Karlsruher Institut für Technologie
Institut für Algebra und Geometrie
PD Dr. Stefan Kühnlein   Dipl.-Math. Jochen Schröder

Algebra – Problem Sheet 8

Exercise 1 (5 points)
Let $K \subseteq L$ be a finite field extension. Remember that for any $a \in L$ the map $x \mapsto ax$ is an endomorphism φ_a of L. Define the following maps from L to K via the transformation matrices.
trace: $\mathrm{tr}_{L|K} = \mathrm{tr} : L \to K$, $a \mapsto \mathrm{tr}(\varphi_a)$ where $\mathrm{tr}(\varphi_a)$ is the sum of diagonal elements.
norm: $\mathrm{N}_{L|K} = \mathrm{N} : L \to K$, $a \mapsto \mathrm{N}(\varphi_a) = \det(\varphi_a)$.

Show that trace and norm are well defined maps from L to K. Furthermore show that the norm is multiplicative and that the trace is additive.
Which of the following statements are correct: $\mathrm{N}(a) = 0 \Leftrightarrow a = 0$, $\mathrm{tr}(a) = 0 \Leftrightarrow a = 0$. Prove it or give a counter example.

Now let $K \subseteq L$ be a Galois extension with Galois group G. Prove that $\mathrm{tr}(a) = \sum_{\sigma \in G} \sigma(a)$, $\mathrm{N}(a) = \prod_{\sigma \in G} \sigma(a)$.
(*Hint:* Considering primitive elements first may help.)

Exercise 2 (4 points)
Let $p \in \mathbb{P}$ be the characteristic of the fields K, L where $K \subseteq L$ is a Galois extension of degree p.
Show that the Galois group is cyclic. From now on let σ be a generator.

Now we are going to prove a statement that fits to the characteristic-0-world from the lecture. We want to show that there is a primitive element $a \in L$ with minimal polynomial $X^p - X - c$ for an adequate $c \in K$.

a) Find the Jordan canonical form of σ. (*Hint:* An adequate basis may contain 1, this could be helpful.)

b) Find a basis vector that satisfies the condition on a from the statement.
To show that use the Galois group to write down the minimal polynomial as product of linear factors. Expand this product (*Hint:* Fermat's little theorem may help.) to show that it is of the given form.

Exercise 3 (7 points)
Let $K \subsetneq \mathbb{C}$ be a finite field extension.

a) $K \subseteq \mathbb{C}$ is a Galois extension.

b) There is a $p \in \mathbb{P}$ and a field L such that $K \subseteq L \subseteq \mathbb{C}$ with $[\mathbb{C} : L] = p$.

c) Any p-th root of unity is contained in L.

d) There is an $\alpha \in L$ such that $\mathbb{C} = L(\sqrt[p]{\alpha})$.

e) Let $g \in L[X]$ be a divisor of $X^{(p^2)} - \alpha$ of degree p.
Show that there is a p^2-th root of unity ζ such that $\pm\zeta \cdot \sqrt[p]{\alpha}$ is the constant term of g.
Conclude that $\zeta \notin L$, $\mathbb{C} = L(\zeta)$ and that ζ is a primitive p^2-th root of unity.

f) Let ξ be a primitive p^3-th root of unity. Show that the minimal polynomial $h \in L(X)$ of ξ has degree p.
Show that the coefficients of h lie in $D := L \cap \mathbb{Q}(\xi)$ and conclude that $[\mathbb{Q}(\xi) : D] = p$.

g) Prove that D and $\mathbb{Q}(\zeta)$ are different fields but that $[\mathbb{Q}(\xi) : \mathbb{Q}(\zeta)] = [\mathbb{Q}(\xi) : D]$.
Conclude that $\mathrm{Gal}(\mathbb{Q}(\xi)|\mathbb{Q})$ is not cyclic, $p = 2$[1], $\mathbb{C} = L(i)$.

h) Finally show $\mathbb{C} = K(i)$.

Hand in your solutions until wednesday, December 14th 2011, 7:45 in the yellow box labeled „Algebra“, Allianzgebäude, 1C or bring them directly to the problem class, 8:00.

[1]You may and should use Hilfssatz 4.2.4 from the EAZ script: $(\mathbb{Z}/p^m\mathbb{Z})^\times$ is cyclic for $p \in \mathbb{P} \setminus \{2\}$.