Algorithmic Number Theory
WS 19/20

Prof. Dr. Ulrich Thiel
University of Kaiserslautern

Exercise Sheet 3

Nov 11, 2019

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

Exercise 1. You should at least know one example of a finite field extension that is *not* separable: explain why $\mathbb{F}_p(t^p) \subset \mathbb{F}_p(t)$ is an example.

Exercise 2. Prove that factorial rings are integrally closed.

Exercise 3. Let R be an integrally closed domain with fraction field K and let S be the integral closure of R in a finite separable extension of K. Let $\alpha \in S$.

(a) Show that α is a unit if and only if $N_{L|K}(\alpha)$ is a unit in R.
(b) Show that if $N_{L|K}(\alpha)$ is irreducible, then α is irreducible. Give an example showing that the converse is not true.

Exercise 4. Let $L = K(\alpha)$ be a finite separable extension of degree n. Show that

$$\mathrm{d}_{L|K}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = (-1)^{n(n-1)/2} \cdot \mathrm{N}_{L|K}(\mu'_\alpha(\alpha)) \; ,$$

where μ'_α is the formal derivative of μ_α.

Exercise 5. Let $n \in \mathbb{N}$ and consider the polynomial $f := X^n - 1 \in \mathbb{Q}[X]$. Let L be a splitting field of f over $\mathbb{Q}$. The roots of f in L are called *n-th roots of unity.*

(a) Explain why there are precisely n distinct n-th roots of unity in L and why they form a cyclic subgroup of $L \setminus \{0\}$. A generator of this group is called a *primitive* n-th root of unity.
(b) Explain why the number of primitive n-th root of unity is equal to $\varphi(n)$, the number of positive integers coprime to n.
(c) The polynomial

$$\Phi_n := \prod_{\substack{\zeta \text{ primitive} \\ n\text{-th root of unity}}} (X - \zeta) \in L[X]$$

is called the *n-th cyclotomic polynomial.* Show that $\Phi_n \in \mathbb{Z}[X]$.
(d) Show that Φ_n is irreducible in $\mathbb{Q}[X]$. (You can skip this part as it is not exciting and you may have proven this already in your algebra course).
(e) Explain why L is just the stem field of Φ_n. Conclude that $\dim_\mathbb{Q} L = \varphi(n)$ and that $L = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity.
(f) For $n = p^r$ a prime power show that

$$\mathrm{d}_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(1, \zeta, \ldots, \zeta^{\varphi(p^r)-1}) = \pm p^c \; ,$$

where $c = p^{r-1}(pr - r - 1)$.

Remark. We will eventually show that $\mathbb{Z}[\zeta_n]$ is the ring of integers in $\mathbb{Q}(\zeta_n)$.