CSE291-14: The Number Field Sieve

https://cseweb.ucsd.edu/classes/wi22/cse291-14

Emmanuel Thomé

January 18, 2022

Part 3b

Algebraic Number Theory background

Number fields, algebraic numbers

Algebraic integers, ring of integers

Ideals

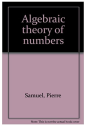
Factoring into prime ideals

Units and the class group

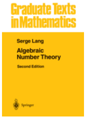
Textbooks

Numerous textbooks available on algebraic number theory.

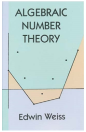
- A good read:
  P. Samuel, Algebraic theory of numbers, Hermann, 1970 (multiple editions).



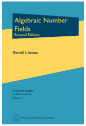
- Not advisable for a first read:
  S. Lang, Algebraic Number Theory, Springer, GTM 110, 1994.



- E. Weiss, Algebraic Number Theory, Dover, Mc-Graw Hill, 1963 (multiple editions).



- G. Janusz, algebraic number fields, AMS, GSM 7, 1996.



Plan

Number fields, algebraic numbers

Algebraic integers, ring of integers

Ideals

Factoring into prime ideals

Units and the class group

Goals

Our goals here:

- define the basic vocabulary: algebraic numbers, number fields.
- give a few examples.
- introduce the very few bits of Galois theory that we need in order to define the norm of an element.

Note: we deliberately don't give proofs. Those can be found in textbooks.

Algebraic numbers

Def. Let $K \subset L$ be two fields. "$x \in L$ is algebraic over K" means:

$$\exists P \in K[X], \quad P(x) = 0.$$

- if all $x \in L$ are algebraic, L/K is an algebraic extension ;
- a finite extension is algebraic ;
- an algebraic extension is not necessarily finite ($\bar{\mathbb{Q}}$).
- Common terminology:
  - Algebraic number = something algebraic over (a finite extension of) $\mathbb{Q}$.
  - Number field = a finite algebraic extension of $\mathbb{Q}$.

Roots of the defining polynomial

Let f be irreducible over $\mathbb{Q}$.

By construction, f has a root in $K = \mathbb{Q}[x]/f$.

Where do the other roots of f lie ?

- In some cases, they are also in K. Some examples:
  - If f has degree 2,
  - If f is a cyclotomic polynomial (e.g. $x^4 + 1 = \Phi_8$).
- Most often they are not. Most typical example: $\mathbb{Q}(\sqrt[3]{2})$.

It is sometimes convenient to think of the roots of f in an algebraic closure of K. For example in $\mathbb{C}$.

This links to the Galois group.

Example

```
sage: K.<h> = NumberField(x^4+1)
sage: h.minpoly()
x^4 + 1
sage: h.minpoly().roots(K)
[(h, 1), (-h, 1), (h^3, 1), (-h^3, 1)]
sage: h.minpoly().change_ring(K).factor()
(x - h) * (x + h) * (x - h^3) * (x + h^3)
```

Example

```
sage: K.<alpha> = NumberField(x^3-2)
sage: alpha.minpoly()
x^3 - 2
sage: alpha.minpoly().roots(K)
[(alpha, 1)]
sage: alpha.minpoly().change_ring(K).factor()
(x - alpha) * (x^2 + alpha*x + alpha^2)
```

On top of K, the field where the other roots of f live is an extension of degree 2.

Splitting field

Let f be irreducible over $\mathbb{Q}$.

- $K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/f$ brings one root to f.
  - there may be more.
  - But α may also be the only root: f may factor in K as

$$f = (x - \alpha) \times (\text{irreducible factor of degree } n - 1).$$

- We may then build another extension, of degree at most $n - 1$.
- And so on and so forth.

The splitting field (normal closure) of f has degree at most $n!$.
This is what happens generically, for f having no magical property.

Galois groups

Normal extension

A field extension L/K is normal if and only if, given $g \in K[x]$ irreducible:

$$g \text{ has a root in } L \Leftrightarrow g \text{ splits completely.}$$

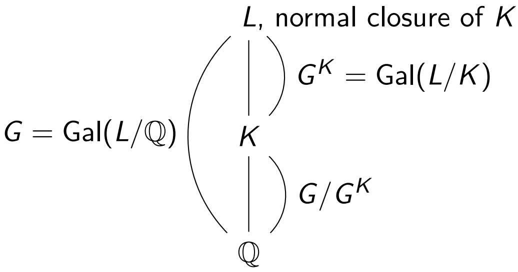
Def. Normal+Separable=Galois (see textbooks, e.g. Stewart). In the NFS world, we're always separable.

