Math 129: Algebraic Number Theory
Tuesdays and Thursdays 10:00–11:30 in SC 310

http://modular.fas.harvard.edu/129

William Stein

Thursday, February 5, 2004

1 Organizational information

Email: was@math.harvard.edu
Office: Science Center 515
Office Phone: 617-495-1790
Mobile Phone: 617-308-0144
Office Hours: Tuesday and Thursday 2–3pm.

The official textbook is Swinnerton-Dyer's *A Brief Guide to Algebraic Number Theory*. I am creating a list of mistakes and typos in the book here:

http://modular.fas.harvard.edu/edu/Spring2004/129/errata.html

I will type up notes every day, and hand out typed homework sets.

2 Mathematical background I assume you have

I will assume you have the following background:

- Basics of finite group theory
- Commutative rings, ideals, quotient rings
- Some exposure to elementary number theory
- Some Galois theory

If you haven't seen finite groups before, you shouldn't take this course. If you haven't seen much elementary ring theory, there is still hope, but you will have to do some additional reading and problems (see me for some ideas). I will briefly review the basics of the Galois theory of number fields.

Some of the homework problems will involve using a computer, but I'll give you examples which you can build on. I will not assume that you have a programming background or know much about algorithms. If you don't have PARI or MAGMA, and don't want to install either one on your computer, you might want to try the following online interface to PARI and MAGMA, which I wrote:

`http://modular.fas.harvard.edu/calc/`

3 How you will be evaluated

Homework is important because it will account for **50%** of your grade. I will assign homework each Thursday (starting Thursday, February 12), and it will be due the following Thursday. *No late homework will be accepted*, but I will ignore one homework score, so you can skip an assignment if you're too busy with other things. Late homework won't be accepted because grading late homework is unfair for the course assistant. You *are* allowed to work with other students on your homework, but you must thank them in your write up for any help. If you get desperate you can also copy a solution from another book; you will receive full credit provided you reword it in your own way, understand the solution, the solution is correct, and you mention that you copied it from the book in your solution.

There will be a final project, which is worth **30%** of your grade.

The remaining **20%** of your grade will be determined by a one-day take-home final exam (pending university approval). Thus there will be **no in-class exams and no midterm**.

4 What is algebraic number theory?

A *number field* K is a finite algebraic extension of the rational numbers $\mathbf{Q}$. Every such extension can be represented as all polynomials in an algebraic number α:

$$K = \mathbf{Q}(\alpha) = \left\{ \sum_{n=0}^{m} a_n \alpha^n : a_n \in \mathbf{Q} \right\}.$$

Here α is a root of a polynomial with coefficients in $\mathbf{Q}$.

Algebraic number theory involves using techniques from (mostly commutative) algebra and finite group theory to gain a deeper understanding of number fields. The main objects that we study in algebraic number theory are number fields, rings of integers of number fields, unit groups, ideal class groups,norms, traces, discriminants, prime ideals, Hilbert and other class fields and associated reciprocity laws, zeta and L-functions, and algorithms for computing each of the above.

4.1 Topics in this course

I hope to cover the following topics in this course.

- Rings of integers of number fields

- Unique factorization of ideals in Dedekind domains
- Structure of the group of units of the ring of integers
- Finiteness of the group of equivalence classes of ideals of the ring of integers (the "class group")
- Decomposition and inertia groups, Frobenius elements
- Ramification
- Discriminant and different
- Quadratic and biquadratic fields
- Cyclotomic fields (and applications)
- How to use a computer to compute with many of the above objects (both algorithms and actual use of PARI and MAGMA).

Note that we will not do anything nontrivial with zeta functions or L-functions. This is to keep the prerequisites to algebra, and so we will have more time to discuss algorithmic questions. Depending on time and your inclination, I may also talk about integer factorization, primality testing, or complex multiplication elliptic curves (which are closely related to quadratic imaginary fields).

