

Algebraic Number Theory

Lecture 15: **Review & Sage**

Henrik Bachmann

Nagoya University, 4th February 2022

www.henrikbachmann.com

Based on the lecture notes available at www.henrikbachmann.com/algnt_2021.html

There you can also find a Jupyter Sage notebook with example code

Goal of this lecture

Goal: Review the content of this course and do some examples in Sage (sagemath.org & cocalc.com).

Overview of what we did:

- 1 Introduction & Basics of algebra
- 2 Integrality
- 3 Trace, Norm, and Discriminant
- 4 Dedekind domains
- 5 Lattices
- 6 Minkowski Theory
- 7 The class number
- 8 Fermat's Last Theorem
- 9 Dirichlet's Unit Theorem
- 10 Extensions of Dedekind domains

① Introduction & Basics of algebra - Prime as a sum of two squares

Theorem (Theorem 1.3)

A prime $p \geq 3$ can be written as a sum of two squares if and only if $p \equiv 1 \pmod{4}$.

For example $13 = 2^2 + 3^2 = (2 - 3i)(2 + 3i)$.

In Sage we create the number field $K = \mathbb{Q}(i)$ and its ring of integers $\mathcal{O}_K = \mathbb{Z}[i]$ by using the minimal polynomial $x^2 + 1$ of i :

```
1 K.<y> = NumberField(x^2+1);  
2 O = K.ring_of_integers();
```

The variable y now is a primitive element (In this case $y = \pm i$) of K . To factor 13 we consider the ideal (13) :

```
1 I=O.ideal(13);  
2 I.factor()
```

Output:

```
1 (Fractional ideal (-3*y - 2)) * (Fractional ideal (2*y + 3))
```

Which gives $(13) = (-3i - 2)(2i + 3) = (2 + 3i)(2 - 3i)$.

① Introduction & Basics of algebra - Prime as a sum of two squares

To deal with primes in Sage one can use the following code, which gives the 550 + 1-th prime

```
1 P = Primes()  
2 P.unrank(550)
```

Output:

```
1 4001
```

Naive way of finding the representation as a sum of two squares (just to see some code)

```
1 p=4001  
2 for a in range(p):  
3     for b in range(1,a+1):  
4         if a^2+b^2==p:  
5             print(a, " ", b)
```

Output:

```
1 49    40
```

Which means $4001 = 49^2 + 40^2$.

① Introduction & Basics of algebra - Factorization in $\mathbb{Z}[\sqrt{-5}]$

Exercise 5

We saw that in $R = \mathbb{Z}[\sqrt{-5}]$ we have the non-unique factorization of 6 into irreducible elements as $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. Find prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3 \subset R$ such that the ideals generated by these elements can be written as

$$(2) = \mathfrak{p}_1^2, \quad (3) = \mathfrak{p}_2\mathfrak{p}_3, \quad (1 + \sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_2, \quad (1 - \sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3$$

and conclude $(6) = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$.

We will use Sage to guess the ideals $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$:

```
1 K.<y> = NumberField(x^2+5); O = K.ring_of_integers();  
2 I=O.ideal(6);  
3 I.factor()
```

Output:

```
1 (Fractional ideal (2, y + 1))^2 * (Fractional ideal (3, y + 1)  
   ) * (Fractional ideal (3, y + 2))
```

$$(y = \pm\sqrt{-5})$$

① Introduction & Basics of algebra - Factorization in $\mathbb{Z}[\sqrt{-5}]$

Want $(6) = p_1^2 p_2 p_3$ with

$$(2) = p_1^2, (3) = p_2 p_3, (1 + \sqrt{-5}) = p_1 p_2, (1 - \sqrt{-5}) = p_1 p_3.$$

```
1 I=0.ideal(6);
2 I.factor()
```

Output:

```
1 (Fractional ideal (2, y + 1))^2 * (Fractional ideal (3, y + 1)
   ) * (Fractional ideal (3, y + 2))
```

