

# Contents

<b>1</b>	<b>Ring Theory</b>	<b>1</b>
<b>2</b>	<b>Prime Ideals</b>	<b>1</b>
2.1	$\mathbb{Z}_K/\mathfrak{p}$ is finite (lemma 5.20)	1
2.2	$K$ is a number field. Every non-zero prime ideal $\mathfrak{p} \subseteq \mathbb{Z}_K$ is maximal (proposition 5.21)	2
<b>3</b>	<b>Fractional Ideals</b>	<b>2</b>
3.1	There are prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$ (lemma 5.24)	2
3.2	$\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow \mathfrak{b}^{-1} \subseteq \mathfrak{a}^{-1}$	2
3.3	$\mathfrak{a}^{-1} = \{\alpha \in K : \alpha\mathfrak{a} \subseteq \mathbb{Z}_K\}$ is a fractional ideal (lemma 5.25)	2
3.4	$\mathfrak{a}$ is a proper ideal of $\mathbb{Z}_K \Rightarrow \mathbb{Z}_K \subsetneq \mathfrak{a}^{-1}$ (lemma 5.26)	3
3.4.1	$\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow \mathfrak{b}^{-1} \subseteq \mathfrak{a}^{-1}$	3
3.5	$\mathfrak{p}$ is maximal $\Rightarrow \mathfrak{p}\mathfrak{p}^{-1} = \mathbb{Z}_K$ (lemma 5.28)	4
3.6	$\mathfrak{a}$ is any ideal $\Rightarrow \mathfrak{a}\mathfrak{a}^{-1} = \mathbb{Z}_K$ (lemma 5.29)	4
3.6.1	Derive identity	5
3.6.2	Prove final statement	5
3.7	Every ideal $\mathfrak{a} \neq 0$ is a product of prime ideals (lemma 5.31)	5
<b>4</b>	<b>Norms of Ideals</b>	<b>5</b>
4.1	$N_{K/\mathbb{Q}}(\langle\alpha\rangle) =  N_{K/\mathbb{Q}}(\alpha) $ (lemma 5.35)	5
4.1.1	Index calculated from determinant	5
4.1.2	Elements of ideal for $\langle\alpha\rangle$	5
<b>5</b>	$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$ (theorem 5.37)	<b>6</b>
5.1	$\mathbb{Z}_K/\mathfrak{p} \cong \mathfrak{a}/\mathfrak{a}\mathfrak{p}$ (lemma 5.36)	6
5.2	Result	6
<b>6</b>	<b>Dimension, Ramification Index and Inertia Degree</b>	<b>6</b>
6.1	Find Change of Basis Matrix	7
6.2	Calculate Index From Basis Transformation Matrix	8
6.3	Using Ring Isomorphisms	8
<b>7</b>	<b>Deconstructing Primes into Ideals (prop 5.42)</b>	<b>8</b>
7.1	Short Explanation	8
7.2	Example	9
7.3	Double Quotienting Ideals Isomorphic to Sum of Ideals	9
7.4	$\mathbb{Z}_K/\mathfrak{p}_1 \cong \mathbb{F}_p[X]/\langle\bar{g}_1(X)\rangle$ and is a Field	10
7.5	$\mathbb{Z}_K/\langle p \rangle \cong \mathbb{F}_p[X]/\langle\bar{g}(X)\rangle$	10
7.6	Deconstructing $p\mathbb{Z}_K$	10

## 1 Ring Theory

- Let  $R$  be an integral domain and  $p \in R$ . If  $\langle p \rangle$  is maximal then  $p$  is irreducible.
- $I$  is a maximal ideal  $\Leftrightarrow R/I$  is a field.
  - Let  $a \in R - I$ . Then  $aR + I = R \Rightarrow 1 \in ab + I$  for some  $b$ . So  $(a + I)(b + I) = 1 + I$ , and every  $a \notin I$  has an inverse.
- Let  $R$  be an integral domain and  $p \in R$ . Then  $\langle p \rangle$  is prime  $\Leftrightarrow p$  is prime.
- Let  $R$  be a ring. Then  $I$  is prime  $\Leftrightarrow R/I$  is an integral domain.
  - $(a + I)(b + I) = I \Rightarrow a$  or  $b \in I$
- Maximal ideals are prime.
- Finite integral domains are fields.

## 2 Prime Ideals

### 2.1 $\mathbb{Z}_K/\mathfrak{p}$ is finite (lemma 5.20)

Let  $\mathfrak{p}$  be a non-zero prime ideal in  $\mathbb{Z}_K$ . Let  $\alpha \in \mathfrak{p}, \alpha \neq 0$ . Then  $N(\alpha) \in \mathbb{Z}$  and  $\alpha | N(\alpha) \Rightarrow N(\alpha) \in \mathfrak{p}$ .

