8. December 2014

Exercise 9 for Number theory III[1]

Kay Rülling

Exercise 9.1. Let k be a field and A a central simple k-algebra. We define the *reduced norm* $\mathrm{Nrd} : A \to k$ as follows: Let L/k be a splitting field for A and pick an isomorphism of k-algebras $\varphi : A \otimes_k L \xrightarrow{\simeq} M_n(L)$. Then for $a \in A$ set

$$\mathrm{Nrd(a)} := \det(\varphi(a \otimes 1)).$$

(1) Show that $\mathrm{Nrd}(a)$ is independent of the choice of the isomorphism φ.
(2) Show that $\mathrm{Nrd}(a)$ is independent of the choice of L.
(3) Show that $\mathrm{Nrd}(a) \in k$. (*Hint:* Use that one can always find a finite Galois extension L/K which splits A.)
(4) Show that $\mathrm{Nrd}(ab) = \mathrm{Nrd}(a)\mathrm{Nrd}(b)$.
(5) For $a \in A$ denote by $\mathrm{Nm}_{A/k}(a) := \det(\mu_a)$ the norm of a (here $\mu_a : A \to A$ is the k-linear endomorphism given by $\mu_a(b) = ab$). Show that $\mathrm{Nm}_{A/k}(a) = \mathrm{Nrd}(a)^n$, where $[A : k] = n^2$.
(6) For $a \in A$ show that

$$\mathrm{Nrd}(a) \in k^\times \Leftrightarrow \mathrm{Nm}_{A/k}(a) \in k^\times \Leftrightarrow a \in A^\times.$$

(*Hint:* Use that $\mathrm{Nm}_{A/k}(a) \in k^\times$ is equivalent to $\mu_a : A \to A$ being bijective.)

Exercise 9.2. Let A be a central simple k-algebra and let $e_1, \ldots, e_{n^2} \in A$ be a k-basis of A. Let L be a splitting field for A, which we can assume to be finite over k.

(1) Show that there is a homogeneous polynomial $N \in L[x_1, \ldots, x_{n^2}]$ of degree n, such that

$$\mathrm{Nrd}(\sum_{i=1}^{n^2} \lambda_i e_i) = N(\lambda_1, \ldots, \lambda_{n^2}), \quad \text{for all } \lambda_i \in k.$$

(2) Show that if k is infinite, then $N \in k[x_1, \ldots, x_{n^2}]$. (*Hint:* Use that $N(\lambda_1, \ldots, \lambda_{n^2}) \in k$, for all $\lambda_i \in k$.)

[1]This exercise sheet will be discussed on December 19. If you have questions or remarks please contact `kay.ruelling@fu-berlin.de` or `kindler@math.fu-berlin.de` or `l.zhang@fu-berlin.de`

(3) Show that also if k is finite, then $N \in k[x_1, \dots, x_{n^2}]$. (*Hint:* First use (2) for $A \otimes_k k(y)$ and conclude that N has coefficients in $L \cap k(y) = k$.)

Exercise 9.3. In this exercise we want to prove the following version of the Theorem of Chevalley-Warning:
Let $\mathbb{F}_q$ be a finite field with $q = p^s$ elements and $f \in \mathbb{F}_q[x_1, \dots, x_n]$ a non-constant homogeneous polynomial of degree $\deg(f) < n$. Then there exists an element $(a_1, \dots, a_n) \in \mathbb{F}_q^n \backslash \{(0, \dots, 0)\}$ with $f(a_1, \dots, a_n) = 0$.
Proceed as follows:

(1) Show that for $n \geq 0$ we have

$$\sum_{a \in \mathbb{F}_q} a^n = \begin{cases} -1, & \text{if } n \geq 1 \text{ and } q-1|n, \\ 0, & \text{else.} \end{cases}$$

(Here we use the convention $a^0 = 1$, for all $a \in \mathbb{F}_q$ including $a = 0$.)

(2) Show that if $m = x_1^{r_1} \cdots x_n^{r_n}$ is a monomial with $\sum_{i=1}^n r_i < n(q-1)$, then $\sum_{a \in \mathbb{F}_q^n} m(a) = 0$.

(3) Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$ be as above. Set $V = \{a \in \mathbb{F}_q^n \mid f(a) = 0\}$ and $P := 1 - f^{q-1} \in \mathbb{F}_q[x_1, \dots, x_n]$. Show that

$$P(a) = \begin{cases} 1, & \text{if } a \in V \\ 0, & \text{if } a \notin V. \end{cases}$$

(4) Conclude from (3), that $|V| = \sum_{a \in \mathbb{F}_q^n} P(a)$.

(5) Conclude from (2), that $|V| \equiv 0 \bmod p$.

(6) Conclude the statement.

Definition 1. *Let k be a field. We say that k is a C1 field if any non-constant homogeneous polynomial $f \in k[x_1, \dots, x_n]$ of degree $\deg(f) < n$ has a non-trivial zero in k^n, i.e. there exists a vector $(a_1, \dots, a_n) \in k^n \setminus \{(0, \dots, 0)\}$ with $f(a_1, \dots, a_n) = 0$.*

C1 are: Algebraically closed fields (clear), finite fields (Theorem of Chevalley-Warning, see above), fields which have transcendence degree 1 over an algebraically closed field (Tsen's Theorem) and complete discrete valuation fields with algebraically closed residue field, e.g. $\mathbb{Q}_p^{\mathrm{ur}}$ (Theorem of Lang).

Exercise 9.4. Let k be a C1 field. Show that the Brauer group of k is trivial, $\mathrm{Br}(k) = 0$. (*Hint:* Use Exercise 9.1, (6) and Exercise 9.2 to show that there is no non-trivial central division k-algebra.)