Algebra 2R

Problem List 1

Weronika Jakimowicz

EXERCISE 1.

Proof that $\mathbb{C} = \mathbb{R}[z]$ *for every complex number* $z \in \mathbb{C} \setminus \mathbb{R}$.

To begin with, let us take any $z \in \mathbb{C} \setminus \mathbb{R}$ such that $z = ai$ for some $a \in \mathbb{R}$. We have that

$$\mathbb{R}[z] = \{f(z) \ : \ f \in \mathbb{R}[X]\}.$$

Let $I = (X^2 + a^2) \triangleleft \mathbb{R}[X]$ be an ideal of $\mathbb{R}[X]$ generated by a polynomial with no real roots. We know that $\mathbb{R}[X]/I \cong \mathbb{C}$.

This is because $\mathbb{R}$ is a field and so $\mathbb{R}[X]$ is an euclidean domain: if we take any $f \in \mathbb{R}[X]$ then we can write it as $f = v(X^2 + a^2) + w$, where w is of degree 0 or 1 ($< \deg(X^2 + a^2)$) and so f in $\mathbb{R}[X]/I$ is represented only by w. Now it is quite easy to map polynomials with real coefficients and maximal degree 1 to $\mathbb{C}$, for example $f : \mathbb{R}[X]/I \to \mathbb{C}$ such that $f(aX + b) = ai + b$. Therefore $\mathbb{R}[X]/I \cong \mathbb{C}$.

Consider the evaluation homomorphism ϕ_z which maps $\mathbb{R}[X] \ni w \mapsto w(z) \in \mathbb{R}[z]$. We can see that $\ker(\phi_z) = (X^2 + a^2) = I$. Therefore, by the fundamental theorem on ring homomorphism we have an isomorphism

$$f : \mathrm{Im}(\phi_z) = \mathbb{R}[z] \to \mathbb{R}[X]/\ker(\phi_z) = \mathbb{R}[X]/I$$

and as mentioned above, $\mathbb{R}[X]/I \cong \mathbb{C}$. Hence, $\mathbb{R}[z] \cong \mathbb{C}$.

i śmiga

EXERCISE 2.

Assume that $K \subset L$ *are fields and* $a, b \in L$. *For a rational function* $f(X) \in K(X)$ *define* $f(a)$ *as* $\frac{g(a)}{h(a)}$, *where* $g, h \in K[X]$, $f = \frac{g}{h}$ *and* $h(a) \neq 0$, *provided such* g, h *exist. If not,* $f(a)$ *is undetermined. Prove that*

(a) if $f(X) \in K(X)$ *and* $f(a)$ *is defined, then* $f(a)$ *is determined uniquely (does not depend on the choice of* g, h*)*

Suppose by contradiction that $f(a)$ depends on which g, h we choose. That means that there exist $g, h, g', h' \in K[X], h(a) \neq 0, h'(a)$ such that $f = \frac{g}{h} = \frac{g'}{h'}$ but $\frac{g(a)}{h(a)} + c = \frac{g'(a)}{h'(a)}$, where $c \in L \setminus \{0\}$.

From $f = \frac{g}{h} = \frac{g'}{h'}$ we get that $g \cdot h' = g' \cdot h$ and in particular

$$(gh')(a) = (g'h)(a)$$
$$g(a)h'(a) = g'(a)h(a)$$
$$g(a)h'(a) - g'(a)h(a) = 0$$

From the assumption that f(a) depends on the choice of polynomials we get that

$$\frac{g'(a)}{h'(a)} = \frac{g(a)}{h(a)} + c$$
$$g'(a)h(a) = g(a)h'(a) + ch'(a)$$
$$g'(a)h(a) - g(a)h'(a) = ch'(a) \neq 0$$

Which is a contradiction because $c \neq 0$, $h'(a) \neq 0$ and we have no zero divisors.

(b) $K(a) = \{f(a) \ : \ f \in K(X)$ *and* $f(a)$ *is defined*$\}$

We know that K(a) is a subfield of L that is generated by $K \cup \{a\}$. Let us label this field as L'. We will show that $L' = K(a)$.

