Algorithmic Number Theory
WS 19/20

Prof. Dr. Ulrich Thiel
University of Kaiserslautern

Exercise Sheet 5

Nov 25, 2019

Exercise 1. Run the complete round-2 algorithm to compute an integral basis of the maximal order in the number field $L = \mathbb{Q}(\alpha)$, where α is a root of:

(a) $f = X^3 - X^2 - 2X - 8$.
(b) $f = X^3 - 9X - 9$.

Exercise 2. Determine the prime numbers p for which the equation order $\mathbb{Z}[\alpha]$ in $L(\alpha)$ is not p-maximal, where α is a root of:

(a) $f = X^3 - 3X + 6$.
(b) $f = X^4 + 5X^2 + 1$.

Exercise 3. Let L be the number field defined by a root α of an irreducible polynomial $f = X^n + aX + b \in \mathbb{Z}[X]$, where $n \in \mathbb{N}$. Show that the discriminant of the equation order $\mathbb{Z}[\alpha]$ is given by

$$d_{\mathbb{Z}[\alpha]} = (-1)^{n(n-1)/2}(n^n b^{n-1} + (1-n)^{n-1} a^n) \ .$$

Exercise 4. Let $n = p^k$ for a prime number p, let ζ be a primitive n-th root of unity, and let $\mathcal{O}$ be the ring of integers in $\mathbb{Q}(\zeta)$. Set $\lambda := 1 - \zeta$. We will show that $\mathcal{O} = \mathbb{Z}[\zeta]$.

(a) Show that $\lambda^{\varphi(n)}\mathcal{O} = p\mathcal{O}$.
(b) Show that $\mathcal{O}/\lambda\mathcal{O} \simeq \mathbb{Z}/p\mathbb{Z}$
(c) Show that the discriminant of $\mathbb{Z}[\zeta]$ is equal to a power of p.
(d) Show that $\mathbb{Z}[\lambda] = \mathbb{Z}[\zeta]$.
(e) Show that $\mathbb{Z}[\lambda] = \mathcal{O}$.