SKETCH SOLUTIONS TO EXERCISE SHEET 12

Solution 12.1:
(a) The volume of $Y(s,0,\tau)$ is

$$\left|\int_{Y(s,0,\tau)} dx_1 dx_2 ... dx_s\right|.$$

Base case:

$$\left|\int_{Y(s,0,\tau)} dx_1\right| = \left|\int_0^\tau dx_1\right| = \frac{\tau}{1!}$$

Induction step:
Suppose the volume of $Y(s',0,\tau)$ is $\frac{\tau^{s'}}{s'!}$ for all $s' < s$.
Using Fubini we get that

$$\left|\int_{Y(s,0,\tau)} dx_1 dx_2 ... dx_s\right| = \left|\int_0^\tau \frac{(\tau - x_s)^{s-1}}{(s-1)!} dx_s\right|.$$

So the volume of $Y(s,0,\tau)$ is

$$\left|\left[\frac{-(\tau - x_s)^s}{s \cdot (s-1)!}\right]_{x_s=0}^{\tau}\right| = \frac{\tau^s}{s!}.$$

(b) The volume of $Y(s,t+1,\tau)$ is

$$\left|\int_{Y(s,t+1,\tau)} dx_1 dx_2 ... dx_s da_1 db_1 ... da_{t+1} db_{t+1}\right|.$$

Using Fubini we get that $\left|\int_{Y(s,t+1,\tau)} dx_1 dx_2 ... dx_s da_1 db_1 ... da_{t+1} db_{t+1}\right|$ is

$$\left|\int_{2|a_{t+1}^2 + b_{t+1}^2|^{1/2} \leq \tau} \frac{(\pi/2)^t (\tau - 2(a_{t+1}^2 + b_{t+1}^2)^{1/2})^{s+2t}}{(s+2t)!} da_{t+1} db_{t+1}\right|.$$

Using the change of variables $a_{t+1} = r\cos(\theta),\ b_{t+1} = r\sin(\theta)$ we get that the volume of $Y(s,t+1,\tau)$ is

$$\left|\int_{r=0}^{\tau/2} \int_{\theta=0}^{2\pi} \frac{(\pi/2)^t (\tau - 2r)^{s+2t}}{(s+2t)!} r\, dr\, d\theta\right|.$$

(b)Fix $s \in \mathbb{N}_0$. We show by induction on t the volume of $Y(s,t,\tau)$ is $\frac{(\pi/2)^t \tau^{s+2t}}{(s+2t)!}$.
Base case: If $s \geq 1$ then part (a) is the base case.

The volume of $Y(0,1,\tau)$ is

$$\left|\int_{Y(0,1,\tau)} da_1 db_1\right| = \left|\int_{|a_1^2+b_1^2|^{1/2}<\tau/2} da_1 db_1\right|$$

. This is just the area of a circle of radius $\tau/2$, so the volume of $Y(0,1,\tau)$ is

$$\frac{\pi\tau^2}{4} = \frac{(\pi/2)\tau^2}{2!}.$$

Induction step:

Suppose the volume of $Y(s,t,\tau)$ is

$$\frac{(\pi/2)^t \tau^{s+2t}}{(s+2t)!}.$$

By part (b) the volume of $Y(s,t+1,\tau)$ is

$$\left|\int_{r=0}^{\tau/2}\int_{\theta=0}^{2\pi} \frac{(\pi/2)^t(\tau-2r)^{s+2t}}{(s+2t)!} r\,dr\,d\theta\right|.$$

This is equal to

$$2\pi\cdot\frac{(\pi/2)^t}{(s+2t)!}\left|\int_{r=0}^{\tau/2}(\tau-2r)^{s+2t} r\,dr\right|.$$

A quick calculation gives us that for any $n\in\mathbb{N}_0$

$$(\tau-2r)^n r = \frac{1}{-2(n+1)}\frac{d}{dr}\left((\tau-2r)^{n+1}r - \frac{(\tau-2r)^{n+2}}{-2\cdot(n+2)}\right)$$

