Mathematics 80220 – Algebraic Number Theory

Spring 2018

Course information

- Instructor: Andrei Jorza, 275 Hurley Hall, `ajorza@nd.edu`
- When: 10:30 – 11:20 MWF

Course description Modern number theory lies at the interplay between algebra, geometry, representation theory, and analysis (and even computer science) and the interactions among these fields led to numerous advances in the last half century. This course is an introduction to algebraic (and a little analytic) number theory: we will study the main objects (number fields and their rings of integers), their properties from a classical perspective, and their connections to algebra, geometry and analysis, while at the same time interact computationally with the main theorems of algebraic number theory in SAGE.

The big picture In a first algebra course you have likely learned about principal ideal domains and the fact in PIDs each element can be factored more or less uniquely into primes. Algebraic number theory is concerned with more general rings of integers in which this property is no longer true. For example in $\mathbb{Z}[\sqrt{-5}]$ one can factor 6 into irreducibles in two ways: $6 = 2 \cdot 3$ or $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Nevertheless, Dedekind proved that in such rings of integers (or, more generally, in Dedekind domains) one can still factor *ideals* uniquely into prime ideals. In the example above this would be $6 = (2, 1 + \sqrt{5}) \cdot (2, 1 - \sqrt{5}) \cdot (3, 1 + \sqrt{5}) \cdot (3, 1 - \sqrt{5})$. In the new language of (fractional) ideals the classical theory over PIDs carries over with a number of changes.

One of the most important changes is the failure of ideals to be generated by a single element. The degree to which ideals fail to be principal is quantified by the *class group*, a finite abelian groups whose order, called the class number, appears crucially in Kummer's proof of special cases of Fermat's Last Theorem. Minkowski's geometry of numbers is an elementary approach to studying lattice points in space which can be used to understand units in rings of integers as well as to find a bound on the class number.

For a finer analysis of ideals in rings of integers one needs to turn to analytic methods. Dirichlet L-functions are generalizations of the Riemann zeta function, whose analytic properties capture an enormous amount of arithmetic properties. For example, a consequence of the meromorphicity of such L-functions is Dirichlet's theorem on primes in arithmetic progressions.

Topics The first part of the course is devoted to understanding number fields and their rings of integers, including unique factorization into prime ideals and the group of units, using Galois theory and ramification theory. We will then study Minkowski's geometry of numbers for the finiteness of the class group, and Kummer's special case of Fermat's Last Theorem.

The second part of the course turns towards soft analytic methods: zeta functions, L-functions, the class number formula, Dirichlet's theorem on primes in arithmetic progression.

The last part of the course is set aside for special topics, depending on the students' preference. Possibilities include: harder analytic results (such as estimating the number of primes or exponential sums), primality testing and public key cryptography, number theory on function fields, elliptic curves mod p, etc.

Prerequisites Knowledge of rings and fields is required, while Galois theory and complex analysis are useful but not prerequisites.