Introduction to SageMath & Algebraic Number Theory

Henrik Bachmann

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 these slides

Goal: Review the content of the course "Algebraic Number Theory" 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

Theorem (Theorem 1.3)

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

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

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

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

Output:

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

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

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

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

Output:

```
4001
```

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

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

Output:

```
49   40
```

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

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 $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$:

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

Output:

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

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

Want $(6) = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$ with $(2) = \mathfrak{p}_1^2$, $(3) = \mathfrak{p}_2\mathfrak{p}_3$, $(1+\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_2$, $(1-\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3$.

```
I=O.ideal(6);
I.factor()
```

Output:

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

Check if the guess is correct:

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

Output:

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

Definition (Definition 2.1 & 2.6)

(i) 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**.

(ii) 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 $a_1, \ldots, a_n \in \mathbb{Z}$ with

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0\,.$$

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 $\boldsymbol{K}$**.

(iii) $\mathcal{O}_K$ 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

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

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

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

Output:

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

Proposition (Proposition 3.6)

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

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

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

$$\mathrm{N}_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x) \,.$$

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

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

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

Output:

```
-1.49021612009995
-0.524888598656405
1.00755235937818 - 0.513115795597015*I
1.00755235937818 + 0.513115795597015*I
```

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

Output:

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

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

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

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

Output:

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

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

Output:

```
y^2 - 3  has norm  13.0000000000000  and trace  -8.00000000000000
```

Let $f(x) = x^4 - 2x^2 + x + 1 = \prod_{j=1}^{4}(x - \theta_i)$ 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:

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

Output:

```
y^2 - 3  has norm  13.0000000000000 + 8.88178419700125e-16*I  and trace
     -8.00000000000000
```

Definition (Definition 3.8)

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

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

Definition (Definition 3.14)

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

Definition (Definition 3.18)

The **discriminant of the number field $\boldsymbol{K}$** is defined by

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

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

③ Trace, Norm, and Discriminant - Calculating the discriminant

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

```
g(x)=x^3-x^2-2x-8
K.<y> = NumberField(g(x))

print("K is a",K,"\nThe degree is ", K.degree())
[r,s]=K.signature()
print("K has",r," real embeddings and ",s, "pair of complex embeddings")

# Using the built in function for the discriminant & integral basis
print("discriminant: ", K.discriminant())
print("integral basis: ",K.integral_basis())
```

Output:

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

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

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

```
# Calculating the discriminant by using an integral basis
B=K.integral_basis()
embeddings=K.embeddings(CC)
n=K.degree();
mat=matrix.zero(CC,n,n)

for i in range(n):
    for j in range(n):
        mat[i,j]=embeddings[i](B[j])

print(det(mat)^2)
```

Output:

```
-503.000000000000
```

Definition (Definition 4.2)

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

(i) R is noetherian,

(ii) R is integrally closed,

(iii) 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.

Definition (Definition 4.8)

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

- (i) A **fractional ideal** of K is a finitely generated $\mathcal{O}$-submodule $\mathfrak{a} \neq \{0\}$ of K.
- (ii) Fractional ideals in $\mathcal{O}$ are called **integral ideals** of K.
- (iii) 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)

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

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

- (i) **centrally symmetric** if for all $x \in X$ we also have $-x \in X$.
- (ii) **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

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

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

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

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

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.

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

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

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

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

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 $\tau \in \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, such that $c_\tau = c_{\overline{\tau}}$ 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 $\tau \in \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$.

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

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

Theorem (Theorem 7.6)

The ideal class group $\mathrm{Cl}_K = {}^{J_K}\!/\!{}_{P_K}$ is finite. Its order $h_k = |\,\mathrm{Cl}_K\,|$ is called the ***class number*** *of K.*

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:

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

Output:

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

Definition (Definition 7.9)

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

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

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

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

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

Output:

```
RHS: 1.40496294620815
LHS:  1.40496290972109
```

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

$$x^n + y^n = z^n \,. \tag{1}$$

We are interest 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 $k = 2, 4, \ldots, p-3$. 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 $h_{\mathbb{Q}(\zeta_p)}$.

```
# Check if a prime is regular by using the definition
p=7
K.<y> = CyclotomicField(p)
classnumber = K.class_number()
print("class number: ", classnumber)

if classnumber % p != 0:
        print(p, " is regular")
else:
        print(p, " is not regular")
```

Output:

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

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

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 $k = 2, 4, \ldots, p-3$.

```
# Using Kummer's criteria to check if a prime is regular
p=37
regular=True
for k in range(2,p-2):
    if k % 2 ==0 and bernoulli(k).numerator() % p == 0:
        regular=False
        break

if regular:
        print(p, " is regular")
else:
        print(p, " is not regular")
```

Output:

```
37  is not regular
```

```
# Give all non-regular primes up to a given bound
P = Primes()

for n in range(30):
    p = P.unrank(n)
    regular=True
    for k in range(2,p-2):
        if k % 2 ==0 and bernoulli(k).numerator() % p == 0:
            regular=False
            break

    if not regular:
        print(p, " is not regular")
```

Output:

```
37  is not regular
59  is not regular
67  is not regular
101  is not regular
103  is not regular
```

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 $\epsilon_1, \ldots, \epsilon_t$, 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 $\nu_1, \ldots, \nu_t \in \mathbb{Z}$.

⑨ Dirichlet's Unit Theorem - Example

There exist units $\epsilon_1, \ldots, \epsilon_t$, 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 $\nu_1, \ldots, \nu_t \in \mathbb{Z}$.

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

Output:

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

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

Setup in this section:

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

$$\begin{tikzcd} K \arrow[r, hook] & L \\ A \arrow[u, hook] \arrow[r, hook] & \mathcal{O} \arrow[u, hook] \end{tikzcd}$$

Proposition (Proposition 10.1 & 10.2)

(i) *$\mathcal{O}$ is a Dedekind domain.*

(ii) *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:

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

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

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}\,. \tag{2}$$

Definition (Definition 10.3)

- (i) The exponent e_i in (2) is called the **ramification index** of $\mathfrak{P}_i$ over $\mathfrak{p}$.
- (ii) 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

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

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

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

Output:

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

Definition

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

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

(i) $\mathfrak{p}$ is said to **split completely** (or **totally split**) in L, if $r = n = [L : K]$, i.e. $e_i = f_i = 1$ for all $i = 1, \ldots, r$.

(ii) $\mathfrak{p}$ is called **nonsplit** if $r = 1$, i.e. there is just one prime ideal in $\mathcal{O}$ over $\mathfrak{p}$.

(iii) $\mathfrak{P}_i$ 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**.

(iv) $\mathfrak{p}$ 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.

(v) The extension L/K is called unramified if all prime ideals $\mathfrak{p} \subset A$ are unramified.