$L' \subseteq K(a)$

Let us take any $x \in L'$. Then x is a finite linear combination of elements from K and $\{a.a^{-1}\}$:

$$x = \sum_{0 \leq k \leq n} \alpha_k a^{i_k k}, \quad i_k \in \{1, -1\}, \ \alpha_k \in K.$$

We need to change this into a rational function. Take $p_k \in K[X]$ such that $p_k(X) = \alpha_k X^k$. We have that

$$x = \sum_{0 \leq k \leq n} p_k(a^{i_k}).$$

It is clear that when working with rational functions we may say that $p_k(a^{-1}) = \frac{1}{p'_k(a)}$ where $p_k(X) = \alpha_k^{-1} X^k$.

$$x = \sum_{0 \leq k \leq n} p_k(a^{i_k}) = \frac{\sum\limits_{0 \leq k \leq n} p_k(a) \prod\limits_{\substack{0 \leq l \leq n, \\ i_l = -1}} p'_k(a)}{\prod\limits_{\substack{0 \leq k \leq n \\ i_k = -1}} p'_k(a)} \in K(a)$$

$K(a) \subseteq L'$

Let us take any $f \in K(X)$ such that f(a) is defined. We may write $f = \frac{g}{h}$ for $g, h \in K[X]$ and $h(a) \neq 0$. We have that $g(a) \in L'$ and $h(a) \in L'$. Therefore, $\frac{g(a)}{h(a)} = g(a) \cdot [h(a)]^{-1} \in L'$.

(c) $K(a, b) = (K(a))(b)$

Let

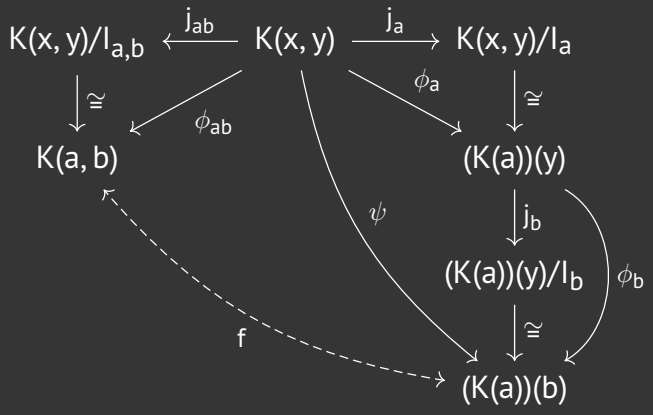
$$I_{ab} = I((a, b)/K[x, y])$$
$$I_a = I(a/(K[y])[x])$$
$$I_b = I(b/(K(a))(y))$$

and j_a, j_b, j_{ab} are quotient functions defined as below. We know that $\ker(j_a) = I_a$, $\ker(j_b) = I_b$ and $\ker(j_{ab}) = I_{ab}$. Let ϕ_a be an evaluation function that substitutes only one variable:

$$\phi_a : K(x, y) \to (K(a))(y)$$

$$\phi_a(f(x, y)) = f(a, y)$$

that is ϕ_a returns a rational function with changed coefficients. ϕ_b, ϕ_{ab} are defined as evaluation functions without such modifications.



Function ψ is a ring homomorphism defined as composition of ϕ_a and ϕ_b:

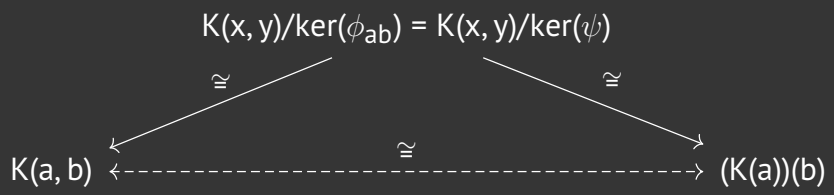
$$\psi : K(x, y) \to (K(a))(y)$$

$$\psi = \phi_b \circ \phi_a$$

For f to be an isomorphism

$$f : (K(a))(b) \to K(a, b)$$

we need to show that $\ker(\phi_{ab}) = \ker(\psi)$ because then



$\ker(\phi_{ab}) = \ker(\psi)$

$\subseteq$

$f \in \ker(\phi_{ab})$ means that $f(a, b) = 0$. That is, either of the following is true for any $x, y \in K$

$f(a, b) = 0$ this directly implies that $f \in \ker(\psi)$.

$f(a, y) = 0$ the same as above.

$f(x, b) = 0$ we know that for any $x \in K$ $f(x, b) = 0$ then for $x = a$ this is also true and so $f(a, b) = 0$ and $f \in \ker(\psi)$.

$\supseteq$

$f \in \ker(\psi)$ means that $f(a, b) = 0$ or $f(a, y) = 0$. This means that $f \in \ker(\phi_{ab})$.

Therefore, there exists an isomorphism $K(a, b) \cong (K(a))(b)$.

EXERCISE 3.

Assume that $K \subseteq L$ *are fields and* $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ *have degree* 1.

