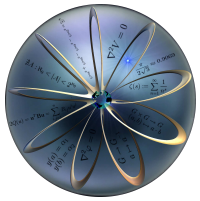

planetmath.org

Math for the people, by the people.

algebraic number theory

Canonical name	AlgebraicNumberTheory
Date of creation	2013-03-22 15:08:05
Last modified on	2013-03-22 15:08:05
Owner	alozano (2414)
Last modified by	alozano (2414)
Numerical id	34
Author	alozano (2414)
Entry type	Topic
Classification	msc 11S99
Classification	msc 11R99
Classification	msc 11-01
Related topic	NormAndTraceOfAlgebraicNumber
Related topic	ModularForms
Related topic	HeckeOperator
Related topic	BibliographyForNumberTheory
Related topic	ArithmeticOfEllipticCurves
Related topic	ClassNumbersAndDiscriminantsTopicsOnClassGroups
Related topic	ExamplesOfRingOfIntegersOfANumberField
Related topic	NumberField
Related topic	TheoryOfAlgebraicNumbers
Related topic	TheoryOfRa

Algebraic Number Theory

This entry is a of to entries on algebraic number theory in Planetmath (therefore to be always **under construction**). It is the hope of the author(s) that someday this can be used as a "graduate text" to learn the subject by reading the individual entries listed here. Each a brief description of the concepts, which is expanded in the entries. Some of the concepts might be missing in Planetmath as of today (please consider writing an entry on them!). In to organize the entry in sections, we followed the main reference [**?**].

1 Introduction

The entry number theory contains a nice introduction to the broad subject. From very early on, mathematicians have tried to understand the integer solutions of polynomial equations (e.g. Pythagorean triples). One of the main motivational examples for the subject is Fermat's Last Theorem (when does $x^n + y^n = z^n$ have integer solutions?). The study of integer solutions immediately leads to the study of algebraic numbers (see `http://planetmath.org/Y2X32`$y^2 = x^3 - 2$ for an example). Algebraic number theory is the study of algebraic numbers, their properties and their applications.

- As an introduction, the reader should be comfortable with the basic theory of rational and irrational numbers, and its complementary entry, the basic theory of algebraic and transcendental numbers.

2 Number Fields and Rings of Integers

1. The main object of study in algebraic number theory is the number field. A number field K is a finite field extension of $\mathbb{Q}$. Since a finite extension of fields is an algebraic extension, $K/\mathbb{Q}$ is algebraic. Thus, every $\alpha \in K$ is an `http://planetmath.org/AlgebraicNumber`algebraic number.

2. The ring of integers of K, usually denoted by $\mathcal{O}_K$, is the set of all algebraic integers of K. $\mathcal{O}_K$ is a commutative ring with `http://planetmath.org/Unity`identity. See examples of ring of integers of a number field.

3. Real and complex embeddings of a number field. Read also about totally real and imaginary fields.

4. Norm and trace of an algebraic number. See also http://planetmath.org/NormAndTraceOfA entry. One also can take the norm of an ideal.

5. The discriminant of a number field measures the ramification of the field (read the following section for more details on ramification).

6. http://planetmath.org/RingOfIntegersOfANumberFieldIsFinitelyGeneratedOverMath ring of integers of a number field is finitely generated over $\mathbb{Z}$.

7. Euclidean number fields.

3 Decomposition of Prime Ideals

1. It is a well-known fact that the ring of integers of a number field is a Dedekind domain.

2. Every non-zero fractional ideal in a Dedekind domain is invertible. In fact, the set of all non-zero fractional ideals forms a group under multiplication (see also Prüfer ring and multiplication ring).

3. Notice that the ring of integers $\mathcal{O}_K$ of a number field is not necessarily a PID nor a UFD (see example of ring which is not a UFD). However, every fractional ideal in a Dedekind domain factors uniquely as a product of powers of prime ideals. In particular, the ideals of $\mathcal{O}_K$ factor uniquely as a product of prime ideals.

4. Let F/K be an extension of number fields. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, then $\mathfrak{p}\mathcal{O}_F$ is an ideal of F. What is the factorization of $\mathfrak{p}\mathcal{O}_F$ into prime ideals of F? Read about splitting and ramification in number fields and Galois extensions for a detailed explanation and definitions of the terminology.

5. In to understand ramification in a more general setting, read http://planetmath.org/Ramif inertia group and decomposition group.

