Michaelmas 2012, NT III/IV, Solutions to Problem Sheet 4.

1 (i) $\theta = \sqrt[3]{7}$ has min. poly. $X^3 - 7$ in $\mathbb{Q}[X]$ (irreducible over $\mathbb{Q}$ by Eisenstein's Criterion with prime 7). So $n = |K : \mathbb{Q}| = 3$ with basis $\mathcal{B} = \{1, \theta, \theta^2\}$ over $\mathbb{Q}$.

Put $\alpha = a + b\theta + c\theta^2$. We find

$$\left\{\begin{array}{ll} \hat{\alpha}(1) = & a + b\theta + c\theta^2 \\ \hat{\alpha}(\theta) = & 7c + a\theta + b\theta^2 \\ \hat{\alpha}(\theta^2) = & 7b + 7c\theta + a\theta^2 \end{array}\right\} \text{ and so the matrix of } \hat{\alpha} \text{ is } A = \begin{pmatrix} a & 7c & 7b \\ b & a & 7c \\ c & b & a \end{pmatrix}.$$

Hence $\mathrm{Tr}_K(\alpha) = \mathrm{Tr}(A) = 3a$ and $N_K(\alpha) = \det(A) = \cdots = a^3 + 7b^3 + 49c^3 - 21abc$.

(ii) Let $f(X) = X^3 + X^2 + 2$. By the Gauss Lemma any root of $f(X)$ in $\mathbb{Q}$ must be an integer dividing the constant term, i.e. ± 1 or ± 2. Neither of these work. So $f(X)$ has no roots in $\mathbb{Q}$. Thus, since $f(X)$ is only cubic, it is irreducible in $\mathbb{Q}[X]$. Hence $f(X)$ is the min. poly. of θ over $\mathbb{Q}$, $n = |K : \mathbb{Q}| = 3$ and we can take $\mathcal{B} = \{1, \theta, \theta^2\}$ as a basis for K over $\mathbb{Q}$.

Put $\alpha = a + b\theta + c\theta^2$. We find

$$\left\{\begin{array}{lllll} \hat{\alpha}(1) = & & = & a & +b\theta & +c\theta^2 \\ \hat{\alpha}(\theta) = & a\theta + b\theta^2 + c\theta^3 & = & -2c & +a\theta & +(b-c)\theta^2 \\ \hat{\alpha}(\theta^2) = & -2c\theta + a\theta^2 + (b-c)\theta^3 & = & 2(c-b) & -2c\theta & +(a+c-b)\theta^2 \end{array}\right\}$$

$$\text{And so the matrix of } \hat{\alpha} \text{ is } A = \begin{pmatrix} a & -2c & 2(c-b) \\ b & a & -2c \\ c & b-c & a+c-b \end{pmatrix}.$$

Thus $\mathrm{Tr}_K(\alpha) = \mathrm{Tr}(A) = 3a - b + c$ and

$N_K(\alpha) = \det(A) = a^3 - 2b^3 + 4c^3 - a^2b + a^2c + 2b^2c - 4ac^2 + 6abc$.

2 (i)Let $f(X) = X^4 + 2X + 2$. Then $f(X)$ irreducible over $\mathbb{Q}$ by Eisenstein's Criterion with prime 2. Thus $f(X)$ is the min. poly. of θ over $\mathbb{Q}$, $n = |K : \mathbb{Q}| = \deg(f) = 4$ and we can take $\mathcal{B} = \{1, \theta, \theta^2, \theta^3\}$ as a basis for K over $\mathbb{Q}$.

We find

$$\left\{\begin{array}{llllll} \widehat{\theta^3}(1) = & & & & & \theta^3 \\ \widehat{\theta^3}(\theta) = \theta^4 = & -2 & -2\theta & & & \\ \widehat{\theta^3}(\theta^2) = & & -2\theta & -2\theta^2 & & \\ \widehat{\theta^3}(\theta^3) = & & & -2\theta^2 & -2\theta^3 & \end{array}\right\}. \text{ So } M = \begin{pmatrix} 0 & 0 & 0 & 1 \\ -2 & -2 & 0 & 0 \\ 0 & -2 & -2 & 0 \\ 0 & 0 & -2 & -2 \end{pmatrix}^t$$

is the matrix of $\widehat{\theta^3}$. Thus $\mathrm{Tr}_K(\theta^3) = \mathrm{Tr}(M) = -6$.