5 Some applications of algebraic number theory

The following examples are meant to convince you that learning algebraic number theory now will be an excellent investment of your time. If an example below seems vague to you, it is safe to ignore it.

1. **Integer factorization** using the number field sieve. The number field sieve is the asymptotically fastest known algorithm for factoring general large integers (that don't have too special of a form). Recently, in December 2003, the number field sieve was used to factor the RSA-576 \$10000 challenge:

$$\begin{aligned}
&188198812920607963838697239461650439807163563379417382700 7\ldots\\
&\ldots 633564229888597152346654853190606065047430453173880113033 9\ldots\\
&\ldots 6716199692321205734031879550656996221305168759307650257059\\
&= 398075086424064937397125500550386491199064362342526708406\ldots\\
&\quad\ldots 385189575946388957261768583317\\
&\qquad\times 472772146107435302536223071973048224632914695302097116\ldots\\
&\qquad\quad\ldots 459852171130520711256363590397527
\end{aligned}$$

(The ... indicates that the newline should be removed, not that there are missing digits.) For more information on the NFS, sieve the paper by Lenstra et al. on the Math 129 web page.

2. **Primality test:** Agrawal and his students Saxena and Kayal from India recently (2002) found the first ever deterministic polynomial-time (in the number of digits) primality test. There methods involve arithmetic in quotients of $(\mathbf{Z}/n\mathbf{Z})[x]$, which are best understood in the context of algebraic number theory. For example, Lenstra, Bernstein, and others have done that and improved the algorithm significantly.

3. **Deeper point of view** on questions in number theory:

   (a) Pell's Equation ($x^2 - dy^2 = 1$) $\Longrightarrow$ Units in real quadratic fields $\Longrightarrow$ Unit groups in number fields

   (b) Diophantine Equations $\Longrightarrow$ For which n does $x^n + y^n = z^n$ have a nontrivial solution in $\mathbf{Q}(\sqrt{2})$?

   (c) Integer Factorization $\Longrightarrow$ Factorization of ideals

   (d) Riemann Hypothesis $\Longrightarrow$ Generalized Riemann Hypothesis

   (e) Deeper proof of Gauss's quadratic reciprocity law in terms of arithmetic of cyclotomic fields $\mathbf{Q}(e^{2\pi i/n})$, which leads to class field theory.

4. Wiles's proof of **Fermat's Last Theorem**, i.e., $x^n + y^n = z^n$ has no nontrivial integer solutions, uses methods from algebraic number theory extensively (in addition to many other deep techniques). Attempts to prove Fermat's Last Theorem long ago were hugely influential in the development of algebraic number theory (by Dedekind, Kummer, Kronecker, et al.).

5. **Arithmetic geometry:** This is a huge field that studies solutions to polynomial equations that lie in arithmetically interesting rings, such as the integers or number fields. A famous major triumph of arithmetic geometry is Faltings's proof of Mordell's Conjecture.

   Theorem 5.1 (Faltings). *Let X be a plane algebraic curve over a number field K. Assume that the manifold $X(\mathbf{C})$ of complex solutions to X has genus at least 2 (i.e., $X(\mathbf{C})$ is topologically a donut with two holes). Then the set $X(K)$ of points on X with coordinates in K is finite.*

   For example, Theorem 5.1 implies that for any $n \geq 4$ and any number field K, there are only finitely many solutions in K to $x^n + y^n = 1$. A famous open problem in arithmetic geometry is the Birch and Swinnerton-Dyer conjecture, which gives a deep conjectural criterion for exactly when $X(K)$ should be infinite when $X(\mathbf{C})$ is a torus.

Remark 5.2. If you find that this course is not advanced enough for you, Barry Mazur is teaching a graduate-level algebraic number theory course at exactly the same time. Switching won't complicate your schedule, but the overlap is unfortunate. His course will assume that you know substantial commutative algebra, and will cover more analytic topics.

