Problem sheet 4 Solutions

Problem 1

Note that $K(t)/\langle f(t)\rangle$ is a field if and only if $\langle f(t)\rangle$ is a maximal ideal. Hence, it suffices to show that $f(t)$ is irreducible if and only if $\langle f(t)\rangle$ is a maximal ideal.

Suppose that $f(t)$ is irreducible and I is an ideal containing $\langle f(t)\rangle$. Since $K(t)$ is Euclidean, $K(t)$ is a principal ideal domain. It follows that there exists $g(t) \in K(t)$ such that $I = \langle g(t)\rangle$. As $\langle f(t)\rangle \subseteq \langle g(t)\rangle$, we have $g(t)|f(t)$. Since $f(t)$ is irreducible, either $g(t)$ or $\frac{f(t)}{g(t)}$ is a unit, hence either $I = K(t)$ or $I = \langle f(t)\rangle$. Thus, $\langle f(t)\rangle$ is a maximal ideal.

Conversely, if $f(t)$ is reducible, then there exist $g(t), h(t) \in K(t)$ such that neither $g(t)$ nor $h(t)$ is a unit. Then $\langle g(t)\rangle \neq K(t)$ is an ideal properly containing $\langle f(t)\rangle$, so $\langle f(t)\rangle$ is not a maximal ideal.

Problem 2

Suppose that $\mathfrak{b}$ is a fractional ideal, i.e. there exist $\mathfrak{a} \in O_K$ and $c \in O_K \setminus \{0\}$ such that $\mathfrak{b} = c^{-1}\mathfrak{a}$. Then the condition (a) is clear. We also have (b) since $\mathfrak{b}O_K = c^{-1}\mathfrak{a}O_K \subseteq c^{-1}\mathfrak{a} = \mathfrak{b}$. The condition (c) also holds for $x = c$.

Conversely, suppose that $\mathfrak{b}$ satisfies (a),(b), and (c). Let $x \in O_K$ be the element satisfying $x\mathfrak{b} \subseteq O_K$ as in (c). Then (a) and (b) imply that $\mathfrak{a} = x\mathfrak{b}$ is an ideal of O_K. Thus $\mathfrak{b} = x^{-1}\mathfrak{a}$ is a fractional ideal.

Problem 3

$\{1, \frac{1+\sqrt{-3}}{2}\}$ is an integral basis of K, so $x + y\sqrt{-3}$ with $x, y \in \mathbb{Q}$ is contained in O_K if and only if $x + y, x - y \in \mathbb{Z}$. It follows that

$$\begin{aligned}
\mathfrak{a}^{-1} &= \{\alpha \in K : \alpha\mathfrak{a} \subseteq O_K\} \\
&= \{x + y\sqrt{-3} : x, y \in \mathbb{Q}, (x + y\sqrt{-3})\left\langle 2, \frac{1-\sqrt{-3}}{2}\right\rangle \subseteq O_K\} \\
&= \{x + y\sqrt{-3} : x, y \in \mathbb{Q}, 2x + 2y\sqrt{-3}, \frac{x+3y}{2} + \frac{y-x}{2}\sqrt{-3} \in O_K\} \\
&= \{x + y\sqrt{-3} : 2x + 2y, 2x - 2y, 2y, x + y \in \mathbb{Z}\} \\
&= \{x + y\sqrt{-3} : 2y, x - y \in \mathbb{Z}\} = O_K.
\end{aligned}$$

Problem 4

(a) $\{1, \sqrt{5}\}$ is an integral basis of $\mathbb{Q}(\sqrt{5})$. Let M_1 be the base-change matrix from $\{1, \sqrt{5}\}$ to $\{2, 1+\sqrt{5}\}$, and M_2 be the base-change matrix from $\{1, \sqrt{5}\}$ to $\{3, 1-\sqrt{5}\}$. Then we have

$$M_1 = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 3 & 0 \\ 1 & -1 \end{pmatrix}.$$

Since $O_K/\mathfrak{p}_1 \cong \mathbb{Z}^2/(M_1\mathbb{Z}^2) \cong \mathbb{Z}/2\mathbb{Z}$ and $O_K/\mathfrak{p}_2 \cong \mathbb{Z}^2/(M_2\mathbb{Z}^2) \cong \mathbb{Z}/3\mathbb{Z}$ are fields, $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are maximal ideals. By Proposition 4.65 we also have

$$|O_K/\mathfrak{p}_1| = N(\mathfrak{p}_1) = |\det(M_1)| = 2,$$

$$|O_K/\mathfrak{p}_2| = N(\mathfrak{p}_2) = |\det(M_2)| = 3.$$

(b) Suppose that $\mathfrak{p}_1$ is a principal ideal, i.e. there exists $x \in O_K \backslash O_K^\times$ such that $\langle x \rangle = \langle 2, 1+\sqrt{-5} \rangle$. Then $x|2$ and $x|1+\sqrt{-5}$, hence $N(x)|N(2) = 4$ and $N(x)|N(1+\sqrt{-5}) = 6$. It follows that $N(x) = 2$. However, there is no $x \in O_K$ satisfying $N(x) = 2$ as there is no integral solution of $a^2 + 5b^2 = 2$. Thus, $\mathfrak{p}_1$ is not a principal ideal. The same argument still works for $\mathfrak{p}_2$.

(c) Note that

$$\begin{aligned}\mathfrak{p}_1\mathfrak{p}_2 &= \langle 2 \cdot 3, 2 \cdot (1-\sqrt{-5}), (1+\sqrt{-5}) \cdot 3, (1+\sqrt{-5})(1-\sqrt{-5})) \rangle \\ &= \langle 6, 2(1-\sqrt{-5}), 3(1+\sqrt{-5}).\rangle\end{aligned}$$

As $6 = (1+\sqrt{-5})(1-\sqrt{-5})$ and $3(1+\sqrt{-5}) = (-2+\sqrt{-5})(1-\sqrt{-5})$, we have $\mathfrak{p}_1\mathfrak{p}_2 \subseteq \langle 1-\sqrt{-5} \rangle$. On the other hand, $1-\sqrt{-5} \in \mathfrak{p}_1\mathfrak{p}_2$ since $1-\sqrt{-5} = 6-(2-2\sqrt{-5})-(3+3\sqrt{-5})$. Thus, $\mathfrak{p}_1\mathfrak{p}_2$ is principal and $1-\sqrt{-5}$ is a generator.

Problem 5

Recall that $\mathbb{Z}[i]$ is a Euclidean domain (see the proof of Theorem 4.8), hence $\mathbb{Z}[i]$ is a principal ideal domain. It follows that all fractional ideals in $\mathbb{Z}[i]$ must be in a form of $\frac{b}{a}\mathbb{Z}[i]$, where $a, b \in \mathbb{Z}[i]$, $a \neq 0$, and $\gcd(a, b) = 1$.

Problem 6

Let $e_1 = 1, e_2, \cdots, e_n$ be a $\mathbb{Z}$-basis of O_K, and $f_1, \cdots, f_n$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$, where n is the degree of K. Let M be the integral base-change matrix from $e_1, \cdots, e_n$ to $f_1, \cdots, f_n$. Note that there exists integral matrix X such that

$XM = MX = \det(M)\,\mathrm{Id}_n$. It follows that X is the integral base-change matrix from $f_1, \cdots, f_n$ to $\det(M)e_1, \cdots, \det(M)e_n$. In particular, $N(\mathfrak{a}) = \det(M) = \det(M)e_1$ can be expressed by an integral linear combination of $f_1, \cdots, f_n$, hence $N(\mathfrak{a}) \in \mathfrak{a}$.