$\mathrm{Gal}(L/K)$: group of automorphisms of L leaving K fixed.

In the NFS context, L is never computed, and we are not really interested in $\mathrm{Gal}(L/\mathbb{Q})$ either. However:

- $\mathrm{Gal}(L/\mathbb{Q})$ is the Galois-related thing which is a group.
- We are interested in its action on K.

Galois group (2)



- When we speak of "the Galois group of f", or of K, we're implying G.
- But G can be partitioned into cosets, each acting in a unique way on K (elements of G do not leave K fixed!).

A "random" polynomial of degree n has Galois group $\mathfrak{S}_n$.

Embeddings into $\mathbb{C}$

Take for example $K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/_{x^3-2}$. We have three embeddings of K into $\mathbb{C}$.

$$\phi_1 : \begin{cases} K & \to & \mathbb{C}, \\ \alpha & \mapsto & \sqrt[3]{2}, \end{cases} \quad \phi_2 : \begin{cases} K & \to & \mathbb{C}, \\ \alpha & \mapsto & j\sqrt[3]{2}, \end{cases} \quad \phi_3 : \begin{cases} K & \to & \mathbb{C}, \\ \alpha & \mapsto & j^2\sqrt[3]{2}. \end{cases}$$

The Galois group of $x^3 + 2$ is $\mathfrak{S}_3$, of order 6.

Given $K = \mathbb{Q}(\alpha)$, the set of roots in a splitting field is:
$(\alpha_1, \ldots, \alpha_n) = (\alpha^\sigma)_{\sigma \in G/G_K}$. (notation: $\alpha^\sigma = \sigma(\alpha)$)

The Galois group thus controls the various existing embeddings into $\mathbb{C}$.

Norm, trace, etc

Symmetric functions of the roots are defined over $\mathbb{Q}$ (because by Galois theory, they are fixed by G).

Two important examples. Let $\zeta \in K$.

$$\mathrm{Tr}_{K/\mathbb{Q}}(\zeta) = \sum_{\sigma \in G/G_K} \zeta^\sigma,$$

$$\mathrm{Norm}_{K/\mathbb{Q}}(\zeta) = \prod_{\sigma \in G/G_K} \zeta^\sigma.$$

In particular the norm can be turned into something very algorithmic, computable, and useful.

Computing the norm

Let $A(\alpha) = \sum_i a_i \alpha^i$ denote an element of K.

- A denotes a polynomial with coefficients in $\mathbb{Q}$.
- The Galois conjugates are $A(\alpha)^\sigma = A(\alpha^\sigma)$.
- But note also that $\{\alpha^\sigma\}_{\sigma \in G/G_K}$ are exactly the roots of f.

Thus the computation of the norm is achieved by the Resultant of f and A.

The resultant is the product of the evaluations of a polynomial at all the roots of another.

- it is an eminently computable thing!
  Only arithmetic in the coefficient ring is needed.
- and we will deal with simple cases only.

The norm and the resultant

Definition of $\mathrm{Res}(u(x), v(x))$

$$\mathrm{Res}(u(x), v(x)) = \mathrm{lc}(u)^{\deg v} \prod_{u(\mu)=0} v(\mu) = \mathrm{lc}(v)^{\deg u} \prod_{v(\nu)=0} u(\nu),$$

$$= \text{(also) determinant of the Sylvester matrix.}$$

Repeat: the roots of f are $\{\alpha^\sigma\}_{\sigma \in G/G_K}$.
IOW: $f = \mathrm{lc}(f) \prod_{\sigma \in G/G_K} (x - \alpha^\sigma)$
Therefore

$$\mathrm{Norm}_{K/\mathbb{Q}}(A(\alpha)) = \prod_{\sigma \in G/G_K} A(\alpha^\sigma) = \prod_{r \in \text{roots of } f} A(r)$$

$$= (1/f_n)^{\deg A} \mathrm{Res}(f, A).$$

Notice that we do not need to compute L or $\mathrm{Gal}(L/K)$.