$\mathbb{Z}_K$  has integral basis

$$\mathbb{Z}_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$$

Since  $N\omega_i \in \mathfrak{p}$  by the nature of ideals, then  $a_i\omega_i \equiv b_i\omega_i \pmod{\mathfrak{p}}$  where  $0 \leq b_i < N$ . It could be smaller but we have established an upper bound for  $b_i$ , so  $\mathbb{Z}_K/\mathfrak{p}$  is finite.

## 2.2 $K$ is a number field. Every non-zero prime ideal $\mathfrak{p} \subseteq \mathbb{Z}_K$ is maximal (proposition 5.21)

Proof:

- Prime ideal  $\mathfrak{p} \Rightarrow \mathbb{Z}_K/\mathfrak{p}$  is an integral domain.
- $\mathbb{Z}_K/\mathfrak{p}$  is finite (lemma 5.20).
- Finite integral domain is a field.
- $\mathbb{Z}_K/\mathfrak{p}$  is a field  $\Rightarrow \mathfrak{p}$  is a maximal ideal.

## 3 Fractional Ideals

### 3.1 There are prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$ (lemma 5.24)

$\mathfrak{a}$  is a non-zero ideal of  $\mathbb{Z}_K$ .

$\mathbb{Z}_K$  is Noetherian. Since  $\mathfrak{a}$  forms an ascending chain  $\mathfrak{a} \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$ , it eventually terminates.

There are no prime ideals  $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$ . The same is true for all ideals in the chain  $\mathfrak{a}_i$ .

Lets take  $\mathfrak{a}$  to be the largest ideal in the chain.

$\mathfrak{a}$  is not prime otherwise  $\mathfrak{p}_1 = \mathfrak{a} \subseteq \mathfrak{a}$  and the proof is finished.

So there are ideals  $\mathfrak{a}_1, \mathfrak{a}_2$  in  $\mathbb{Z}_K$  such that  $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}, \mathfrak{a}_1 \not\subseteq \mathfrak{a}, \mathfrak{a}_2 \not\subseteq \mathfrak{a}$  Write

$$\mathfrak{b}_1 = \mathfrak{a} + \mathfrak{a}_1, \mathfrak{b}_2 = \mathfrak{a} + \mathfrak{a}_2$$

Then we can see that

$$\mathfrak{b}_1\mathfrak{b}_2 = (\mathfrak{a} + \mathfrak{a}_1)(\mathfrak{a} + \mathfrak{a}_2) = \mathfrak{a} + \mathfrak{a}_1\mathfrak{a} + \mathfrak{a}_2\mathfrak{a} + \mathfrak{a}_1\mathfrak{a}_2$$

Since  $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$ , so  $\mathfrak{b}_1\mathfrak{b}_2 \subseteq \mathfrak{a}$ . But also observe that

$$\mathfrak{a} \subsetneq \mathfrak{b}_1, \mathfrak{a} \subsetneq \mathfrak{b}_2$$

Since  $\mathfrak{b}_1, \mathfrak{b}_2$  are bigger than  $\mathfrak{a}$ , then by  $\mathfrak{a}$ 's maximality, there exist prime ideals  $\mathfrak{p}_i$  such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq \mathfrak{b}_1$$

$$\mathfrak{p}_{s+1} \cdots \mathfrak{p}_t \subseteq \mathfrak{b}_2$$

$$\Rightarrow \mathfrak{p}_1 \cdots \mathfrak{p}_t \subseteq \mathfrak{b}_1\mathfrak{b}_2 \subseteq \mathfrak{a}$$

Which is a contradiction.

### 3.2 $\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow \mathfrak{b}^{-1} \subseteq \mathfrak{a}^{-1}$

Let  $\beta \in \mathfrak{b}^{-1}$

$$\beta\mathfrak{b} \subseteq \mathbb{Z}_K$$

but  $\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow \beta\mathfrak{a} \subseteq \mathbb{Z}_K$  and so

$$\beta \in \mathfrak{a}^{-1}$$

### 3.3 $\mathfrak{a}^{-1} = \{\alpha \in K : \alpha\mathfrak{a} \subseteq \mathbb{Z}_K\}$ is a fractional ideal (lemma 5.25)

$$\mathfrak{a}^{-1} = \{\alpha \in K : \alpha\mathfrak{a} \subseteq \mathbb{Z}_K\}$$

Let  $\gamma \in \mathfrak{a}$  and  $\mathfrak{c} = \gamma\mathfrak{a}^{-1}$ . Take  $i, i' \in \mathfrak{c}$ , then  $i = \gamma\beta, i' = \gamma\beta'$  with  $\beta, \beta' \in \mathfrak{a}^{-1}$ .

$$(\beta + \beta')\mathfrak{a} = \beta\mathfrak{a} + \beta'\mathfrak{a} \subseteq (\mathbb{Z}_K + \mathbb{Z}_K) = \mathbb{Z}_K$$

Let  $i = \gamma\beta \in \mathfrak{c}$  with  $\gamma \in \mathfrak{a}, \beta \in \mathfrak{a}^{-1}$  and  $r \in \mathbb{Z}_K$ . We want to show that  $ri \in \mathfrak{c}$ .

