Contents

Exercise 3.15

Verify that if $K = \mathbb{Q}(\sqrt{-2}, \sqrt{-5})$ then an integral basis is given by $\{1, \sqrt{-2}, \sqrt{-5}, \frac{\sqrt{-2}+\sqrt{10}}{2}\}$.

See proposition 2.34 that integral elements of $\mathbb{Z}[\sqrt{d}]$ have the form $\mathbb{Z} + \mathbb{Z}\sqrt{d}$ when $d \equiv 2, 3 \mod 4$.

Adding α with its conjugates creates elements of the form $2a + 2k\sqrt{d} \in \mathbb{Z}_K$ where $d \in \{-2, -5, 10\}$. $-2 \equiv 2 \mod 4, -5 \equiv 3 \mod 4, 10 \equiv 2 \mod 4$. So we know by above that these elements are from $\mathbb{Z} + \mathbb{Z}\sqrt{d}$. So $2a, 2k \in \mathbb{Z}$.

Follow method of previous section.

$$A = 2a, B = 2b, C = 2c, D = 2d \in \mathbb{Z}$$
$$a = \frac{A}{2}, b = \frac{B}{2}, c = \frac{C}{2}, d = \frac{D}{2}$$

$$\begin{aligned}
\alpha &= a + b\sqrt{-2} + c\sqrt{-5} + d\sqrt{10} \\
&= \frac{A}{2} + \frac{B}{2}\sqrt{-2} + \frac{C}{2}\sqrt{-5} + \frac{D}{2}\sqrt{10} \\
\alpha_2 &= a - b\sqrt{-2} + c\sqrt{-5} - d\sqrt{10} \\
\alpha\alpha_2 &= ((a + c\sqrt{-5}) - (b\sqrt{-2} + d\sqrt{10}))((a + c\sqrt{-5}) + (b\sqrt{-2} + d\sqrt{10})) \\
&= (a + c\sqrt{-5})^2 - (b\sqrt{-2} + d\sqrt{10})^2 \\
&= a^2 + 2\sqrt{-5}ac - 5c^2 + 2b^2 - 2\sqrt{-20}bd - 10d^2 \\
&= \frac{A^2 - 5C^2 + 2B^2 - 10D^2}{4} + \frac{AC - 2BD}{2}\sqrt{-5}
\end{aligned}$$

First note that $AC - 2BD \equiv AC \equiv 0 \mod 2$, which means either A or C are even.

$$\begin{aligned}
A^2 - 5C^2 + 2B^2 - 10D^2 &\equiv 0 \mod 2 \\
&\equiv A^2 - 5C^2 \mod 2 \\
&\equiv A + C \mod 2
\end{aligned}$$

$A \mod 2$	$C \mod 2$	$A + C \mod 2$
0	0	0
0	1	1
1	0	1

So A and C are both even.

Now we look at B and D. Note that by the last step $A^2 \equiv 0 \mod 4$ and $C^2 \equiv 0 \mod 4$.

$$A^2 - 5C^2 + 2B^2 - 10D^2 \equiv 2B^2 - 10D^2 \equiv 0 \mod 4$$

$$2B^2 - 10D^2 = 4p \implies B^2 - 5D^2 = 2p$$
$$B^2 - 5D^2 \equiv B^2 + D^2 \equiv 0 \mod 2$$
$$\implies B + D \equiv 0 \mod 2$$

$B \mod 2$	$D \mod 2$	$B + D \mod 2$
0	0	0
0	1	1
1	0	1
1	1	0

So $B \equiv D \equiv 0 \mod 2$ or $B \equiv D \equiv 1 \mod 2$. Remembering $A \equiv C \equiv 0 \mod 2$, we now have 2 cases.

Case 1: A, B, C, D are all even

$$A \equiv C \equiv 0 \mod 2$$
$$B \equiv D \equiv 0 \mod 2$$

$$A = 2a, B = 2b, C = 2c, D = 2d \in \mathbb{Z}$$

Earlier we found
$$2\alpha = A + B\sqrt{-2} + C\sqrt{-5} + D\sqrt{10}$$
with $A, B, C, D \in \mathbb{Z}$.

But now we know $A, B, C, D \in 2\mathbb{Z}$. So $a, b, c, d \in \mathbb{Z}$.

Which is integral over $\{1, \sqrt{-2}, \sqrt{-5}, \sqrt{10}\}$ and so also over $\{1, \sqrt{-2}, \sqrt{-5}, \frac{\sqrt{-2}+\sqrt{10}}{2}\}$ since $\sqrt{10} = 0 \cdot 1 - 1 \cdot \sqrt{-2} + 0\sqrt{-5} + 2\frac{\sqrt{-2}+\sqrt{10}}{2}$

Case 2: A, B are even, C, D are odd

Now we do the other case.

$$A \equiv C \equiv 0 \mod 2$$
$$B \equiv D \equiv 1 \mod 2$$

$$A = 2a, B = 2b, C = 2c, D = 2d$$

Here $A, C \in 2\mathbb{Z}$ so $a, c \in \mathbb{Z}$. But this is not true for B, D which are odd integers.

a, c are integers, but b, d are halves of odd integers.

$$\alpha = a + b\sqrt{-2} + c\sqrt{-5} + d\sqrt{10}$$

which has as basis $\{1, \sqrt{-2}, \sqrt{-5}, \frac{\sqrt{-2}+\sqrt{10}}{2}\}$

So we managed to reduce all elements of $\mathbb{Z}_K$ which both have the same basis. We therefore conclude that the entire ring has that integral basis too.

