# Problem sheet 5 Solutions

## Problem 1

(a)

$$\begin{aligned}\mathfrak{p}^2 &= \langle 2^2, 2(1+\sqrt{-5}), (1+\sqrt{-5})^2\rangle \\ &= \langle 4, 2+2\sqrt{-5}, -4+2\sqrt{-5}\rangle = \langle 2\rangle,\end{aligned}$$

$$\mathfrak{p}\mathfrak{q} = \langle 2\cdot 3, 2(1+\sqrt{-5}), 3(1+\sqrt{-5}), (1+\sqrt{-5})^2\rangle = \langle 1+\sqrt{-5}\rangle.$$

(b) Observe that $N(\mathfrak{p})^2 = N(\mathfrak{p}^2) = N(2) = 4$ and $N(\mathfrak{p})N(\mathfrak{q}) = N(\mathfrak{p}\mathfrak{q}) = N(1+\sqrt{-5}) = 6$. It follows that $N(\mathfrak{p}) = 2$ and $N(\mathfrak{q}) = 3$, hence $\mathfrak{p}$ and $\mathfrak{q}$ are maximal.

(c) We have

$$\begin{aligned}\mathfrak{p} &= \{2(a+b\sqrt{-5}) + (1+\sqrt{-5})(c+d\sqrt{-5}) : a,b,c,d\in\mathbb{Z}\} \\ &= \{2(a-b-3d) + (1+\sqrt{-5})(2b+c+d) : a,b,c,d\in\mathbb{Z}\} \\ &= \{2x + (1+\sqrt{-5})y : x,y\in\mathbb{Z}\},\end{aligned}$$

$$\begin{aligned}\mathfrak{q} &= \{3(a+b\sqrt{-5}) + (1+\sqrt{-5})(c+d\sqrt{-5}) : a,b,c,d\in\mathbb{Z}\} \\ &= \{3(a-b-2d) + (1+\sqrt{-5})(3b+c+d) : a,b,c,d\in\mathbb{Z}\} \\ &= \{3x + (1+\sqrt{-5})y : x,y\in\mathbb{Z}\}.\end{aligned}$$

Hence, $\{2, 1+\sqrt{-5}\}$ is a $\mathbb{Z}$-basis of $\langle 2, 1+\sqrt{-5}\rangle$, and $\{3, 1+\sqrt{-5}\}$ is a $\mathbb{Z}$-basis of $\langle 3, 1+\sqrt{-5}\rangle$.

## Problem 2

(a) Since $N(\mathfrak{a})|N(6) = 36 = 2^2 3^2$, we shall factorize $\langle 2\rangle$ and $\langle 3\rangle$ into maximal ideals. The minimal polynomial of $\mathbb{Z}[\sqrt{-5}]$ is $x^2+5$. We factorize the minimal polynomial modulo 2 and 3:

$$x^2+5 \equiv (x+1)^2 \pmod 2, \quad x^2+5 \equiv (x+1)(x-1) \pmod 3.$$

Applying Dedekind's criterion, we can factorize $\langle 2\rangle$ and $\langle 3\rangle$ as follows:

$$\begin{aligned}\langle 2\rangle =& \mathfrak{p}_2^2, & \mathfrak{p}_2 &= \langle 2, 1+\sqrt{-5}\rangle, \\ \langle 3\rangle =& \mathfrak{p}_3\mathfrak{p}_3', & \mathfrak{p}_3 &= \langle 3, 1+\sqrt{-5}\rangle, \mathfrak{p}_3' = \langle 3, 1-\sqrt{-5}\rangle.\end{aligned}$$

Note that $N(\mathfrak{p}_2) = 2$ and $N(\mathfrak{p}_3) = N(\mathfrak{p}_3') = 3$. We also observe that neither $\mathfrak{p}_3^2$ nor $\mathfrak{p}_3'^2$ does not contain 6. Hence, $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_3', \mathfrak{p}_2^2 = \langle 2\rangle, \mathfrak{p}_3\mathfrak{p}_3' = \langle 3\rangle, \mathfrak{p}_2\mathfrak{p}_3 = \langle 1+\sqrt{-5}\rangle, \mathfrak{p}_2\mathfrak{p}_3' = \langle 1-\sqrt{-5}\rangle$, $\mathfrak{p}_2^2\mathfrak{p}_3 = \langle 6, 2+2\sqrt{-5}\rangle, \mathfrak{p}_2^2\mathfrak{p}_3' = \langle 6, 2-2\sqrt{-5}\rangle, \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3' = \langle 6, 3+3\sqrt{-5}\rangle, \mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}_3' = \langle 6\rangle$ are all the ideals containing 6.

