# Algebraic Number Theory
# MATH 512

## Solutions to Assignment 3

**1.** Throughout, we let $\mathrm{Gal}(L/\mathbb{Q}) = \langle\sigma\rangle$. Assume (i). Let $\alpha = x+y\sqrt{-k}$, so that $\alpha^{1+\sigma} = p$. Then $(\alpha)_{\mathcal{O}_L}^{1+\sigma} = (p)_{\mathcal{O}_L}$. Since $p$ is unramified in $L$ by assumption, $p$ splits into distinct primes $(\alpha)_{\mathcal{O}_L}$ and $(\alpha)_{\mathcal{O}_L}^{\sigma}$. Further, these primes are principal and therefore split completely in $M/L$. Thus $p$ splits completely in $M/\mathbb{Q}$.

Conversely, assume (ii). Then $p$ splits in $L/\mathbb{Q}$, i.e. $(p)_{\mathcal{O}_L} = \mathfrak{p}\mathfrak{q}$ with $\mathfrak{p} \neq \mathfrak{q}$, and because $\mathfrak{p}$ and $\mathfrak{q}$ split completely in $M/L$, they are necessarily principal. Hence $\mathfrak{p} = (\alpha)_{\mathcal{O}_L}$ for some $\alpha \in \mathcal{O}_L$, and $\mathfrak{q} = (\alpha)_{\mathcal{O}_L}^{\sigma}$. Therefore $(p)_{\mathcal{O}_L} = (\alpha^{1+\sigma})_{\mathcal{O}_L}$, i.e. $p = \alpha^{1+\sigma}u$ for some $u \in \mathcal{O}_L^{\times}$. Writing $\alpha = x + y\sqrt{-k}$ with $x, y \in \mathbb{Z}$, we see that $u = p/(x^2 + ky^2)$, a positive rational, and is therefore equal to 1. Thus $x^2 + ky^2 = p$.

**2.** Suppose $\mathfrak{p}$ is a prime of $L$ that ramifies in $M/L$, and let $p$ be the rational prime below $\mathfrak{p}$. Then $p$ ramifies in $M/\mathbb{Q}$, and so must ramify in $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and in $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ by the remark at the beginning of the question sheet. However, this is impossible since only 2 ramifies in $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and only 3 ramifies in $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$. Thus every prime ideal of $L$ is unramified in $M/L$.

**3.** We use the fact that every ideal class can be represented by an ideal of norm at most

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d_L|}, \tag{1}$$

where $n = [L : \mathbb{Q}] = 2$, $2r_2 = 2$ is the number of non-real complex embeddings of $L$, and $d_L = -24$ is the discriminant of $L$. Computing this number explicitly, we see that the greatest integer less than or equal to it is 3. Thus every ideal class can be represented by a product of primes above 2 and 3. Since 2 and 3 ramify in $L$, we have $(2) = \mathfrak{p}^2$ and $(3) = \mathfrak{q}^2$, with $\mathfrak{p}, \mathfrak{q}$ prime. Further, because $\mathfrak{p}$ and $\mathfrak{q}$ have norm 2 and 3 respectively, any non-trivial ideal class is represented by either $\mathfrak{p}$ or $\mathfrak{q}$. Thus $\mathrm{Cl}(L)$ has order at most 3.

Observe now that $\mathfrak{p}$ cannot be principal, for if $\mathfrak{p} = (\alpha)$ with $\alpha = a + b\sqrt{-6}$ and $a, b \in \mathbb{Z}$, then

$$\begin{aligned} 2 &= \mathbf{N}\mathfrak{p} \\ &= |N(\alpha)| \\ &= a^2 + 6b^2, \end{aligned}$$

which is impossible. Therefore the class of $\mathfrak{p}$ in $\mathrm{Cl}(L)$ has order 2, so that $|\mathrm{Cl}(L)| = 2$.

(b) $2 = [\mathbb{Q}(\sqrt{2}, \sqrt{-3}) : L]$, which, by question **2.**, divides $[M : L] = |\mathrm{Cl}(L)| = 2$. Hence $\mathbb{Q}(\sqrt{2}, \sqrt{-3}) = M$. (In fact, we see now that in **2.**, after showing that

$|\mathrm{Cl}(L)| \leq 3$, we may have completed the proof that $|\mathrm{Cl}(L)| = 2$ by comparing field degrees in the above manner.)