Now put $\alpha = a + b\theta$. We find

$$\left\{\begin{array}{llllll} \widehat{\alpha}(1) & = & a & +b\theta & & \\ \widehat{\alpha}(\theta) & = & & a\theta & +b\theta^2 & \\ \widehat{\alpha}(\theta^2) & = & & & a\theta^2 & +b\theta^3 \\ \widehat{\alpha}(\theta^3) = a\theta^3 + b\theta^4 & = & -2b & -2b\theta & & +a\theta^3 \end{array}\right\}.$$

$$\text{So } M = \begin{pmatrix} a & b & 0 & 0 \\ 0 & a & b & 0 \\ 0 & 0 & a & b \\ -2b & -2b & 0 & a \end{pmatrix}^t$$

is the matrix of $\widehat{a + b\theta}$. Thus $N_K(a + b\theta) = \det(M) = \ldots = a^4 - 2ab^3 + 2b^4$.

7 (ii) Let $f(X) = X^4 + 1$. Then $f(X+1) = X^4 + 4X^3 + 6X^2 + 4X + 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion with prime 2 and so $f(X)$ is irreducible, also. Thus $f(X)$ is the min. poly. of θ over $\mathbb{Q}$, $n = |K : \mathbb{Q}| = \deg(f) = 4$ and we can take $\mathcal{B} = \{1, \theta, \theta^2, \theta^3\}$ as a basis for K over $\mathbb{Q}$.

We find

$$\left\{\begin{array}{lll} \widehat{\theta^3}(1) & = & \theta^3 \\ \widehat{\theta^3}(\theta) & = \theta^4 = & -1 \\ \widehat{\theta^3}(\theta^2) & = & -\theta \\ \widehat{\theta^3}(\theta^3) & = & -\theta^2 \end{array}\right\}. \quad \text{So } M = \begin{pmatrix} 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix}^t.$$

is the matrix of $\widehat{\theta^3}$. Thus $\mathrm{Tr}_K(\theta^3) = \mathrm{Tr}(M) = 0$.

Now put $\alpha = a + b\theta$. We find

$$\left\{\begin{array}{lllll} \widehat{\alpha}(1) & = a & +b\theta & & \\ \widehat{\alpha}(\theta) & = & a\theta & +b\theta^2 & \\ \widehat{\alpha}(\theta^2) & = & & a\theta^2 & +b\theta^3 \\ \widehat{\alpha}(\theta^3) = a\theta^3 + b\theta^4 & = -b & & & +a\theta^3 \end{array}\right\}.$$

$$\text{So } M = \begin{pmatrix} a & b & 0 & 0 \\ 0 & a & b & 0 \\ 0 & 0 & a & b \\ -b & 0 & 0 & a \end{pmatrix}^t$$

is the matrix of $\widehat{a + b\theta}$. Thus $N_K(a + b\theta) = \det(M) = \ldots = a^4 + b^4$.

3 (i) and (ii): Multiply out.

(iii) The roots of $Z^n - 1$ are ζ^r for $r = 0, 1, \ldots, n-1$.
So $Z^n - 1 = \prod_{r=1}^{n-1}(Z - \zeta^r)$.
Thus $X^n - Y^n = Y^n((X/Y)^n - 1) = Y^n \prod_{r=1}^{n-1}((X/Y) - \zeta^r) = \prod_{r=1}^{n-1}(X - \zeta^r Y)$.

4 (i) $(1+\theta, 2)_R(1 - \theta + \theta^2, 2)_R = (1 + \theta^3, 2(1 - \theta + \theta^2), 2(1+\theta), 4)$
$= (8, 2(1 - \theta + \theta^2), 2(1+\theta), 4)$
$= (8, 2(1 - 2\theta), 2(1+\theta), 4) \quad [\![g_2 - \theta g_3]\!]$
$= (8, 2(3), 2(1+\theta), 4) \quad [\![g_2 + 2g_3]\!]$
$= (8, 2, 2(1+\theta), 4) \quad [\![g_2 - g_4]\!]$
$= (2) \quad$ (since 2 divides all the *other* generators).

