April 19th, 2013

Zahlentheorie II

Exercise sheet 3

Exercise 1 (2 Points)**.** Let K be a finite extension of $\mathbb{Q}$, and $\mathcal{O}_K$ the integral closure of $\mathbb{Z}$ in K. Show that the Dedekind domain $\mathcal{O}_K$ has infinitely many prime ideals.

Exercise 2 (Trace maps, 4 points)**.** Let K be a field and R a commutative K-algebra with unit, which is finite dimensioal as K-vector space. For $x \in R$, multiplication by x induces a homomorphism of K-vector spaces $R \to R$, $r \mapsto xr$, and we write $\mathrm{Tr}_{R/K}(x) \in K$ for its trace. (Recall that for an endomorphism $\phi : V \to V$ of a finite dimensional K-vector space V, the trace $\mathrm{Tr}(\phi)$ is the sum of the diagonal elements of any matrix representing ϕ.)

Prove the following statements:

(1) $\mathrm{Tr}_{R/K}$ defines a K-linear map $R \to K$.

(2) (*Transitivity of the trace*) If L is a finite field extension of K, and R a finite dimensional L-algebra, then

$$\mathrm{Tr}_{R/K} = \mathrm{Tr}_{L/K}\mathrm{Tr}_{R/L}.$$

(3) If R, S are finite dimensional K-algebras, then the cartesian product $R \times S$ is a finite dimensional K-algebra, and $\mathrm{Tr}_{(R\times S)/K}((x, y)) = \mathrm{Tr}_{R/K}(x) + \mathrm{Tr}_{S/K}(y)$ for all $(x, y) \in R \times S$.

(4) (*Base change formula*) If R is a finite dimensional K-algebra and L/K an algebraic extension (not necessarily finite), then $\mathrm{Tr}_{(R\otimes_K L)/L} = \mathrm{Tr}_{R/K} \otimes_K L$, i.e.

$$\mathrm{Tr}_{(R\otimes_K L)/L}(x \otimes y) = y\mathrm{Tr}_{R/K}(x)$$

for all $x \otimes y \in R \otimes_K L$.

Exercise 3 (6 Points)**.** Let K be a field. A polynomial $f(x) \in K[x]$ is called *separable* if $f(x)$ does not have multiple zeroes in an algebraic extension of K. Let L/K be an algebraic field extension. An element $\alpha \in L$ is called *separable over* K if the minimal polynomial $m_\alpha(x) \in K[x]$ of α is separable. An algebraic extension extension L/K is called *separable* if every element of L is separable over K.

Let K be a field. For a polynomial $f(x) = \sum_{i=0}^n a_i x^i \in K[x]$ we write $f'(x) := \sum_{i=1}^n i \cdot a_i x^{i-1}$ for its *formal derivative*.

(1) If $f(x) \in K[x]$ is a polynomial, then $f(x)$ is separable if and only if $f(x)$ is coprime to $f'(x)$, i.e. if the ideal spanned by $f(x)$ and $f'(x)$ is $K[x]$.

(2) If K is of characteristic 0, every algebraic extension L of K is separable over K.

(3) If K has characteristic $p > 0$, and if $f(x) \in K[x]$ is an irreducible polynomial, show that there exists a unique integer $k \geq 0$ and a unique *separable* irreducible polynomial $f_{\mathrm{sep}}(x) \in K[x]$, such that $f(x) = f_{\mathrm{sep}}(x^{p^k})$.

(4) If K is a field of characteristic $p > 0$, show that the map $(K, +) \to (K, +)$, $\lambda \mapsto \lambda^p$ is an injective morphism of abelian groups. The field K is called *perfect* if the above map is bijective.

(5) If K is a perfect field of characteristic $p > 0$, then every algebraic extension L of K is separable.

(6) Give an example of an inseparable finite extension. (Hint: Think about the field of rational functions $\mathbb{F}_p(x)$).

Exercise 4 (Primitive Element Theorem, 3 points)**.** Let L/K be a finite extension and assume that it only has finitely many subextensions, i.e. that there are only finitely many fields M with $K \subsetneq M \subsetneq L$. Show that there exists an $\alpha \in L$ such that $L = K(\alpha)$. (Hint: There are two cases: K is a finite field, and K is an infinite field. The first case follows from the general structure of finite fields. For the second case: Reduce the problem to $L = K(\beta_1, \beta_2)$ and find $\lambda \in K$ such that $L = K(\beta_1 + \lambda\beta_2)$).