(c) Firstly, the equation has no integral solutions when $p$ is 2 or 3, so we may assume that $p$ is unramified in $L$ and therefore apply question **1.** Hence the equation has a solution if and only if $p$ splits completely in $M/\mathbb{Q}$, and by the remark at the beginning of the question sheet, this happens if and only if $p$ splits completely in both $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$, that is to say $\left(\frac{2}{p}\right) = \left(\frac{-3}{p}\right) = 1$. By quadratic reciprocity, this happens if and only if $(-1)^{(p^2-1)/8} = \left(\frac{p}{3}\right) = 1$, i.e. $p \equiv 1$ or $7 \bmod 8$ and $p \equiv 1 \bmod 3$, i.e. $p \equiv 1$ or $7 \bmod 24$.

**4.** Note that we may take $\zeta_8 = \frac{1}{\sqrt{2}}(1+i)$: begin by observing that $(1+i)^2 = 2i$. This also shows that $\sqrt{2} \in L$, since $i = \zeta_8^2 \in L$. Now let $G_p$ be the decomposition group of $p$ in $G = \mathrm{Gal}(L/\mathbb{Q})$, and recall that $G_p$ is generated by the Frobenius $\varphi_p : \zeta_8 \mapsto \zeta_8^p$. By Dedekind's theorem on the splitting of primes, $\left(\frac{2}{p}\right) = 1$ if and only if $p$ splits in $\mathbb{Q}(\sqrt{2})$, if and only if $\sqrt{2} \in L^{G_\mathfrak{p}}$, if and only if $\varphi_p(\sqrt{2}) = \sqrt{2}$. Therefore we may complete our solution by showing that $\varphi_p$ fixes $\sqrt{2}$ if and only if $p \equiv 1$ or $-1 \bmod 8$.

We may speed up our verification if we notice that

$$\sqrt{2} = \frac{1+i}{\zeta_8} = \frac{1+\zeta_8^2}{\zeta_8} = \zeta_8 + \zeta_8^{-1}.$$

Also, the minimal polynomial for $\zeta_8$ over $\mathbb{Q}$ is $x^4+1$ since $\zeta_8^2$ is a primitive 4th root of unity, and so the sum of the four primitive 8th roots of unity is 0, i.e. $\zeta_8^3 + \zeta_8^{-3} = -(\zeta_8 + \zeta_8^{-1})$. Hence, since $\varphi_p(\sqrt{2}) = \varphi_p(\zeta_8 + \zeta_8^{-1}) = \zeta_8^p + \zeta_8^{-p}$, we now see immediately that $\varphi_p(\sqrt{2}) = \sqrt{2}$ if and only if $p \equiv 1$ or $-1 \bmod 8$.

**5.** We begin by observing that for a positive integer $a$, $|\mathcal{O}_K : a\mathcal{O}_K| = |N(a)| = a^{[K:\mathbb{Q}]} = a^n$, i.e. there are $a^n$ residue classes mod $a\mathcal{O}_K$. Now, take $l$ *as given in the question* and choose elements $\gamma_1, \ldots, \gamma_l$ as in the proof of Lemma 43. Also let $f = \llbracket (3b)^n \rrbracket$. Assume that for each $a = 1, \ldots, f$, the number of $i \in \{1, \ldots, l\}$ such that $|N(\gamma_i)| = a$ is no more than $a^n$. Then $l \leq \sum_{a=1}^{f} a^n = l - 1$, a contradiction. Therefore there exists $a \in \{1, \ldots, f\}$ such that more than $a^n$ of the $\gamma_i$ have $|N(\gamma_i)| = a$, in other words, more than $|\mathcal{O}_K : a\mathcal{O}_K|$ of the $\gamma_i$ have $|N(\gamma_i)| = a$. Therefore, as stated at the beginning of the proof of Lemma 43, there exist $i, j$ distinct with $\gamma_i\gamma_j^{-1} \in U_K$.