But note that  $r \in \mathfrak{a}^{-1}$ , so  $r\beta \in \mathfrak{a}^{-1} \Rightarrow ri = \gamma(r\beta) \in \mathfrak{c}$ .

```

sage: K.<a> = NumberField(x^2 + 5)
sage: O = K.ring_of_integers()
sage: I = O.ideal(1 + a)
sage: (1 - a) * I
Fractional ideal (6)
sage: (1 - a)/6 * I
Fractional ideal (1)
sage: 1 - a in I^-1
True
sage: a in I^-1
True
sage: I.basis()
[6, a + 1]
sage: factor(I)
(Fractional ideal (2, a + 1)) * (Fractional ideal (3, a + 1))

```

### 3.4 $\mathfrak{a}$ is a proper ideal of $\mathbb{Z}_K \Rightarrow \mathbb{Z}_K \subsetneq \mathfrak{a}^{-1}$ (lemma 5.26)

#### 3.4.1 $\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow \mathfrak{b}^{-1} \subseteq \mathfrak{a}^{-1}$

Let  $\beta \in \mathfrak{b}^{-1}$ , then  $\beta\mathfrak{b} \subseteq \mathbb{Z}_K$ .

But  $\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow \beta\mathfrak{a} \subseteq \mathbb{Z}_K$

So  $\beta \in \mathfrak{a}^{-1}$ .

Section 4.6 shows  $\langle 1 - \sqrt{-5} \rangle$  is not prime.

```

sage: K.<a> = NumberField(x^2 + 5)
sage: O = K.ring_of_integers()
sage: I = O.ideal(1 + a)
sage: (1 - a) * I
Fractional ideal (6)
sage: (1 - a)/6 * I
Fractional ideal (1)
sage: 1 - a in I^-1
True
sage: a in I^-1
True
sage: I.basis()
[6, a + 1]
sage: I.is_prime()
False
sage: I.is_maximal()
False
sage: I
Fractional ideal (a + 1)
sage: factor(I)
(Fractional ideal (2, a + 1)) * (Fractional ideal (3, a + 1))
sage: J = O.ideal(2, a + 1)
sage: J.is_prime()
True
sage: 7 + a in J
True
sage: = O.ideal(7 + a)
sage: factor()
(Fractional ideal (2, a + 1)) * (Fractional ideal (3, a + 1))^3
sage: J.is_prime(), J.is_maximal() # of course
(True, True)
sage: O.ideal(3 + a+ 1)^3
Fractional ideal (43*a + 4)
sage: = (43*a + 4)*(10 + a) # choose any random value from the ideal
sage: in O.ideal(3 + a+ 1)^3

```

```

True
sage: in
False
sage: *J
Fractional ideal (277830, 7*a + 150115)
sage:
Fractional ideal (a + 7)
sage: 277830 in
True
sage: 7*a + 150115 in
True
sage: *^-1*J
Fractional ideal (5145, 7*a + 910)
sage: # which is a subset of Z_K
sage: *^-1
Fractional ideal (119/2*a + 35/2)
sage: J
Fractional ideal (2, a + 1)
sage: (119/2*a + 35/2)*J
Fractional ideal (5145, 7*a + 910)
sage: # so therefore *^-1 is a subset of J^-1
sage: J^-1
Fractional ideal (1, 1/2*a + 1/2)
sage: # we can see it consists of all odd halves of a
sage: # and any integer multiple of 1/2
sage: # which *^-1 = <119/2*a + 35/2> is a member of
sage: (a + 7)*0
Fractional ideal (a + 7)
sage:
434*a - 175
sage: N.<a> = Integers(5) []
sage: N(a + 7)
a + 2
sage: N(434*a - 175)
4*a
sage: # so they are different

```

$$\alpha \in \mathfrak{p} \Rightarrow \langle \alpha \rangle \subseteq \mathfrak{p}$$

And there exists

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \langle \alpha \rangle$$

but since  $r$  is minimal

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq \langle \alpha \rangle$$

Let  $\beta \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ , then  $\beta \notin \langle \alpha \rangle$ .

$$\beta \mathfrak{p} \subseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r \Rightarrow \beta \mathfrak{p} \subseteq \langle \alpha \rangle$$

$$\alpha^{-1} \beta \mathfrak{p} \subseteq \mathbb{Z}_K$$

$$\alpha^{-1} \beta \in \mathfrak{p}^{-1}$$

But also  $\beta \notin \langle \alpha \rangle$

$$\Rightarrow \alpha^{-1} \beta \notin \mathbb{Z}_K$$

### 3.5 $\mathfrak{p}$ is maximal $\Rightarrow \mathfrak{p}\mathfrak{p}^{-1} = \mathbb{Z}_K$ (lemma 5.28)

$\mathfrak{p}^{-1}$  strictly contains  $\mathbb{Z}_K$ , so there is a non-integer element  $\theta \in \mathfrak{p}^{-1}$ , and  $\mathfrak{p}\theta \not\subseteq \mathfrak{p}$ . But  $\mathfrak{p}$  is maximal, so  $\mathfrak{p}\mathfrak{p}^{-1} = \mathbb{Z}_K$ .