(ii) $(1+\theta, 2)_R^3 = \cdots = ((1+\theta)^3, 2(1+\theta)^2, 4(1+\theta), 8)_R$
$= (1+\theta)((1+\theta)^2, 2(1+\theta), 4, 1 - \theta + \theta^2)_R$
$= (1+\theta)((1+\theta)^2, 2(1+\theta), 4, -3\theta)_R \quad [\![g_4 - g_1]\!]$
$= (1+\theta)((1+\theta)^2, 2(1+\theta), 4, -3\theta, 21)_R \quad [\![g_5 = -\theta^2 g_4]\!]$
$= (1+\theta)R \quad [\![\gcd(4, 21) = 1]\!]$.

(iii) We must show that, for α and $\beta \in R$, $\psi(\alpha) \in \mathbb{Z}^{\geq 0}$ (this is clear from the formula of Q6(i)) and that

(a) $\psi(\alpha\beta) = \psi(\alpha)\psi(\beta)$ (clear from properties of a norm);
(b) $\psi(\alpha) = 0 \implies \alpha = 0$ (clear from properties of a norm)) and
(c) $\psi(\alpha) = 1 \implies \alpha \in R^*$.

So we only need bother with (c).

Suppose $\psi(\alpha) = 1$ so $N_K(\alpha) = \pm 1$. Put $\alpha = a + b\theta + c\theta^2$ with $a, b, c \in \mathbb{Z}$.

Putting $X = a$, $Y = b\theta$ and $Z = c\theta^2$ in Q8(ii) we find
$\pm 1 = N_K(\alpha) = a^3 + 7b^3 + 49c^3 - 21abc = \alpha(a^2 + b^2\theta^2 + 7c^2\theta - ab\theta - 7bc - ac\theta^2)$.
Thus $\pm(a^2 + b^2\theta^2 + 7c^2\theta - ab\theta - 7bc - ac\theta^2)$ is an inverse for α in R.
So $\alpha \in R^*$, as required.

(iv) Note that the converse of (iii) above is also true.For if $\alpha \in R^*$ then $\alpha\beta$ =1 for some $\beta \in R$ and $\psi(\alpha)\psi(\beta) = \psi(\alpha\beta) = \psi(1) = 1$. So $\psi(\alpha) = 1$.

Now if $(1+\theta, 2)_R = (\alpha)_R$ then, by (ii), $(\alpha^3)_R = (\alpha)_R^3 = (1+\theta)_R$.
So $\alpha^3 = u(1 - \theta)$, for some unit u.

Thus $\psi(\alpha)^3 = \psi(\alpha^3) = \psi(u)\psi(1 - \theta) = 1 \times 8$.

And hence $\psi(\alpha) = 2$.

But then, putting $\alpha = a + b\theta + c\theta^2$ with $a, b, c \in \mathbb{Z}$,

$a^3 + 7b^3 + 49c^3 - 21abc = N_K(\alpha) = \pm 2$ and $a^3 \equiv \pm 2 \bmod 7$. $(*)$

But, mod 7, we have

x	0	± 1	± 2	± 3
x^3	0	± 1	± 1	∓ 1

So the cubes mod 7 are ± 1 and $(*)$ is impossible.

Thus $(1+\theta, 2)_R$ is not principal.

5 Put θ for $\dfrac{1+i}{\sqrt{2}}$. Clearly $\theta = \dfrac{(1+i)\sqrt{2}}{2} \in \mathbb{Q}[i, \sqrt{2}]$.

Hence $\mathbb{Q}[\theta] \subseteq \mathbb{Q}[i, \sqrt{2}]$.

On the other hand $i = \theta^2 \in \mathbb{Q}[\theta]$ and hence $\sqrt{2} = \dfrac{1+i}{\frac{1+i}{\sqrt{2}}} = \dfrac{1+\theta^2}{\theta} \in \mathbb{Q}[\theta]$.

Whence $$\mathbb{Q}[i, \sqrt{2}] \subseteq \mathbb{Q}[\theta].$$

Thus $$\mathbb{Q}[\theta] = \mathbb{Q}[i, \sqrt{2}] \; (= L). \tag{ii}$$

Now, since $L = \mathbb{Q}[\sqrt{2}][i]$ and since the min. poly. of i over $\mathbb{Q}[\sqrt{2}]$ must divide X^2+1,

$$|L : \mathbb{Q}[\sqrt{2}]| \leq \deg(X^2+1) = 2.$$

But $|L : \mathbb{Q}[\sqrt{2}]| \neq 1$ else $i \in L = \mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$. Contradiction.