6. See the entry ramification of archimedean places for the case of infinite places.

7. An important example: http://planetmath.org/PrimeIdealDecompositionInQuadraticE ideal decomposition in quadratic extensions of $\mathbb{Q}$.

8. Another important case: http://planetmath.org/PrimeIdealDecompositionInCyclotomi ideal decomposition in cyclotomic extensions of $\mathbb{Q}$.

9. Explicit examples of prime ideal decomposition in number fields.

10. More generally, read calculating the splitting of primes.

4 Ideal Class Groups

The ideal class group $\mathrm{Cl}(K)$ of a number field K is the quotient group of all fractional ideals modulo principal fractional ideals. In some sense, it measures the arithmetic complexity of the number field (how far K is from being a PID). The class number of K, denoted by h_K, is the of $\mathrm{Cl}(K)$. See topics on ideal class groups and discriminants for a detailed exposition.

5 The Unit Group

The unit group of a number field K is the group of units of the ring of integers $\mathcal{O}_K$, and it is usually denoted by $\mathcal{O}_K^\times$.

1. The structure of the unit group is described by Dirichlet's unit theorem, which asserts the existence of a system of fundamental units.

2. An application of Dirichlet's unit theorem: units of quadratic fields.

3. The regulator is an important invariant of the unit group (it appears in the http://planetmath.org/ClassNumberFormulaclass number formula).

4. The cyclotomic units are a subgroup of the group of units of a cyclotomic field with very interesting properties. The cyclotomic units are algebraic units.

6 Zeta Functions and L-functions

1. The prototype of zeta function is $\zeta(s)$, the `http://planetmath.org/RiemannZetaFunctionR` zeta function (the entry also discusses the famous Riemann hypothesis).

2. More generally, for every number field K one can define a Dedekind zeta function $\zeta_K(s)$.

3. The Dedekind zeta function of a number field satisfies the so-called class number formula, which relates many of the invariants of the number field.

7 Class Field Theory

Class field theory studies the abelian extensions of number fields.

1. The Kronecker-Weber theorem classifies the possible abelian extensions of $\mathbb{Q}$.

2. The abelian extensions of quadratic imaginary number fields can be described using elliptic curves with complex multiplication.

3. The Artin map is an important tool in class field theory. Class field theory and the Artin map can be presented in of `http://planetmath.org/Idele`idèles and `http://planetmath.org/Adele`adèles.

4. The Hilbert class field H of a number field K is the maximal unramified abelian extension of K. The key property of H is that the Galois group $\mathrm{Gal}(H/K)$ is isomorphic to the ideal class group $\mathrm{Cl}(K)$.

5. Ray class fields are maximal abelian extensions with conductor. See also ray class groups.

8 Local Fields

Many problems in number theory can be treated "locally" or one prime at a . For this, one works over local fields, like $\mathbb{Q}_p$ or the completion of a number field at a prime $\mathfrak{P}$.

1. Definition of http://planetmath.org/LocalFieldlocal field.

2. The main example and motivation: the http://planetmath.org/PAdicIntegers$p$-adic rationals and the p-adic integers (see also http://planetmath.org/PAdicValuation$p$-adic valuation).

3. Let v be a valuation of the field K (see the entry http://planetmath.org/Valuationvaluatio for a comprehensive introduction). The http://planetmath.org/Completioncompletion of K with respect to v is a local field. For example, $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the http://planetmath.org/PAdicValuation$p$-adic valuation.

4. Read also about discrete valuation rings.

5. Hensel's lemma provides a criterion to prove the existence of roots of polynomials in local fields. See also examples for Hensel's lemma.

9 Galois Representations

1. Recall that a number field is a finite extension of $\mathbb{Q}$. We can also study infinite extensions. Read about infinite Galois theory.

2. Some number theorists would say that algebraic number theory is the study of the absolute Galois group of $\mathbb{Q}$, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

3. In order to understand $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, one studies Galois representations (the entry is an excellent overview and introduction to Galois representation theory).

10 Elliptic Curves

Elliptic curves are, essentially, equations of the form $y^2 = x^3 + Ax + B$. Read the entry on the arithmetic of elliptic curves for a full account of this beautiful theory.

11 Modular Forms

1. Definition of modular form and the Hecke algebra of Hecke operators.

References

[Mar] Daniel A. Marcus, *Number Fields*, Springer, New York.

Note: If you would like to contribute to this entry, please send an email to the author (alozano).