Prove that $\mathbb{Z}_K \neq \mathbb{Z}[\gamma]$

$$\gamma = \frac{\sqrt{-2} + \sqrt{10}}{2}$$

```
sage: var("a b c d")
(a, b, c, d)
sage: y = (sqrt(-2) + sqrt(10))/2
sage: e = a + b*y + c*y^2 + d*y^3 == 0
sage: e = e.expand()
sage: e
1/2*sqrt(10)*sqrt(-2)*c + 1/2*sqrt(10)*b + 1/2*sqrt(-2)*b + 1/2*sqrt(10)*d + 7/2*sqrt(-2)*d + a + 2*c =
```

$$\frac{1}{2}\sqrt{10}\sqrt{-2}c + \frac{1}{2}\sqrt{10}b + \frac{1}{2}\sqrt{-2}b + \frac{1}{2}\sqrt{10}d + \frac{7}{2}\sqrt{-2}d + a + 2\,c = 0$$

Tidying up

$$\frac{1}{2}\sqrt{-2}\sqrt{-5}\sqrt{-2}c + \frac{1}{2}\sqrt{10}b + \frac{1}{2}\sqrt{-2}b + \frac{1}{2}\sqrt{10}d + \frac{7}{2}\sqrt{-2}d + a + 2\,c = 0$$

$$a + 2c + \frac{1}{2}\sqrt{-2}b + \frac{7}{2}\sqrt{-2}d - \sqrt{-5}c + \frac{1}{2}\sqrt{10}b + \frac{1}{2}\sqrt{10}d = 0$$

$$(a + 2c) + \left(\frac{b + 7d}{2}\right)\sqrt{-2} - c\sqrt{-5} + \frac{b + d}{2}\sqrt{10} = 0$$

We will now search for basis elements which cannot be computed from powers of γ. We can use the last equation before to convert elements from the basis $\{1, \gamma, \gamma^2, \gamma^3\}$ to $\{1, \sqrt{-2}, \sqrt{-5}, \sqrt{10}\}$. We are interested to in reverse, and see if there are elements from the $\langle\sqrt{-2}, \sqrt{-5}\rangle$ basis to $\langle\gamma\rangle$.

Let M be a 4x4 matrix transform that takes the basis for $\langle\gamma\rangle$ to $\langle\sqrt{-2}, \sqrt{-5}\rangle$.

$$M\mathbf{v} = \mathbf{A}$$

A is the result of the change of basis. So we can actually compute values from $\langle sqrt{-2}, sqrt{-5}\rangle$ in terms of γ. But these elements must be integers, otherwise it is not $\mathbb{Z}[\gamma]$.

$$\begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 7 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a + 2c \\ b + 7d \\ c \\ b + d \end{pmatrix}$$

where A is our basis. We are interested in

$$\begin{pmatrix} 0 \\ 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 2 \end{pmatrix}$$

Which correspond to the basis over $\langle\sqrt{-2}, \sqrt{-5}\rangle$.

$$(a + 2c) + \left(\frac{b + 7d}{2}\right)\sqrt{-2} - c\sqrt{-5} + \frac{b + d}{2}\sqrt{10} = 0$$

Trying the first one, we get

```
sage: M = matrix([
....:     [1, 0, 2, 0],
....:     [0, 1, 0, 7],
....:     [0, 0, 1, 0],
....:     [0, 1, 0, 1]
....: ])
sage: v = vector([0, 2, 0, 0])
sage: M^-1*v
(0, -1/3, 0, 1/3)
```

So therefore $\sqrt{-2} \notin \mathbb{Z}[\gamma]$.

Exercise 3.16

$$f(\gamma) = 0$$
$$3 \mid g(\gamma) \implies g(\gamma) \equiv 0 \mod 3$$
$$g(X) \equiv f(X)u(X) \mod 3$$

likewise

$$g(X) \equiv f(X)u(X) \mod 3$$
$$\implies g(\gamma) \equiv f(\gamma)u(\gamma) \equiv 0 \mod 3$$

$$g(X) = 3a(X) + f(X)u(X)$$

$\mathbb{Q}[\sqrt[3]{175}]$

Note there's a mistake on the first page. $\alpha' = \alpha^2/5$. The book erroneously shows 7.

```
sage: K.<a> = NumberField(x^3 - 175)
sage: L.<X> = K[]
sage: K2.<w> = K.extension(X^2 + X + 1)
sage: K3.<j, k> = K2[]
sage: b = a^2/5
sage: c1 = (j*a + k*b)/5
sage: c2 = (j*a*w + k*b*w^2)/5
sage: c3 = (j*a*w^2 + k*b*w)/5
sage: c1*c2*c3
7/5*j^3 + 49/25*k^3
```