How to find rings of integers

Let $\alpha$ be a root of $x^4-3$, let $K=\mathbb{Q}(\alpha)$.
Find $\mathcal{O}_K$.

Step 1: Find $m_\alpha$. We know $\alpha$ is a root of $x^4-3$ and this is irred as its Eisenstein with $p=3$ (also its monic) so $m_\alpha = x^4-3$.

**Remark 2.2.11.** Note that this also gives us an algorithm for finding an integral basis as follows:

1. Pick $B$ a basis consisting of algebraic integers and calculate $\Delta(B)$.
2. For each prime $p$ such that $p^2 \mid \Delta(B)$ we can use Lemma 2.2.7 to get a new basis $B'$ with smaller discriminant.
3. Now, repeat step one.

Step 2 Take $B=\{1,\alpha,\alpha^2,\alpha^3\}$ as our initial basis

Compute $\Delta(B)$

**Theorem 2.2.25.** *Let $K=\mathbb{Q}(\alpha)$ a number field with $m_\alpha(x)=x^n+ax+b$. Then*

$$\Delta(\{1,\alpha,\ldots,\alpha^{n-1}\}) = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n).$$

$$\Delta(B) = (-1)^6\left(4^4\cdot(-3)^3\right) = -2^8\cdot 3^3$$

Note that we have:

$1, \beta, \ldots, \beta^{n-1}$

**Lemma 2.2.7.** *Let $K$ be a number field and $B = \{b_1, \dots, b_n\}$ be a basis for $K/\mathbb{Q}$ consisting of algebraic integers. If $B$ is not an integral basis then there exists an algebraic integer of the form*

$$\alpha = \frac{x_1 b_1 + \cdots + x_n b_n}{p}$$

$$\frac{x + x_1\beta + \cdots + x_n\beta^{n-1}}{p}$$

*where $p$ is a prime and $x_i \in \{0, \dots, p-1\}$ with not all $x_i$ zero. Moreover, if $x_i \neq 0$ and we let $B'$ be the basis obtained by replacing $b_i$ with $\alpha$, then*

$$\Delta(B') = \frac{x_i^2}{p^2}\Delta(B).$$

*In particular $p^2 \mid \Delta(B)$.*

So if $B$ is not integral basis, then we can find $B'$ s.t $\Delta(B') < \Delta(B)$

in particular we remove a $p^2$ from $\Delta(B)$

So we only need to worry about $p = 2, 3$

But Note we have the following result:

**Lemma 2.2.21.** *Let $K = \mathbb{Q}(\alpha)$ and $\alpha$ be an algebraic integer such that $m_\alpha$ satisfies Eisensteins Criterion 1.2.15 for a prime $p$. Then none of the elements*

$$\phi = \frac{1}{p}(x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1})$$

*is an algebraic integer, where $n = \deg(m_\alpha)$ and $x_i \in \{0, \dots, p-1\}$.*

So with this none of the elements

$$\frac{x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3}{3} \in \mathcal{O}_K$$

with $x_i \in \{0, 1, 2\}$

So we don't have to worry about $p=3$

left with $p=2$. i.e we need to check

if any element of the form

$$\frac{x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3}{2} \in \mathcal{O}_K$$

With $x_i \in \{0,1\}$. This can be done

but there is a better way:

Hint: Find a change of variables to make $x^4-3$

Eisenstein at $p=2$ and $3$.

Note that $f(x) = (x+3)^4 - 3$

$$= x^4 + 12x^3 + 54x^2 + 108x + 78$$

This is Eisenstein at $p=2$ and $3$.

