Algebraic Number Theory

Exercise Sheet 7

Prof. Dr. Nikita Geldhauser	Winter Semester 2024-25
PD Dr. Maksim Zhykhovich	03.12.2024

Exercise 1. Let A be a Dedekind ring and K the field of fractions of A. Let L be finite separable field extension of K. Let B be the integral closure of A in L. Let $\alpha \in B$ and let $f(X) \in K[X]$ be the minimal polynomial of α over K.
(1) Show that $f(X) \in A[X]$ (compare with Exercise 2, Sheet 1).
(2) Assume that $B = A[\alpha]$. Let ρ be a prime ideal in A. Choose monic pairwise different polynomials $g_1(X), ..., g_r(X) \in A[X]$, such that they are irreducible modulo ρ (that is in $(A/\rho)[X]$) and $f(X) = \prod_{i=1}^{r} g_i(X)^{e_i}$ modulo ρ.
Show that $\rho B = \prod_{i=1}^{r} (\rho, g_i(\alpha))^{e_i}$ is the decomposition of the ideal ρB into the product of powers of different prime ideals.
Hint: Use the same arguments as in the proof of Exercise 2, Sheet 5.

Exercise 2. We have seen in the lecture that 6 decomposes not uniquely as a product of irreducible elements in $\mathbb{Z}[\sqrt{-5}]$, namely $6 = 2{\cdot}3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Interpret the last equalities in terms of the decomposition of fractional ideals.
Hint: Using Exercise 1 find the decomposition of (2) and (3) into the product of prime ideals.

Exercise 3. Let A be an integral, noetherian, local ring, such that its maximal ideal is principal and non-zero. Show that A is a dvr.
Hint: Proceed in the same way as in the proof of Satz 27 (last Claim).

Exercise 4. Let A be a dvr with maximal ideal $\mathfrak{m}$ and uniformizing element π. Let $P(X) \in A[X]$ be a monic polynomial. Set $B := A[X]/(P)$.
(1) Suppose that the reduction of P modulo $\mathfrak{m}$ is irreducible. Show that B is a dvr and π is a uniformizing element of B.
Hint: Use Exercise 3.
(2) Let $P(X) = X^n + a_{n-1}X^{n-1} + ... + a_0$. Suppose that a_0 is a uniformizing element of A and $a_0 \mid a_i$ for every $i = 1, ..., n-1$. Show that B is a dvr and the class of X is a uniformizing element of B.
Hint: Use Eisenstein's criterion.