(a) Prove that if the system of equations $f_1 = \ldots = f_m = 0$ *has a solution in* L *then it has a solution in* K. *(hint: use linear algebra).*

Let

$$f_i = \sum_{1 \le k \le n} b_{i,k} X_k$$

for $i = 1, \ldots, m$.

We are working on linear equations, therefore we can construct a matrix that stores the same information as the system of equations $f_1 = \ldots = f_m$. Let

$$f_i = \sum_{1 \leq k \leq n} b_{i,k} X_k$$

for $i = 1, \ldots, m$. The matrix representation of this system of equations is:

$$\begin{bmatrix} b_{1,1} & b_{1,2} & b_{1,3} & \ldots & b_{1,n-1} & b_{1,n} \\ b_{2,1} & b_{2,2} & b_{2,3} & \ldots & b_{2,n-1} & b_{2,n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ b_{m,1} & b_{m,2} & b_{m,3} & \ldots & b_{m,n-1} & b_{1,n} \end{bmatrix} X = 0.$$

Using Gaussian algorithm, we can create an upper triangular matrix with coefficients from K. The solution would be found by backwards substitution. That is, a_n would be in the bottom right corner of the matrix and it is an element of K because such are the coefficients within my matrix. Then a_{n-1} would be a combination of a_n with two elements of K, hence it would still be in K and so on. Each a_i would be a linear combination of elements from K and a_k, $k < i$, which we know are in K.

i śmiga

(b) Does K *contain a generic solution of this system (over* K*)?*

From Remark 1.4. we know that $\bar{a}$ is a generic solution $\iff$ for any other solution $\bar{a}' \in K^n$ we have only one homomorphism $h : K[\bar{a}] \to K[\bar{a}]$ such that $h(\bar{a}) = h(\bar{a}')$ and $h \restriction K = id_K$. It is suffice to notice that because $K[\bar{a}]$ and $K[\bar{a}']$ are evaluations of polynomials with coefficients from K, then they are finite combinations of elements from K and therefore $K[\bar{a}] \subseteq K$ and $K[\bar{a}'] \subseteq K$. Therefore $h \subseteq id_K$ and thus is unique.

!!!!!!!!!! I SHOULD ACTUALLY SAY THAT THERE IS IDENTITY

ZADANIE 4.

ZADANIE 5.

Which of the following solutions of the equation $X_1^2 - X_2^3 = 0$ *in the field of rational functions* $\mathbb{C}(X)$ *are generic over the field* $\mathbb{Q}$*?*

(a) $(1, 1)$

Ok, so a solution is generic if $\{g \in K[X] \ : \ g(a) = 0\} = (f_1, \ldots, f_m)$. So maybe I should look for all polynomials that $g(1, 1) = 0$?

$$(x - 1), (y - 1)$$

And it is quite difficult to make a linear polynomial from a polynomial of order 3.

$(\sqrt[6]{8}, \sqrt[6]{4})$

$$(x^6 - 8) = (x^2 - 2)(x^4 + 2x^2 + 4)$$

$$(y^6 - 4) = (y^3 - 2)(y^3 + 2)$$

So the

$$I(\bar{a}/K = \mathbb{Q}) = ((x^2 - 2), (y^3 - 2))?$$

Suppose that $((x^2 - 2), (y^3 - 2)) = ((x^2 - y^3))$. Then we would have that for some $p, q \in \mathbb{Q}[X]$

$$\begin{cases} x^2 - 2 = p(x^2 - y^3) \\ y^3 - 2 = q(x^2 - y^3) \end{cases}$$

But like, p cannot reduce the degree of y ans q cannot reduce the degree of x so this is absurd.

$(1, \cos\frac{2}{3}\pi + i \sin\frac{2}{3}\pi)$

To jest generowane przez x^2 i $y^3 - 1 = (y - 1)(y^2 + y + 1)$?

ZADANIE 6.

Assume that $f \in K[X]$ *is irreducible,* $\deg(f) = n > 0$, $\mathrm{char}(K) = 0$ *and* L *is the splitting field of polynomial* f *over* K. *Prove that the field* L *has at least* n *distinct automorphisms.*

First of all, I need f to have n distinct roots in L.

If a is at least a double root of f then $f'(a) = 0$. Let

$$f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \ldots + \alpha_1 x + \alpha_0$$

where $\alpha_n \neq 0$. Then, the derivative is

$$f'(x) = n\alpha_n x^{n-1} + (n - 1)\alpha_{n-1} x^{n-1} + \ldots + \alpha_1$$

and because we $\mathrm{char}(K) = 0$, then $n\alpha_n = \alpha_n + \ldots + \alpha_n \neq 0$. Thus, $f'(x) \not\equiv 0$.