So the volume of $Y(s,t+1,\tau)$ is

$$\left|2\pi\cdot\frac{(\pi/2)^t}{(s+2t)!}\cdot\frac{1}{-2((s+2t)+1)}\left[(\tau-2r)^{(s+2t)+1}r - \frac{(\tau-2r)^{(s+2t)+2}}{-2\cdot((s+2t)+2)}\right]_{r=0}^{\tau/2}\right|.$$

This is

$$\left|2\pi\cdot\frac{(\pi/2)^t}{(s+2t)!}\cdot\frac{1}{-2((s+2t)+1)}\cdot\frac{(\tau)^{(s+2t)+2}}{-2\cdot((s+2t)+2)}\right|.$$

So the volume of $Y(s,t+1,\tau)$ is

$$\frac{(\pi/2)^{t+1}\tau^{s+2(t+1)}}{(s+2(t+1))!}.$$

Thus, by induction on t we have that the volume of $Y(s,t,\tau)$ is

$$\frac{(\pi/2)^t\tau^{s+2t}}{(s+2t)!}$$

(d) The volume of $X(s,t,\tau)$ is 2^s times the volume of $Y(s,t,\tau)$ since $X(s,t,\tau)$ is symmetric about the x_i-axis for $1\le i\le s$.

Solution 12.2:
Let $K = \mathbb{Q}(\sqrt{d})$. The Minkowski bound c_K is

$$\frac{1}{2}\left(\frac{4}{\pi}\right)^t \sqrt{|D_K|}$$

where t is the number of pairs of complex embeddings of K in $\mathbb{C}$ and D_K is the discriminant of K.

d	-1	-3	-7	2	3	6	13	17
d mod 4	3	1	1	2	3	2	1	1
$\lvert D_K\rvert$	4	3	7	8	12	24	13	17
c_K	$4/\pi$	$2\sqrt{3}/\pi$	$2\sqrt{7}/\pi$	$\sqrt{2}$	$\sqrt{3}$	$\sqrt{6}$	$\sqrt{13}/2$	$\sqrt{17}/2$

If $c_K < 2$ then all ideal classes of $\mathcal{O}_K$ contain an ideal of norm 1. Thus all ideal classes of $\mathcal{O}_K$ contain a principal ideal. So $\mathcal{O}_K$ is a principal ideal domain. The table above shows that c_K is smaller than 2 for $d = -1, -3, -7, 2, 3$ and 13. Thus, for these values of d, the ring of integers $\mathcal{O}_K$ is a principal ideal domain.

For $d = 6$, $c_K < 3$. Thus every ideal class of $\mathcal{O}_K$ contains an ideal of norm 1 or 2. So every ideal class contains a product of prime ideals which either divide $\langle 2\rangle$ or are principal.

Since $-2 = 2^2 - 6 \cdot 1^2$,

$$\langle 2\rangle = \langle 2-\sqrt{6}\rangle\langle 2+\sqrt{6}\rangle.$$

Since

$$N(2-\sqrt{6}) = N(2+\sqrt{6}) = -2,$$

the ideals $\langle 2-\sqrt{6}\rangle$ and $\langle 2+\sqrt{6}\rangle$ are prime. Thus all ideal classes of $\mathcal{O}_K$ contain a principal ideal. Therefore $\mathcal{O}_K$ is a principal ideal domain.

For $d = 17$, $c_K < 3$. Thus every ideal class of $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{17}}{2}]$ contains and ideal of norm 1 or 2. So every ideal class contains a product of prime ideals which either divide $\langle 2\rangle$ or are principal.

The ideals $\langle 1 + \frac{1+\sqrt{17}}{2}\rangle$ and $\langle 2 - \left(\frac{1+\sqrt{17}}{2}\right)\rangle$ both have norm 2. So they are prime. Since

$$\langle 2\rangle = \langle 1 + \frac{1+\sqrt{17}}{2}\rangle\langle 2 - \left(\frac{1+\sqrt{17}}{2}\right)\rangle,$$

all ideal classes of $\mathcal{O}_K$ contain a principal ideal. Thus $\mathcal{O}_K$ is a principal ideal domain.

Solution 2.3: Let $K = \mathbb{Q}(\sqrt{-5})$. Then $D_K = -20$ and $c_K = 2\sqrt{20}/\pi < 3$. So every ideal class of $\mathcal{O}_K$ contains an ideal of norm 1 or 2. If $I \lhd \mathcal{O}_K$ and $N(I) = 2$ then I is a prime ideal occurring in the factorisation of $\langle 2 \rangle$ into prime ideals.