Check if the guess is correct:

```
1 p1=0.ideal(2,y+1); p2=0.ideal(3,y+1); p3=0.ideal(3,y+2);
2 print("p1^2 = ",p1^2)
3 print("p2*p3 = ",p2*p3)
4 print("p1*p2 = ",p1*p2)
5 print("p1*p3 = ",p1*p3)
```

Output:

```
1 p1^2 = Fractional ideal (2)
2 p2*p3 = Fractional ideal (3)
3 p1*p2 = Fractional ideal (y + 1)
4 p1*p3 = Fractional ideal (-y + 1)
```

② Integrality - Recall some notations

Definition (Definition 2.1 & 2.6)

- ④ An **algebraic number field** K is a finite field extension of \mathbb{Q} , i.e. $\mathbb{Q} \subset K$ and $\dim_{\mathbb{Q}} K < \infty$. The elements of K are called **algebraic numbers**.
- ④ A number $x \in K$ of an algebraic number field is called an **algebraic integer** if it is the zero of a monic polynomial with integer coefficients, i.e. there exist some $a_1, \dots, a_n \in \mathbb{Z}$ with

$$x^n + a_1x^{n-1} + \dots + a_n = 0.$$

We denote the set of all algebraic integers of a number field K by

$$\mathcal{O}_K = \{x \in K \mid x \text{ algebraic integer}\}$$

This is called the **ring of integers of K** .

- ④ \mathcal{O}_K is the **integral closure** of \mathbb{Z} in K .

③ Trace, Norm, and Discriminant - Definition

Definition (Definition 3.4)

Let L/K be a finite field extension with $[L : K] = n$. For $x \in L$ define the K -linear map on the n -dimensional K -vector space L by

$$\begin{aligned} T_x : L &\longrightarrow L \\ \alpha &\longmapsto x \cdot \alpha. \end{aligned}$$

Then we define the **trace** and **norm** of x by

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}(T_x), \quad \mathrm{N}_{L/K}(x) = \det(T_x).$$

For $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, and $m = a + bi \in L$ we have $\mathrm{Tr}_{L/K}(m) = 2a$ and $\mathrm{N}_{L/K}(m) = a^2 + b^2$.

```
1 K.<y> = NumberField(x^2+1)
2 m=5+4*y
3 print("The element ",m," has norm ",m.norm()," and trace ",m.
   trace())
```

Output:

```
1 The element 4*y + 5 has norm 41 and trace 10
```


③ Trace, Norm, and Discriminant - Calculation of Norm & Trace

Proposition (Proposition 3.6)

Let L/K be a finite field extension with $[L : K] = n$ and $\text{char}(K) = 0$ or $|K| < \infty$. If $\sigma_i : L \rightarrow \bar{K}$ for $i = 1, \dots, n$ denotes the n embeddings of L in \bar{K} , then for $x \in L$ we have

$$f_x(\lambda) = \prod_{i=1}^n (\lambda - \sigma_i(x)),$$

$$\text{Tr}_{L/K}(x) = \sum_{i=1}^n \sigma_i(x),$$

$$N_{L/K}(x) = \prod_{i=1}^n \sigma_i(x).$$

(Here $f_x(\lambda)$ is the characteristic polynomial of T_x)

③ Trace, Norm, and Discriminant - Calculation of Norm & Trace

Let $f(x) = x^4 - 2x^2 + x + 1 = \prod_{j=1}^4 (x - \theta_j)$ and $K = \mathbb{Q}(\theta) \cong \mathbb{Q}[X]/f(X)$.

```
1 f(x)=x^4-2*x^2+x+1
2 for r in f.roots():
3     print(r[0].n())
```

Output:

```
1 -1.49021612009995
2 -0.524888598656405
3 1.00755235937818 - 0.513115795597015*I
4 1.00755235937818 + 0.513115795597015*I
```

```
1 K.<y> = NumberField(f(x))
2 print("K is a",K,"\nThe degree is ", K.degree())
3 [r,s]=K.signature()
4 print("K has",r," real embeddings and ",s," pair of complex
    embeddings")
```

Output:

```
1 K is a Number Field in y with defining polynomial x^4 - 2*x^2
    + x + 1
2 The degree is 4
3 K has 2 real embeddings and 1 pair of complex embeddings
```

③ Trace, Norm, and Discriminant - Calculation of Norm & Trace

Let $f(x) = x^4 - 2x^2 + x + 1 = \prod_{j=1}^4 (x - \theta_j)$ and $K = \mathbb{Q}(\theta) \cong \mathbb{Q}[X]/f(X)$.