Common case in NFS

In the NFS context, we often consider algebraic numbers like $a - b\alpha$. Their norm can be computed easily.

$$\begin{aligned}\mathrm{Norm}_{K/\mathbb{Q}}(a - b\alpha) &= \frac{1}{f_n}\,\mathrm{Res}(f, a - bx) = \frac{b^n}{f_n} f(\frac{a}{b}),\\ &= \frac{1}{f_n}\left(f_n a^n + f_{n-1} a^{n-1} b + \cdots + f_0 b^n\right).\end{aligned}$$

If one introduces the homogeneous polynomial

$$F(X, Y) = Y^n f(X/Y) = f_n X^n + f_{n-1} X^{n-1} Y + \cdots + f_0 Y^n,$$

then $\mathrm{Norm}_{K/\mathbb{Q}}(a - b\alpha) = \frac{1}{f_n} F(a, b)$.

Note: F is more than a computational hack. It means something.

Working in K

More generally, one may compute in number fields using polynomials in a generating element.

Trace, norm, etc of an element ζ correspond to trace, determinant of the multiplication-by-ζ matrix in any basis. We even have:

Definition: Characteristic polynomial of an algebraic number

The char. poly. of an algebraic number ζ is the char. poly. of the multiplication-by-ζ matrix in any basis.

Definition: Minimal polynomial of an algebraic number

The minimal polynomial of an algebraic number ζ is the min. poly. of the multiplication-by-ζ matrix in any basis.

Software

Software for working with number fields:

- Pari/gp (GPL). Most advanced. Interface is very bad.
- Sage. Includes pari, but lots of glue code missing.
- Magma. Includes a severely outdated version of pari. But interface is very complete. Good enough for our purposes.

Keep in mind: norm, resultant, Galois group

- The norm of any algebraic number can be computed.
- It is obviously a multiplicative thing.
- To compute it, the Resultant can be used.
- $\text{Norm}(a - b\alpha) = \frac{1}{f_n}\text{Res}(a - bx, f) = \frac{1}{f_n}F(a, b)$.
- The Galois group dwells somewhere around. It's often the full symmetric group. We don't have to bother much with it, except maybe know that it exists.
- All of this is readily available in computer software.

Plan

Number fields, algebraic numbers

Algebraic integers, ring of integers

Ideals

Factoring into prime ideals

Units and the class group

Goals

Goal here:

- Give a proper definition of the ring of integers of a number field.

Integrality

Definition: integral element

Let $A \subset B$ be two rings. "$x \in L$ is integral over A" means:

$$\exists P \in A[X], \quad P \text{ monic and } P(x) = 0.$$

Prop. $x \in L$ is integral over A iff $\exists M$ f.g. A-module with $xM \subset M$.

Def. Elements of B which are integral over A form the integral closure of A in B (which is an A-algebra).

Def. A ring is integrally closed if it is its own integral closure in its field of fractions.

Examples:
- $\mathbb{Z}$ is integrally closed.
- An integral closure is integrally closed.

Algebraic integers

In the number field case:

Definition: algebraic integer

Let K be a number field. An algebraic number $\zeta \in K$ is an algebraic integer iff it is integral over $\mathbb{Z}$.

Criterion: an algebraic number is integral iff its characteristic polynomial has coefficients in $\mathbb{Z}$.

Example

```
sage: K.<z>=NumberField(x^2+11)
sage: z.charpoly()
x^2 + 11
sage: ((z+1)/2).charpoly()
x^2 - x + 3
```

Sometimes, there are surprising algebraic integers!

Ring of integers

Definition: ring of integers

Def. Let $K/\mathbb{Q}$ be a number field. The ring of integers $\mathcal{O}_K$ of K is the integral closure of $\mathbb{Z}$ in K.

Prop. $\mathcal{O}_K$ is a finitely generated torsion-free $\mathbb{Z}$-module.

- Finitely generated: there is a basis over $\mathbb{Z}$.
- Torsion-free: there is no way to multiply something by an integer and get zero.

Ring of integers

Properties we expect and appreciate:

- all algebraic integers are in the ring of integers.
- the ring of integers is a ring.

$\mathcal{O}_K$ is the most reasonable $\mathbb{Z}$-like ring to work with within K.

Unfortunately, computing $\mathcal{O}_K$ is difficult.

Example

```
sage: K.<alpha>=NumberField(x^3+7)
sage: OK=K.ring_of_integers()
sage: OK.basis()
[1, alpha, alpha^2]
sage: K.<alpha>=NumberField(x^4 - 2*x^3 - 2*x^2 - 2*x + 1)
sage: OK=K.ring_of_integers()
sage: OK.basis()
[1/2*alpha^2 + 1/2, 1/2*alpha^3 + 1/2*alpha, alpha^2, alpha^3]
```

Examples of algebraic integers

Textbook case: $f \in \mathbb{Z}[x]$ monic and irreducible.

