Algebraic number theory

Algebraic number theory is a major branch of number theory which studies algebraic structures related to algebraic integers. This is generally accomplished by considering a ring of algebraic integers $\mathcal{O}$ in an algebraic number field $K/\mathbb{Q}$, and studying their algebraic properties such as factorization, the behaviour of ideals, and field extensions. In this setting, the familiar features of the integers—such as unique factorization—need not hold. The virtue of the primary machinery employed—Galois theory, group cohomology, group representations, and $L$-functions—is that it allows one to deal with new phenomena and yet partially recover the behaviour of the usual integers.

## Contents

- 1 Basic notions
  - 1.1 Unique factorization and the ideal class group
  - 1.2 Factoring prime ideals in extensions
  - 1.3 Primes and places
  - 1.4 Units
  - 1.5 Local fields
- 2 Major results
  - 2.1 Finiteness of the class group
  - 2.2 Dirichlet's unit theorem
  - 2.3 Artin reciprocity
  - 2.4 Class number formula
- 3 Notes
- 4 References
  - 4.1 Introductory texts
  - 4.2 Intermediate texts
  - 4.3 Graduate level accounts
  - 4.4 Specific references
- 5 See also

## Basic notions

### Unique factorization and the ideal class group

One of the first properties of $\mathbb{Z}$ that can fail in the ring of integers $\mathcal{O}$ of an algebraic number field $K$ is that of the unique factorization of integers into prime numbers. The prime numbers in $\mathbb{Z}$ are generalized to irreducible elements in $\mathcal{O}$, and though the unique factorization of elements of $\mathcal{O}$ into irreducible elements may hold in some cases (such as for the Gaussian integers $\mathbb{Z}[i]$), it may also fail, as in the case of $\mathbb{Z}[\sqrt{-5}]$ where

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

The ideal class group of $\mathcal{O}$ is a measure of how much unique factorization of elements fails; in particular, the ideal class group is trivial if, and only if, $\mathcal{O}$ is a unique factorization domain.
Factoring prime ideals in extensions

Unique factorization can be partially recovered for $O$ in that it has the property of unique factorization of ideals into prime ideals (i.e. it is a Dedekind domain). This makes the study of the prime ideals in $O$ particularly important. This is another area where things change from $\mathbb{Z}$ to $O$: the prime numbers, which generate prime ideals of $\mathbb{Z}$ (in fact, every single prime ideal of $\mathbb{Z}$ is of the form $(p) = p\mathbb{Z}$ for some prime number $p$,) may no longer generate prime ideals in $O$. For example, in the ring of Gaussian integers, the ideal $2\mathbb{Z}[i]$ is no longer a prime ideal; in fact

$$2\mathbb{Z}[i] = ((1 + i)\mathbb{Z}[i])^2.$$

On the other hand, the ideal $3\mathbb{Z}[i]$ is a prime ideal. The complete answer for the Gaussian integers is obtained by using a theorem of Fermat's, with the result being that for an odd prime number $p$

- $p\mathbb{Z}[i]$ is a prime ideal if $p \equiv 3 \pmod{4}$
- $p\mathbb{Z}[i]$ is not a prime ideal if $p \equiv 1 \pmod{4}$.

Generalizing this simple result to more general rings of integers is a basic problem in algebraic number theory. Class field theory accomplishes this goal when $K$ is an abelian extension of $\mathbb{Q}$ (i.e. a Galois extension with abelian Galois group).

Primes and places

An important generalization of the notion of prime ideal in $O$ is obtained by passing from the so-called \textit{ideal-theoretic} approach to the so-called \textit{valuation-theoretic} approach. The relation between the two approaches arises as follows. In addition to the usual absolute value function $|\cdot| : \mathbb{Q} \to \mathbb{R}$, there are absolute value functions $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ defined for each prime number $p$ in $\mathbb{Z}$, called $p$-adic absolute values. Ostrowski's theorem states that these are all possible absolute value functions on $\mathbb{Q}$ (up to equivalence). This suggests that the usual absolute value could be considered as another prime. More generally, a \textbf{prime of an algebraic number field} $K$ (also called a \textbf{place}) is an equivalence class of absolute values on $K$. The primes in $K$ are of two sorts: $\mathcal{P}$-adic absolute values like $|\cdot|_p$, one for each prime ideal $\mathcal{P}$ of $O$, and absolute values like $|\cdot|$ obtained by considering $K$ as a subset of the complex numbers in various possible ways and using the absolute value $|\cdot| : \mathbb{C} \to \mathbb{R}$. A prime of the first kind is called a \textbf{finite prime} (or \textbf{finite place}) and one of the second kind is called an \textbf{infinite prime} (or \textbf{infinite place}). Thus, the set of primes of $\mathbb{Q}$ is generally denoted \{ 2, 3, 5, 7, ..., $\infty$ \}, and the usual absolute value on $\mathbb{Q}$ is often denoted $|\cdot|_\infty$ in this context.