### 3.6 $\mathfrak{a}$ is any ideal $\Rightarrow \mathfrak{a}\mathfrak{a}^{-1} = \mathbb{Z}_K$ (lemma 5.29)

By the prev lemma, max ideals  $\mathfrak{p}\mathfrak{p}^{-1} = \mathbb{Z}_K$ . So  $\mathfrak{a}$  is not maximal.

### 3.6.1 Derive identity

$\mathfrak{ap}^{-1}$  is an ideal.

$$\mathfrak{a} \subseteq \mathfrak{ap}^{-1}$$

but  $\exists \theta \in \mathfrak{p}^{-1} : \theta \notin \mathbb{Z}_K$  so  $\mathfrak{a} \subsetneq \mathfrak{ap}^{-1}$ .

Since  $\mathfrak{ap}^{-1}$  is an ideal, and  $\mathfrak{a}$  is the biggest such that  $\mathfrak{a}\mathfrak{a}^{-1} = \mathbb{Z}_K$  then

$$\mathfrak{ap}^{-1}(\mathfrak{ap}^{-1}) = \mathbb{Z}_K$$

### 3.6.2 Prove final statement

$$\begin{aligned} \mathfrak{ap}^{-1}(\mathfrak{ap}^{-1}) &= \mathbb{Z}_K \\ [\mathfrak{p}^{-1}(\mathfrak{ap}^{-1})] \cdot \mathfrak{a} &= \mathbb{Z}_K \\ \Rightarrow \mathfrak{p}^{-1}(\mathfrak{ap}^{-1}) &\subseteq \mathfrak{a}^{-1} \end{aligned}$$

by the definition of a fractional ideal.

$$\Rightarrow \mathfrak{ap}^{-1}(\mathfrak{ap}^{-1}) \subseteq \mathfrak{a}\mathfrak{a}^{-1}$$

## 3.7 Every ideal $\mathfrak{a} \neq 0$ is a product of prime ideals (lemma 5.31)

Every maximal ideal is prime.

Let  $\mathfrak{a}$  be the biggest ideal not a product of primes. Then it is contained in  $\mathfrak{p}$  prime and so we can write.

$$\begin{aligned} \mathfrak{ap}^{-1} &= \mathfrak{p}_1 \cdots \mathfrak{p}_r \\ \Rightarrow \mathfrak{a} &= \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_r \end{aligned}$$

## 4 Norms of Ideals

### 4.1 $N_{K/\mathbb{Q}}(\langle \alpha \rangle) = |N_{K/\mathbb{Q}}(\alpha)|$ (lemma 5.35)

#### 4.1.1 Index calculated from determinant

See Alaca ANT theorem 9.1.2.

Let  $G$  be a free Abelian group with  $n$  generators  $\omega_1, \dots, \omega_n$ .

$$G = \{x_1\omega_1 + \cdots + x_n\omega_n : x_i \in \mathbb{Z}\}$$

Let  $H$  be a subgroup of  $G$  generated by  $n$  elements  $\eta_1, \dots, \eta_n$

$$H = \{y_1\eta_1 + \cdots + y_n\eta_n : y_i \in \mathbb{Z}\}$$

Because each  $\eta_i \in H \subseteq G$  we have

$$\eta_i = c_{i,1}\omega_1 + \cdots + c_{i,n}\omega_n$$

Let  $C = (c_{i,j})$  be an  $n \times n$  matrix. Then

$$[G : H] = \begin{cases} |\det(C)| & \text{if } \det(C) \neq 0 \\ \infty & \text{if } \det(C) = 0 \end{cases}$$

where  $|\det(C)|$  means absolute value of  $C$ 's determinant.

#### 4.1.2 Elements of ideal for $\langle \alpha \rangle$

$$\langle \alpha \rangle = \mathbb{Z}\alpha\omega_1 + \cdots + \mathbb{Z}\alpha\omega_n$$

$$\alpha\omega_1 = a_{1,1} + \cdots + a_{n,1}\omega_n$$

$$\alpha\omega_2 = a_{1,2} + \cdots + a_{n,2}\omega_n$$

...

$$\alpha\omega_n = a_{1,n} + \cdots + a_{n,n}\omega_n$$

$$\alpha \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = \begin{pmatrix} a_{1,1} & \cdots & a_{n,1} \\ & \cdots & \\ a_{1,n} & \cdots & a_{n,n} \end{pmatrix} \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}$$

The definition of norm from 3.2, is given as the determinant of that transform matrix.

## 5 $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ (theorem 5.37)

Let  $\mathfrak{p}$  be a non-zero prime ideal of  $\mathbb{Z}_K$ .

