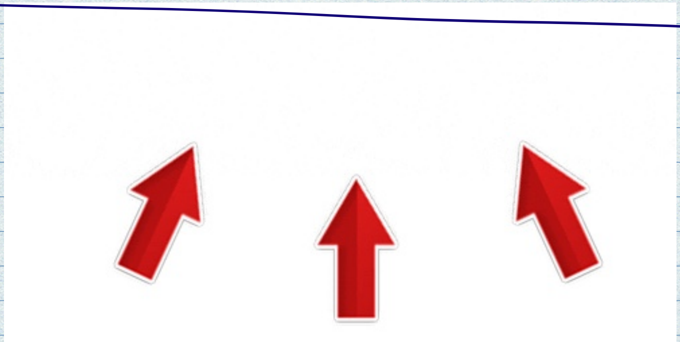
- 76 is Not Square-free !! $\quad 76 = \boxed{2^2} 19$

$n \in \mathbb{Z}$ is Square-free if there Not exist a prime number p such that $p^2 \mid n$.



- $K = \mathbb{Q}(\alpha)$ with α a root of $x^5 - 37$

Wanted to find $\mathcal{O}_K$.

So we might start by computing the discriminant of $B = \{1, \alpha, \ldots, \alpha^4\}$

$$\boxed{\Delta(\{1, \alpha, \ldots, \alpha^4\}) = 5^5 \cdot 37^4}$$

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

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

Trick or Shortcut : Use this theorem

$a = 0 \quad b = -37 \quad n = 5$

$$\Delta(\{1, \alpha, \dots, \alpha^4\}) = (-1)^{\frac{5\cdot 4}{2}} \cdot (5^5 \cdot 37^4 + 0)$$

$$= 5^5 \cdot 37^4$$

by 2.2.7

This is Not Square-free! Need to check at

$p = 5$ or $p = 37$ if $\exists$

$$\frac{a_0 + \dots + a_4\alpha^4}{p} \in \mathcal{O}_K \qquad a_i \in \{0, \dots, p-1\}$$

$m_\alpha = x^5 - 37$ Not Eis at 5

This is Eisenstein at $p = 37$

So by 2.2.21 we know

there are no alg. ints

of the form

$$\frac{a_0 + \dots + a_4\alpha^4}{37} \quad \text{with } a_i \in \{0, \dots, 36\}$$

Here we still need to check

if

$$\frac{a_0 + \dots + a_4\alpha^4}{5} \in \mathcal{O}_K$$

$(x+2)^5 - 37 = m_\beta(x)$

which is Eisenstein at $p = 5$

but not at 37

So again we know that

there are no alg ints

of the form

$$\frac{a_0 + a_1\beta + \dots + a_4\beta^4}{5}$$

$a_i \in \{0, \dots, 4\}$

$$\frac{a_0 + \dots a_4\beta^4}{37} \in \mathcal{O}_K$$

37

$$(x+37)^5 - 37 = m_\gamma(x)$$

Then this is Eisenstein at $p=5$ and 37

So using 2.21 twice we get

$\gamma = \alpha - 37$

$$\mathbb{Z}[\alpha] = \mathbb{Z}[\gamma] = \mathcal{O}_{\mathbb{Q}(\gamma)} = \mathcal{O}_{\mathbb{Q}(\alpha)}$$

- To get marks not only do you need to get the right answer but you need to show you know **how** to get the answers

"Factoring Primes"

Let K be a number field. We saw last week was that if $\mathfrak{a} \subseteq \mathcal{O}_K$ then we can write it uniquely as a product of prime ideals

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n} \quad \text{with } \mathfrak{p}_i \text{ distinct prime ideals}$$

How do we find such a factorization?

I'll explain how to do this for ideals of the form $p\mathcal{O}_K = (p)$ for p a prime number

Corollary 3.5.11. *Let K be a number field of degree n over $\mathbb{Q}$ and let $\alpha \in \mathcal{O}_K$ be a primitive element so that $K = \mathbb{Q}(\alpha)$.*

Let p be a prime number not dividing $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ and let

size of the quotient $\mathcal{O}_K / \mathbb{Z}[\alpha]$ as abelian group

reduce mod p

$$\overline{m}_\alpha(x) = \overline{m}_1(x)^{e_1} \ldots \overline{m}_r(x)^{e_r}$$

factorization into irred polys in $\mathbb{F}_p[x]$

be the reduction modulo p of the minimal polynomial m_α of α. Then in $\mathcal{O}_K$ the ideal (p) factorizes as

are prime ideals

$$(p) = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$$

where $\mathfrak{p}_i = (p, m_i(\alpha))$ and $f_{\mathfrak{p}_i|p} = \deg(\overline{m}_i)$ and $e_i = e_{\mathfrak{p}_i|p}$.

m_i is any poly in $\mathbb{Z}[x]$ such that $m_i(x) \bmod p = \overline{m}_i(x)$

Example: $K = \mathbb{Q}(\alpha)$ with α a root of $x^3 - 2x + 2$

In this case, we saw in sheet 5 that

$$\mathcal{O}_K = \mathbb{Z}[\alpha] \quad \text{so} \quad [\mathcal{O}_K : \mathbb{Z}[\alpha]] = 1$$

therefore Cor. 3.5.11 works for all primes.

- $p = 2$ and lets factor (2):

We look at $m_\alpha(x) \equiv x^3 - 2x + 2 \mod 2$

$$\equiv x^3 \bmod 2$$

let $\overline{m}_1(x) = x$ in $\mathbb{F}_2[x]$

and we take $m_1(x) = x \in \mathbb{Z}[x]$

We could have taken $x+2$, $x+4$ .. $4x^2+x+2$

We let $P = (2, m_1(\alpha)) = (2, \alpha)$

then Cor says $(2) = (2, \alpha)^3$

where P is a prime ideal

- $p = 3$ lets factor (3).

- $\overline{m_\alpha}(x) \equiv x^3 - 2x + 2 \mod 3$

$$\longrightarrow \boxed{\equiv (x-2)(x^2 + 2x + 2) \mod 3}$$

$$\equiv (x+1)(x^2 + 2x - 1) \mod 3$$

$\overline{m}_1(x) = x - 2$ | $m_1(x) = x - 2 \in \mathbb{Z}[x]$

$\overline{m}_2(x) = x^2 + 2x + 2$ | $m_2(x) = x^2 + 2x + 2$

then $(3) = (3, \alpha - 2)(3, \alpha^2 + 2\alpha + 2)$

$= P_3 P_3'$ we get

$f_{P_3|3} = 1 \qquad f_{P_3'|3} = 2$

$N(P_3) = 3^{f_{P_3|3}} = 3$

$N(P_3') = 3^2.$