Problem list 5

Weronika Jakimowicz

Exercise 1. Assume that $char(K) = p > 0$, $K \subseteq L$ is an algebraic field extension and $a \in L \setminus K$. Prove that a^{p^l} is separable over K for some $l \geq 0$.

Aim: show that for some n the minimal polynomial of a^{p^n} is not in $K[x^p]$.

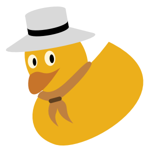
I will draw a diagram cuz they are fun 

$$w_a(x) = b + b_0^0 x + ... + b_{n_0}^0 x^{n_0}$$

$$a \text{ not separable}$$
$$\Downarrow$$
$$w_a(x) = b + b_0^1 x^p + ... + b_{n_1}^1 (x^p)^{n_1} \in K[x^p]$$

but after plugging in a we get that this is the minimal polynomial of a^p :

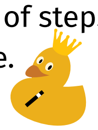
$$w_{a^p}(x) = b + b_0^1 x + ... + b_{n_1}^1 x^{n_1}$$



$$a^p \text{ not separable}$$
$$\Downarrow$$
$$w_{a^p}(x) = b + b_0^2 x^p + ... + b_{n_2}^2 (x^p)^{n_2}$$

here if we plug in a^p we get a minimal polynomial of $a^{p \cdot p} = a^{p^2}$

$$\Downarrow$$
$$\text{etc.}$$

Each time we ramove a portion of coefficients from the original w_a while not changing the degree of it. Therefore, this process will end at some point and the number of steps we took would be my n (or l if we stick to the notation in excercise) for which a^{p^n} is separable. 

I spend half an hour placing those ducks instead of writing my solutions and I regret nothing. Please enjoy my duckies.

Exercise 4.

(a) Prove that Frobenius automorphism $\psi_n(x) = x^p$ is a generator of the group $Gal(F(p^n)/F(p))$.

(a)

I. $\psi_n(x) \in Gal(F(p^n)/F(p))$

It is a quick one: I just need to show that for $a \in F(p)$ $a^p = a$. Take $F(p)^*$, it is a cyclic ($\cong \mathbb{Z}_p$) group of order $p - 1$. Hecne, $a^{p-1} = 1$ and $a^{p-1} \cdot a = a^p = a$.

II. $ord(\psi_n(x)) = [F(p^n) : F(p)] = n$

Firstly, something that took me a while (unfortunatelly), $Gal(F(p^n)/F(p))$ is cyclic. Here is a very unofficial way of how I explained it to myself.

Well, "normal" automorphisms $Aut(F(p^n)) \cong Aut(\mathbb{Z}_{p^n})$, which is a cyclic group and $Gal(F(p^n)/F(p)) \leq Aut(F(p^n))$ so it is also cyclic. I also know that $F(p^n)$ is a vector field over $F(p)$ of some element of order n. Every automorphism from $Gal(F(p^n)/F(p))$ must permute this little fella without touching anything from $F(p)$, so I am left with some n elements in $Gal(F(p^n)/F(p))$.

With that out of the way, let us work on the order of ψ_n. Take any $a \in F(p^n) \setminus F(p)$. We know that $F(p^n)^*$ has $p^n - 1$ elements, so $a, a^2, ..., a^{p^n-1}$ are all different elements (and each of them generates the whole thing). So $a, a^p, a^{p^2}, ..., a^{p^{n-1}}$ are all different and there are exactly $n - 1$ of them. If we pass $a^{p^{n-1}}$ once more through ψ_n we get $a^{p^n} = a$ and so the order of ϕ_n is the order of the whole group in which it sits so ϕ_n is a generator.

Exercise 7.

(a) Assume that L is a finite extension of the field $\mathbb{Q}$ of odd degree. Prove that L is isomorphic over $\mathbb{Q}$ with a subfield of the field $\mathbb{R}$.

Let $L = \mathbb{Q}(a_1, ..., a_n)$ for some $a_1, ..., a_n \in \mathbb{C} \setminus \mathbb{Q}$, each has the minimal polynomial of odd degree because otherwise the whole L would have even degree (from $[M : K] = [M : L][L : K]$, $K \subseteq K \subseteq M$). Since if a_i is a root of a polynomial, then also $\overline{a_i}$ is a root of it. Hence, for each $i = 1, ..., n$ we have $\overline{a_i} \in L$.

Of course, this is also true for elements from $\mathbb{Q}$. Each rational number is equal to its conjugate. Furthermore, since conjugation is distributive with respect to both multiplication and addition, every element has its conjugate in L.

Therefore, conjugation is an automorphism of L. Applying conjugation twice to the same element $z \in \mathbb{C}$ gives us z. Furthermore, conjugation $\in Gal(L/\mathbb{Q})$. And I would say that $|Gal(L/\mathbb{Q})| = [L : \mathbb{Q}]$ cuz then I get to a nice conclusion that all those elements must be from $\mathbb{R}$ (conjugating them once gives the original because order of conjugation must be odd and divide $[L : \mathbb{Q}]$) and life is nice and peaceful.