### 5.1 $\mathbb{Z}_K/\mathfrak{p} \cong \mathfrak{a}/\mathfrak{ap}$ (lemma 5.36)

There is no ideal  $\mathfrak{b}$  between  $\mathfrak{ap} \subsetneq \mathfrak{b} \subsetneq \mathfrak{a}$ . To see this simply multiply through by  $\mathfrak{a}^{-1}$ , and note  $\mathfrak{p}$  is maximal. So either  $\mathfrak{b} = \mathfrak{a}$  or  $\mathfrak{ap}$ .

Choose  $\alpha \in \mathfrak{a}$  with  $\alpha \notin \mathfrak{ap}$ . Then because of above  $\langle \alpha, \mathfrak{ap} \rangle = \mathfrak{a}$ .

$$\phi : \mathbb{Z}_K \rightarrow \mathfrak{a}/\mathfrak{ap}$$

$$\phi(x) = \alpha x + \mathfrak{ap}$$

is surjective. The kernel is  $\langle \mathfrak{p} \rangle$  since  $\alpha \langle \mathfrak{p} \rangle = \mathfrak{ap}$ .

The book has a typo on the last line of the proof. It should be  $\mathbb{Z}_K/\mathfrak{p} \cong \mathfrak{a}/\mathfrak{ap}$ .

### 5.2 Result

Factorise  $\mathfrak{b}$  into prime ideals and so we just deal with  $\mathfrak{b} = \mathfrak{p}$ .

$$\phi : \mathbb{Z}_K/\mathfrak{ap} \rightarrow \mathbb{Z}_K/\mathfrak{a}$$

$$\phi(\alpha + \mathfrak{ap}) = \alpha + \mathfrak{a}$$

is a homomorphism. So

$$\begin{aligned} \left| \frac{\mathbb{Z}_K/\mathfrak{ap}}{\mathfrak{a}/\mathfrak{ap}} \right| &= \left| \frac{\mathbb{Z}_K/\mathfrak{ap}}{\mathbb{Z}_K/\mathfrak{p}} \right| = |\mathbb{Z}_K/\mathfrak{a}| \\ \Rightarrow N(\mathfrak{ab}) &= |\mathbb{Z}_K/\mathfrak{ap}| = |\mathbb{Z}_K/\mathfrak{a}| \cdot |\mathbb{Z}_K/\mathfrak{p}| = N(\mathfrak{a})N(\mathfrak{b}) \end{aligned}$$

## 6 Dimension, Ramification Index and Inertia Degree

$\mathbb{Z}_K$  is  $n = [K : \mathbb{Q}]$  dimension vector space. See section 3.4.

$$|\mathbb{Z}_K/\langle p \rangle| = p^n$$

By CRT  $\mathbb{Z}_K/\langle p \rangle \cong \mathbb{Z}_K/\mathfrak{p}_1^{e_1} \times \mathbb{Z}_K/\mathfrak{p}_r^{e_r}$ .

$$|\mathbb{Z}_K/\mathfrak{p}_i^{e_i}| = N(p_i)^{e_i} = [\mathbb{Z}_K/\mathfrak{p}_i : \mathbb{F}_p]^{e_i} = (p^{f_i})^{e_i}$$

$$n = e_1 f_1 + \cdots + e_r f_r$$

```
sage: # See chapter 3.6.1
sage: y = ( (sqrt(2) + sqrt(6))/2 )
sage: minpoly(y)
x^4 - 4*x^2 + 1
sage: K.<a> = NumberField(x^4 - 4*x^2 + 1)
sage: O = K.ring_of_integers()
sage: I = O.ideal(5)
sage: I
Fractional ideal (5)
sage: factor(I)
(Fractional ideal (a^3 - 5*a + 1)) * (Fractional ideal (a^3 - 5*a - 1))
sage: A, B = O.ideal(a^3 - 5*a + 1), O.ideal(a^3 - 5*a - 1)
```

```

sage: A*B
Fractional ideal (5)
sage: A.ramification_index(), B.ramification_index()
(1, 1)
sage: I.norm()
625
sage: A.norm(), B.norm()
(25, 25)
sage: A.norm() * B.norm()
625
sage: ( ( y^3 - 5*y + 1 )*( y^3 - 5*y - 1 ) ).expand()
5

```

## 6.1 Find Change of Basis Matrix

The ideal  $\langle \gamma^3 - 5\gamma + 1 \rangle$  consists of elements  $a + b\gamma + c\gamma^2 + d\gamma^3 \in \mathbb{Z}_K$  multiplied by  $\gamma^3 - 5\gamma + 1$ .

$$\begin{aligned}
\mathbb{Z}_K &= \mathbb{Z}[\gamma], \quad \gamma = \frac{\sqrt{2} + \sqrt{6}}{2}, \quad \alpha = \sqrt{6} - 1 \\
\mathbb{Z}_K &= \mathbb{Z} + \mathbb{Z}\gamma + \mathbb{Z}y^2 + \mathbb{Z}y^3 \\
\langle \alpha \rangle &= \mathbb{Z}\alpha + \mathbb{Z}\alpha\gamma + \mathbb{Z}\alpha\gamma^2 + \mathbb{Z}\alpha\gamma^3 \\
\sqrt{2} &= \gamma^3 - 3\gamma, \quad \sqrt{3} = \gamma^2 - 2 \\
\alpha &= -\gamma^3 + 5\gamma - 1
\end{aligned}$$

