Algebraic Number Theory

Exercise Sheet 5

PD Dr. Maksim Zhykhovich Winter Semester 2026-27, 12.11.2026

Exercise 1. Let $\mathbb{Q} \subset L$ be a number field and let α be an element in L, which is integral over $\mathbb{Z}$. Let $P(X)$ be the minimal polynomial of α over $\mathbb{Q}$. Recall that $P(X) \in \mathbb{Z}[X]$ (see Exercise 2, Sheet 1). Show that $\mathbb{Z}[X]/(P(X)) \simeq \mathbb{Z}[\alpha] \subset L$.

Exercise 2. Let A be a ring and let I, J be two ideals in A.
(1) Let $f : A \to B$ be a surjective ring homomorphism. Show that $f(I)$ is an ideal in B.
(2) Let $\varphi : A \to A/I$ be the canonical ring homomorphism. Show that

$$A/(I+J) \simeq (A/I)/\widetilde{J},$$

where $\widetilde{J} = \varphi(J)$ is an ideal in A/I. *Hint:* Consider $A/I \to A/(I+J)$.
(3) Deduce from (2) the following isomorphism of rings, which we will use often in the lectures and exercises

$$(A/I)/\widetilde{J} \simeq (A/J)/\widetilde{I},$$

where $\widetilde{I}$ is the image of I in A/J.
(4) Let $\alpha \in \mathbb{C}$ be a root of $X^3 + 2X + 1$ and let $L = \mathbb{Q}(\alpha)$. Recall that $\mathcal{O}_L = \mathbb{Z}[\alpha] \subset L$ (see Exercise 1, Sheet 3).
Using Exercise 1 and question (3) show that

a) (3) is a prime ideal in $\mathcal{O}_L$.
b) (2) is not a prime ideal in $\mathcal{O}_L$.
c) $\rho_1 = (2, \alpha+1)$, $\rho_1 = (2, \alpha^2+\alpha+1)$ are prime ideals in $\mathcal{O}_L$ and $(2) = \rho_1\rho_2$.

Exercise 3. Let $L = \mathbb{Q}(i)$ be the quadratic field with $i^2 = -1$. Recall that the ring of Gaussian integers $\mathcal{O}_L = \mathbb{Z}[i]$ is a PID. Let p be a prime number.
(1) Show that p remains prime in $\mathbb{Z}[i]$ if and only if $p \equiv 3 \bmod 4$.
Hint: Use Exercise 1 and Exercise 2.3.
(2) (**Fermat's two-square theorem**) Deduce from (1) that a prime number p can be written as a sum of two squares of integers if and only if $p \not\equiv 3 \bmod 4$.

Exercise 4. Recall that for any prime number p the ring $\mathbb{Z}_{(p)}$ is a dvr and $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}_{(p)}$. Let $L = \mathbb{Q}(i)$ be the quadratic field with $i^2 = -1$. Find all primes p for which the integral closure of $\mathbb{Z}_{(p)}$ in L is a dvr.
Hint: Use first Exercise 4, Sheet 4.