So $$|L : \mathbb{Q}[\sqrt{2}]| = 2. \tag{$*$}$$

Moreover $|\mathbb{Q}[\sqrt{2}] : \mathbb{Q}| = 2$ ($X^2 - 2$ is irreducible over $\mathbb{Q}$ with root $\sqrt{2}$).

Therefore $|L : \mathbb{Q}| = |L : \mathbb{Q}[\sqrt{2}]| \cdot |\mathbb{Q}[\sqrt{2}] : \mathbb{Q}| = 2 \times 2 = 4.$ This proves (i).

(iii): Now $\theta^4 = i^2 = -1$. So θ is a root of $X^4 + 1 \in \mathbb{Q}[X]$.

Moreover, the min. poly. of θ in $\mathbb{Q}[X]$ must have degree

$$|\mathbb{Q}[\theta] : \mathbb{Q}| \overset{\text{(ii)}}{=} |L : \mathbb{Q}| \overset{\text{(i)}}{=} 4.$$

Hence $X^4 + 1$ is this minimum polynomial. This proves (iii)a.

Again, $\theta^2 - \sqrt{2}\theta + 1 = i - (1+i) + 1 = 0$. So θ is a root of $X^2 - \sqrt{2}X + 1 \in \mathbb{Q}[\sqrt{2}][X]$.

And the minimum polynomial of θ in $\mathbb{Q}[\sqrt{2}][X]$ must have degree

$$\big|\mathbb{Q}[\theta] : \mathbb{Q}[\sqrt{2}]\big| = |L : \mathbb{Q}[\sqrt{2}]| \overset{(*)}{=} 2.$$

Hence $X^2 - \sqrt{2}X + 1$ is this minimum polynomial. This proves (iii)b.

6 (i) Put $\theta = \sqrt{2} + \sqrt[3]{3}$ and $L = \mathbb{Q}[\sqrt{2}\sqrt[3]{3}]$. Certainly $L \supseteq \mathbb{Q}[\theta]$. Now

$$\theta - \sqrt{2} = \sqrt[3]{3}\,,$$

so

$$\theta^3 - 3\sqrt{2}\theta^2 + 6\theta - 2\sqrt{2} = 3\,,$$

i.e.,

$$\theta^3 + 6\theta - 3 = (3\theta^2 + 2)\sqrt{2}\,. \tag{1}$$

Thus $\sqrt{2} = (\theta^3 + 6\theta - 3)/(3\theta^2 + 2) \in \mathbb{Q}[\theta]$ and $\sqrt[3]{3} = \theta - \sqrt{2} \in \mathbb{Q}[\theta]$.

Hence $\mathbb{Q}[\theta] \supseteq L$ and so $\mathbb{Q}[\theta] = L$ and we have (i).

(ii) Put $K_1 = \mathbb{Q}[\sqrt{2}]$ and $K_2 = \mathbb{Q}[\sqrt[3]{3}]$.

Using the minimum polynomials of $\sqrt{2}$ and $\sqrt[3]{3}$ over $\mathbb{Q}$, we have

$$|K_1 : \mathbb{Q}| = \deg(X^2 - 2) = 2 \text{ and } |K_2 : \mathbb{Q}| = \deg(X^3 - 3) = 3.$$

Also

$$|L : K_1| \leq \deg(X^3 - 3) = 3$$

since $L = K_1[\sqrt[3]{3}]$ and since $X^3 - 3$, even if not actually equal to the minimum polynomial of $\sqrt[3]{3}$ over K_1, must certainly be divisible by it.
Hence, by the Tower Theorem,

$$|L : \mathbb{Q}| = |L : K_1| \cdot |K_1 : \mathbb{Q}| \le 3 \times 2 = 6.$$

Moreover, from the first equality,

$$2 = |K_1 : \mathbb{Q}| \text{ divides } |L : \mathbb{Q}|$$

and, similarly,

$$3 = |K_2 : \mathbb{Q}| \text{ divides } |L : \mathbb{Q}|.$$

So, in fact, $|L : \mathbb{Q}|$ is divisible by 6. Hence $|L : \mathbb{Q}| = 6$. This proves (ii).
[We now have that $|K_1[\sqrt[3]{3}] : K_1| = \dfrac{|L : \mathbb{Q}|}{|K_1 : \mathbb{Q}|} = 3$. Hence the minimum polynomial of $\sqrt[3]{3}$ over K_1 has degree 3 (and so it must be $X^3 - 3$ after all).]