Let $K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/f$.

- Then α is an algebraic integer.
- So are all $a - b\alpha$ with $a, b \in \mathbb{Z}$,
- or $A(\alpha)$ with $A \in \mathbb{Z}[x]$. But $\mathcal{O}_K$ may be larger than $\mathbb{Z}[\alpha]$!

Real-life case: f not monic

Say $f = f_n x^n + \cdots$. Let $\hat{\alpha} = f_n \alpha$. We have:

$$\begin{aligned} 0 = f_n^{n-1} f(\alpha) &= f_n^n \alpha^n + f_n^{n-1} f_{n-1} \alpha^{n-1} + \cdots + f_n^{n-1} f_0, \\ &= \hat{\alpha}^n + f_{n-1} \hat{\alpha}^{n-1} + f_n f_{n-2} \hat{\alpha}^{n-2} + \cdots + f_n^{n-1} f_0. \end{aligned}$$

So $\hat{\alpha}$ is an algebraic integer. But $\mathcal{O}_K$ may be larger than $\mathbb{Z}[\hat{\alpha}]$!

Integral basis

We can always fabricate subrings of $\mathcal{O}_K$ of the form $\mathbb{Z}[\alpha]$.

But in general $\mathcal{O}_K$ needs not be of that form.

Which best form can we expect in full generality ?

- $\mathcal{O}_K$ can be written as: $\mathcal{O}_K = \mathbb{Z}\omega_1 + \cdots \mathbb{Z}\omega_n$,
- where ω_i are algebraic integers of the form $\frac{1}{d}A_i(\alpha)$ for some common denominator d (hard task: find the ω_i).
- $(\omega_i)_i$ is a $\mathbb{Q}$-basis of K.
- The matrix whose rows are coefficients of A_i may be put into Hermite normal form. Internally this is what is done in software.

Keep in mind

- The ring of integers $\mathcal{O}_K$ is cool.
- The minimal polynomials of its elements are in $\mathbb{Z}[x]$ and monic.
- $\mathcal{O}_K$ is a ring, with a basis.
- It is unfortunately rarely as simple as $\mathbb{Z}[\alpha]$.
- When we start from a non-monic definition polynomial, its root is not an algebraic integer, and $\mathbb{Z}[f_n\alpha]$ is typically much smaller than $\mathcal{O}_K$.

Further topic: orders

Orders (= certain types of subrings) in number fields are useful. These must be introduced in order to explain how to compute $\mathcal{O}_K$.

A picture

$$\begin{array}{ccc} K & & \\ \Big| & & \\ \mathbb{Q} & \supset & \mathbb{Z} \end{array}$$

We are chiefly interested in:

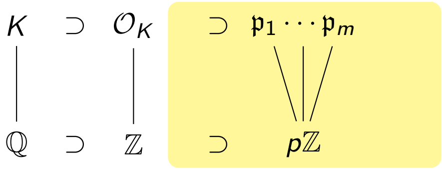
A picture

$$\begin{array}{ccc} K & \supset & \mathcal{O}_K \\ | & & | \;\text{integral closure} \\ \mathbb{Q} & \supset & \mathbb{Z} \end{array}$$

We are chiefly interested in:

- The ring of integers $\mathcal{O}_K$, as a first-class citizen in this big picture. Not necessarily that we must compute it.

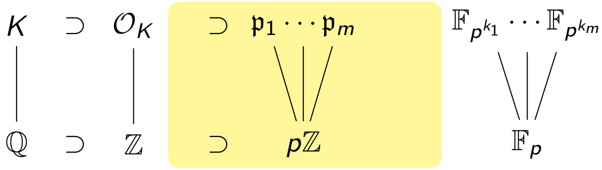
A picture



We are chiefly interested in:

- The ring of integers $\mathcal{O}_K$, as a first-class citizen in this big picture. Not necessarily that we must compute it.
- The decomposition (factorization) of prime (ideals) of $\mathbb{Z}$ in $\mathcal{O}_K$.

