Problem List 3

Algebra 2r

Weronika Jakimowicz

Exercise 1. Let K be a field.

(a) Prove that the field extension $L \supseteq K$ is transcendental, where $L = K(X)$ is the field of rational functions in varriable X over K.

(b) Let $M = L[\sqrt{X}]$ be an algebraic extension of the field L by an element $Y = \sqrt{X}$ such that $Y^2 - X = 0$ in the field M. Prove that M and L are isomorphic over K.

(b)

We kave $L = K(X)$ and $M = L[Y]$ and $Y^2 - x = 0$. We claim that $L \cong_K M$.

$$f_1 : L \to M$$

$$f_1(p) = p(Y)$$

$$f_2 : M \to L$$

$$y \mapsto x$$

$$x \mapsto x^2$$

So take a function $h \in L$, then $f_2(f_1(h)) = f_2(h(y)) = h(x)$

Exercise 2. Let K be a field.

(a) Let $g \in K(X) \setminus K$. Prove that X is algebraic over the field $K(g)$. In particular $[K(X) : K(g)] < \infty$. What is the degree of this extreme?

(b) For g as in (c) prove that $K(g)$ is isomorphic with $K(X)$ over K.

(a)

First of all, we know that there exist $p, q \in K[Y]$ such that

$$g = \frac{p}{q}$$

$$gq = p$$

and so

$$g(x)q(y) - p(y) = w(y) \in K(g)[Y]$$

Now consider $w(x)$

$$w(x) = g(x)q(x) - p(x) = p(x) - p(x) = 0$$

hence, X is algebraic over $K(g)$.

$[K(X) : K(g)] = \max(\deg(p), \deg(q))$.Because $\frac{1}{g}$ and g generate the same extension, then we can assume that $\deg(p) \geq \deg(q) = k$. It is obvious that $\deg(w) \leq k$, we need to show that $\deg(w) \geq k$.

Take $(1, ..., x^{k-1})$ which is linearly independent. We take some coefficients $a_0, ..., a_{k-1} \in K(g)$ such that

$$a_0 + a_1x + ... + a_{k-1}x^{k-1} = 0$$

Now, multiply by all denominators of a_i to obtain

$$a'_0 + a'_1 x + \dots + a'_{k-1} x^{k-1} = 0$$

Therefore, a'_i are all polynomials and we have:

$$a'_i = b_i + \frac{p}{q} R_i\left(\frac{p}{q}\right),$$

where $b_i \in K$: we just take a constant term and remove x from it.

Notice that there exists $b_i \neq 0$, otherwise we could just divide the whole thing by $\frac{p}{q}$ and repeat the process one more time.

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Exercise 3. Let $v_1, \dots, v_n$ be vertices of a regular n-gon inscribed in a circle on the plane $\mathbb{R}^2$ with equation $x^2 + y^2 = 1$. What is the linear dimension over $\mathbb{Q}$ of the system of vectors $v_1, \dots, v_n$.

Without the loss of generality, I will consider polygons with one vertex in $(1, 0)$. Then, the remaining vertices are in $(\cos \frac{2\pi k}{n}, \sin \frac{2\pi k}{n})$, for $k = 1, \dots, n-1$. Now, let me switch where I live and let us consider roots of

$$x^n - 1.$$

We have n roots $z_1, \dots, z_n$ in $\mathbb{C}$. Notice, that $z_k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}$ and adding complex numbers works almost like adding vectors in 2D. The minimal polynomial over $\mathbb{Q}$ of each of z_k is $F_n(x)$. Therefore, $\dim(v_1, \dots, v_n) = \dim(z_1, \dots, z_n) = \phi(n)$, where ϕ is Euler's function.

Well, I think I kinda showed it before XD

Exercise 5. (a) Prove that $j(F_m(x))$ need not be irreducible over $F(p)$.

(b) Prove that if $k, l \in \mathbb{N}^+$ are coprime, then $k | l^{\phi(k)} - 1$ (hint: consider the ring $\mathbb{Z}_k$).

(a) Take $F_3(x) = x^2 + x + 1$, its image in $\mathbb{Z}_3$ is the same. But $x^2 + x + 1 = (x + 2)^2$ in $\mathbb{Z}_3$ and so is reducible.

(b) Take the ring $\mathbb{Z}_k$, then we know that $|\mathbb{Z}_k^*| = \phi(k)$ and $l \in \mathbb{Z}_k$. So there must exist an $a \in \mathbb{N}$ such that $l^a = 1$ in $\mathbb{Z}_k$, which implies that $k | l^a - 1$. We know that l is a generator of $\mathbb{Z}_k^*$, so l has order $\phi(k)$. Therefore, $a = \phi(a)$.