(b) As $18 = 2\cdot 3^2$, we factorize $\langle 2\rangle$ and $\langle 3\rangle$ into maximal ideals. The minimal polynomial of $\mathbb{Z}[\sqrt{5}]$ is $x^2-5$. We first factorize the minimal polynomial modulo 2 and 3:

$$x^2 - 5 \equiv (x+1)^2 \pmod 2, \quad x^2 - 5 \equiv x^2 + 1 \pmod 3.$$

Applying Dedekind's criterion, we can factorize $\langle 2\rangle$ and $\langle 3\rangle$ as follows:

$$\begin{aligned}\langle 2\rangle =&\mathfrak{p}_2^2, \qquad \mathfrak{p}_2 = \langle 2, 1+\sqrt{5}\rangle,\\ \langle 3\rangle =&\mathfrak{p}_3, \qquad \mathfrak{p}_3 = \langle 3, (\sqrt{5})^2+1\rangle = \langle 3\rangle.\end{aligned}$$

Note that $N(\mathfrak{p}_2) = 2$ and $N(\mathfrak{p}_3) = 3^2$. It follows that the unique ideal in $\mathbb{Z}[\sqrt{5}]$ with norm 18 is $\mathfrak{p}_2\mathfrak{p}_3$.

(c) Recall that $\{1, \alpha = \frac{1+\sqrt{-3}}{2}\}$ is an integral basis of $L$. The minimal polynomial of $\alpha$ is $x^2 - x + 1$. As $12 = 2^2\cdot 3$, we factorize $\langle 2\rangle$ and $\langle 3\rangle$ into maximal ideals:

$$\begin{aligned}\langle 2\rangle =&\mathfrak{p}_2, \qquad \mathfrak{p}_2 = \langle 2\rangle,\\ \langle 3\rangle =&\mathfrak{p}_3^2, \qquad \mathfrak{p}_3 = \langle \sqrt{-3}\rangle.\end{aligned}$$

We have $N(\mathfrak{p}_2) = 2^2$ and $N(\mathfrak{p}_3) = 3$. Hence, $\mathfrak{p}_2\mathfrak{p}_3$ is the unique ideal in $O_L$ of norm 12.

## Problem 3

Since $N(\mathfrak{a})|N(5-2\sqrt{-5}) = 45 = 3^2\cdot 5$, we shall factorize $\langle 3\rangle$ and $\langle 5\rangle$ into maximal ideals. We factorize the minimal polynomial $x^2+5$ modulo 2 and 3:

$$x^2 + 5 \equiv (x+1)(x-1) \pmod 3, x^2 + 5 \equiv x^2 \pmod 5.$$

Applying Dedekind's criterion, we can factorize $\langle 3\rangle$ and $\langle 5\rangle$ as follows:

$$\begin{aligned}\langle 3\rangle =&\mathfrak{p}_3\mathfrak{p}_3', \qquad \mathfrak{p}_3 = \langle 3, 1+\sqrt{-5}\rangle, \mathfrak{p}_3' = \langle 3, 1-\sqrt{-5}\rangle,\\ \langle 5\rangle =&\mathfrak{p}_5^2, \qquad \mathfrak{p}_5 = \langle \sqrt{-5}\rangle.\end{aligned}$$

By straightforward calculations, one can check that $5-2\sqrt{-5} \in \mathfrak{p}_3'$ but $5-2\sqrt{-5} \notin \mathfrak{p}_3$. Thus, we have factorization $\mathfrak{a} = \mathfrak{p}_3'^2\mathfrak{p}_5$.

