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 ($< \mathrm{def}(X^2 + a^2)$) 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 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

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

for $i = 1, \ldots, m$. Take $\overline{a} = (a_1, \ldots, a_n)$ be a solution from L. We have

$$0 = f_i(\overline{a}) = \sum_{1 \leq k \leq n} b_{i,k} a_k.$$

This is a linear combination of elements from L and therefore we have three possibilities:

1. $(\forall\ k = 1, \ldots, n)\ b_{i,k} = 0$ and so this equation does not influence the remaining $(m - 1)$ polynomials. From those remaining polynomials either one has non-zero coefficients $b_{j,k}$ (in this case we jump to case 2 or 3) or all polynomials from the set of equations are trivial and any sequence from K is a solution.

2. $(\forall\ k = 1, \ldots, n)\ a_k = 0$ and hence $\bar{a} = (0, \ldots, 0) \in K^n$ is a solution.

3. a_k and $b_{i,k}$ are linearly dependent and

$$\begin{aligned}
0 &= \sum_{1 \leq k \leq n} a_k b_{i,k} \\
0 &= a_1 b_{i,1} + \sum_{2 \leq k \leq n} a_k b_{i,k} \\
-a_1 b_{i,1} &= \sum_{2 \leq k \leq n} a_k b_{i,k} \\
b_{i,1} &= \sum_{2 \leq k \leq n} [a_k(-a_1)^{-1}] b_{i,k}
\end{aligned}$$

The last operation is permitted because we are inside a field and $-a_1$ is non-zero, therefore it has a multiplicative inverse. We have that

$$\sum_{2 \leq k \leq n} [a_k(-a_1)^{-1}] b_{i,k} \in K$$

and so $a_k(-a_1)^{-1} \in K \implies a_1, a_k \in K$.

i śmiga

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