Let $\beta$ be a root of $f(x)$ $\quad \beta = \alpha + 3$

$K' = \mathbb{Q}(\beta)$ then we know that

$$\Delta(\{1, \beta, \ldots, \beta^3\}) = \Delta(\{1, \alpha, \ldots, \alpha^3\})$$

By Q. 5.6 of the probs sheet

$$K' \cong K = \mathbb{Q}(\alpha) \Rightarrow \mathcal{O}_{K'} \cong \mathcal{O}_K$$

Now, we know from by using 22.11 twice
with $p=2$ and $p=7$ that

$$\mathcal{O}_K \cong \mathcal{O}_{K'} = \mathbb{Z}[\beta] = \mathbb{Z}[\alpha]$$

$$\rightarrow \mathcal{O}_K = \mathbb{Z}[\alpha] \qquad \square$$

---

<u>Warning:</u> its not always possible to find some
$\alpha \in K$ s.t $\mathcal{O}_K \cong \mathbb{Z}[\alpha]$

For example: $K = \mathbb{Q}(\sqrt{7}, \sqrt{10})$
Then $\nexists\, \alpha$ s.t $\mathcal{O}_K \cong \mathbb{Z}[\alpha]$

---

## Units in rings of integers

Units in $\mathcal{O}_K = \mathcal{O}_K^{\times} = \{\alpha \in \mathcal{O}_K \mid \exists \beta \in \mathcal{O}_K \text{ s.t } \alpha\beta = 1\}$

<u>Prop:</u> $\mathcal{O}_K^{\times} = \{\alpha \in \mathcal{O}_K \mid N_{K/\mathbb{Q}}(\alpha) = \pm 1\}$

<u>e.g</u> $K = \mathbb{Q}(\sqrt{5})$ and $\varphi = \frac{1+\sqrt{5}}{2} \in \mathcal{O}_K$

is it a unit? $N_{K/\mathbb{Q}}(\varphi) = \left(\frac{1+\sqrt{5}}{2}\right)\left(\frac{1-\sqrt{5}}{2}\right)$

$$= \frac{1-5}{4} = -1$$

**Theorem** (Dirichlet's Unit theorem)

Let $K$ be a number field and

$$\mu_K = \{\text{set of roots of unity in } K\}$$
$$= \{x \in K \mid x^n = 1 \text{ for some } n\}$$
$$= K \cap \{\text{all roots of unity}\}$$

Then
$$\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^{r_1 + r_2 - 1}$$

$r_1 = $ # of real embedding of $K$

$r_2 = $ # of complex conj pairs of embeddings

i.e. if $s = r_1 + r_2 - 1$ then $\exists\, u_1, \dots, u_s \in \mathcal{O}_K^\times$

s.t. $\forall\, v \in \mathcal{O}_K^\times$ we can write

$$v = \xi^a \cdot u_1^{b_1} \cdots u_s^{b_s} \qquad a, b_i \in \mathbb{Z},\ \xi \in \mu_K$$

$$\mathcal{O}_K^\times \longrightarrow \mu_K \times \mathbb{Z}^{r_1 + r_2 - 1}$$
$$v = \xi^a \cdot u_1^{b_1} \cdots u_s^{b_s} \longmapsto (\xi^a, b_1, \dots, b_s)$$

---

We also want to study ideals in $\mathcal{O}_K$

- One thing we show is that for any non-zero ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ that

$$\left| \mathcal{O}_K / \mathfrak{a} \right| < \infty \quad \text{(i.e. is finite)}$$

we will use this to define the Norm of an ideal

$$N(\mathfrak{a}) = \left| \mathcal{O}_K / \mathfrak{a} \right|$$

One Consequence of this is that if $\mathfrak{p} \subseteq \mathcal{O}_K$ is a prime ideal, then

$\mathcal{O}_K / \mathfrak{p}$ is a finite integral domain i.e. its a field!

ie $\mathfrak{p}$ must be maximal.

So in $\mathcal{O}_K$ all prime ideals are maximal!

Turns out there is a nice class of rings which have the following 3 properties

- all prime ideals are maximal
- They are noetherian (i.e. Every ideal is fin. generated)

- They are integrally closed in their field of fractions

(e.g. $\mathcal{O}_K$ is int. closed in $K$

i.e. if $\alpha \in K$ and $\alpha$ satisfies

$$\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 = 0$$

$$a_i \in \mathcal{O}_K \Rightarrow \alpha \in \mathcal{O}_K$$ )

Rings that satisfy these 3 properties are called Dedekind Domain.