Elements in  $\langle \alpha \rangle$  are of the form

$$\begin{aligned}
&(a + b\gamma + c\gamma^2 + d\gamma^3)(-\gamma^3 + 5\gamma - 1) \\
&\text{minpoly}(\gamma) = \gamma^4 - 4\gamma^2 + 1 \\
&\implies \gamma^4 = 4\gamma^2 - 1
\end{aligned}$$

```

sage: var("a b c d y")
(a, b, c, d, y)
sage: Y = (sqrt(2) + sqrt(6))/2
sage: y4 = 4*y^2 - 1
sage: (y4.subs({y: Y}) - Y^4).expand()
0
sage: e = ( (a + b*y + c*y^2 + d*y^3)*(-y^3 + 5*y - 1) ).expand(); e
-d*y^6 - c*y^5 - b*y^4 + 5*d*y^4 - a*y^3 + 5*c*y^3 - d*y^3 + 5*b*y^2 - c*y^2 + 5*a*y - b*y - a
sage: e = e.subs({y^4: y4}).expand(); e
-d*y^6 - c*y^5 - a*y^3 + 5*c*y^3 - d*y^3 + b*y^2 - c*y^2 + 20*d*y^2 + 5*a*y - b*y - a + b - 5*d
sage: e = e.subs({y^5: y*y4}).expand(); e
-d*y^6 - a*y^3 + c*y^3 - d*y^3 + b*y^2 - c*y^2 + 20*d*y^2 + 5*a*y - b*y + c*y - a + b - 5*d
sage: e = e.subs({y^6: y^2*y4}).expand(); e
-4*d*y^4 - a*y^3 + c*y^3 - d*y^3 + b*y^2 - c*y^2 + 21*d*y^2 + 5*a*y - b*y + c*y - a + b - 5*d
sage: e = e.subs({y^4: y4}).expand(); e
-a*y^3 + c*y^3 - d*y^3 + b*y^2 - c*y^2 + 5*d*y^2 + 5*a*y - b*y + c*y - a + b - d
sage: e.collect(y)
-(a - c + d)*y^3 + (b - c + 5*d)*y^2 + (5*a - b + c)*y - a + b - d

```

$$\begin{pmatrix} -a+b-d \\ 5a-b+c \\ b-c+5d \\ -a+c-d \end{pmatrix} = \begin{pmatrix} -1 & 1 & 0 & -1 \\ 5 & -1 & 1 & 0 \\ 0 & 1 & -1 & 5 \\ -1 & 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

```

sage: A = matrix([
.....:     [-1, 1, 0, -1],
.....:     [5, -1, 1, 0],
.....:     [0, 1, -1, 5],
.....:     [-1, 0, 1, -1]
.....: ])
sage: A.determinant()
25

```

## 6.2 Calculate Index From Basis Transformation Matrix

We can perform 2 operations on this change of basis matrix which keep it valid. See Alaca 9.1.2.

Let  $G = \{x_1\omega_1 + x_2\omega_2 + x_3\omega_3 + x_4\omega_4 : x_i \in \mathbb{Z}\}$  with a subgroup  $H$  defined by a basis

$$\eta_i = c_{i,1}\omega_1 + c_{i,2}\omega_2 + c_{i,3}\omega_3 + c_{i,4}\omega_4$$

We can add and subtract these basis from each other leaving the subgroup  $H$  intact. Observe that

$$\{\eta_1, \eta_2, \eta_3, \eta_4\} \text{ and } \{\eta_1, \eta_2 + k\eta_3, \eta_3, \eta_4\}$$

both generate the same group.

There is a slightly more difficult column operation. We simplify notation below. Assume we are swapping columns 2 and 3 of the 2nd row.

$$\begin{aligned} \eta_2 &= c_1\omega_1 + c_2\omega_2 + c_3\omega_3 + c_4\omega_4 \\ &= (c_1\omega_1 + c_4\omega_4) + c_2\omega_2 + c_3\omega_3 \\ &= (c_1\omega_1 + c_4\omega_4) + (c_2 + c_3)\omega_2 + c_3(\omega_3 - \omega_2) \\ &= c_1\omega_1 + \bar{c}_2\omega_2 + c_3\bar{\omega}_3 + c_4\omega_4 \end{aligned}$$

where

$$\bar{c}_2 = c_2 + c_3, \quad \bar{\omega}_3 = \omega_3 - \omega_2$$

Which will leave also  $G$  unchanged. Now we end up with

$$G = \langle \bar{\omega}_1, \bar{\omega}_2, \bar{\omega}_3, \bar{\omega}_4 \rangle$$

$$H = \langle d_1\bar{\omega}_1, d_2\bar{\omega}_2, d_3\bar{\omega}_3, d_4\bar{\omega}_4 \rangle$$

See the script ch5-degree.sage where we use this method to compute the degree.