6 Finitely generated abelian groups

We will now prove the structure theorem for finitely generated abelian groups, since it will be crucial for much of what we will do later.

Let $\mathbf{Z} = \{0, \pm 1, \pm 2, \ldots\}$ denote the ring of integers, and for each positive integer n let $\mathbf{Z}/n\mathbf{Z}$ denote the ring of integers modulo n, which is a cyclic abelian group of order n under addition.

Definition 6.1. A group G is *finitely generated* if there exists $g_1, \ldots, g_n \in G$ such that every element of G can be obtained from the g_i.

Theorem 6.2 (Structure Theorem for Abelian Groups). *Let G be a finitely generated abelian group. Then there is an isomorphism*

$$G \cong (\mathbf{Z}/n_1\mathbf{Z}) \oplus (\mathbf{Z}/n_2\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/n_s\mathbf{Z}) \oplus \mathbf{Z}^r,$$

where $n_1 > 1$ and $n_1 \mid n_2 \mid \cdots \mid n_s$. Furthermore, the n_i and r are uniquely determined by G.

We will prove the theorem as follows. We first remark that any subgroup of a finitely generated free abelian group is finitely generated. Then we see that finitely generated abelian groups can be presented as quotients of finite rank free abelian groups, and such a presentation can be reinterpreted in terms of matrices over the integers. Next we describe how to use row and column operations over the integers to show that every matrix over the integers is equivalent to one in a canonical diagonal form, called the Smith normal form. We obtain a proof of the theorem by reinterpreting Smith normal form in terms of groups.

Proposition 6.3. *Suppose G is a free abelian group of finite rank n, and H is a subgroup of G. Then H is a free abelian group generated by at most n elements.*

The key reason that this is true is that G is a finitely generated module over the principal ideal domain $\mathbf{Z}$. We will give a complete proof of a beautiful generalization of this result in the context of Noetherian rings next time, but will not prove this proposition here.

Corollary 6.4. *Suppose G is a finitely generated abelian group. Then there are finitely generated free abelian groups F_1 and F_2 such that $G \cong F_1/F_2$.*

Proof. Let $x_1, \ldots, x_m$ be generators for G. Let $F_1 = \mathbf{Z}^m$ and let $\varphi : F_1 \to G$ be the map that sends the ith generator $(0, 0, \ldots, 1, \ldots, 0)$ of $\mathbf{Z}^m$ to x_i. Then φ is a surjective homomorphism, and by Proposition 6.3 the kernel F_2 of φ is a finitely generated free abelian group. This proves the corollary. □

Suppose G is a nonzero finitely generated abelian group. By the corollary, there are free abelian groups F_1 and F_2 such that $G \cong F_1/F_2$. Choosing a basis for F_1, we obtain an isomorphism $F_1 \cong \mathbf{Z}^n$, for some positive integer n. By Proposition 6.3,

$F_2 \cong \mathbf{Z}^m$, for some integer m with $0 \leq m \leq n$, and the inclusion map $F_2 \hookrightarrow F_1$ induces a map $\mathbf{Z}^m \to \mathbf{Z}^n$. This homomorphism is left multiplication by the $n \times m$ matrix A whose columns are the images of the generators of F_2 in $\mathbf{Z}^n$. The *cokernel* of this homomorphism is the quotient of $\mathbf{Z}^n$ by the image of A, and the cokernel is isomorphic to G. By augmenting A with zero columns on the right we obtain a square $n \times n$ matrix A with the same cokernel. The following proposition implies that we may choose bases such that the matrix A is diagonal, and then the structure of the cokernel of A will be easy to understand.

Proposition 6.5 (Smith normal form). *Suppose A is an $n \times n$ integer matrix. Then there exist invertible integer matrices P and Q such that $A' = PAQ$ is a diagonal matrix with entries $n_1, n_2, \ldots, n_s, 0, \ldots, 0$, where $n_1 > 1$ and $n_1 \mid n_2 \mid \ldots \mid n_s$. This is called the Smith normal form of A.*

We will see in the proof of Theorem 6.2 that A' is uniquely determined by A.

