Prof. Dr. Fabien Morel
Laurenz Wiesenberger

TUTORIAL SHEET 7
ALGEBRA
SUGGESTED SOLUTIONS

Winter term 25/26
December 8, 2025

Exercise 1.

(i) Let R and S be rings, and let $\varphi : R \to S$ be a ring homomorphism. Show that φ is injective if and only if $\ker(\varphi) = 0$.

Suggested solution. "$\Rightarrow$" If φ is injective, then $\varphi(0) = 0$ and thus $\ker(\varphi) = \{0\}$.

"$\Leftarrow$" Assume $\ker(\varphi) = \{0\}$. Let $x, y \in R$ and suppose $\varphi(x) = \varphi(y)$. Then

$$\varphi(x) - \varphi(y) = 0 \quad \Longrightarrow \quad \varphi(x - y) = 0.$$

Since $\ker(\varphi) = \{0\}$, we obtain $x - y = 0$, hence $x = y$. Therefore φ is injective.

□

(ii) Show that every ring homomorphism $\varphi : K \to L$, where K and L are fields, is injective.

Suggested solution. From the lecture we know that $\varphi(K^\times) \subseteq L^\times$. Since K is a field, every non-zero $x \in K$ is invertible, and thus

$$x \in K^\times \quad \Longrightarrow \quad \varphi(x) \neq 0.$$

Hence $\ker(\varphi) = \{0\}$. By part (i) it follows that φ is injective.

□

Exercise 2.

(1) Let k be a field with $|k| = \infty$. Consider the evaluation map from the lecture

$$\mathrm{ev} : k[X] \longrightarrow \mathrm{Map}(k, k), \quad P \longmapsto (x \mapsto P(x)).$$

Show that ev is a ring monomorphism.

Note: The same statement remains true for the polynomial ring $k[X_1, \ldots, X_n]$ in n variables.

Suggested solution. In the lecture it was already shown that

$$\mathrm{ev} : k[X] \longrightarrow \mathrm{Map}(k, k), \qquad P \longmapsto (x \mapsto P(x)),$$

is a ring homomorphism. Thus it suffices to show that ev is injective, provided that $|k| = \infty$.

Let $P \neq 0$. From linear algebra we know that a non-zero polynomial of degree d has at most d zeros. In particular, P cannot vanish on all of k because k is infinite. Hence the polynomial function

$$k \longrightarrow k, \qquad x \mapsto P(x)$$

is not the zero map. Therefore $\mathrm{ev}(P) \neq 0$, which shows that

$$\ker(\mathrm{ev}) = \{0\}.$$

By the previous exercise, this implies that ev is injective.

Generalisation to several variables.

The general case for $k[X_1, \ldots, X_n]$ is not harder. We prove the statement by induction on the number of variables. For $n = 1$ the claim was shown above.

Assume the claim holds for $n \in \mathbb{N}$. We show it also holds for $n + 1$.

Let

$$f \in k[X_1, \ldots, X_{n+1}] = k[X_1, \ldots, X_n][X_{n+1}]$$

be non-zero. Then f can be written as

$$f = \sum_{i=0}^{m} g_i(X_1, \ldots, X_n)\, X_{n+1}^i,$$

with $g_i \in k[X_1, \ldots, X_n]$ and $g_m \neq 0$. Since $g_m \neq 0$, by the induction hypothesis the polynomial function induced by g_m is not the zero map. Hence there exist $(a_1, \ldots, a_n) \in k^n$ such that

$$g_m(a_1, \ldots, a_n) \neq 0.$$

Now consider the polynomial in one variable

$$h(X_{n+1}) := \sum_{i=0}^{m} g_i(a_1, \ldots, a_n)\, X_{n+1}^i.$$

Since $g_m(a_1, \ldots, a_n) \neq 0$, we have $h \neq 0$. By the case $n = 1$, there exists $a_{n+1} \in k$ such that $h(a_{n+1}) \neq 0$. Consequently,

$$f(a_1, \ldots, a_n, a_{n+1}) \neq 0.$$

Thus the polynomial function induced by f is not the zero function, and therefore the evaluation map is injective in $n + 1$ variables as well.

$\square$

(2) Does the statement in (1) remain true if k is a finite field?

Suggested solution. Let p be a prime number. From the lecture we know that $\mathbb{F}_p$ is a field of cardinality p. Consider the polynomial

$$P = X^p - X \in \mathbb{F}_p[X].$$

Clearly, $P \neq 0$ as a polynomial. However, for every $x \in \mathbb{F}_p$ we have

$$P(x) = x^p - x = 0.$$

The identity $x^p = x$ for all $x \in \mathbb{F}_p$ follows directly from Fermat's Little Theorem (or equivalently from Lagrange's Theorem applied to the multiplicative group $\mathbb{F}_p^\times$, which has order $p-1$).

This argument generalizes to any finite field. Indeed, let $\mathbb{F}$ be a finite field. Then $\mathbb{F}$ has characteristic p, and we will later see in the lecture that

$$|\mathbb{F}| = p^n \quad \text{for some } n \in \mathbb{N}.$$

Thus you can consider the polynomial

$$P = X^{p^n} - X,$$

and using Lagrange's Theorem yields $P(x) = 0$, for all $x \in \mathbb{F}$.