Exercise 6. Find the minimal polynomials over $\mathbb{Q}$ fot the following numbers:

(a) $\sqrt{2} + \sqrt{3}$

$$\begin{aligned}
x - (\sqrt{2} + \sqrt{3}) &= 0 \\
x - \sqrt{2} &= \sqrt{3} \\
(x - \sqrt{2})^2 &= 3 \\
x^2 - x2\sqrt{2} + 2 &= 3 \\
x^2 - 1 &= x2\sqrt{2} \\
(x^2 - 1)^2 &= 8x^2 \\
x^4 - 2x^2 + 1 &= 8x^2 \\
x^4 - 10x^2 + 1 &= 0
\end{aligned}$$

Exercise 7. Prove (using Liouville Lemma) that the number

$$\sum_{n=1}^{\infty} \frac{1}{2^{n!}}$$

is transcendental. (the real numbers, whose transcendence follows from Liouville Lemma are called Liouville numbers).

Liouville Lemma states that if $a \in \mathbb{R}$ is an algebraic number of degree $N > 1$, then there exists $c \in \mathbb{R}_+$ such that for all $\frac{p}{q} \in \mathbb{Q}$ the following is true:

$$\left| a - \frac{p}{q} \right| \geq \frac{c}{q^N}$$

If a number fails to meet this criterion, then it is called transcendental.

Ok, so I have no clue what the degree of my number is, but let me assume that it is some $N \in \mathbb{N}$. Now, let

$$p = \sum_{n=1}^{N+k} 2^{(N+k)! \cdot n!}.$$

Then, we have that

$$\sum_{n=1}^{\infty} \frac{1}{2^{n!}} = \frac{p}{2^{(N+k)!}} + \sum_{n=N+k}^{\infty} \frac{1}{2^{n!}}$$

with $q = 2^{(N+k)!}$. From this we get

$$\left| \sum_{n=1}^{\infty} \frac{1}{2^{n!}} - \frac{p}{2^{(N+k)!}} \right| = \left| \sum_{n=N+k+1}^{\infty} \frac{1}{2^{n!}} \right| \leq (\text{☕})$$

and notice that

$$\sum_{n=N+k+1}^{\infty} \frac{1}{2^{n!}} \leq \sum_{n=N+k+1}^{\infty} \frac{1}{2^{n}} = \frac{1}{2^{(N+k+1)!}} \frac{1}{1 - \frac{1}{2}} = \frac{2}{2^{(N+k+1)!}}$$

$$(\text{☕}) \leq \frac{2}{2^{(N+k+1)!}} = \frac{2}{q^{N+k+1}} < \frac{1}{q^{N+k}}$$

for any $k \in \mathbb{N}$ and so we cannot choose one universal c such that this inequality changes to $\geq$ for all. Thus, the number from the problem is a Liouville number.

Exercise 8. Assume that $M \supseteq K$ is an algebraic field extension and L_1, L_2 are intermedaite fields (that is: $K \subseteq L_1, L_2 \subseteq M$). As usual, $L_1[L_2] = L_2[L_1]$ denotes the subring of M generated by $L_1 \cup L_2$. Prove that

(a) $L_1[L_2]$ isa subfield of M (denoted by L_1L_2)

(b) $[L_1L_2 : K] \leq [L_1 : K][L_2 : K]$

(c) Assume $L_1 \cap L_2 = K$. Do we have equality in (b) then?

(a) Let $a \in L_1L_2$, it is easy to see that a is in M. Hence, a is algebraic over K and there exists a minimal irreducible polynomial

$$f(x) = \sum_{i=1}^{n} \alpha_i x^i + \alpha_0$$

such that $\alpha_0 \neq 0$ and $f(a) = 0$. Therefore, we have that

$$0 = \sum_{i=1}^{n} \alpha_i a^i + \alpha_0$$

$$-\alpha_0 = a \left[\sum_{i=1}^{n} \alpha_i a^{i-1} \right]$$

$$1 = a \left[(-\alpha_0)^{-1} \sum_{i=1}^{n} \alpha_i a^{i-1} \right]$$

(b) Let $L_1 = K(a_1, ..., a_n)$ and $L_2 = K(b_1, ..., b_m)$. Then $[L_1 : K] = n, [L_2 : K] = m$. Take $y \in L_1L_2$, then it is equal to some $\sum \alpha_i\beta_i$ for $\alpha_i \in L_1$ and $\beta_i \in L_2$. Therefore, we can easily use nm combinations of elements from the basis to write y.

(c) Nope