From Aufgabe 1.4 we have that

$$\langle 2 \rangle = \langle 2, 1 + \sqrt{-5} \rangle \langle 2, 1 - \sqrt{-5} \rangle$$

and that

$$\langle 2, 1 + \sqrt{-5} \rangle \text{ and } \langle 2, 1 - \sqrt{-5} \rangle$$

are prime.

The equation $a^2 + 5b^2 = \pm 2$ has no solution mod 5. Thus $\mathbb{Z}[\sqrt{-5}]$ has no elements with norm ± 2.

Let $a, b \in \mathbb{Z}$. We have that $a + b\sqrt{-5} \in \langle 2, 1 + \sqrt{-5} \rangle$ if and only if $a \equiv b \mod 2$. So $N(\langle 2, 1 + \sqrt{-5} \rangle) = 2$.

Thus $\langle 2, 1 + \sqrt{-5} \rangle$ is not principal. So the class number of $\mathcal{O}_K$ is at least 2.

Thus the class group of $\mathcal{O}_K$ has two elements the ideal class of $\mathcal{O}_K$ and the ideal class of $\langle 2, 1 + \sqrt{-2} \rangle$.

Let $K = \mathbb{Q}(\sqrt{10})$. Then $D_K = 40$ and $c_K = \sqrt{40}/2 = \sqrt{10} < 4$. In order to calculate the class group we need need to find the prime factorisations of $\langle 2 \rangle$ and $\langle 3 \rangle$.

Let $a, b \in \mathbb{Z}$. We have that $a + b\sqrt{10} \in \langle 2, \sqrt{10} \rangle$ if and only if a is even. Thus $|\mathcal{O}_K / \langle 2, \sqrt{10} \rangle| = 2$. So $\langle 2, \sqrt{10} \rangle$ is prime and contains 2. Since

$$\langle 2, \sqrt{10} \rangle^2 = \langle 4, 2\sqrt{10}, 10 \rangle = \langle 2, 2\sqrt{10} \rangle = \langle 2 \rangle,$$

the ideal $\langle 2, \sqrt{10} \rangle$ is the only prime ideal dividing 2.

Suppose, for a contradiction, that $\langle 2, \sqrt{10} \rangle$ is principal with generator $a + b\sqrt{10}$. Then $|N(a + b\sqrt{10})| = N(\langle 2, \sqrt{10} \rangle) = 2$. So $a^2 - 10b^2 = \pm 2$. So $a^2 \equiv \pm 2 \mod 5$. But 2 and -2 are not squares mod 5. Thus $\langle 2, \sqrt{10} \rangle$ is not principal.

Let $a, b \in \mathbb{Z}$. We have that $a + b\sqrt{10} \in \langle 3, 1 - \sqrt{10} \rangle$ if and only if $a \equiv -b \mod 3$. Thus $|\mathcal{O}_K / \langle 3, 1 - \sqrt{10} \rangle| = 3$. So $\langle 3, 1 - \sqrt{10} \rangle$ is prime.

Let $a, b \in \mathbb{Z}$. We have that $a + b\sqrt{10} \in \langle 3, 1 + \sqrt{10} \rangle$ if and only if $a \equiv b \mod 3$. Thus $|\mathcal{O}_K / \langle 3, 1 + \sqrt{10} \rangle| = 3$. So $\langle 3, 1 + \sqrt{10} \rangle$ is prime.

Suppose, for a contradiction, that $\langle 3, 1+\sqrt{10} \rangle$ (respectively $\langle 3, 1-\sqrt{10} \rangle$) is principal with generator $a+b\sqrt{10}$. Then $|N(a+b\sqrt{10})| = N(\langle 3, 1+\sqrt{10} \rangle) = N(\langle 3, 1 - \sqrt{10} \rangle) = 3$. So $a^2 - 10b^2 = \pm 3$. So $a^2 \equiv \pm 3 \mod 5$. But 3 and -3 are not a squares mod 5. Thus neither $\langle 3, 1 + \sqrt{10} \rangle$ nor $\langle 3, 1 + \sqrt{10} \rangle$ are principal.