We calculate the norm and trace of the element $a = \theta^2 - 3$:

```
1 # Using the built-in functions for norm and trace
2 a=y^2-3
3 print(a, " has norm ", a.norm(), " and trace ", a.trace())
```

Output:

```
1 y^2 - 3 has norm 13 and trace -8
```

```
1 # Calculating the norm&trace of y^2-3 by using the roots of f
2 p(x)=x^2-3
3 norm=1
4 trace=0
5 for r in f.roots():
6     norm*=p(r[0])
7     trace+=p(r[0])
8 print(a, " has norm ", norm.n(), " and trace ", trace.n())
```

Output:

```
1 y^2 - 3 has norm 13.000000000000000 and trace
  -8.000000000000000
```

③ Trace, Norm, and Discriminant - Calculation of Norm & Trace

Let $f(x) = x^4 - 2x^2 + x + 1 = \prod_{j=1}^4 (x - \theta_j)$ and $K = \mathbb{Q}(\theta) \cong \mathbb{Q}[X]/f(X)$.

We can also calculate the norm and trace of the element $a = \theta^2 - 3$ by using the embeddings created by sage:

```
1 # Calculating the norm&trace of y^2-3 by using the C-
   embeddings
2 embeddings=K.embeddings(CC);
3 a=y^2-3
4 norm=1
5 trace=0
6 for e in embeddings:
7     norm*=e(a)
8     trace+=e(a)
9 print(a, " has norm ", norm.n(), " and trace ", trace.n())
```

Output:

```
1 y^2 - 3 has norm 13.000000000000000 + 8.88178419700125e-16*I
   and trace -8.000000000000000
```

③ Trace, Norm, and Discriminant - Discriminant: Definition

Definition (Definition 3.8)

The **discriminant** of a basis $\alpha_1, \dots, \alpha_n$ of L is defined by

$$d(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2.$$

Definition (Definition 3.14)

An **integral basis** of B over A is a system of elements $\omega_1, \dots, \omega_n \in B$, such that each $b \in B$ can be written uniquely as a linear combination $b = a_1\omega_1 + \dots + a_n\omega_n$, with $a_1, \dots, a_n \in A$.

Definition (Definition 3.18)

The **discriminant of the number field K** is defined by

$$d_K = d(\omega_1, \dots, \omega_n),$$

where $\omega_1, \dots, \omega_n$ is an integral basis of K/\mathbb{Q} . (This always exists)

③ Trace, Norm, and Discriminant - Calculating the discriminant

Let $g(x) = x^3 - x^2 - 2x - 8 = \prod_{j=1}^3 (x - \theta_j)$ and $K = \mathbb{Q}(\theta) \cong \mathbb{Q}[X]/g(X)$.

```
1 g(x)=x^3-x^2-2x-8
2 K.<y> = NumberField(g(x))
3
4 print("K is a",K,"\nThe degree is ", K.degree())
5 [r,s]=K.signature()
6 print("K has",r," real embeddings and ",s, "pair of complex
      embeddings")
7
8 # Using the built in function for the discriminant & integral
      basis
9 print("discriminant: ", K.discriminant())
10 print("integral basis: ",K.integral_basis())
```

Output:

```
1 K is a Number Field in y with defining polynomial x^3 - x^2 -
      2*x - 8
2 The degree is 3
3 K has 1 real embeddings and 1 pair of complex embeddings
4 discriminant: -503
5 integral basis: [1, 1/2*y^2 + 1/2*y, y^2]
```