## 6.3 Using Ring Isomorphisms

$$\sigma_1 : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \\ \sqrt{6} \mapsto \sqrt{6} \end{cases} \quad \sigma_2 : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \\ \sqrt{6} \mapsto -\sqrt{6} \end{cases} \quad \sigma_3 : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \\ \sqrt{6} \mapsto -\sqrt{6} \end{cases} \quad \sigma_4 : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \\ \sqrt{6} \mapsto \sqrt{6} \end{cases}$$

$$\begin{aligned} N(\sqrt{6} - 1) &= \sigma_1(\sqrt{6} - 1)\sigma_2(\sqrt{6} - 1)\sigma_3(\sqrt{6} - 1)\sigma_4(\sqrt{6} - 1) \\ &= (\sqrt{6} - 1)(-\sqrt{6} - 1)(-\sqrt{6} - 1)(\sqrt{6} - 1) \\ &= 25 \end{aligned}$$

```
sage: R.<x> = PolynomialRing(ZZ, 1)
sage: I = Ideal([x^4 - 4*x^2 + 1, x^3 - 5*x + 1])
sage: I.groebner_basis()
[x^2 + 4*x + 1, 5]
```

Which isomorphic to  $\mathbb{F}_{5^2}$ .

## 7 Deconstructing Primes into Ideals (prop 5.42)

### 7.1 Short Explanation

$$\mathbb{Z}_K/\langle p \rangle \cong \mathbb{F}_p[\gamma] \cong \mathbb{F}_p[X]/\langle \bar{g}(X) \rangle$$

By CRT

$$\mathbb{F}_p[X]/\langle \bar{g}(X) \rangle \cong \mathbb{F}_p[X]/\langle \bar{g}_1(X)^{e_1} \rangle \times \cdots \times \mathbb{F}_p[X]/\langle \bar{g}_r(X)^{e_r} \rangle$$

The map  $\mathbb{Z}_K \rightarrow \mathbb{F}_p[X]/\langle \bar{g}_1(X)^{e_1} \rangle \times \cdots \times \mathbb{F}_p[X]/\langle \bar{g}_r(X)^{e_r} \rangle$  has kernel

$$\langle p, g_1(\gamma)^{e_1} \rangle \cap \cdots \cap \langle p, g_r(\gamma)^{e_r} \rangle$$



$\mathfrak{p}_i^{e_i} \subseteq \langle p, g_i(\gamma)^{e_i} \rangle$  because

$$\mathfrak{p}_i^{e_i} = \langle p^{e_i}, p^{e_i-1}g_i(\gamma), \dots, pg_i(\gamma)^{e_i-1}, g_i(\gamma)^{e_i} \rangle$$

Finally

$$\begin{aligned} \langle p \rangle &= \langle p, g_1(\gamma)^{e_1} \rangle \cap \dots \cap \langle p, g_r(\gamma)^{e_r} \rangle \\ &\Rightarrow \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r} \subseteq \langle p \rangle \end{aligned}$$

Taking norms, we see that  $n = e_1 f_1 + \dots + e_r f_r$ , so the inclusion is actually an equality.

## 7.2 Example

$$K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$$\gamma = \frac{\sqrt{2} + \sqrt{6}}{2}$$

$$g(X) = X^4 - 4X^2 + 1$$

$$p = 5$$

$$\begin{aligned} \bar{g}(X) &= X^4 + X^2 + 1 \\ &= (X^2 + X + 1)(X^2 + 4X + 1) \end{aligned}$$

$$g_1(X) = (X^2 + X + 1), g_2(X) = X^2 + 4X + 1$$

$$\mathfrak{p}_1 = \langle 5, \gamma^2 + \gamma + 1 \rangle, \mathfrak{p}_2 = \langle 5, \gamma^2 + 4\gamma + 1 \rangle$$

## 7.3 Double Quotienting Ideals Isomorphic to Sum of Ideals

Observe the lattice when we collapse normal subgroups down to 0.

$$\frac{\langle p \rangle}{\langle g(X) \rangle} \subseteq \frac{\mathbb{Z}[X]}{\langle g(X) \rangle} \Leftrightarrow \langle p \rangle \subseteq \mathbb{Z}[X]$$

$$\phi : \mathbb{Z}[X]/\langle g(X) \rangle \rightarrow \mathbb{Z}[X]/\langle p, g(X) \rangle$$

$$\phi(r + \langle g(X) \rangle) = r + \langle p, g(X) \rangle$$

$$\ker \phi = \langle p, g(X) \rangle$$

Then observe

$$\phi(r + \langle g(X) \rangle) = 0 \Leftrightarrow r \in \langle p, g(X) \rangle \Leftrightarrow r + \langle g(X) \rangle \in \langle p, g(X) \rangle$$

By first iso theorem with the homomorphism  $\phi$ , we see that

$$(\mathbb{Z}[X]/\langle g(X) \rangle)/\langle p, g(X) \rangle \cong \mathbb{Z}[X]/\langle p, g(X) \rangle$$

Alternatively we can observe that  $\langle g(X) \rangle \subseteq \langle p, g(X) \rangle \subseteq \mathbb{Z}[X]$ , and then by the third theorem

$$\frac{\mathbb{Z}[X]/\langle g(X) \rangle}{\langle p, g(X) \rangle/\langle g(X) \rangle} \cong \frac{\mathbb{Z}[X]}{\langle p, g(X) \rangle}$$

since  $\langle p, g(X) \rangle/\langle g(X) \rangle = \langle p, g(X) \rangle$ .