Since

$$\langle 3, 1 + \sqrt{10} \rangle \langle 3, 1 - \sqrt{10} \rangle = \langle 3 \rangle,$$

the ideals

$$\langle 3, 1+\sqrt{10}\rangle \text{ and } \langle 3, 1-\sqrt{10}\rangle =$$

are the only prime ideals dividing $\langle 3\rangle$.

We now know that our class group contains at least 2 elements since $\mathbb{Z}[\sqrt{10}]$ is not a principal ideal domain and at most 4 elements. Thus the ideal class group of $\mathcal{O}_K$ is isomorphic to $\mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_4$.

Since $-2+\sqrt{10} \in \langle 3, 1+\sqrt{10}\rangle$ and $-2+\sqrt{10} \in \langle 2, \sqrt{10}\rangle$, we know that

$$I\langle 3, 1+\sqrt{10}\rangle\langle 2, \sqrt{10}\rangle = \langle -2+\sqrt{10}\rangle$$

for some $I \lhd \mathcal{O}_K$.

Thus

$$N(I)\cdot 3\cdot 2 = N(I)N(\langle 3, 1+\sqrt{10})N(\langle 2, \sqrt{10}\rangle) = |N(-2+\sqrt{10})| = 6.$$

So $N(I) = 1$. Thus $I = \mathcal{O}_K$. Thus

$$\langle 3, 1+\sqrt{10}\rangle\langle 2, \sqrt{10}\rangle = \langle -2+\sqrt{10}\rangle.$$

So our ideal class group has 2 elements: the ideal class of $\mathcal{O}_K$ and the ideal class of $\langle 2, \sqrt{10}\rangle$.

Solution 12.4:

(a) Let $K = \mathbb{Q}(\sqrt{d})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Let $x, y \in \mathbb{Z}$. The element $x + y\sqrt{d} \in \mathcal{O}_K$ has norm 1 if and only if $x^2 - dy^2 = 1$. So it is enough to show that there are infinitely many elements of $\mathcal{O}_K$ with norm 1. An element a of $\mathcal{O}_K$ has norm ± 1 if and only if a is a unit. The field K has 2 real embeddings into $\mathbb{C}$. So by the Dirichlet unit theorem $\mathcal{O}_K^\times$ has free rank 1. Thus $\mathcal{O}_K^\times$ contains an element u of infinite order. Since u is a unit, it has norm ± 1. Thus, since the norm is multiplicative, $w = u^2$ has norm 1 and w^n has norm 1 for all $n \in \mathbb{N}$. Since u is of infinite order, so is w. Thus $w^n = w^m$ implies $n = m$ for all $m, n \in \mathbb{N}$. Thus $\mathcal{O}_K$ contains infinitely many elements of norm 1.

(b) Let $K = \mathbb{Q}(\sqrt{d})$. Then $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Suppose that $a, b \in \mathbb{Z}$ and $a + b\frac{1+\sqrt{d}}{2}$ has norm 1. Then

$$a^2 + ab + \frac{1-d}{4}b^2 = 1.$$

So

$$4 = 4a^2 + 4ab + (1-d)b^2 = (2a+b)^2 - db^2.$$

Note that if $a + b\frac{1+\sqrt{d}}{2} \neq c + d\frac{1+\sqrt{d}}{2}$ then $a + 2b \neq c + 2d$ or $b \neq d$. Thus it is enough to show that $\mathcal{O}_K$ contains infinitely many elements with norm 1. The field K has 2 real embeddings into $\mathbb{C}$. So by the Dirichlet unit theorem $\mathcal{O}_K^\times$ has free rank 1. Using exactly the same argument as above we get that $\mathcal{O}_K$ has infinitely many elements with norm 1.

