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, $f(a) = 0$

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. f is irreducible so it cannot be divided by anything but itself and so $f|w_m$.

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.

EXERCISE 5.

(a) Prove that if $K \subseteq L$ *are finite fields,* $|K| = p^m, |L| = p^n$, *then* $m|n$.

Let $[L : K] = d$. Then we have that the basis of L over K has d elements. Every element of L can be expressed as a linear combination of elements from the basis with coefficients from K. There are

$$|K|^d = p^{md}$$

such combinations. Hence $|L| = p^{md} = p^n \implies n = md \implies m|n$.

(b) Prove that every field with p^n *elements contains a unique subfield with* p^m *elements, where* $m|n$.

"Proof graph" of existence

$$\begin{array}{c} x \in \mu_{p^n-1}(L) \implies x \in \mu_{p^m-1}(L) \\ \downarrow \\ x^{p^n-1} = 1 \implies x^{p^m-1} = 1 \implies x^{p^m} = x \\ \downarrow \\ x \in \mathrm{Fix}(x^{p^m}) \subseteq L \\ \downarrow \\ |\mathrm{Fix}(x^{p^m})^*| = |\mu_{p^m-1}| = p^m - 1 \implies |\mathrm{Fix}(x^{p^m})| = p^m \end{array}$$

Let $n = md$ for some $m, d \in \mathbb{N}$. Notice that $\mu_{p^m-1}(L) \subseteq \mu_{p^n-1}(L)$ because if $x \in \mu_{p^m-1}$ then

$$x^{p^n-1} - 1 = (x^{p^m-1} - 1)(x^{p^{n-m}} + x^{p^{n-m-1}} + \ldots + 1)$$

and so $x^{p^m-1} - 1$ must be equal to zero. Setting an $x \in \mu_{p^m-1}(L)$ allows us to do the following computation:

$$x^{p^m-1} - 1 = 0$$

$$x^{p^m-1} = 1$$

$$x^{p^m} = x$$

which gives us an endomorphism $f(x) = x^{p^m}$. From ex. 3. we know that Fix(f) is a subfield of L and from the reasoning above we know that Fix(L) contains the elements from $\mu_p(L)$ (which according to Theorem 3.4. has cardinality $p^m - 1$) and $\{0\}$. Thus, $|\mathrm{Fix}(f)| = p^m$.

"Proof graph" of uniqueness:

$$\begin{array}{c} \text{suppose that } K_1, K_2 \subseteq L, |K_1| = |K_2| = p^m \\ \downarrow \\ |K_1^*| = p^m - 1 = |K_2^*| \\ \downarrow \\ K_1^* = \mu_{p^m}(L) = K_2^* \\ \lightning \end{array}$$

Suppose that there exist two subfields $K_1, K_2 \subseteq L$ with $|K_1| = p^m = |K_2|$. Then $|K_1^*| = p^m - 1$ and $|K_2^*| = p^m - 1$, which from Theorem 3.4. means that

$$K_1^* = \mu_{p^m-1}(L)$$

$$K_2^* = \mu_{p^m-1}(L).$$

From the fact that $K_1^* = K_2^*$ follows that $K_1 = K_2$, which is a contradiction.

Theorem 3.4. Let $G < \mu(K)$ and G is finite with $|G| = n$. Then:

1. $G = \mu_n(K)$
2. G is cyclic
3. if $\mathrm{char}(K) = p > 0$ then $p \nmid n$.

EXERCISE 6.

Let $F(p^n)$ be a field with p^n elements. From Problem 5 it follows from that

$$F(p) \subseteq F(p^2) \subseteq F(p^{3!}) \subseteq \ldots \subseteq F(p^{n!}) \subseteq \ldots$$

(after suitable identifications of isomorphic fields). Let

$$F = \bigcup_{n>0} F(p^{n!})$$

Prove that the field F is algebraically closed. (hint: use Problem 4.)

A field is algebraically closed if every non-constant polynomial $f \in F[X]$ has a root in F.

"Proof graph"

$$\begin{array}{c} \text{Ex. 4: } (\forall\ f \in F[X])\ f\text{-irreducible} \implies f|w_m \\ \downarrow \\ (\forall\ n \in \mathbb{N})(\exists\ a_1, \ldots, a_n \in F)\ w_n(a_i) = 0.\ i = 1, \ldots, n \\ \downarrow \\ w_n(a_i) = 0 \implies f(a_i) = 0 \text{ for some } i \in \{1, \ldots, n\} \end{array}$$

Because all polynomials in F[X] are either irreducible or a product of irreducible polynomials, it is sufficient to show that every irreducible polynomial in F[X] has a root in F. Let $f \in F[X]$ be irreducible and $n = \deg(f)$. From Ex. 4 we know that $f|w_{p^{nk}-1}$ for some $k \in \mathbb{N}$ and so they must have a common root. Thus, it will be sufficient to show that all roots of $w_{p^{nk}-1}$ are within F.

Take $n \in \mathbb{N}$ and consider $w_n(x) \in F[X]$. The field $F(p^k)$ such that $n < p^k$ will have all roots of $w_n(x)$. But $F(p^k) \subseteq F$ so we have that F also contains all roots of $w_n(x)$.

The above reasoning was conducted for arbitrary chosen n, so it will be true for $p^{nk} - 1$ and so F contains all roots of $p^{nk} - 1$, meaning that f contains at least one root in F and so F is algebraically closed.