Algebra 2R

Problem List 2

Weronika Jakimowicz

EXERCISE 4.

Assume that K is a finite field, characteristic p.

(a) Prove that every irreducible polynomial $f \in K[x]$ divides the polynomial $w_n(x) = x^n - 1$ for some n not divisible by p. (hint: prove that the splitting field of f is finite.)

Let f be an irreducible polynomial $f \in K[x]$ and $n = \deg(f) > 0$ and let $a_1, \ldots, a_r \in L \supseteq K$ be its roots, where L is the splitting field of f over K. Because K is finite, i can say that $|K| = q$.

For my convenience, I will consider $g = b_n^{-1} f$, where b_n is the leading coefficient in f. So now g is a monic polynomial and considering the splitting field of f is the same as considering the splitting field of g - I just multiplied a polynomial by a nonzero constant.

Lemacik: *The splitting field of* g *(equivalently, of* f*) is finite.*

We will construct the splitting field of K as such:

$$L_1 = K(a_1)$$

$$L_2 = L_1(a_2)$$

$$L_i = L_{i-1}(a_i)$$

and then $L = L_r$.

Let

$$f(x) = \prod_{i=1}^{r} (x - a_i)^{k_i}$$

and notice that $\sum k_i = n$.

I will show that $[L_r : K] = \prod_{i=1}^{r} k_i < \infty$ using finite induction.

1. $[L_1 : K]$. We know that g in L_1 can be written as

$$g = (x - a_1)^{k_1} u_1,$$

where $u_1 \in L_1[x]$ is an irreducible polynomial such that $u_1(a) \neq 0$. Then, the ideal

$$I(a_1/K) = \{w \in K[x] \ : \ w(a_1) = 0\} = ((x - a_1)^{k_1})$$

because even though I write $(x - a_1)^{k_1}$, I know that a polynomial of this form is irreducible in K[x] if $a_1 \notin K$. Which must be the case because we started from a polynomial that is not a product of linear polynomials.

From Remark 4.4. (below) I know that $[L_1 : K] = \deg((x - a_1)^{k_1}) = k_1$.

2. $[L_{i+1} : L_i] = q^{k_{i+1}}$

Right now we have that

$$g = (x - a_{i+1})^{k_{i+1}} u_{i+1}(x) \prod_{j=1}^{i} (x - a_j)^{k_j}$$

which looks horrific but I am trying to be formal and so on. I want $u_{i+1}(a_{i+1}) \neq 0$. The product part is a linear combination of polynomials from L_i and $(x - a_{i+1})^{k_{i+1}}$ is a linear combination of polynomials from L_{i+1} but not from L_i. And so is irreducible over L_i. So now we have that

$$I(a_{i+1}/K) = ((x - a_{i+1}))^{k_{i+1}}$$

by the same argument as above. Thus, from remark 4.4. (still there) we have that $[L_{i+1} : L_i] = k_{i+1}$.

Now that we are done, we will use Fact 4.5. (even belower). We see, from condition, that

$$K \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L_r = L$$

and now:

$$[L_r : K] = [L_r : L_{r-1}][L]$$

Remark 4.4. *Suppose that* $I(a/K) = (f)$ *and* f *is monic. Then:*

1. f *is the minimal monic polynomial such that* $f(a) = 0$
2. $\deg(f) = [K(a) : K]$, *thus the degree of the minimal polynomial is equal to the dimension of the linear space* $K(a)$ *over* K.

Fact 4.5 *Let* $K \subseteq L \subseteq M$ *be extensions of fields. Then*

$$[M : K] = [M : L][L : K]$$