Problem sheet 3 Solutions

Problem 1

Note that the norm of $a + b\sqrt{-d} \in K$ with $a, b \in \mathbb{Q}$ is given by $a^2 + db^2$.

Case 1: $d \not\equiv 3 \pmod 4$.

In this case $\{1, \sqrt{-d}\}$ is an integral basis of K, so any element in O_K can be written $a + b\sqrt{-d}$, where $a, b \in \mathbb{Z}$. Since $N(a + b\sqrt{-d}) = a^2 + db^2$ is always bigger than 1 unless $(a, b) = (\pm 1, 0)$, ± 1 are the only units in O_K.

Case 2: $d \equiv 3 \pmod 4$ and $d \geq 7$.

In this case $\{1, \frac{1+\sqrt{-d}}{2}\}$ is an integral basis of K, so any element in O_K can be written $a + b\left(\frac{1+\sqrt{-d}}{2}\right)$, where $a, b \in \mathbb{Z}$. Since $N\left(a + b\left(\frac{1+\sqrt{-d}}{2}\right)\right) = a^2 + ab + (\frac{d+1}{4})b^2$ is always bigger than 1 unless $(a, b) = (\pm 1, 0)$, ± 1 are the only units in O_K.

Case 3: $d = 3$.

In this case $\{1, \frac{1+\sqrt{-3}}{2}\}$ is an integral basis of K, and the norm of $a + b\left(\frac{1+\sqrt{-3}}{2}\right)$ is $a^2 + ab + b^2$. The integral solutions of $a^2 + ab + b^2 = \pm 1$ are $(a, b) = (\pm 1, 0), (0, \pm 1), (\pm 1, \mp 1)$, and these solutions are corresponding to $\pm 1, \pm\omega, \pm\omega^2$, which are the units in O_K.

Problem 2

$\{1, \sqrt{2}\}$ is an integral basis of K. To show that there are infinitely many units in O_K, it suffices to prove that there are infinitely many integral solutions of $N(x + y\sqrt{2}) = \pm 1$, i.e. $(x + y\sqrt{2})(x - y\sqrt{2}) = \pm 1$. We can easily find a solution $(x_1, y_1) = (1, 1)$. Now we generate infinitely many integral solutions from $(x_1, y_1) = (1, 1)$. From $(1 + \sqrt{2})(1 - \sqrt{2}) = 1$, we have

$$(1 + \sqrt{2})^n (1 - \sqrt{2})^n = (-1)^n.$$

We can write $(1 + \sqrt{2})^n = x_n + y_n\sqrt{2}$ and $(1 - \sqrt{2})^n = x_n - y_n\sqrt{2}$ for some $x_n, y_n \in \mathbb{N}$, and one can also check x_n is increasing. Hence, $N(x_n + y\sqrt{2}) = \pm 1$ for all $n \in \mathbb{N}$ and $x_n + y_n\sqrt{2}$'s are infinitely many units O_K.

Problem 3

(a) The minimal polynomial of ζ is $f(t) = t^4 + t^3 + t^2 + t + 1$. Let $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ be the complex embeddings of K and let $\theta_i = \sigma_i(\zeta)$ for $i = 1, 2, 3, 4$. We also write

$$s_1 = \sum_{i=1}^{4} \theta_i, \quad s_2 = \sum_{i \neq j} \theta_i\theta_j, \quad s_3 = \sum_{i \neq j \neq k} \theta_i\theta_j\theta_k, \quad s_4 = \prod_{i=1}^{4} \theta_i.$$

From the coefficients of the minimal polynomial $f(t)$ we evaluate $s_1 = -1$, $s_2 = 1$, $s_3 = -1$, and $s_4 = 1$. Then

$$\begin{aligned} N(\zeta + 2) &= \prod_{i=1}^{4} \sigma_i(\zeta + 2) = \prod_{i=1}^{4} (\theta_i + 2) \\ &= 16 + 8s_1 + 4s_2 + 2s_3 + s_4 = 11. \end{aligned}$$

Similarly, we also get $N(\zeta - 2) = 16 - 8s_1 + 4s_2 - 2s_3 + s_4 = 31$.

(b) As $N(\zeta+2) = 11$ and $N(\zeta-2) = 31$ are primes, $\zeta+2$ and $\zeta-2$ are irreducible in $\mathbb{Z}[\zeta]$.

Problem 4

(a) Suppose that $x = ab$ for some $a, b \in R$. If x is prime, then either $x|a$ or $x|b$. To prove that x is irreducible, it suffices to show that either a or b is a unit. Without loss of generality, we may assume $x|a$, i.e. there exists $c \in R$ such that $a = xc$. It follows that $x = ab = xcb$. Since R is an integral domain we have $1 = cb$, hence b is a unit.

(b) The converse is false: 2 is irreducible but not a prime in $\mathbb{Z}[\sqrt{-5}]$.

Let us consider the factorization $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{5})$. Since $N(2) = 4$ and $N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$, 2 does not divide neither $1 + \sqrt{-5}$ nor $1 - \sqrt{-5}$. Hence, 2 is not a prime in $\mathbb{Z}[\sqrt{-5}]$.

Now we show that 2 is irreducible. If there exist $a, b \in O_K \setminus O_K^\times$ such that $2 = ab$, then we have $N(a)N(b) = N(2) = 4$, so $N(a) = N(b) = 2$. However, it is impossible because the norm of any element in O_K must be in form of $x^2 + 5y^2$, where $x, y \in \mathbb{Z}$. Thus, 2 is irreducible.

(c) For any $x \in \mathbb{Z}[\sqrt{-5}]$ we claim that if $5|N(x)$, then $\sqrt{-5}|x$. To see this, let $x = a + b\sqrt{-5}$ for some $a, b \in \mathbb{Z}$. If $5|N(x) = a^2 + 5b^2$, then we have $5|a$, so we can write $a = 5a'$ for some $a' \in \mathbb{Z}$. It follows that $x = 5a' + b\sqrt{-5} = \sqrt{-5}(b - a'\sqrt{-5})$, hence $\sqrt{-5}|x$.

Now we prove that $\sqrt{-5}$ is a prime. If $\sqrt{-5}|xy$, then $5 = N(\sqrt{-5})|N(x)N(y)$. It implies that either $5|N(x)$ or $5|N(y)$. By the above claim, we conclude that either $\sqrt{-5}|x$ or $\sqrt{-5}|y$.

Problem 5

(a) Observe that $f^{-1}(I)$ is the kernel of the map $R \to S \to S/I$. It implies that $f^{-1}(I)$ is an ideal of R.

(b) False. Let $R = \mathbb{Z}$, $S = \mathbb{Q}$, and $\sigma : \mathbb{Z} \to \mathbb{Q}$ be the inclusion map. For any $n \in \mathbb{N}$, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ but not an ideal of $\mathbb{Q}$.

Problem 6

As $\mathbb{Z}[i]$ is a Euclidean domain, we may apply Euclidean division algorithm. As a result, the greatest common divisor of $4 + 7i = (2 + i)(3 + 2i)$ and $1 + 3i = (2 + i)(1 + i)$ is $2 + i$.