Algorithmic Number Theory Prof. Dr. Ulrich Thiel
WS 19/20 University of Kaiserslautern

Exercise Sheet 2

Nov 4, 2019

Please tell me in/after the lecture on Monday what you want to have discussed

Exercise 1. Let $f \coloneqq X^3 - 3X - 1 \in \mathbb{Q}[X]$.

(a) Prove that f is irreducible.

(b) Let $L = K[X]/(f)$ be the stem field of f over $\mathbb{Q}$ and consider $\beta \coloneqq X^4 + 2X^3 + 3 \in \mathbb{Q}[X]$ as an element of L. Express β in the standard basis of L and compute its inverse.

Exercise 2. Determine a primitive element for the extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Exercise 3. Let $K \subseteq L \subseteq M$ be finite extensions with $K \subseteq M$ separable. Show that $\mathrm{Tr}_{L|K} \circ \mathrm{Tr}_{M|L} = \mathrm{Tr}_{M|K}$ and $\mathrm{N}_{L|K} \circ \mathrm{N}_{M|L} = \mathrm{N}_{M|K}$.

Exercise 4. Let D be a square-free integer. Show that the ring of integers in $\mathbb{Q}(\sqrt{D})$ is $\mathbb{Z}[\omega]$, where

$$\omega = \begin{cases} \sqrt{D} & \text{if } D \equiv 2, 3 \bmod 4 \\ \frac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \bmod 4 \end{cases}$$

Exercise 5. Let L be the splitting field of $X^8 - 2$ over $\mathbb{Q}$. Compute the minimal polynomial, characteristic polynomial, norm, and trace of $\alpha \coloneqq \sqrt[8]{2} \in L$.