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.

Lemaczysko: *An irreducible polynomial* $g \in K[X]$ *is the minimal polynomial for some root* a, $f(a) = 0$

As K is a field, the ring $K[X]$ is an euclidean domain. Let us suppose that $h \in K[X]$ is the minimal polynomial of a in K such that $\deg(h) < \deg(g)$. We have that there exists $p, r \in K[X]$ such that

$$f = hp + r$$

but notice that $f(a) = 0$ and $h(a) = 0$, so $r = 0$ and we would have $f = hp$ but f was irreducible.

Lemat: *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 $L = L_r$.

1. $[L_1 : K] = n$. The ideal

$$I(a_1/K) = \{w \in K[X] \ : \ w(a_1) = 0\} = (g)$$

because g is irreducible. We showed that g is minimal in Lemaczysko and so from Remark 4.5. (below) we have that $[L_1 : K] = \deg(g) = n$.

2. $[L_{i+1} : L_i] = n$. Once again, g is irreducible over L_i (because not all roots of g are in L_i)

$$I(a_{i+1}/K) = \{w \in K[X] \subseteq L_i[X] \ : \ w(a_{i+1}) = 0\} = (g)$$

and it follows from Remark 4.5. (once again) that $[L_{i+1}, L_i] = \deg(g) = n$.

Now, using Fact 4.6. (even belower) We have that

$$[L:K] = [L_r : L_{r-1}][L_{r-1} : L_{r-2}] = \ldots = \prod_{i=1}^{r}[L_i : L_{i-1}] = n^r < \infty.$$

If the original field K had p^k elements, then the new field would have p^l elements, where $l = k \cdot [L:K]$. Therefore, we have p^l elements in the base of L over K.

Now we want to show that $v_n(a_1) = 0$ and from this and the fact that K[X] is euclidean conclude that "gcd" of those two polynomials cannot be 1, hence g divides v_n.

We know that $v_n(a_1) = 0$. Suppose that $g \nmid v_n$, then we would be able to find $c, b \in K[X]$ such that

$$g \cdot c + v_n \cdot b = 1$$

but then

$$g(a_1) \cdot c(a_1) + v_n(a_1) \cdot b(a_1) = 1$$

which gives a contradiction. Hence, $g|v_n$ and because $v_n|w_n$ we have that $g|w_n$.

Remark 4.5.or some i *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 4.6 *Let* $K \subseteq L \subseteq M$ *be extensions of fields. Then*

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