Proof. The matrix P will be a product of matrices that define elementary row operations and Q will be a product corresponding to elementary column operations. The elementary operations are:

1. Add an integer multiple of one row to another (or a multiple of one column to another).

2. Interchange two rows or two columns.

3. Multiply a row by -1.

Each of these operations is given by left or right multiplying by an invertible matrix E with integer entries, where E is the result of applying the given operation to the identity matrix, and E is invertible because each operation can be reversed using another row or column operation over the integers.

To see that the proposition must be true, assume $A \neq 0$ and perform the following steps (compare Artin's *Algebra*, page 459):

1. By permuting rows and columns, move a nonzero entry of A with smallest absolute value to the upper left corner of A. Now attempt to make all other entries in the first row and column 0 by adding multiples of row or column 1 to other rows (see step 2 below). If an operation produces a nonzero entry in the matrix with absolute value smaller than $|a_{11}|$, start the process over by permuting rows and columns to move that entry to the upper left corner of A. Since the integers $|a_{11}|$ are a decreasing sequence of positive integers, we will not have to move an entry to the upper left corner infinitely often.

2. Suppose a_{i1} is a nonzero entry in the first column, with $i > 1$. Using the division algorithm, write $a_{i1} = a_{11}q + r$, with $0 \leq r < a_{11}$. Now add $-q$ times the first row to the ith row. If $r > 0$, then go to step 1 (so that an entry with absolute value at most r is the upper left corner). Since we will only perform

step 1 finitely many times, we may assume $r = 0$. Repeating this procedure we set all entries in the first column (except a_{11}) to 0. A similar process using column operations sets each entry in the first row (except a_{11}) to 0.

3. We may now assume that a_{11} is the only nonzero entry in the first row and column. If some entry a_{ij} of A is not divisible by a_{11}, add the column of A containing a_{ij} to the first column, thus producing an entry in the first column that is nonzero. When we perform step 2, the remainder r will be greater than 0. Permuting rows and columns results in a smaller $|a_{11}|$. Since $|a_{11}|$ can only shrink finitely many times, eventually we will get to a point where every a_{ij} is divisible by a_{11}. If a_{11} is negative, multiple the first row by -1.

After performing the above operations, the first row and column of A are zero except for a_{11} which is positive and divides all other entries of A. We repeat the above steps for the matrix B obtained from A by deleting the first row and column. The upper left entry of the resulting matrix will be divisible by a_{11}, since every entry of B is. Repeating the argument inductively proves the proposition. □

Example 6.6. The matrix $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ is equivalent to $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ and the matrix $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$ is equivalent to $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Note that the determinants match, up to sign.

Theorem 6.2. Suppose G is a finitely generated abelian group, which we may assume is nonzero. As in the paragraph before Proposition 6.5, we use Corollary 6.4 to write G as a the cokernel of an $n \times n$ integer matrix A. By Proposition 6.5 there are isomorphisms $Q : \mathbf{Z}^n \to \mathbf{Z}^n$ and $P : \mathbf{Z}^n \to \mathbf{Z}^n$ such that $A' = PAQ$ is a diagonal matrix with entries $n_1, n_2, \ldots, n_s, 0, \ldots, 0$, where $n_1 > 1$ and $n_1 \mid n_2 \mid \ldots \mid n_s$. Then G is isomorphic to the cokernel of the diagonal matrix A', so

$$G \cong (\mathbf{Z}/n_1\mathbf{Z}) \oplus (\mathbf{Z}/n_2\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/n_s\mathbf{Z}) \oplus \mathbf{Z}^r, \tag{6.1}$$

as claimed. The n_i are determined by G, because n_i is the smallest positive integer n such that nG requires at most $s + r - i$ generators (we see from the representation (6.1) of G as a product that n_i has this property and that no smaller positive integer does).

□