May 7th, 2014

Algebraic Number Theory

Prof. H. Esnault

Exercise sheet 4[1]

Exercise 1. Let $A \subseteq B$ be an extension of rings. Assume that B is a free A-module of rank n. Then for any $b \in B$ there is a homomorphism of A-modules

$$m_b : B \to B$$

sending $x \mapsto xb$ for all $x \in B$. If $\{e_1, e_2, \cdots, e_n\}$ is a basis for the free A-module B, then there is a $n \times n$-matrix M_b with entries in A which corresponds uniquely to the A-linear map m_b. We define the *norm* of B/A to be the function

$$N_{B/A} : B \to A$$

sending $b \mapsto \det(M_b)$.

(1) Show that if we choose another basis $\{e'_1, e'_2, \cdots, e'_n\}$ of B then we get the same norm function. Thus the notion of norm is well defined. This justifies the notation $N_{B/A}$.

(2) Show the following equalities:
   (a) $N_{B/A}(bb') = N_{B/A}(b)N_{B/A}(b')$ for $b, b' \in B$;
   (b) $N_{B/A}(a) = a^n$ for $a \in A$.

Exercise 2. Let $K \subseteq L$ be a finite field extension of degree n, $b \in L$, m be the degree of the extension $K \subseteq K[b]$, $r = \frac{n}{m}$.

(1) Show that there is a unique monic polynomial $f(X) \in K[X]$ which satisfies
   (a) $f(b) = 0$;
   (b) for any polynomial $g(X) \in K[X]$ with the property that $g(b) = 0$ we have $f(X)|g(X)$.

   Such a polynomial is called the *minimal polynomial* of b over K. What is the degree of $f(X)$?

(2) Show that
$$N_{L/K}(b) = (N_{K[b]/K}(b))^r.$$

(3) Let $f(X) = X^m + c_{m-1}X^{m-1} + \cdots + c_0 \in K[T]$ be the minimal polynomial of b over K. Show that $N_{K[b]/K} = (-1)^m c_0$.

[1] If you want your solutions to be corrected, please hand them in just before the lecture on May 14th. If you have any questions concerning these exercises you can contact Lei Zhang via l.zhang@fu-berlin.de or come to Arnimallee 3 112A.

(4) Let $f(X)$ be the minimal polynomial of b over K. Let $b_1 := b, b_2, b_3, \cdots, b_m$ be the roots of $f(X)$ in the algebraic closure of L. Show that

$$N_{L/K}(b) := (b_1 b_2 b_3 \cdots b_m)^r.$$

(5) Assume that L/K is separable. Let $\sigma_1, \sigma_2, \cdots, \sigma_n$ be distinct embeddings from L to the algebraic closure $\bar{L}$ of L which stablizes K, i.e. $\sigma_i : L \to \bar{L}$ are ring homomorphisms which satisfy $\sigma_i(s) = s$ for all $s \in K$, where i ranges from 1 to n. Show that

$$N_{L/K}(b) = \sigma_1(b)\sigma_2(b) \cdots \sigma_n(b).$$

Is it still true when L/K is not separable?

(6) Show that if L/K is separable and $K \subseteq K' \subseteq L$ is a subextension, then we have

$$N_{L/K} = N_{K'/K} \circ N_{L/K'}.$$

(Remark: this formula is also true when L/K is not separable, but one needs more work to do this.)

(7) Let A be a integrally closed domain with quotient field K. Show that if $b \in L$ is integral over A then $N_{L/K}(b) \in A$.

Exercise 3. Let p be a prime number, $\mathbb{F}_p$ be the finite field of p elements. Consider the field $K := \mathbb{F}_p(t)$, the degree 1 transcendental extension of $\mathbb{F}_p$. The equation $X^p - t$ has a solution in the algebraic closure $\bar{K}$ of K which we denote by $t^{\frac{1}{p}}$. Let $L = K(t^{\frac{1}{p}})$.

(1) Show that the equation $X^p - t = 0$ has only one solution in $\bar{K}$. This justifies the notation $t^{\frac{1}{p}}$.

(2) What is the trace of $t^{\frac{1}{p}}$?

(3) What is $N_{L/K}(t^{\frac{1}{p}})$?

Exercise 4. Let m be a square free integer, i.e. $m \in \mathbb{Z}$ and there is no prime number $p \in \mathbb{N}^+$ such that $p^2 | m$. Show that the integral closure A of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{m})$ equals

$$A = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{if } m \equiv 2 \text{ or } 3 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}] & \text{if } m \equiv 1 \bmod 4. \end{cases}$$

(Hint: mimic the proof of Exercise 2.4. Let $\alpha = r + s\sqrt{m}$ $(r, s \in \mathbb{Q})$ be an element in $\mathbb{Q}(\sqrt{m})$ which is integral over A. Show that if $s \neq 0$ and $m \neq 1$ then $f(X) = X^2 - 2rX + r^2 - ms^2$ is the minimal polynomial of $r + s\sqrt{m}$. Since α is integral over A, it is also integral over $\mathbb{Z}$. Show that $f(X)$ has $\mathbb{Z}$-coefficients, i.e. $2r, r^2 - ms^2 \in \mathbb{Z}$. Then deduce that

if $r \in \mathbb{Z}$ then $s \in \mathbb{Z}$, if $r \notin \mathbb{Z}$ then $\beta = \alpha - \frac{1+\sqrt{m}}{2}$ is integral over A. But $r - \frac{1}{2} \in \mathbb{Z}$, so $\beta \in \mathbb{Z}[\sqrt{m}]$.)