Another way to see this is to observe that $\mathbb{F}[X]$ contains infinitely many elements, for example the monomials X^n for all $n \in \mathbb{N}$. In contrast, $\mathrm{Map}(k,k)$ has only $|k|^{|k|}$ elements. Hence, there cannot exist an injective map from $\mathbb{F}[X]$ into $\mathrm{Map}(k,k)$.

□

Exercise 3.

(1) Let R be a ring, and let

$$f(X) = \sum_{n=0}^{\infty} a_n X^n \in R[[X]].$$

Show that f is invertible in $R[[X]]$ if and only if $a_0 \in R^\times$.

Suggested solution. Let $f(X) = \sum_{n=0}^{\infty} a_n X^n \in R[[X]]$.

"$\Rightarrow$" Assume that f is invertible in $R[[X]]$. Then there exists a power series $g(X) = \sum_{n=0}^{\infty} b_n X^n \in R[[X]]$ such that $f \cdot g = 1$. In particular, $a_0 b_0 = 1$. Thus $a_0 \in R^\times$.

"$\Leftarrow$" Now assume that $a_0 \in R^\times$. We construct an inverse $g(X) = \sum_{n=0}^{\infty} b_n X^n$ recursively. Set

$$b_0 := a_0^{-1}.$$

Suppose that $b_0, b_1, \ldots, b_n$ are already defined. The coefficient of X^{n+1} in fg equals

$$a_0 b_{n+1} + \sum_{i=1}^{n+1} a_i b_{n+1-i}.$$

Since we require $fg = 1$, this coefficient must be zero. Hence we define

$$b_{n+1} := -a_0^{-1} \sum_{i=1}^{n+1} a_i \, b_{n+1-i}.$$

This recursion uniquely determines all coefficients b_n, and then a direct verification shows that indeed $f \cdot g = 1$.

□

(2) Deduce from (1) that the power series $1 - X$ is invertible in $R[[X]]$, and compute its inverse explicitly.

Suggested solution. We apply the recursion from part (1) to the series

$$f(X) = 1 - X.$$

Here, $a_0 = 1$ and $a_1 = -1$, while $a_n = 0$ for all $n \geq 2$.

The inverse $g(X) = \sum_{n=0}^{\infty} b_n X^n$ satisfies $f \cdot g = 1$, and the recursion from (1) gives:

$$b_0 = a_0^{-1} = 1,$$

$$b_1 = -a_0^{-1} a_1 b_0 = -1 \cdot (-1) \cdot 1 = 1.$$

Assume inductively that $b_0 = b_1 = \cdots = b_n = 1$. Then, using $a_0 = 1$, $a_1 = -1$, and all other $a_k = 0$, the recursion yields

$$b_{n+1} = -a_0^{-1} \sum_{i=1}^{n+1} a_i b_{n+1-i} = -1 \cdot (a_1 b_n) = -1 \cdot ((-1) \cdot 1) = 1.$$

Thus, by induction: $b_n = 1$ for all $n \geq 0$.

Therefore,

$$f^{-1}(X) = \sum_{n=0}^{\infty} X^n.$$

In particular,

$$\sum_{n=0}^{\infty} X^n = \frac{1}{1 - X}.$$

□

(3) Let R be an integral domain, and let

$$f(X) = \sum_{n=0}^{\infty} a_n X^n.$$

Define the valuation $v : R[[X]] \to \mathbb{N}_0 \cup \{\infty\}$ by

$$v(f) := \begin{cases} \min\{\, n \in \mathbb{N}_0 \mid a_n \neq 0 \,\}, & \text{if } f \neq 0, \\ \infty, & \text{if } f = 0. \end{cases}$$

Show that for all $f, g \in R[[X]]$:

$$v(fg) = v(f) + v(g), \qquad v(f+g) \geq \min\{v(f), v(g)\}.$$

Suggested solution.

Let R be an integral domain and let

$$f(X) = \sum_{i=0}^{\infty} a_i X^i, \qquad g(X) = \sum_{j=0}^{\infty} b_j X^j$$

be formal power series. We may assume without loss of generality that $f, g \neq 0$. Write

$$v(f) = n, \qquad v(g) = m,$$

so that

$$a_0 = \cdots = a_{n-1} = 0, \quad a_n \neq 0, \qquad b_0 = \cdots = b_{m-1} = 0, \quad b_m \neq 0.$$

(1) $v(fg) = v(f) + v(g)$

Using the definition of multiplication in $R[[X]]$,

$$(fg)(X) = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i \, b_{k-i} \right) X^k.$$

If $k < n+m$, then every pair $(i, k-i)$ satisfies either $i < n$ or $k - i < m$, and hence $a_i = 0$ or $b_{k-i} = 0$. Thus

$$\sum_{i=0}^{k} a_i \, b_{k-i} = 0 \quad \text{for all } k < n+m.$$

For $k = n+m$, the only non-zero contribution comes from $i = n$, giving

$$\sum_{i=0}^{n+m} a_i b_{n+m-i} = a_n b_m \neq 0,$$

since R is an integral domain. Hence $v(fg) = n + m = v(f) + v(g)$.

(2) $v(f+g) \geq \min(v(f), v(g))$

By definition of addition and the above assumptions, we have

$$f+g = \sum_{i=0}^{\infty}(a_i+b_i)X^i = \sum_{i=\min\{n,m\}}^{\infty}(a_i+b_i)X^i.$$

Thus $v(f+g) \geq h = \min(v(f), v(g))$.

$\square$