(iii) Continuing from (1) (squaring both sides) we find:

$$\begin{aligned} \theta^6 + 12\theta^4 - 6\theta^3 + 36\theta^2 - 36\theta + 9 &= (9\theta^4 + 12\theta^2 + 4) \times 2\,, \\ \text{i.e.} \quad \theta^6 - 6\theta^4 - 6\theta^3 + 12\theta^2 - 36\theta + 1 &= 0. \end{aligned}$$

So θ is a zero of $f(X) = X^6 - 6X^4 - 6X^3 + 12X^2 - 36X + 1$.
Now the degree of the min. poly. $p(X)$ of θ over $\mathbb{Q}$ is $|\mathbb{Q}[\theta] : \mathbb{Q}| = |L : \mathbb{Q}| = 6$.
So, since $p(X) \mid f(X)$, we have $p(X) = f(X)$.

7 Choose $n \in \mathbb{Z}^{>0}$ so that $np_\alpha(X) \in \mathbb{Z}[X]$. We claim that $n\alpha$ is an algebraic integer.
Let $p_\alpha(X) = X^m + q_1X^{m-1} + \cdots + q_{m-1}X + q_m$. Then $nq_r \in \mathbb{Z}$ for $r = 1, \ldots, m$.
But $n\alpha$ is a root of

$$\begin{aligned} n^m p_\alpha(X/n) &= n^m((X/n)^m + q_1(X/n)^{m-1} + \cdots + q_{n-1}(X/n) + q_m) \\ &= X^m + nq_1X^{m-1} + \cdots + n^{m-1}q_{n-1}X + n^m q_m \in \mathbb{Z}[X]\,. \end{aligned}$$

So $n\alpha$ is an algebraic integer.

8 Suppose, for a contradiction that S is a UFD.
Choose $\lambda = \alpha/\beta \in K \setminus S$ such that α and $\beta \in S$ and α/β is a root of the polynomial

$f(X) = X^m + \gamma_1X^{m-1} + \cdots + \gamma_{n-1}X + \gamma_m \in S[X]$.

Dividing α and β by their gcd, if necessary, we can assume that $\gcd(\alpha, \beta) = 1$.
Certainly, β is not a unit of S else $\lambda \in S$.
So there is a prime element π of S which divides β in S.
But $\alpha^m + \gamma_1\alpha^{m-1}\beta + \cdots + \gamma_{m-1}\alpha\beta^{m-1} + \gamma_m\beta^m = \beta^m f(\alpha/\beta) = 0$.
So $\pi \mid \beta \mid -(\gamma_1\alpha^{m-1}\beta + \cdots + \gamma_{m-1}\alpha\beta^{m-1} + \gamma_m\beta^m) = \alpha^m$.
But π is prime. So we have (using the obvious generalization of the defining property of prime elements) that $\pi \mid \alpha$. This contradicts the fact that $\gcd(\alpha, \beta) = 1$.

So we have the desired contradiction and S cannot be a UFD.

10 (i) Put $K = \mathbb{Q}[\sqrt{5}]$ and $R = \mathbb{Z}[(1 + \sqrt{5})/2]$.
We define for $\alpha = a + b\sqrt{5} \in K$ $(a,\, b \in \mathbb{Q})$, $\psi(\alpha) = |N_K(\alpha)| = |a^2 - 5b^2|$.
From the properties of N_K we know that ψ is multiplicative ($\psi(\alpha\beta) = \psi(\alpha)\psi(\beta)$) and (since $5 \equiv 1 \mod 4$) that $\psi(R) \subset \mathbb{Z}$.