A picture



We are chiefly interested in:

- The ring of integers $\mathcal{O}_K$, as a first-class citizen in this big picture. Not necessarily that we must compute it.
- The decomposition (factorization) of prime (ideals) of $\mathbb{Z}$ in $\mathcal{O}_K$, and the residue fields.

A picture

$$\begin{array}{ccccccc} K & \supset & \mathcal{O}_K & \supset & \mathcal{O}_K^*, \text{ the unit group} \\ | & & | & & | \\ \mathbb{Q} & \supset & \mathbb{Z} & \supset & \{\pm 1\} \end{array}$$

We are chiefly interested in:

- The ring of integers $\mathcal{O}_K$, as a first-class citizen in this big picture. Not necessarily that we must compute it.
- The decomposition (factorization) of prime (ideals) of $\mathbb{Z}$ in $\mathcal{O}_K$, and the residue fields.
- Other multiplicative structure, e.g. units.

Plan

Number fields, algebraic numbers

Algebraic integers, ring of integers

Ideals

Factoring into prime ideals

Units and the class group

Goals

Our goals here:

- define ideals, operations on ideals, and some vocabulary.
- give a few examples.
- show how it can work algorithmically.

Primes ?

The ring of integers is nice, but lacks one thing: unique factorization.

Example: in $\mathbb{Q}(\sqrt{-5})$, one has $6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, and all "look prime".

However, $\mathcal{O}_K$-ideals do enjoy unique factorization.

Here

$$6\mathcal{O}_K = \left\langle 2, 1+\sqrt{-5} \right\rangle^2 \times \left\langle 3, 1+\sqrt{-5} \right\rangle \times \left\langle 3, 1-\sqrt{-5} \right\rangle,$$

$$\left\langle 1+\sqrt{-5} \right\rangle = \left\langle 2, 1+\sqrt{-5} \right\rangle \times \left\langle 3, 1+\sqrt{-5} \right\rangle,$$

$$\left\langle 1-\sqrt{-5} \right\rangle = \left\langle 2, 1+\sqrt{-5} \right\rangle \times \left\langle 3, 1-\sqrt{-5} \right\rangle.$$

Ideals in $\mathcal{O}_K$

Ideals are very important objects in number fields.

Definition

An ideal I of $\mathcal{O}_K$ is such that:

- I forms an additive group.
- I is stable under multiplication by elements of $\mathcal{O}_K$.

An ideal may be specified by giving a set of generators.

Notation

All sets below are $\mathcal{O}_K$-ideals by construction.

$$\langle x \rangle = x\mathcal{O}_K = \{xa,\ a \in \mathcal{O}_K\}.$$
$$\langle x, y \rangle = \{xa + yb,\ a, b \in \mathcal{O}_K\}.$$
$$\langle x_1, \ldots, x_k \rangle = \{\sum_i x_i a_i,\ a_i \in \mathcal{O}_K\}.$$

Ideals

We can add ideals:

$$I + J = \{\text{ideal generated by sums of elements of } I \text{ and } J\}.$$

We can multiply ideals:

$$I \times J = \{\text{ideal generated by products of elements of } I \text{ and } J\}.$$

We can intersect ideals: $I \cap J =$ set-wise intersection, really!

Note that since an ideal is made of elements of $\mathcal{O}_K$, we have:

- $I \times J \subset I \times \mathcal{O}_K = I$: «to contain is to divide».
- $I \cap J$ really works as the lcm of ideals.
- $I + J$ contains I and J: this is a gcd.
  Ideals such that $I + J = \mathcal{O}_K$ are coprime.
  E.g. two ideals that contain coprime integers are coprime.

Ideals

Definition: prime ideals

An ideal I is prime if $ab \in I$ implies $a \in I$ or $b \in I$.
Fact: if I is prime, then $\mathcal{O}_K/I$ is an integral domain.

Definition: maximal ideals

An ideal I is maximal if it is maximal for inclusion (nobody between I and $\mathcal{O}_K$).
Fact: if I is prime, then $\mathcal{O}_K/I$ is a field.

Fact: in a number field, all prime ideals are maximal. So these two concepts are identical as far as we are concerned.

Fractional ideals

Ideals in $\mathcal{O}_K$ form a multiplicative semigroup. Extension desired !

Def $I \subset K$ is a fractional ideal (of $\mathcal{O}$), or a (fractional) $\mathcal{O}$-ideal iff I is a non-zero $\mathcal{O}$-module and $\exists a \in \mathcal{O},\ aI \subset \mathcal{O}$.

