Prof. Dr. U. Görtz
Dr. F. Fité

Wintersemester 2015/16

ALGEBRAIC NUMBER THEORY I

Problem Set 9

Delivery: 12/1/2016

Exercise 1.

i) Show that $K = \mathbb{Q}(\sqrt{-14})$ has class group isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

Hint: Show that the class group is generated by the prime ideals dividing $2\mathcal{O}_K$ and $3\mathcal{O}_K$, show that they are non principal, and find relations among them by looking at the prime ideal decomposition of $(2+\sqrt{-14})\mathcal{O}_K$.

ii) Show that $K = \mathbb{Q}(\sqrt{-30})$ has class group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Hint: Show that the class group is generated by the prime ideals dividing $2\mathcal{O}_K$, $3\mathcal{O}_K$, and $5\mathcal{O}_K$, show that they are non principal, and find relations among them by finding a principal ideal of norm 30.

iii) Show that $K = \mathbb{Q}(\sqrt{-26})$ has class group isomorphic to $\mathbb{Z}/6\mathbb{Z}$.

Exercise 2. Show that if K is a quadratic imaginary field, then

i) $\mu_K = \{1, -1, i, -i\}$ if $K = \mathbb{Q}(i)$, where $i = \sqrt{-1}$.

ii) $\mu_K = \{\omega^j \mid 0 \leq j \leq 5\}$ if $K = \mathbb{Q}(\omega)$, where $\omega = \frac{1+\sqrt{-3}}{2}$.

iii) $\mu_K = \{\pm 1\}$, otherwise.

Exercise 3. Let $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ be a number field of degree 4. Prove that the cardinality of μ_K is 2, 4, 6, 8, or 12. Give examples of K showing that all these values can occur.

Hint: Use that if ζ_n denotes a primitive n-th root of unity, then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, where $\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^\times$ denotes the Euler φ-function. Note that by the Chinese Remainder Theorem, we have that $\varphi(nm) = \varphi(n)\varphi(m)$ if $(n, m) = 1$. From the easy fact that $\varphi(p^i) = p^{i-1}(p-1)$ if p is a prime and $i \geq 1$, one has

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

where the product runs over primes p dividing n.

Exercise 4. Let p be an odd prime, ζ_p a primitive pth root of unity, and $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ the ring of integers of $K = \mathbb{Q}(\zeta_p)$.

i) Show that if k is an integer such that $0 < k \leq p-1$, then

$$\xi = 1 + \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{k-1} \in \mathcal{O}_K^\times .$$

Hint: Recall that $|N_{K/\mathbb{Q}}(1-\zeta_p)| = |N_{K/\mathbb{Q}}(1-\zeta_p^k)| = p$ and note that $\xi(1-\zeta_p) = 1 - \zeta_p^k$.

ii) Show that the roots of unity of K are of the form $\pm\zeta_p^k$ for $0 \leq k \leq p-1$.

Hint: Let $G \subseteq K^\times$ be the subgroup generated by the roots of unity of K. Thus $G = \langle \zeta_n \rangle$ for a certain primitive n-th root of unity ζ_n. Note that $2p|n$ and $\varphi(n) = \varphi(2p)$.

iii) Take an embedding $K \subseteq \mathbb{C}$. Show that any unit $u \in \mathcal{O}_K^\times$ can be written as $u = \zeta_p^i v$, where $0 \leq i \leq p-1$ and $v \in \mathbb{R} \cap \mathcal{O}_K^\times$.

Hint: Let c denote complex conjugation and note that it restricts to an automorphism of K. Show that $u/c(u)$ is a root of unity in K by noting that the absolute value of all of its Galois conjugates is 1. Note that $\mathfrak{p} = (1-\zeta_p) = (1-c(\zeta_p)) \subseteq \mathcal{O}_K$ by i), and this is a prime ideal by the hint in i). Rule out the possibility $u/c(u) = -\zeta_p^j$, for some $0 \leq j \leq p-1$, by finding a contradiction by reducing modulo $\mathfrak{p}$. Deduce the statement from $u/c(u) = \zeta_p^j$.

iv) Show that the fundamental unit of $\mathbb{Q}(\sqrt{5})$ is $\frac{1+\sqrt{5}}{2}$.

v) Let now $p = 5$, $\zeta = \zeta_5$. Show that

$$\mathcal{O}_K^\times = \{\pm\zeta^i(1+\zeta)^j \mid 0 \leq i \leq 4, j \in \mathbb{Z}\}.$$

Hint: Use that $-\zeta^2(1+\zeta) = (1+\sqrt{5})/2$ (see Ex.1.ii) of PS5, for example) and also take iii) and iv) into consideration.