To show that ψ is a Euclidean norm we must prove that

$\forall\, \alpha,\ \beta \in R$, with $\alpha \neq 0$ $\exists\, \gamma \in R$ such that $\psi(\beta - \alpha\gamma) < \psi(\alpha)$;

Since ψ is multiplicative $\psi(\beta - \alpha\gamma)/\psi(\alpha) = \psi(\lambda - \gamma)$ where $\lambda = \beta/\alpha \in K$. So it is sufficient to show that

$\forall\, \lambda \in K$ $\exists\, \gamma \in R$ such that $\psi(\lambda - \gamma) < 1$.

Let $\lambda \in K$ and put $2\lambda = x + y\sqrt{5}$, where x and y lie in $\mathbb{Q}$.

Take $m = \lfloor y + \frac{1}{2} \rfloor$ and put $s = |y - m|$. (Here we use the notation $\lfloor x \rfloor$ for the largest integer smaller or equal to x.)

We have then $0 \leqslant s \leqslant \frac{1}{2}$.

Take n to be $n = \lfloor x \rfloor$ or $\lfloor x \rfloor + 1$ whichever is congruent to m mod 2.

So we have $r := |x - n| \leq 1$.

Finally, put $\gamma = (n + m\sqrt{5})/2$. Then $\gamma \in R$ since $n \equiv m \mod 2$.

Now

$$N(\lambda - \gamma) = N\left(\frac{(x-n) + (y-m)\sqrt{5}}{2}\right) = \frac{(x-n)^2 - 5(y-m)^2}{4} = \frac{r^2 - 5s^2}{4}.$$

So, since $0 \leqslant s \leqslant \frac{1}{2}$ and $0 \leqslant r \leqslant 1$,

$$-\frac{5}{16} \leqslant -\frac{5s^2}{4} \leqslant N(\lambda - \gamma) \leqslant \frac{r^2}{4} \leqslant \frac{1}{4}.$$

Thus $\psi(\lambda - \gamma) = |N(\lambda - \gamma)| < 1$ as required.

So ψ is a Euclidean Norm on R and R is a Euclidean Ring.

(ii) Put $K = \mathbb{Q}[\sqrt{-11}]$ and $R = \mathbb{Z}[(1 + \sqrt{-11})/2]$.

We define for $\alpha = a + b\sqrt{-11} \in K$ $(a,\, b \in \mathbb{Q})$, $\psi(\alpha) = N_K(\alpha) = a^2 + 11b^2$.

From the properties of N_K we know that ψ is multiplicative ($\psi(\alpha\beta) = \psi(\alpha)\psi(\beta)$) and that (since $-11 \equiv 1 \mod 4$) that $\psi(R) \subset \mathbb{Z}$.

To show that ψ is a Euclidean norm we must prove that

$\forall\, \alpha,\ \beta \in R$, with $\alpha \neq 0\ \exists\, \gamma \in R$ such that $\psi(\beta - \alpha\gamma) < \psi(\alpha)$;

Since ψ is multiplicative $\psi(\beta - \alpha\gamma)/\psi(\alpha) = \psi(\lambda - \gamma)$ where $\lambda = \beta/\alpha \in K$. So it is sufficient to show that

$\forall\, \lambda \in K\ \exists\, \gamma \in R$ such that $\psi(\lambda - \gamma) < 1$.

Let $\lambda \in K$ and put $2\lambda = x + y\sqrt{-11}$, where x and y lie in $\mathbb{Q}$.

Take $m = \lfloor y + \frac{1}{2} \rfloor$ and put $s = |y - m|$.

We have then $0 \leqslant s \leqslant \frac{1}{2}$.

Take n to be $n = \lfloor x \rfloor$ or $\lfloor x \rfloor + 1$ whichever is congruent to m mod 2.

So we have $r := |x - n| \leq 1$.

Finally, put $\gamma = (n + m\sqrt{-11})/2$. Then $\gamma \in R$ since $n \equiv m \mod 2$.

Now

$$\psi(\lambda - \gamma) = \psi\left(\frac{(x-n) + (y-m)\sqrt{-11}}{2}\right) = \frac{(x-n)^2 + 11(y-m)^2}{4} = \frac{r^2 + 11s^2}{4}.$$

So, since $0 \leqslant s \leqslant \frac{1}{2}$ and $0 \leqslant r \leqslant 1$,

$\psi(\lambda - \gamma) \leqslant \dfrac{1 + 11(1/4)}{4} = \dfrac{15}{16} < 1$, as required.

