to be prepared for 20.10.2022

Exercise 6. We can check that the polynomial ring $K[x]$ over a field K is an integral domain by considering the degree function.

1. Prove, by a similar argument, that also the ring $K[[x]]$ of formal power series is an integral domain. Moreover show that K[[x]] is an Euclidean domain by introducing an appropriate function and verifying the required properties.
2. Show that $K[[x]]$ is a local ring.

Exercise 7. Let K be a field, and $f, g \in K[x]$ with $\deg(f) = n$, $\deg(g) = m$.

1. Show that polynomial division with remainder can be performed with at most $(2m+1)(n-m+1)+1$ field operations.
2. What is the maximum number of operations when we assume that f and g are monic?

Exercise 8. Consider a polynomial $f \in R[x]$ of degree $n \geq 0$, where R is a commutative ring with 1. The weight of f is

$$w(f) = \mathrm{card}\{k < n \mid f_k \neq 0\}$$

that is, the number of nonzero coefficients besides the leading coefficient f_n. The *sparse representation* of f is a list $(i, f_i)_{i \in I}$ s.t. $f = \sum_{i \in I} f_i x^i$. Show that two polynomials $f, g \in R[x]$ can be multiplied in sparse representation using at most

$$2w(f)w(g) + w(f) + w(g)$$

arithmetic operations.

Exercise 9. Show that multiplication of two matrices $A \in R^{m \times n}$ and $B \in R^{n \times p}$ (where R is a ring) takes $(2n-1)mp$ arithmetic operations in R.

Exercise 10. Let I be a unique factorization domain. Every $f \in I[x]$ can be decomposed into "content × primitive part"

$$f = \mathrm{cont}(f)\,\mathrm{pp}(f)$$

where $\mathrm{cont}(f) \in I$ and $\mathrm{pp}(f) \in I[x]$ is primitive, i.e., the GCD of all coefficients is 1. This decomposition is unique up to multiplication by units.

Given $f, g \in I[x]$, we write $f \sim g$ if there is a unit ε with $g = \varepsilon f$. Then prove the following:

1. $\mathrm{cont}(fg) \sim \mathrm{cont}(f) \cdot \mathrm{cont}(g)$
2. $\mathrm{pp}(fg) \sim \mathrm{pp}(f) \cdot \mathrm{pp}(g)$.