③ Trace, Norm, and Discriminant - Calculating the discriminant

For an integral basis $\omega_1, \dots, \omega_n$ the discriminant of K is

$$d_K = d(\omega_1, \dots, \omega_n) = \det(\sigma_i(\omega_j))^2.$$

```
1 # Calculating the discriminant by using an integral basis
2 B=K.integral_basis()
3 embeddings=K.embeddings(CC)
4 n=K.degree();
5 mat=matrix.zero(CC,n,n)
6
7 for i in range(n):
8     for j in range(n):
9         mat[i,j]=embeddings[i](B[j])
10
11 print(det(mat)^2)
```

Output:

```
1 -503.0000000000000
```

④ Dedekind domains - Definition & Unique factorization of ideals

Definition (Definition 4.2)

A domain R is called a **Dedekind domain** if

- ① R is noetherian,
- ② R is integrally closed,
- ③ every non-zero prime ideal in R is maximal.

Proposition (Proposition 4.3)

The ring of integers \mathcal{O}_K of an algebraic number field K is a Dedekind domain.

Theorem (Theorem 4.4)

Let \mathcal{O} be a Dedekind domain. Every ideal \mathfrak{a} of \mathcal{O} , which differs from (0) and (1) , admits a factorization

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$$

into nonzero prime ideals \mathfrak{p}_i of \mathcal{O} , which is unique up to the order of the factors.

④ Dedekind domains - Fractional ideals

Definition (Definition 4.8)

Let \mathcal{O} be a Dedekind domain with field of fractions $K = \text{Frac } \mathcal{O}$.

- ④ A **fractional ideal** of K is a finitely generated \mathcal{O} -submodule $\mathfrak{a} \neq \{0\}$ of K .
- ④ Fractional ideals in \mathcal{O} are called **integral ideals** of K .
- ④ For $a \in K^\times$ the module $(a) := a\mathcal{O}$ is a fractional ideal, called a **fractional principal ideal**.

Proposition (Proposition 4.10)

The fractional ideals form an abelian group, the **ideal group** J_K of K . The identity is $(1) = \mathcal{O}$, and the inverse of a fractional ideal \mathfrak{a} is $\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subset \mathcal{O}\}$.

Definition (Definition 4.13)

- ④ By P_K we denote the subgroup of J_K generated by all fractional principal ideals $(a) = a\mathcal{O}$ with $a \in K^\times$.
- ④ The quotient $\text{Cl}_K = J_K/P_K$ is called the **(ideal) class group** of K .

⑤ Lattices - Minkowski's theorem

Let V be an euclidean vector space. A discrete subgroup $\Gamma \subset V$ is called a **lattice** (Def. 5.1 & Prop. 5.3)

Definition (Definition 5.6)

A subset $X \subset V$ is called

- ① **centrally symmetric** if for all $x \in X$ we also have $-x \in X$.
- ② **convex** if for all $x, y \in X$ the line segment $\{ty + (1 - t)x \mid 0 \leq t \leq 1\}$ is contained in X .

Theorem (Minkowski's lattice point theorem, Theorem 5.7)

Let Γ be a complete lattice in the n -dimensional euclidean vector space V and X a centrally symmetric, convex subset of V . Suppose that

$$\text{vol}(X) > 2^n \text{vol}(\Gamma).$$

Then X contains at least one nonzero lattice point $\gamma \in \Gamma$.

⑥ Minkowski Theory - Minkowski space

Consider all embeddings $\tau_i : K \rightarrow \mathbb{C}$ at the same time and define the map

$$j : K \longrightarrow K_{\mathbb{C}} := \prod_{\tau} \mathbb{C}$$
$$a \longmapsto j(a) = (\tau(a))_{\tau} =: (a_{\tau})_{\tau} .$$

Denote by F the complex conjugation acting on $K_{\mathbb{C}}$ and define $\langle x, y \rangle = \sum_{\tau} x_{\tau} \overline{y_{\tau}}$ for $x, y \in K_{\mathbb{C}}$.