## Problem 4

As $24 = 2^3 \cdot 3$, we factorize $\langle 2 \rangle$ and $\langle 3 \rangle$ into maximal ideals. The minimal polynomial of $\mathbb{Z}[\sqrt{6}]$ is $x^2 - 6$. We first factorize the minimal polynomial modulo 2 and 3:

$$x^2 - 6 \equiv x^2 \pmod 2, \quad x^2 - 6 \equiv x^2 \pmod 3.$$

Applying Dedekind's criterion, we can factorize $\langle 2 \rangle$ and $\langle 3 \rangle$ as follows:

$$\begin{aligned} \langle 2 \rangle =& \mathfrak{p}_2^2, \qquad \mathfrak{p}_2 = \langle 2, \sqrt{6} \rangle, \\ \langle 3 \rangle =& \mathfrak{p}_3^2, \qquad \mathfrak{p}_3 = \langle 3, \sqrt{6} \rangle. \end{aligned}$$

Note that $N(\mathfrak{p}_2) = 2$ and $N(\mathfrak{p}_3) = 3$. It follows that the unique ideal in $\mathbb{Z}[\sqrt{6}]$ with norm 24 is $\mathfrak{p}_2^3\mathfrak{p}_3$.

## Problem 5

(a) By Corollary 2.42, we have

$$\Delta[1, \alpha, \alpha^2] = -27 \cdot 2^2 - 4 \cdot 2^3 = -140 = -2^2 \cdot 5 \cdot 7.$$

Note that 2 is the largest integer $N$ such that $N^2 | \Delta[1, \alpha, \alpha^2]$. On the other hand, observe that the minimal polynomial $x^3 + 2x + 2$ satisfies Eisenstein's criterion for $p = 2$. By Proposition 3.30, any $\theta = \frac{1}{2} \sum_{i=0}^{2} a_i \alpha^i$ for $a_i \in \{0, 1\}$ not all 0 is not an algebraic integer. It follows that $\{1, \alpha, \alpha^2\}$ is an integral basis of $K$.

(b) We first factorize the minimal polynomial moudlo 5 and 7:

$$x^3 + 2x + 2 \equiv (x-1)^2(x+2) \pmod 5, \quad x^3 + 2x + 2 \equiv (x-2)^2(x-3) \pmod 7.$$

Applying Dedekind's criterion, we can factorize $\langle 5 \rangle$ and $\langle 7 \rangle$ as follows:

$$\begin{aligned} \langle 5 \rangle =& \mathfrak{p}_5^2\mathfrak{p}_5', \qquad \mathfrak{p}_5 = \langle 5, \alpha - 1 \rangle, \mathfrak{p}_5' = \langle 5, \alpha + 2 \rangle \\ \langle 7 \rangle =& \mathfrak{p}_7^2\mathfrak{p}_7', \qquad \mathfrak{p}_7 = \langle 7, \alpha - 2 \rangle, \mathfrak{p}_7' = \langle 7, \alpha - 3 \rangle. \end{aligned}$$

(c) Let $\alpha, \beta$, and $\gamma$ be the conjugates of $\alpha$. By Vieta's formula, we have $\alpha + \beta + \gamma = 0$, $\alpha\beta + \beta\gamma + \gamma\alpha = 2$, and $\alpha\beta\gamma = -2$. Hence,

$$N(3 - \alpha) = (3 - \alpha)(3 - \beta)(3 - \gamma) = 3^3 - 3^2 \cdot 0 + 3 \cdot 2 + 2 = 35 = 5 \cdot 7.$$

One can check that $3-\alpha \in \mathfrak{p}_5'$ but $3-\alpha \notin \mathfrak{p}_5$, and $3-\alpha \in \mathfrak{p}_7'$ but $3-\alpha \notin \mathfrak{p}_7$. It follows that $\langle 3-\alpha \rangle = \mathfrak{p}_5'\mathfrak{p}_7'$.

(d) Similarly, we calculate

$$N(5-\alpha) = (5-\alpha)(5-\beta)(5-\gamma) = 5^3 - 5^2 \cdot 0 + 5 \cdot 2 + 2 = 137.$$

Since 137 is prime, $5-\alpha$ is irreducible in $O_K$.