We know that $f \in K[X]$ is irreducible and f' has lower degree, hence f' does not divide f. From Bezout's identity I get that there exist $p, q \in K[X] \setminus \{0\}$ such that

$$fp + f'q = 1.$$

If $f'(a) = 0$, then

$$0 = f(a)p(a) + f'(a)q(a) = 1$$

which is a contradiction, hence $f'(a) \neq 0$ and f has only simple roots.

Let $\phi \in \mathrm{Aut}(L)$ such that $\phi_{\restriction K} = \mathrm{id}_K$. Let $a_1, \ldots, a_n \in L$ be roots of f. Then for $i = 1, \ldots, n$ we have

$$0 = \phi(f(a_i)) = \phi\left(\sum_{k=0}^{n} \alpha_k a_i^k\right) = \sum_{k=0}^{n} \phi(\alpha_k a_i^k) =$$

$$= \sum_{k=0}^{n} \phi(\alpha_k)\phi(a_i^k) = \sum_{k=0}^{n} \alpha_k \phi(a_i)^k = f(\phi(a_i))$$

which implies that we can define an automorphism on L by simply mapping a_i to any of the roots of f and keeping the coefficients from K in place. This gives us with at least n such permutations of roots.

ZADANIE 7.

Assume that $K_1 \subseteq K_2 \subseteq K_3 \subseteq \ldots$ is an ascending sequence of fields. Verify in detail that $\bigcup K_n$ is also a field, containing $K_1, K_2, \ldots$ as subfields.

1. Group under addition:

Let $x, y \in K$, then $x, y \in K_i$ and so $x + y \in K_i$, $-x \in K_i$, $-y \in K_i$ because K_i is a field. Therefore, $x + y, -x \in K$.

2. Group under multiplication:

Let $x, y \in K$ then $x, y \in K_i$ and so $xy \in K_i$ and $x^{-1} \in K_i$. Therefore, $xy \in K$ and $x^{-1} \in K$.

3. Identity element & the zero:

I guess it boils down to showing that if $K \subseteq L$ are fields, then $1_K = 1_L$. Consider $x^2 - x \in K[X]$. We know that $1_K, 0_K$ are the two solutions in K and $1_L, 0_L$ are the two solutions in L. Therefore $\{1_K, 0_K\} = \{1_L, 0_L\}$. If $1_K = 0_L$, then for any $x \in K \subseteq L$ we would have that $x = 1_K x = 0_L x = 0_L$ and so x would be a zero divisor in L which cannot be true.

4. No zero divisors?

Suppose that $x, y \in K \setminus \{0\}$ such that $xy = 0$. But $x, y \in K_i$ and so $xy \in K_i$ and because K_i is a field, then $xy \neq 0$

EXERCISE 8.

Prove that the set $\{\sqrt{p} : p$ is a prime number$\}$ is linearly independent over the field $\mathbb{Q}$.

We will prove by induction that for any $p_1, \ldots, p_n$ and any $a_1, \ldots, a_n \in \mathbb{Q}$ the sum

$$\sum a_i \sqrt{p_i} \neq 0$$

For $n = 2$ it is quite simple. If

$$a_1\sqrt{p_1} + a_2\sqrt{p_2} = 0$$

then

$$a_1\sqrt{p_1} = -a_2\sqrt{p_2}$$
$$a_1^2 p_1 = a_2^2 p_2$$

and that cannot be true because p_2 appears once on the RHS and on the left side can only appear even number of times.

Suppose that $\sum_{i=1}^{n} a_i\sqrt{p_i} = A \neq 0$ and if we add $a\sqrt{p}$ then we suddenly get 0:

$$a_1\sqrt{p_1} + a_2\sqrt{p_2} + \ldots + a_n\sqrt{p_n} + a\sqrt{p} = 0$$
$$a_1\sqrt{p_1} + a_2\sqrt{p_2} + \ldots + a_n\sqrt{p_n} = -a\sqrt{p}$$
$$b_1\sqrt{p_1} + b_2\sqrt{p_2} + \ldots + b_n\sqrt{p_n} = \sqrt{p}$$

now, multiplying this by $\sqrt{p}$ on both sides gives us:

$$\sqrt{p}(b_1\sqrt{p_1} + b_2\sqrt{p_2} + \ldots + b_n\sqrt{p_n}) = p \in \mathbb{Q}$$