Definition (Definition 6.1)

Let $K_{\mathbb{R}}$ denote the F -invariant subspace of $K_{\mathbb{C}}$, i.e.

$$K_{\mathbb{R}} = \{z \in K_{\mathbb{C}} \quad \text{mod } z_{\bar{\tau}} = \overline{z_{\tau}}\} .$$

The restriction of \langle, \rangle on $K_{\mathbb{R}}$ gives a scalar product $\langle, \rangle : K_{\mathbb{R}} \times K_{\mathbb{R}} \rightarrow \mathbb{R}$ on the \mathbb{R} -vector space $K_{\mathbb{R}}$. The euclidean vector space $(K_{\mathbb{R}}, \langle, \rangle)$ is called **Minkowski space**.

⑥ Minkowski Theory - Useful theorem

Proposition (Proposition 6.3)

If $\mathfrak{a} \neq 0$ is an ideal of \mathcal{O}_K , then $\Gamma = j(\mathfrak{a})$ is a complete lattice in $K_{\mathbb{R}}$. Its fundamental mesh has volume

$$\text{vol}(\Gamma) = \sqrt{|d_K|}[\mathcal{O}_K : \mathfrak{a}].$$

Theorem (Theorem 6.4)

Let $\mathfrak{a} \neq (0)$ be an ideal of \mathcal{O}_K , and let $c_{\tau} > 0$ be real numbers for each embedding $\tau \in \text{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, such that $c_{\tau} = c_{\bar{\tau}}$ and

$$\prod_{\tau} c_{\tau} > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}[\mathcal{O}_K : \mathfrak{a}].$$

Then there exists an $a \in \mathfrak{a}$, $a \neq 0$ with $|\tau(a)| < c_{\tau}$ for all $\tau \in \text{Hom}_{\mathbb{Q}}(K, \mathbb{C})$.

⑦ The class number - Absolute norm & class number

Definition (Definition 7.1)

Let $\mathfrak{a} \neq (0)$ be an ideal in \mathcal{O}_K . Then the **absolute norm** of \mathfrak{a} is

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

Lemma (Lemma 7.5)

In every ideal $\mathfrak{a} \neq (0)$ of \mathcal{O}_K there exists an $a \in \mathfrak{a}$, $a \neq 0$, with

$$|\mathbf{N}_{K/\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi} \right)^2 \sqrt{|d_K|} \mathfrak{N}(\mathfrak{a}) .$$

Theorem (Theorem 7.6)

The ideal class group $\text{Cl}_K = J_K / P_K$ is finite. Its order $h_K = |\text{Cl}_K|$ is called the **class number** of K .

⑦ The class number - Calculation

Let $K = \mathbb{Q}(\sqrt{-5})$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. The class number is $h_K = 2$ and we can compute the classes as follows:

```
1 K.<y> = NumberField(x^2+5)
2 CK = K.class_group();
3 print(CK)
4 print("generators: ",CK.gen())
5 print("class number: ",K.class_number())
```

Output:

```
1 Class group of order 2 with structure C2 of Number Field in y
   with defining polynomial x^2 + 5
2 generators: Fractional ideal class (2, y + 1)
3 class number: 2
```

⑦ The class number - Dedekind zeta function & Analytic class number formula

Definition (Definition 7.9)

The **Dedekind zeta function** of a number field K is defined for $z \in \mathbb{C}$ with $\operatorname{Re}(z) > 1$ by

$$\zeta_K(z) = \sum_{(0) \neq \mathfrak{a} \subset \mathcal{O}_K} \frac{1}{\mathfrak{N}(\mathfrak{a})^z}.$$

Theorem (Analytic class number formula, Theorem 7.11)

The residue of ζ_K at $z = 1$ is given by

$$\lim_{z \rightarrow 1} (z - 1) \zeta_K(z) = \frac{2^r (2\pi)^s h_K R_K}{\omega_K \sqrt{|d_K|}},$$

where R_K is the regulator of K and ω_K is the number of roots of unity in K .