#### 7.4 $\mathbb{Z}_K/\mathfrak{p}_1 \cong \mathbb{F}_p[X]/\langle \bar{g}_1(X) \rangle$ and is a Field

$$\mathbb{Z}_K/\mathfrak{p}_1 = \mathbb{Z}[\gamma]/\langle 5, \gamma^2 + \gamma + 1 \rangle$$

$$\phi : \mathbb{Z}[\gamma] \rightarrow \mathbb{Z}[X]/\langle g(X) \rangle$$

$$\phi(a_0 + a_1\gamma + a_2\gamma^2 + a_3\gamma^3) = a_0 + a_1X + a_2X^2 + a_3X^3 + \langle g(X) \rangle$$

$$\frac{\mathbb{Z}[\gamma]}{\langle p, g_1(\gamma) \rangle} \cong \frac{\mathbb{Z}[X]/\langle g(X) \rangle}{\langle p, g_1(X), g(X) \rangle / \langle g(X) \rangle} \cong \frac{\mathbb{Z}[X]}{\langle p, g_1(X), g(X) \rangle}$$

But also going in reverse with  $\psi : \mathbb{Z}[X]/\langle p \rangle \rightarrow \mathbb{F}_p$

$$\frac{\mathbb{Z}[X]}{\langle p, g_1(X), g(X) \rangle} \cong \frac{\mathbb{Z}[X]/\langle p \rangle}{\langle p, g_1(X), g(X) \rangle / \langle p \rangle} \cong \frac{\mathbb{F}_p[X]}{\langle \bar{g}_1(X), \bar{g}(X) \rangle}$$

Note that  $\bar{g}_1(X)|\bar{g}(X)$

$$\mathbb{Z}_K/\mathfrak{p}_1 \cong \mathbb{F}_p[X]/\langle \bar{g}_1(X) \rangle$$

$\bar{g}_1(X)$  is irreducible  $\Rightarrow \langle \bar{g}_1(X) \rangle$  is a prime ideal  $\Rightarrow$  the right hand side is a field, and so  $\mathfrak{p}_1$  is a prime ideal.

#### 7.5 $\mathbb{Z}_K/\langle p \rangle \cong \mathbb{F}_p[X]/\langle \bar{g}(X) \rangle$

$$\begin{aligned} \mathbb{Z}_K/\langle p \rangle &= \mathbb{Z}[\gamma]/\langle p \rangle \\ &\cong \frac{\mathbb{Z}[X]/\langle g(X) \rangle}{\langle p, g(X) \rangle / \langle g(X) \rangle} \\ &= \frac{\mathbb{Z}[X]}{\langle p, g(X) \rangle} \\ &\cong \frac{\mathbb{Z}[X]/\langle p \rangle}{\langle p, g(X) \rangle / \langle p \rangle} \end{aligned}$$

But let  $r \in \langle p, g(X) \rangle / \langle p \rangle \subseteq \mathbb{Z}[X]/\langle p \rangle$ , then  $r = ap + bg(X) \in \langle p, g(X) \rangle + \langle p \rangle = \langle p, g(X) \rangle$

$$\begin{aligned} \frac{\mathbb{Z}[X]/\langle p \rangle}{\langle p, g(X) \rangle / \langle p \rangle} &= \frac{\mathbb{Z}[X]/\langle p \rangle}{\langle p, g(X) \rangle} \\ &\cong \frac{\mathbb{F}_p[X]}{\langle \bar{g}(X) \rangle} \\ &\cong \mathbb{Z}_K/\langle p \rangle \end{aligned}$$

#### 7.6 Deconstructing $p\mathbb{Z}_K$

There is a map  $\mathbb{Z}_K \rightarrow \mathbb{Z}_K/\langle p \rangle$  with kernel  $\langle p \rangle$ .

Then for each component of the decomposed  $\mathbb{Z}_K/\langle p \rangle$ , there is another map  $\mathbb{Z}_K/\langle p \rangle \rightarrow \mathbb{Z}_K/\mathfrak{p}_1 \cong \mathbb{F}_p[X]/\langle \bar{g}_1(X) \rangle$  by  $\gamma \rightarrow X \pmod{\langle p, g_1(X) \rangle}$ . So the kernel is  $\langle p, g_1(\gamma) \rangle$ .

$$p\mathbb{Z}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$