Terminology:
- Integral ideal: ideal of $\mathcal{O}$.
- Fractional ideal: more general.

Informally: fractional ideal = ideal with denominator.

Definition of ideal division

$$I^{-1} = \{a \in K, aI \subset \mathcal{O}_K\}.$$

Fractional ideals

Fantastic properties of $\mathcal{O}_K$

$\mathcal{O}_K$ is a Dedekind domain (integrally closed, Noetherian, all prime ideals maximal).
This implies that the fractional $\mathcal{O}_K$-ideals form a group with unique factorization.

Representing ideals

Note: $\mathcal{O}_K$ is not in general a principal ideal domain.

- Ideals can be represented by a set of generators.
  Two are always enough.
- Fractional ideals: integer denominator, + generators.
- Principal ideals: one generator is possible, but often not worthwhile (or too large)

Algorithmically, it is sometimes useful to represent ideals more generally as $\mathbb{Z}$-modules within K, with generators in HNF form.

(HNF = Hermite Normal Form = like Gauss, but on integer matrices)

Example

```
sage: K.<alpha>=NumberField(x^3+7)
sage: OK=K.ring_of_integers()
sage: [K(c) for c in OK.basis()]
[1, alpha, alpha^2]
sage: OK.ideal(11).factor()
(Fractional ideal (11, alpha^2 + 5*alpha + 3))
 * (Fractional ideal (11, alpha - 5))
sage: I11a=OK.ideal(11).factor()[0][0]
sage: I11b=OK.ideal(11).factor()[1][0]
sage: I11a.basis()
[11, 11*alpha, alpha^2 + 5*alpha + 3]
sage: I11b.basis()
[11, alpha + 6, alpha^2 + 8]
sage: OK.ideal(29).factor()
(Fractional ideal (-2*alpha^2 + 3*alpha + 10))
 * (Fractional ideal (-alpha^2 + 2*alpha - 2))
```

HNF means algorithms

```
sage: L=[u*v for u in I11a.basis() for v in I11b.basis()]
sage: L
[121,
 11*alpha + 66,
 11*alpha^2 + 88,
 121*alpha,
 11*alpha^2 + 66*alpha,
 88*alpha - 77,
 11*alpha^2 + 55*alpha + 33,
 11*alpha^2 + 33*alpha + 11,
 11*alpha^2 + 33*alpha - 11]
sage: m=matrix(ZZ,[uv.vector() for uv in L])
sage: m1=m.hermite_form(include_zero_rows=False)
sage: m1
[11  0  0]
[ 0 11  0]
[ 0  0 11]
sage: ideal([OK(v) for v in m1.rows()])
Fractional ideal (11)
```

Plan

Number fields, algebraic numbers

Algebraic integers, ring of integers

Ideals

Factoring into prime ideals

Units and the class group

Ideals above ideals

For I an $\mathcal{O}_K$-ideal, $I \cap \mathbb{Z}$ is a $\mathbb{Z}$-ideal.
$I \cap \mathbb{Z} = p\mathbb{Z} \Leftrightarrow$ "I lies above p".

What are the prime ideals that lie above p.

Surely, $\langle p \rangle = p\mathcal{O}_K$ is one such ideal, but are there ideals that contain (divide) $\langle p \rangle = p\mathcal{O}_K$?

Obvious mathematical breakthrough

We are attempting to factor the prime number p in the number field K.

Number fields must be Bill Gates' delight!

> *The obvious mathematical breakthrough would be development of an easy way to factor large prime numbers.*

Norm of ideals

The quotient ring $\mathcal{O}_K/I$ is always finite.

- Norm $I \stackrel{\text{def}}{=} \#(\mathcal{O}_K/I)$. If K is Galois, $\prod_\sigma I^\sigma = \langle \text{Norm}\, I \rangle$.
- If I is principal, $\text{Norm}\, \langle \gamma \rangle = |\text{Norm}\, \gamma|$.
  (beware: this is only for (fractional) $\mathcal{O}_K$-ideals).
- The norm is multiplicative: $\text{Norm}\, IJ = \text{Norm}\, I \cdot \text{Norm}\, J$.

For example, in a number field of degree n, the norm of $\langle p \rangle$ is p^n.
We look for the largest ideals that contain (divide) $\langle p \rangle$.

- Their norm has to be a p-th power.
- There are generally several such prime ideals above p.

