Algebra 2R

Problem List 2

Weronika Jakimowicz

EXERCISE 3.

Assume that $f : K \to K$ is a non-zero endomorphism (e.g. the Frobenius function)/ Prove that $Fix(f) = \{x \in K : f(x) = x\}$ is a subfield of the field K

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 $f \in K[x]$ of degree $n = \deg(f) > 0$. Without loss of generality assume that f is monic. Let $a \in L \supseteq K$ be one of its roots, where L is the splitting field of f over K. Because K is finite, i can say that $|K| = p^k$.

"Proof graph"

$$
\begin{array}{c}
\text{irreducible} \implies \text{minimal} \\
\downarrow \\
[L : K] = n < \infty \\
\downarrow \\
w_m(a) = 0 \\
\downarrow \\
f | w_m
\end{array}
$$

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

$$w_m(x) = x^m - 1 = (x-1)\underbrace{(x^{m-1} + x^{m-2} + \ldots + x + 1)}_{v_m(x)}$$

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 $\deg(h) < \deg(f)$. 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* f *is finite.*

The ideal

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

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

Lemacik: *This is not really a lemma but the third step in the diagram:* $w_m(a) = 0$ *for* $m = p^{kn} - 1$.

Now let us look at L^*, which is the multiplicative group of L. Because L was a field, we know that

$$|L| = p^{kn} = p^l$$

($[L : K] = n$ and there were p^k elements in K) and that

$$|L^*| = |L \setminus \{0\}| = p^l - 1.$$

Furthermore, we know that every finite group is isomorphic to the field $\mathbb{Z}_p$ so we must have that L^* is a cyclic group with $a \in L^*$ as one of its generators. We know that $a^{p^l} = a$ will "loop back" inside of L^* and so $a^{p^l-1} = 1$ inside of L^*. This gives us the following equality:

$$w_{p^l-1}(a)a^{p^l-1} - 1 = 1 - 1 = 0$$

with $p \nmid p^l - 1$.

Lemaciuś: *Once again not a lemma but showing that* f *divides* w_m, m *as above.*

What remains now is to show that $f|w_m$. Suppose that this is untrue and that their "gcd" is equal to 1. Then by Bezout's identity we have that there exist $c, d \in K[X]$ such that

$$f(x)c(x) + w_m(x)d(x) = 1$$

but for $x = a$ we would have $0 = 1$ which is a contradiction. Hence, one has to divide the other. It is quite logical that the minimal polynomial cannot have degree higher than the number of elements in a field and so $n \leq p^k < p^{kn} - 1$ and so $\deg(f) < \deg(w_m)$ implying that $f|w_m$.

Remark 4.5. *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.