June 18, 2014

Algebraic Number Theory

Prof. H. Esnault

Exercise sheet 10[1]

Definition. *Let d be a square free integer and $K = \mathbb{Q}(\sqrt{d})$; let $\mathcal{O}_K$ be its ring of integers. We define the following sets of prime numbers:*

- $\mathscr{D} := \{p \in \mathbb{Z} \,|\, p \text{ decomposes in } K\}$
- $\mathscr{I} := \{p \in \mathbb{Z} \,|\, p\mathcal{O}_K \text{ is prime}\}$
- $\mathscr{R} := \{p \in \mathbb{Z} \,|\, p \text{ ramifies in } K\}$

Since $[K : \mathbb{Q}] = 2$, every prime number lies in $\mathscr{D}$, $\mathscr{I}$ or $\mathscr{R}$.

Write δ for the discriminant of K. Recall that for an ideal $I \subset \mathcal{O}_K$ we follow Milne in writing $\mathbb{N}(I) = |\mathcal{O}_K : I|$.

- *A nonzero ideal $I \subset \mathcal{O}_K$ is called* normalized *if it satisfies the following two conditions*
  (a) $\mathbb{N}(I) = \prod_{r\in\mathscr{R}} r^{e_r} \prod_{p\in\mathscr{D}} p^{e_p}$ *with $e_r \in \{0,1\}$ and $e_p \geq 0$*
  (b) *The inequality*
  $$\mathbb{N}(I) \leq \begin{cases} \frac{1}{2}\sqrt{|\delta|} & \text{if } \delta > 0 \\ \frac{2}{\pi}\sqrt{|\delta|} & \text{if } \delta < 0 \end{cases}$$
  holds.
- *I is called* primitive *if there exists no $m \in \mathbb{Z} \setminus \{1\}$ such that $m\mathcal{O}_K | I$.*
- *The set of normalized primitive ideals of $\mathcal{O}_K$ is denoted by $\mathscr{N}$.*

Exercise 1. Let d be a square free integer and $K = \mathbb{Q}(\sqrt{d})$. Show that every fractional ideal of K is equivalent to an ideal in $\mathscr{N}$. (*Hint*: Use the Minkowski bound.)

Exercise 2. Infer from the previous exercise that if $d > 0$, then the class number of K is 1 in the cases $\delta = 5, 8, 12, 13$, and if $d < 0$, then the class number is 1 if $\delta = -3, -4, -7, -8$.

Exercise 3. We use the notation from the previous exercise. Let

$$x = (u + v\sqrt{d})/2,$$

with

[1] If you want your solutions to be corrected, please hand them in just before the lecture on June 25th. If you have any questions concerning these exercises you can contact Lars Kindler via kindler@math.fu-berlin.de or come to Arnimallee 3 112A.

- $u, v \in \mathbb{Z}$
- $u \equiv v \mod 2$,
- and $u, v \in 2\mathbb{Z}$ if $d \equiv 2, 3 \mod 4$.

Let $I \in \mathscr{N}$ and $m := \mathbb{N}(I)$. Show that the following statements are equivalent:

(a) $x\mathcal{O}_K$ is primitive with $\mathbb{N}(x\mathcal{O}_K) = m$

(b) $(u^2 - v^2 d)/4 = \pm m$, and

$$\begin{cases} \gcd(u/2, v/2) = 1 & \text{if } d \equiv 2, 3 \mod 4 \\ \gcd((u-v)/2, v) = 1 & \text{if } d \equiv 1 \mod 4 \end{cases}$$

(*Hint:* This is easier than it looks.)

Exercise 4. Again, let $K = \mathbb{Q}(\sqrt{d})$. Show that the class number of K is 2 if $d = 10$ or $d = -15$.

Hint for $d = 10$:

(a) Show (or accept) that there are prime ideals $Q, P, P' \subset \mathcal{O}_K$, such that $2\mathcal{O}_K = Q^2$, $3\mathcal{O}_K = PP'$, and that $\mathbb{N}(Q) = 2$, $\mathbb{N}(P) = \mathbb{N}(P') = 3$.

(b) Deduce that

$$\{m \in \mathbb{Z} | \exists I \in \mathscr{N}, m = \mathbb{N}(I)\} = \{1, 2, 3\}.$$

(c) Use the previous exercise to show that Q, P, P' are not principal, and that QP and QP' are principal.

(d) Conclude Q, P, P' generate the same class in $\mathrm{Cl}(K)$, and that the class number of K is 2.