The set of infinite primes of $K$ can be described explicitly in terms of the embeddings $K \to \mathbb{C}$ (i.e. the non-zero ring homomorphisms from $K$ to $\mathbb{C}$). Specifically, the set of embeddings can be split up into two disjoint subsets, those whose image is contained in $\mathbb{R}$, and the rest. To each embedding $\sigma : K \to \mathbb{R}$, there corresponds a unique prime of $K$ coming from the absolute value obtained by composing $\sigma$ with the usual absolute value on $\mathbb{R}$; a prime arising in this fashion is called a \textbf{real prime} (or \textbf{real place}). To an embedding $\tau : K \to \mathbb{C}$ whose image is \textit{not} contained in $\mathbb{R}$, one can construct a distinct embedding $\bar{\tau}$, called the \textbf{conjugate embedding}, by composing $\tau$ with the complex conjugation map $\mathbb{C} \to \mathbb{C}$. Given such a pair of embeddings $\tau$ and $\bar{\tau}$, there corresponds a unique prime of $K$ again obtained by composing $\tau$ with the usual absolute value (composing $\bar{\tau}$ instead gives the same absolute value function since $|\bar{z}| = |z|$ for any complex number $z$, where $\bar{z}$ denotes the complex conjugate of $z$). Such a prime is called a \textbf{complex prime} (or \textbf{complex place}). The description of the set of infinite primes is then as follows: each infinite prime corresponds either to a unique embedding $\sigma : K \to \mathbb{R}$, or a pair of conjugate embeddings $\tau$, $\bar{\tau} : K \to \mathbb{C}$.
The number of real (respectively, complex) primes is often denoted \( r_1 \) (respectively, \( r_2 \)). Then, the total number of embeddings \( K \hookrightarrow \mathbb{C} \) is \( r_1 + 2r_2 \) (which, in fact, equals the degree of the extension \( K/\mathbb{Q} \)).

**Units**

The fundamental theorem of arithmetic describes the multiplicative structure of \( \mathbb{Z} \). It states that every non-zero integer can be written (essentially) uniquely as a product of prime powers and \( \pm 1 \). The unique factorization of ideals in the ring \( O \) recovers part of this description, but fails to address the factor \( \pm 1 \).

The integers 1 and -1 are the invertible elements (i.e. units) of \( \mathbb{Z} \). More generally, the invertible elements in \( O \) form a group under multiplication called the **unit group** of \( O \), denoted \( O^\times \). This group can be much larger than the cyclic group of order 2 formed by the units of \( \mathbb{Z} \). Dirichlet's unit theorem describes the abstract structure of the unit group as an abelian group. A more precise statement giving the structure of \( O^\times \otimes \mathbb{Z} \) as a Galois module for the Galois group of \( K/\mathbb{Q} \) is also possible.\(^{[1]}\) The size of the unit group, and its lattice structure give important numerical information about \( O \), as can be seen in the class number formula.

**Local fields**

*Main article: Local field*

Completing a number field \( K \) at a place \( w \) gives a complete field. If the valuation is archimedean, one gets \( \mathbb{R} \) or \( \mathbb{C} \), if it is non-archimedean and lies over a prime \( p \) of the rationals, one gets a finite extension \( K_w/\mathbb{Q}_p \), a complete, discrete valued field with finite residue field. This process simplifies the arithmetic of the field and allows the local study of problems. For example the Kronecker–Weber theorem can be deduced easily from the analogous local statement. The philosophy behind the study of local fields is largely motivated by geometric methods. In algebraic geometry, it is common to study varieties locally at a point by localizing to a maximal ideal. Global information can then be recovered by gluing together local data. This spirit is adopted in algebraic number theory. Given a prime in the ring of algebraic integers in a number field, it is desirable to study the field locally at that prime. Therefore one localizes the ring of algebraic integers to that prime and then completes the fraction field much in the spirit of geometry.

**Major results**

**Finiteness of the class group**

One of the classical results in algebraic number theory is that the ideal class group of an algebraic number field \( K \) is finite. The order of the class group is called the class number, and is often denoted by the letter \( h \).

**Dirichlet's unit theorem**

*Main article: Dirichlet's unit theorem*

Dirichlet's unit theorem provides a description of the structure of the multiplicative group of units \( O^\times \) of the ring of integers \( O \). Specifically, it states that \( O^\times \) is isomorphic to \( G \times \mathbb{Z}^r \), where \( G \) is the finite cyclic group consisting of all the roots of unity in \( O \), and \( r = r_1 + r_2 - 1 \) (where \( r_1 \) (respectively, \( r_2 \)) denotes the
set of real embeddings (respectively, pairs of conjugate non-real embeddings) of \( K \). In other words, \( O^\times \)
is a finitely generated abelian group of rank \( r_1 + r_2 - 1 \) whose torsion consists of the roots of unity in \( O \).

### Artin reciprocity

*Main article: Artin reciprocity law*

See also

- Quadratic reciprocity
- Cubic reciprocity
- Quartic reciprocity

### Class number formula

*Main article: Class number formula*

### Notes

1. ^ See proposition VIII.8.6.11 of Neukirch, Schmidt & Wingberg 2000

### References

#### Introductory texts


#### Intermediate texts

- Daniel A. Marcus, "Number Fields"

#### Graduate level accounts


#### Specific references

- Neukirch, Jürgen; Schmidt, Alexander; Wingberg, Kay (2000), *Cohomology of Number Fields*,
See also

- Arithmétique modulaire A survey of number theory, with applications (in French Wikipedia)
- Langlands program
- Adele ring
- Tamagawa number
- Iwasawa theory
- Arithmetic algebraic geometry

Retrieved from "http://en.wikipedia.org/wiki/Algebraic_number_theory"
Categories: Algebraic number theory