Prime ideals

Important case when I is maximal (same as prime, for us):

- then $\mathcal{O}_K/I$ is a field.
- If I lies above p, then $\mathcal{O}_K/I$ is an extension of $\mathbb{F}_p = \mathbb{Z}/(\mathbb{Z} \cap I)$.
- The degree $[\mathcal{O}_K/I : \mathbb{Z}/(\mathbb{Z} \cap I)]$ is called the residue class degree or inertia degree of I.
- The inertia degree is commonly denoted f, but we also have f lying around...

Factorization of $p\mathcal{O}_K$

Guiding principle

Try to «read» the factorization of $\langle p \rangle$ from that of f mod p.

Caveat: This does not always work!

Condition (Dedekind criterion):

- if we have defined orders and indices of orders: p coprime to $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ (IOW, $\mathbb{Z}[\alpha]$ is p-maximal). In particular, if $\nu_p(\operatorname{disc} f) \leq 1$, then our condition is satisfied.
- if not, the only thing we can do is to write sufficient conditions that guarantee that we are in the easy case.

Sufficient conditions for the Dedekind crit.

In we are in any of the following situations:

- $\mathcal{O}_K = \mathbb{Z}[\alpha]$
- or $p \nmid f_n \operatorname{disc} f$ "coarse Dedekind criterion"
- or, informally, if $\mathcal{O}_K$ is not very different from $\mathbb{Z}[\alpha]$, as far as p is concerned

then the Dedekind criterion holds and we are in the easy case: the factorization of $\langle p \rangle$ is directly linked to that of $f \bmod p$.

Factorization of $\langle p \rangle = p\mathcal{O}_K$

Nice situation, when $\mathbb{Z}[\alpha]$ is p-maximal.

- Factors of $p\mathcal{O}_K$ correspond to factors of f mod p.
- Inertia degrees are degrees of irreducible factors.
- Ideal multiplicities are multiplicities of irr. factors.

Example. Let $K = \mathbb{Q}(\alpha)$ with $\alpha^3 = 2$.

- $\langle 2 \rangle = \mathfrak{a}_2^3$, with $\mathfrak{a}_2 = \langle 2, \alpha \rangle$. $\mathcal{O}_K/2\mathcal{O}_K \cong (\mathbb{F}_2)^3$.
- $\langle 3 \rangle = \mathfrak{a}_3^3$, with $\mathfrak{a}_3 = \langle 3, \alpha + 1 \rangle$. $\mathcal{O}_K/3\mathcal{O}_K \cong (\mathbb{F}_3)^3$.
- $X^3 - 2 \equiv (X+2)(X^2+3X-1) \mod 5$, thus $\langle 5 \rangle = \mathfrak{a}_5\mathfrak{b}_5$, with $\mathfrak{a}_5 = \langle 5, \alpha + 2 \rangle$ and $\mathfrak{b}_5 = \langle 5, \alpha^2 + 3\alpha - 1 \rangle$. $\mathcal{O}_K/5\mathcal{O}_K \cong \mathbb{F}_5 \times \mathbb{F}_{5^2}$.

More taxonomy

Definitions

- p is inert in K if $\langle p \rangle$ is a prime ideal (hence $\mathcal{O}_K/p\mathcal{O}_K \equiv \mathbb{F}_{p^d}$).
- p ramifies in K if $\langle p \rangle$ has a repeated factor ($\Rightarrow p \mid \operatorname{disc} K$).
- p splits completely in K if $\langle p \rangle$ factorizes only into prime ideals of inertia degree 1.

Prime ideals of $\mathcal{O}_K$ also inherit this terminology: inert, ramified.

Unramified ideals have multiplicity 1 in the factorization of $(I \cap \mathbb{Z})\mathcal{O}_K$.

Examples on previous slide: $\mathfrak{a}_2, \mathfrak{a}_3$ ramified. $\mathfrak{a}_5, \mathfrak{b}_5$ unramified.

Important, for f defining a p-maximal $\mathbb{Z}[\alpha]$:

- p ramifies iff f has a repeated factor (i.e. $p \mid \operatorname{disc} f$).
- Also holds more generally: p ramifies iff $p \mid \operatorname{disc} K$.

