MATH 511
EXERCISES 4

A. ZEYTİN

Throughout by K we denote a number field and by $\mathcal{O}_K$ its ring of integers. By R we denote a commutative ring with unity.

(1)

(2) Set $K = \mathbf{Q}(\sqrt{-17})$.
- ▶ Determine the ring of integers of K. More precisely, show that $\mathcal{O}_K = \mathbf{Z}[\sqrt{-17}]$.
- ▶ Show that factorization in $\mathcal{O}_K$ is not unique. Hint: Try to factor 18. And deduce that $h_K > 1$, in fact, it is equal to 4.

  Set $\wp_1 = \langle 2, 1+\sqrt{-17}\rangle$, $\wp_2 = \langle 3, 1+\sqrt{-17}\rangle$ and $\wp_3 = \langle 3, 1-\sqrt{-17}\rangle$.
- ▶ Show that $18 \in \wp_1^2$ and deduce $\wp_1^2$ is a factor of (18).
- ▶ Without using the previous part show that $\nu_{\wp_1}((18)) = 2$, $\nu_{\wp_2}((18)) = 2$ and $\nu_{\wp_3}((18)) = 2$.
- ▶ Determine the factorization of (18) in $\mathcal{O}_K$.
- ▶ Determine $\nu_{\wp_1}((2))$ in $\mathcal{O}_K$.
- ▶ Show that $(3) = \wp_2\wp_3$ in $\mathcal{O}_K$.
- ▶ Compute the norms of all the ideals $\wp_1$, $\wp_2$, $\wp_3$, (18) and verify the multiplicativity of norm on ideals.

(3) Set $K = \mathbf{Q}(\sqrt{-5})$ and $\wp_1 = \langle 2, 1+\sqrt{-5}\rangle$, $\wp_2 = \langle 3, 1+\sqrt{-5}\rangle$, and $\wp_3 = \langle 3, 1-\sqrt{-5}\rangle$.
- ▶ Show that for each $i = 1, 2, 3$ the ideal $\wp_i$ is maximal, hence prime.
- ▶ Compute $\nu_{\wp_1}(2)$ and show that $(2) = \wp_1^2$
- ▶ Compute $\nu_{\wp_2}(3)$ and $\nu_{\wp_3}(3)$ and show that $(3) = \wp_2\wp_3$.
- ▶ Compute $\nu_{\wp_i}((6))$ for $i = 1, 2, 3$ and given the fact that no other ideals appear in the factorization of (6) determine the factorization of (6).
- ▶ Eplain $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ using the above computations.
- ▶ Compute the norms of all the ideals $\wp_1$, $\wp_2$, $\wp_3$, (2), (3), (6) and verify the multiplicativity of norm on ideals.
- ▶ Can the ideals $\wp_i$, $i = 1, 2, 3$ be pricipal. Which ones are equivalent in the class group?

(4) Set $K = \mathbf{Q}(\sqrt{-6})$ and $\wp_1 = \langle 2, \sqrt{-6}\rangle$.
- ▶ Show that $\wp_1$ is a maximal ideal, hence a prime ideal.
- ▶ Calculate $\nu_{\wp_1}(6)$.
- ▶ Find another prime ideal $\wp_2$ so that $(6) = \wp_1^2\wp_2^2$.
- ▶ Use this to explain the two factorings of 6 as $\sqrt{-6} \cdot -\sqrt{-6}$ and $2 \cdot 3$.

(5) Factorize
- ▶ (6) in $\mathbf{Z}[\sqrt{-5}]$,
- ▶ (18) in $\mathbf{Z}[\sqrt{2}]$,
- ▶ (30) in $\mathbf{Z}[\sqrt{-29}]$.

(6) Sketch the following lattices and their fundamental domains in $\mathbf{R}^2$ to observe that fundamental domain of a lattice is not uniquely determined until one specifies a set of generators:
- ▶ $(-1, 2)$ and $(2, 2)$
- ▶ $(1, 1)$ and $(2, 3)$
- ▶ $(1, \pi)$ and $(\pi, 1)$
- ▶ $(-1, -1)$ and $(0, 1)$

(7) Find two different fundamental domains for the lattice L in $\mathbf{R}^3$ generated by $(0, 0, 1)$, $(0, 2, 0)$ and $(1, 1, 1)$. Show that volumes of the two fundamental domains are equal. Prove more generally that any fundamental domain of any lattice has same volume.

(8) This exercise sketches a proof of the *two squares theorem*: if p is a prime number congruent to 1 modulo 4, then p is a sum of two squares:

- ► Let p be such a prime. Show that the multiplicative group of the field with p elements has an element, say u, of order 4. In particular $u^2 = -1$.
- ► Show that the set $L = \{(a, b) \in \mathbf{Z}^2 \colon b \equiv ua \mod p\}$ is a lattice in $\mathbf{R}^2$. Can you determine one?
- ► Show that the index $[\mathbf{Z}^2 : L] = p$ and deduce that if T is a fundamental domain for T, then $\mathrm{vol}(T) = p$.
- ► Apply Minkowski's theorem to the circle centered at the origin and of radius $r^2 = \frac{3p}{2}$ to get the result.

(9) Prove that not every integer is a sum of three squares.

(10) This exercise outlines a proof of *four squares theorem*: every positive integer is a sum of four integer squares:

- ► Let p be an odd prime. ($p = 2$ can be written as $1^2+1^2+0^2+0^2$.) Show that the congruence $u^2+v^2+1 \equiv 0 \mod p$ always has a solution in $\mathbf{Z}$.
- ► Fix a solution of the above congruence, and show that the set
$$L = \{(a, b, c, d) \in \mathbf{Z}^4 \colon c \equiv ua + vb \text{ and } d \equiv ub - va \mod p\}$$
is in fact a lattice in $\mathbf{R}^4$ with $[\mathbf{Z}^4 \colon L] = p^2$.
- ► Apply again Minkowski's theorem to the sphere in $\mathbf{R}^4$ of radius determined by $r^2 = 1.9p$ (in fact something greater than $16p^2$ is enough!) to deduce the result for the prime number p.
- ► Finish the general case using the identity:
$$(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) =$$
$$(aA - bB - cC - dD)^2 + (aB + bA + cD - dC)^2 + (aC - bD + cA + dB)^2 + (aD + bC - cB + dA)^2$$

(11) Find the embeddings $\sigma_i \colon K \longrightarrow \mathbf{C}$ for the following fields and determine the integers s and t

- ► $\mathbf{Q}(\sqrt{5})$
- ► $\mathbf{Q}(\sqrt{-5})$
- ► $\mathbf{Q}(\sqrt[4]{5})$
- ► $\mathbf{Q}(\sqrt[3]{5})$
- ► $\mathbf{Q}(e^{2\pi\sqrt{-1}/p})$, for a prime number p.

(12) Let K be a number field of degree n. Show that
$$\Delta(\alpha_1, \ldots, \alpha_n) = (\det(\sigma_i(\alpha_j)))$$