⑦ The class number - Analytic class number formula for $\mathbb{Q}(\sqrt{-5})$

$$\lim_{z \rightarrow 1} (z-1)\zeta_K(z) = \frac{2^r (2\pi)^s h_K R_K}{\omega_K \sqrt{|d_K|}}$$

```
1 # Analytic class number formula
2 K.<y> = NumberField(x^2+5)
3 DZ = K.zeta_function()
4 [r,s]=K.signature()
5 RK=K.regulator()
6 wK=K.zeta_order()
7 dK=K.discriminant()
8 hK=K.class_number()
9 print("RHS:", 2^r*(2*pi.n())^s*hK*RK/(wK*sqrt(abs(dK.n()))))
10 print("LHS: ", (0.9999999-1)*DZ(0.9999999))
```

Output:

```
1 RHS: 1.40496294620815
2 LHS: 1.40496290972109
```


⑧ Fermat's Last Theorem - Kummer's result

Recall that for $n \geq 1$ the **Fermat equation** is

$$x^n + y^n = z^n. \quad (1)$$

We are interested in non-trivial solutions ($xyz \neq 0$) for (1) with $x, y, z \in \mathbb{Z}$.

Definition (Definition 8.2)

A prime p is called **regular** if p does not divide $h_{\mathbb{Q}(\zeta_p)}$.

Theorem (Kummer 1850, Theorem 8.3)

- ① If $n = p \geq 3$ is a regular prime then there are no non-trivial solutions to (1).
- ② A prime p is regular if and only if it does not divide the numerator of the Bernoulli numbers B_k for $k = 2, 4, \dots, p-3$. Here the **Bernoulli numbers** B_k are defined by their exponential generating series

$$\sum_{k \geq 0} \frac{B_k}{k!} X^k := \frac{X}{e^X - 1}.$$

⑧ Fermat's Last Theorem - Regular primes

Definition (Definition 8.2)

A prime p is called **regular** if p does not divide $h_{\mathbb{Q}(\zeta_p)}$.

```
1 # Check if a prime is regular by using the definition
2 p=7
3 K.<y> = CyclotomicField(p)
4 classnumber = K.class_number()
5 print("class number: ", classnumber)
6
7 if classnumber % p != 0:
8     print(p, " is regular")
9 else:
10    print(p, " is not regular")
```

Output:

```
1 class number: 1
2 7 is regular
```

Notice that this becomes really (!) slow for larger primes p .

⑧ Fermat's Last Theorem - Regular primes with Kummer's criteria

Kummer's criteria: A prime p is regular if and only if it does not divide the numerator of the Bernoulli numbers B_k for $k = 2, 4, \dots, p - 3$.

```
1 # Using Kummer's criteria to check if a prime is regular
2 p=37
3 regular=True
4 for k in range(2,p-2):
5     if k % 2 ==0 and bernoulli(k).numerator() % p == 0:
6         regular=False
7         break
8
9 if regular:
10     print(p, " is regular")
11 else:
12     print(p, " is not regular")
```

Output:

```
1 37 is not regular
```

⑧ Fermat's Last Theorem - Regular primes with Kummer's criteria II

```
1 # Give all non-regular primes up to a given bound
2 P = Primes()
3
4 for n in range(30):
5     p = P.unrank(n)
6     regular=True
7     for k in range(2,p-2):
8         if k % 2 ==0 and bernoulli(k).numerator() % p == 0:
9             regular=False
10            break
11
12 if not regular:
13     print(p, " is not regular")
```

Output:

```
1 37 is not regular
2 59 is not regular
3 67 is not regular
4 101 is not regular
5 103 is not regular
```

⑨ Dirichlet's Unit Theorem - Statement

Denote by $\mu(K)$ the set of roots of unity contained in a number field K .

Theorem (Dirichlet's unit theorem, Theorem 9.4)

The unit group \mathcal{O}_K^\times is given by a direct product of the cyclic group $\mu(K)$ and a free abelian group of rank $r + s - 1$, i.e.

$$\mathcal{O}_K^\times \cong \mu(K) \oplus \mathbb{Z}^{r+s-1}.$$

This theorem implies that there exist units $\epsilon_1, \dots, \epsilon_t$, with $t = r + s - 1$, called the **fundamental units**, such that any unit $\epsilon \in \mathcal{O}_K^\times$ can be written as

$$\epsilon = \zeta \epsilon_1^{\nu_1} \cdots \epsilon_t^{\nu_t}$$

with $\zeta \in \mu(K)$ and $\nu_1, \dots, \nu_t \in \mathbb{Z}$.