Factoring ideals into prime ideals

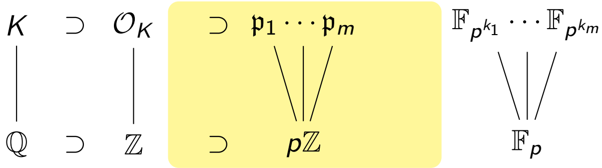
Given a (possibly fractional) $\mathcal{O}_K$-ideal I, how do we factor it into prime ideals?

$$I = I_1 \cdot I_2 \cdot \cdots \cdot I_k.$$

This is a two-step process:

- Factor Norm I.
- For each p^k that appears in the factorization, find which of the prime ideals above p have a non-zero valuation at I.
- If I is fractional, one simple way to go is to factor the integral ideal dI first, and then divide by the prime ideals that divide $d\mathcal{O}_K$.

Prime ideals above primes



Breathe

Things to keep in mind:

Ideals, in general, are things that we can deal with:

- they have bases (as $\mathbb{Z}$-modules) or generators (as $\mathcal{O}_K$ modules).
- operations: $+$, $\times$ (also: $\cap$).
- we can do operations on ideals using linear algebra.

Prime numbers in $\mathbb{Z}$ factor into prime ideals in $\mathcal{O}_K$.

Prime ideals in $\mathcal{O}_K$:

- are always above some rational prime p in $\mathbb{Z}$.
- lead to finite fields of the form $\mathcal{O}_K/I$ (finite field extending $\mathbb{F}_p$).

Easy ideals

Some ideals are very easy to work with.
When I is unramified and has residue class degree 1, then $I = (p, \alpha - r)$ for some $r \in \mathbb{F}_p$. This corresponds to the field isomorphism:

$$\begin{cases} \mathcal{O}_K/I & \to & \mathbb{F}_p, \\ \alpha & \mapsto & r \end{cases}$$

Note: these ideals are the most common ones!

- There are only finitely many prime ideals whose norm is not coprime to disc K.
- Among the unramified prime ideals, those of residue class degree > 1 are less frequent.

Factorization of $\langle a - b\alpha \rangle = (a - b\alpha)\mathcal{O}_K$

Important case for NFS: factorization of $I = \langle a - b\alpha \rangle$.

It's actually easy to find the easy prime ideals that divide I.

See next lecture.

Further topics

Non-easy ideals

While non-easy ideals are exceedingly rare in the NFS context, there are a few situations where we want to deal with the mildly complicated process of finding their valuations in factorizations. This is covered in books (e.g. Cohen). I probably won't cover it.

Distribution of prime factoring patterns

When factoring $\langle p \rangle$, factoring patterns are not random at all. They are prescribed by a very important theorem called Chebotarev's density theorem, which ties these patterns to the Galois group.
Again, I probably won't cover it.

Plan

Number fields, algebraic numbers

Algebraic integers, ring of integers

Ideals

Factoring into prime ideals

Units and the class group

Units

Which elements of $\mathcal{O}_K$ are invertible ?

Theorem

An algebraic integer $x \in \mathcal{O}_K$ is invertible iff $\mathrm{Norm}_{K/\mathbb{Q}}(x) = \pm 1$.

Caveat: $x \in K$ with Norm $= 1$ has no reason to be a unit in $\mathcal{O}_K$.

As an abelian group, U_K has:

- A (finite!) torsion subgroup U_{tors} (roots of unity) ;
- a rank, so that $U_K \cong U_{\mathrm{tors}} \times \mathbb{Z}^{\mathrm{rank}}$.

Units

Finding torsion units is essentially trivial.

Finding the rank of the torsion-free part is also trivial (Dirichlet Unit Theorem).

It is very difficult to find the generators of the torsion-free part.

The class group

Principal ideals form a subgroup of the group of (fractional) ideals.

Class group, class number

The quotient $I(\mathcal{O}_K)/K^\times$ is called the class group $\mathrm{Cl}(\mathcal{O}_K)$.
Its order is called the class number of $\mathcal{O}_K$, often denoted h.

Fact: the class group is a finite abelian group.

Various consequences of the definition:

- An ideal is principal iff it maps to zero in the class group.
- If $h = 1$ (the class group is trivial) then any ideal is principal.
- If the exponent of the class group is λ, then for any ideal, I^λ is principal.

Computing the class group

Computing the class number (and structure of $\mathrm{Cl}(\mathcal{O}_K)$) is hard.

It is linked to the computation of a system of generators for units.

The number field sieve does in fact include the statement of a method for tackling the problem.

Generally, the complexity for computing h is subexponential.

Further topics

There is a lot more to say about the unit group and the class group (which are intimately related).