(For a more geometrical solution, find a point in the plane that has the same distance to its three closest lattice points which form an isosceles triangle, e.g. 0, 1 and $(1 + \sqrt{-11})/2$. Then compute that distance, it turns out to be < 1.)

So ψ is a Euclidean Norm on R and R is a Euclidean Ring.

(iii) Put $K = \mathbb{Q}[\sqrt{7}]$ and $R = \mathbb{Z}[\sqrt{7}]$.

We define for $\alpha = a + b\sqrt{7} \in K$ $(a,\, b \in \mathbb{Q})$, $\psi(\alpha) = |N_K(\alpha)| = |a^2 - 7b^2|$.

Reasoning as in part (i) we find that it is sufficient to prove that

$\forall\, \lambda \in K\ \exists\, \gamma \in R$ such that $\psi(\lambda - \gamma) < 1$.

Let, then, $\lambda \in K$ and put $\lambda = x + y\sqrt{7}$, where x and y lie in $\mathbb{Q}$.

Take $m = \lfloor y + \frac{1}{2} \rfloor$ and put $s = |y - m|$.

We have then $0 \leqslant s \leqslant \frac{1}{2}$. Note that s is rational.

Choose $n_1 = \lfloor x + \frac{1}{2} \rfloor = \lfloor x \rfloor$ or $\lfloor x \rfloor + 1$ (the latter unless $\lfloor x \rfloor$ is nearer to x).
Put $r = |x - n_1|$. Then $r \leq \frac{1}{2}$.

If $n_1 = \lfloor x \rfloor$ take $n_2 = n_1 - 1$ and if $n_1 = \lfloor x \rfloor + 1$ take $n_2 = n_1 + 1$
In either case $|x - n_2| = r + 1$.

Now we may take, for $i = 1, 2$, $\gamma_i = n_i + m\sqrt{7} \in R$.
Put $\delta_i = N(\lambda - \gamma_i) = (x - n_i)^2 - 7(y - m)^2$. So $\delta_1 = r^2 - 7s^2$ and

$$\delta_2 = (1 + r)^2 - 7s^2 = \delta_1 + 1 + 2r. \tag{1}$$

It is sufficient to prove that one of $|\delta_1|$ and $|\delta_2|$ is less than 1 because then we could take γ to be γ_1 or γ_2 as appropriate.

Suppose then that $|\delta_1| \not< 1$. We will show that $|\delta_2| < 1$.

Now $0 \leqslant s \leqslant \frac{1}{2}$ and $0 \leqslant r \leqslant \frac{1}{2}$. So

$$-\frac{7}{4} \leqslant -7s^2 \leqslant \delta_1 \leqslant r^2 \leqslant \frac{1}{4}. \tag{2}$$

If $|\delta_1| = 1$ then, by (2), $\delta_1 = -1$. Therefore, by (1), $\delta_2 = 2r$.

But in this case $r \neq \frac{1}{2}$ because we then would have $-1 = \delta_1 = \frac{1}{2}^2 - 7s^2$ which gives $7s^2 = 5/4$ and this is impossible since s is rational.
Hence, in this case, $|\delta_2| = 2r < 1$.

If $|\delta_1| > 1$ then, by (2), $\quad -\frac{7}{4} \leqslant \delta_1 < -1.$

So, by (1), $\quad -\frac{3}{4} \leqslant -\frac{7}{4} + 1 + 2r \leqslant \delta_2 < 2r \leqslant 1.$

So $|\delta_2| < 1$ as required.

Thus ψ is a Euclidean Norm on R and R is a Euclidean Ring.

11 From the lectures we know that, in a UFD, for $D \equiv 1 \pmod 8$, the prime 2 in $\mathbb{Z}$ splits in $\mathcal{O}_D$ into two primes which have a norm dividing the norm of 2 (which is 4), and hence would have to have the norm 2 each. But for $D < -7$ no such element exists (for $D = -7$ such a splitting of 2 is possible (how?), and the ring $\mathcal{O}_{-7}$ is indeed a UFD...).

12 Use that an algebraic integer α divides its norm, and that the norm of α is an integer.