⑨ Dirichlet's Unit Theorem - Example

There exist units $\epsilon_1, \dots, \epsilon_t$, with $t = r + s - 1$, called the **fundamental units**, such that any unit $\epsilon \in \mathcal{O}_K^\times$ can be written as

$$\epsilon = \zeta \epsilon_1^{\nu_1} \cdots \epsilon_t^{\nu_t}$$

with $\zeta \in \mu(K)$ and $\nu_1, \dots, \nu_t \in \mathbb{Z}$.

```
1 K.<y> = NumberField(x^2-7)
2 UK = UnitGroup(K);
3 print(UK);
4 print("generators: ", UK.gens_values())
5 zeta=UK.gens()[0]
6 eps1=UK.gens()[1]
```

Output:

```
1 Unit group with structure C2 x Z of Number Field in y with
   defining polynomial x^2 - 7
2 generators: [-1, 3*y - 8]
```

Here we see that $8 + 3\sqrt{7}$ is the fundamental unit for $K = \mathbb{Q}(\sqrt{7})$.

10 Extensions of Dedekind domains - Notations

Setup in this section:

- A : Dedekind domain,
- $K = \text{Frac } A$,
- L/K : finite extension,
- \mathcal{O} : integral closure of A in L .

$$\begin{array}{ccc} K & \hookrightarrow & L \\ \uparrow & & \uparrow \\ A & \hookrightarrow & \mathcal{O} \end{array}$$

Proposition (Proposition 10.1 & 10.2)

- \mathcal{O} is a Dedekind domain.
- Let \mathfrak{p} be a prime ideal of A then $\mathfrak{p}\mathcal{O} \neq \mathcal{O}$.

A prime ideal $\mathfrak{p} \neq (0)$ of A decomposes in \mathcal{O} in a unique way into a product of prime ideals:

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

10 Extensions of Dedekind domains - Fundamental identity

A prime ideal $\mathfrak{p} \neq (0)$ of A decomposes in \mathcal{O} in a unique way into a product of prime ideals:

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}. \quad (2)$$

Definition (Definition 10.3)

- 1 The exponent e_i in (2) is called the **ramification index** of \mathfrak{P}_i over \mathfrak{p} .
- 2 The degree of the field extension

$$f_i = \left[\mathcal{O}/\mathfrak{P}_i : A/\mathfrak{p} \right]$$

is called the **inertia degree** of \mathfrak{P}_i over \mathfrak{p} .

Theorem (Fundamental identity, Definition 10.4)

We have

$$\sum_{i=1}^r e_i f_i = n = [L : K].$$

⑩ Extensions of Dedekind domains - Example

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, \quad e_i: \text{ramification index}, \quad f_i = \left[\mathcal{O}/\mathfrak{P}_i : A/\mathfrak{p} \right]: \text{inertia degree}$$

```
1 # Calculate the ramification indices and inertia degrees
2 K.<y> = NumberField(x^2+1)
3 p=K.ideal(53)
4 fac=K.factor(p)
5 print("The ideals over ", p, " are:")
6 for P in fac:
7     print(P[0], "with ramification index e =", P[1], " and
8         inertia degree f =", P[0].residue_class_degree())
```

Output:

```
1 The ideals over Fractional ideal (53) are:
2 Fractional ideal (-2*y + 7) with ramification index e = 1 and
   inertia degree f = 1
3 Fractional ideal (2*y + 7) with ramification index e = 1 and
   inertia degree f = 1
```

10 Extensions of Dedekind domains - Ramification

Definition

Let $\mathfrak{p} \subset A$ be a prime ideal with the following factorization in \mathcal{O}