Solution 12.5:

Let $a, b \in \mathbb{Z}$. The element $a + b\sqrt{3}$ is a unit in $\mathcal{O}_{\mathbb{Q}(\sqrt{3})} = \mathbb{Z}[\sqrt{3}]$ if and only if

$$a^2 - 3b^2 = N(a + b\sqrt{3}) = \pm 1.$$

If $a + b\sqrt{3}$ is a torsion element of $\mathcal{O}_K^\times$ then $|a + b\sqrt{3}| = 1$. Since

$$1 = |N(a + b\sqrt{3})| = |a - b\sqrt{3}||a + b\sqrt{3}|,$$

we have that $|a - b\sqrt{3}| = 1$. Thus

$$2 = |a + b\sqrt{3}| + |a - b\sqrt{3}| \geq |2a|.$$

So $1 \geq |a|$. So $a = -1, 0$ or 1. If $a = \pm 1$ then $b = 0$ because $a^2 - 3b^2 = \pm 1$. If $a = 0$ then $a + b\sqrt{3}$ is not a unit.

Thus the only torsion elements of $\mathcal{O}_K$ are ± 1.

The field $\mathbb{Q}(\sqrt{3})$ has two real embeddings. So by the Dirichlet unit theorem the free rank of $\mathcal{O}_K^\times$ is 1. So $\mathcal{O}_K^\times$ is isomorphic to $\{\pm 1\} \times \mathbb{Z}$.

We now show that if $u \in \mathcal{O}_K^\times$ is such that $u > 1$ and has the property that:

$$\text{for all } w \in \mathcal{O}_K,\ w > 1 \text{ implies } w \geq u$$

then $\mathcal{O}_K$ is generated by the set $\{-1, u\}$. Note that the following argument works for all real quadratic extensions of $\mathbb{Q}$.

First suppose that $x \in \mathcal{O}_K^\times$ and $x > 1$. Since $u > 1$ there exists an $n \in \mathbb{N}$ such that $u^n \leq x < u^{n+1}$. So $1 \leq x/u^n < u$. Since x/u^n is a unit by choice of u, $x = u^n$.

Suppose $x \in \mathcal{O}_K^\times$ with $0 < x < 1$. Then $1/x$ is a unit and $1/x > 1$. Thus there exists an $n \in \mathbb{N}$ with $1/x = u^n$. So $x = u^{-n}$.

So for all $x \in \mathcal{O}_K^\times$ with $x > 0$ there exists an $n \in \mathbb{Z}$ such that $u^n = x$.

Suppose $x \in \mathcal{O}_K$ and $x < 0$. Then $-x$ is a unit and $-x > 0$. Thus there exists an $n \in \mathbb{Z}$ such that $-x = u^n$. So $x = -u^n$.

Thus all $x \in \mathcal{O}_K$ are of the form $\pm u^n$ for some $n \in \mathbb{Z}$.

It remains to show that $2 + \sqrt{3}$ is a unit and that for all $a, b \in \mathbb{Z}$ with $a^2 - 3b^2 = \pm 1$ and $1 < a + b\sqrt{3}$,

$$2 + \sqrt{3} \leq a + b\sqrt{3}.$$

First note that $N(2 + \sqrt{3}) = 2^2 - 3 = 1$. So $2 + \sqrt{3}$ is a unit.

Suppose $a, b \in \mathbb{Z}$ with $a^2 - 3b^2 = 1$ and $1 < a + b\sqrt{3}$. Then $0 < a - b\sqrt{3} < 1$. So $1 < 2a$. So $a \geq 1$. So $b\sqrt{3} > a - 1 > 0$. So $b \geq 1$. So $\sqrt{3} \leq b\sqrt{3} < a$. Thus $2 \leq a$. Therefore $2 + \sqrt{3} \leq a + b\sqrt{3}$.

Suppose $a, b \in \mathbb{Z}$ with $a^2 - 3b^2 = -1$ and $1 < a + b\sqrt{3}$. Then $0 < -a + b\sqrt{3} < 1$. So $1 < 2\sqrt{3}b$. So $b \geq 1$. Since $a > b\sqrt{3} - 1 > 0$, we have $a \geq 1$. Now, if $a + b\sqrt{3} < 2 + \sqrt{3}$ then $a < 2$. So $a = 1$. So $1 + b\sqrt{3} < 2 + \sqrt{3}$. So $1 \leq b < 2$. But $1 + \sqrt{3}$ is not a unit in $\mathcal{O}_K$. Therefore $2 + \sqrt{3} \leq a + b\sqrt{3}$.