NMAI 076 - Algebra 2 - spring semester 2022/23

Homework 2

Deadline 22.05.2023, 10:40

Exercise 1. (10 points) Prove or disprove the following statements.

(1.1) All the algebraic extension fields of $\mathbb{Q}$ of degree 2 are isomorphic as rings.

(1.2) All the algebraic extension fields of $\mathbb{R}$ of degree 2 are isomorphic as rings.

(1.3) Let $f = x^8 + \sqrt{2}x^6 + 3 \in \mathbb{R}[x]$ and let $\alpha \in \mathbb{C}$ be such that $f(\alpha) = 0$. Then α is algebraic (over $\mathbb{Q}$).

(1.4) Let $f \in \mathbb{C}[x]$ and let $\alpha \in \mathbb{C}$. If $f \notin \mathbb{Q}[x]$ and α is algebraic, then $f(\alpha) \neq 0$.

(1.5) Let $f \in \mathbb{C}[x]$ and let $\alpha \in \mathbb{C}$. If α is transcendental and $f(\alpha) = 0$, then $f \notin \mathbb{Q}[x]$.

Exercise 2. (10 points) Determine the splitting field of $f = x^4 + 5x^2 + 5 \in \mathbb{Q}[x]$ and its degree over $\mathbb{Q}$.

Exercise 3. (10 points) The product $c = a \cdot b$ of two numbers given in binary expansion $a = \sum_{i=0}^{l} a_i 2^i$ and $b = \sum_{i=0}^{l} b_i 2^i$ can be computed as follows: multiply the polynomials $A = \sum a_i x^i$ and $B = \sum b_i x^i$ over $\mathbb{Z}[x]$, using fast multiplication in a ring $\mathbb{Z}_M[x]$ for big enough M, i.e. $M > 2(l+1)$. Then, evaluate $c = A \cdot B(2)$. This is the base principle of the Schönhage-Strassen-Algorithm for the multiplication of integers. The algorithm has time complexity $O(l \log(l) \log\log(l))$, which was the best-known until 2007.

(3.1) We showed that our fast multiplication algorithm for polynomials f, g in $\mathbf{T}[x]$ of degree less or equal than l takes $O(l \log(l))$ steps. So why does Schönhage-Strassen not have complexity $O(l \log(l))$? (*Hint:* what did we mean by "steps" in our analysis?)

(3.2) Instead of working in finite fields, Schönehage-Strassen uses the Fast Fourier Transform for polynomials from $\mathbb{Z}_M[x]$, with $M = 2^{2^{k-1}u} + 1$ for $u, k \in \mathbb{N}$. In general, such M is not prime. To show that FFT in $\mathbb{Z}_M[x]$ still works:

(a) Show that $\omega = 2^u$ is a 2^k-th primitive root of unity in $\mathbb{Z}_M$.

(b) Check that the inverse Fourier transformation can still be computed as in Proposition 10.1. (i.e. is everything well-defined? Does the proof still work?)

(c) For a number $x \in \mathbb{N}$ given in binary, how can one most efficiently compute $x \cdot \omega^i$? (this is the main benefit of this choice of M!)