It is a consequence of Galois theory that a finite *separable* extension L/K only has finitely many subextensions (you do not need to prove this).

Exercise 5 (Separable extensions, 4 Points)**.** Show that the following statements about a finite extension $K \subset L$ of fields are equivalent (Hint: Exercise 3, (3) can be helpful.)

(1) L/K is separable.
(2) The trace map $\mathrm{Tr}_{L/K} : L \to K$ is not constant 0.
(3) The map $T : L \times L \to K$, $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ is a nondegenerate symmetric K-bilinear form. (Recall: K-bilinear means that the maps $T(-, x)$ and $T(x, -)$ are K-linear for every $x \in L$, and nondegenerate means that for every $x \in L \setminus \{0\}$, there is $y \in L$ such that $T(x, y) \neq 0$.)
(4) The extension L/K is generated by a separable element, i.e. $L = K(\alpha)$, with α separable over K.

Hints.

(1) $\Rightarrow$ (2)**:** Reduce to the case $L = K(\alpha)$ by using the transitivity of the trace (Exercise 2), and the fact that $\mathrm{Tr}_{L/K}$ is either 0 or surjective because it is a K-linear map to the 1-dimensional K-vector space K.

Next let $\overline{K}$ be an algebraic closure of K, and consider the finite dimensional $\overline{K}$-algebra $K(\alpha) \otimes_K \overline{K}$. Show that it is a finite cartesian product of fields which are isomorphic to $\overline{K}$, by using that $K(\alpha) = K[x]/(m_\alpha(x))$ and that α is separable. Here $m_\alpha(x)$ is the minimal polynomial of α. Now use Exercise 2, (3) to conclude the argument.

(2) $\Rightarrow$ (1)**:** If L/K is not separable, there exists $\alpha \in L$ which is not separable over K. Again use the transitivity of the trace to reduce to the case $L = K(\alpha)$ with α inseparable. Now we use the same trick as in the previous direction: Think about the $\overline{K}$-algebra $K(\alpha) \otimes_K \overline{K}$ and show that $\mathrm{Tr}_{K(\alpha)\otimes_K \overline{K}/\overline{K}} = 0$. Conclude that $\mathrm{Tr}_{K(\alpha)/K} = 0$ by using the base-change formula and the fact that a linear map $\phi : V \to W$ of K-vector spaces is 0 if and only if the base changed map $\phi \otimes \mathrm{id}_{\overline{K}} : V \otimes_K \overline{K} \to W \otimes_K \overline{K}$ is 0.

(2) $\Leftrightarrow$ (3)**:** This is entirely formal.

(1) $\Rightarrow$ (4)**:** This is Exercise 4.

(4) $\Rightarrow$ (2)**:** See the hints for (1) $\Rightarrow$ (2).

Exercise 6 (6 Points)**.** Let k be an algebraically closed field of characteristic $p > 0$. Consider the discrete valuation ring $R := k[\![t]\!]$ and its fraction field $K := k(\!(t)\!)$. Let $L = K(\!(t)\!)[u]/(u^p - u - 1/t)$, and define S to be the integral closure of R in L.

(1) Show that L/K is a finite, separable extension.
(2) Show that $u \notin S$, but $u^{-1} \in S$. Let $\mathfrak{P}$ a prime ideal of S containing u^{-1}, and write $t = (u^{-1})^n v$ for some $v \in S \setminus \mathfrak{P}$ and some $n \in \mathbb{N}$. Conclude that S is a discrete valuation ring, i.e. a local Dedekind domain. (Hint: Use the formula

$$[L : K] = \sum_{\mathfrak{P}|(t)} e_{\mathfrak{P}} f_{\mathfrak{P}}$$

from Proposition 10 of Serre's *Local fields*.)

(3) From your computation in the previous part of the exercise, find an uniformizer for S, and read off the ramification index of the maximal ideal of S over the maximal ideal of R.

At the latest, hand in your solutions on **May 8**. For questions, feel free to send an email to `kindler@math.fu-berlin.de` or come to A3.112A.