so $K[\alpha]$ is unramified over K.

(b) Let D/K be a central division algebra of rank n^2 and L a maximal subfield which is unramified over K. The residue field of L is the unique extension of degree n of the finite field k, hence it is d. Moreover $\operatorname{Gal}(L/K) = \operatorname{Gal}(d/k)$; let $\sigma \in \operatorname{Gal}(L/K)$ be the lift of the Frobenius automorphism of d/k. By the Noether-Skolem theorem, there exists $\alpha \in D$ such that $\sigma(y) = \alpha y \alpha^{-1}$ for every $y \in L$. If $\alpha' \in D$ is a second such element, then

$$\alpha y \alpha^{-1} = \alpha' y \alpha'^{-1}$$

for all $y \in L$, so $\alpha^{-1}\alpha' \in C_D(L) = L$. As L/K is unramified $v_D(L) = v_L(L) \subseteq \mathbb{Z}$, so $v_D(\alpha) = v_D(\alpha') \mod \mathbb{Z}$. Write $\operatorname{inv}_L(D) := v_D(\alpha) \mod \mathbb{Z}$.

If $L' \subseteq D$ is a second maximal subfield unramified over K, then $L \cong L'$ as extensions of K, as the isomorphism class of an unramified extension of K is determined by its degree. Thus, again by the Noether-Skolem theorem, there exists an element $\beta \in D$ such that $L = \beta L' \beta^{-1}$. If $\sigma' : L' \to L'$ is a lift of the Frobenius automorphism, then

$$y \mapsto \beta^{-1}\sigma'(\beta y \beta^{-1})\beta$$

is a lift of Frobenius to L. If σ' is conjugation by α', then

$$\operatorname{inv}_L(D) = v_D(\beta^{-1}\alpha'\beta) \mod \mathbb{Z} = v_D(\alpha') \mod \mathbb{Z} = \operatorname{inv}_{L'}(D).$$

Thus $\operatorname{inv}_L(D)$ does not depend on L, and we write $\operatorname{inv}(D) := \operatorname{inv}_L(D)$.

From the construction it is clear that if $D \cong D'$ are two isomorphic central division algebras over K, then $\operatorname{inv}(D) = \operatorname{inv}(D')$, because any such isomorphism preserves the (unique) absolute value on D extending the absolute value on K.

(c) Every class of $\operatorname{Br}(K)$ is represented by a central division algebra D over K, which is unique up to isomorphism. Thus inv defines a map $\operatorname{Br}(K) \to \mathbb{Q}/\mathbb{Z}$.