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

- ④ \mathfrak{p} is said to **split completely** (or **totally split**) in L , if $r = n = [L : K]$, i.e. $e_i = f_i = 1$ for all $i = 1, \dots, r$.
- ④ \mathfrak{p} is called **nonsplit** if $r = 1$, i.e. there is just one prime ideal in \mathcal{O} over \mathfrak{p} .
- ④ \mathfrak{P}_i is called **unramified** over A (or K) if $e_i = 1$ and if the extension $\mathcal{O}/\mathfrak{P}_i/A/\mathfrak{p}$ is separable. Otherwise \mathfrak{P}_i is called **ramified**. If $e_i > 1$ and $f_i = 1$ then \mathfrak{P}_i is called **totally ramified**.
- ④ \mathfrak{p} is called **unramified** if all \mathfrak{P}_i over \mathfrak{p} are unramified. Otherwise, \mathfrak{p} is called **ramified**. In particular, if \mathfrak{p} split completely then it is unramified.
- ④ The extension L/K is called unramified if all prime ideals $\mathfrak{p} \subset A$ are unramified.

Bonus - Finite multiple zeta values

Next semester, I will offer a course dealing with the following objects:

Definition

For integers $k_1, \dots, k_r \geq 1$ the **finite multiple zeta value** is defined by

$$\zeta_{\mathcal{A}}(k_1, \dots, k_r) = \left(\sum_{p > m_1 > \dots > m_r > 0} \frac{1}{m_1^{k_1} \dots m_r^{k_r}} \pmod{p} \right)_{p \text{ prime}} \in \mathcal{A},$$

where \mathcal{A} is given by

$$\mathcal{A} = \prod_{p \text{ prime}} \mathbb{F}_p / \bigoplus_{p \text{ prime}} \mathbb{F}_p.$$

These objects satisfy various relations which we will try to understand.

Example

$$\zeta_{\mathcal{A}}(4, 1) - \zeta_{\mathcal{A}}(1, 4) + \zeta_{\mathcal{A}}(3, 2) = 0$$

Bonus - The algebra \mathcal{A}

We have an embedding $\mathbb{Q} \xrightarrow{i} \mathcal{A}$, since for $\frac{a}{b} \in \mathbb{Q}$ we can get a solution x_p of

$$b x_p - a \equiv 0 \pmod{p}$$

for all but finitely many p . Set $x_p = 0$ if it does not exist and define

$$i\left(\frac{a}{b}\right) = (x_2, x_3, x_5, x_7, \dots) \in \mathcal{A} = \prod_{p \text{ prime}} \mathbb{F}_p / \bigoplus_{p \text{ prime}} \mathbb{F}_p.$$

$\implies \mathcal{A}$ is a \mathbb{Q} -algebra.

Example

$$i\left(\frac{3}{10}\right) = (0, 0, 0, 1, 8, 12, 2, 6, 21, \dots).$$

One can show that the space spanned by all finite multiple zeta values is a subalgebra of \mathcal{A} .

Bonus - FMZ in depth 1 and 2

Proposition

- Depth 1: For $k \geq 1$ we have $\zeta_{\mathcal{A}}(k) = 0$.
- Depth 2: For $k_1, k_2 \geq 1$ we have

$$\zeta_{\mathcal{A}}(k_1, k_2) = \left((-1)^{k_1} \binom{k_1 + k_2}{k_2} \frac{B_{p-k_1-k_2}}{k_1 + k_2} \right)_{p \text{ prime}}.$$

- Clearly $\zeta_{\mathcal{A}}(k_1, k_2) = 0$ if $k_1 + k_2$ is even.
- It is expected, that $\zeta_{\mathcal{A}}(k_1, k_2) \neq 0$ if $k_1 + k_2$ is odd.
- We do not know any example for k_1, \dots, k_r for which we can prove $\zeta_{\mathcal{A}}(k_1, \dots, k_r) \neq 0$.

One connection to the current course is the following observation:

Proposition

If there are infinitely many regular primes then $\zeta_{\mathcal{A}}(k_1, k_2) \neq 0$ for $k_1 + k_2$ odd.