Algebraic Number Theory - Notes (by Evan Dummit, 2024, v. 0.02)

Contents

0 Algebraic Number Theory

These are lecture notes for the graduate course Math 7315: Algebraic Number Theory, taught at Northeastern in Fall 2024.

0.1 (Sep 4) Overview, Number Fields and Algebraic Integers

- The goal of this course is to provide an introduction to algebraic number theory, which (broadly speaking) uses the language and tools of abstract algebra to study number theory.
  - ○ To illustrate, here are some fundamental things from classical number theory: primes, unique factorizations, congruences and modular arithmetic, Fermat's and Euler's theorems, the prime number theorem, quadratic reciprocity (and higher reciprocity), and the prime number theorem.
  - ○ It was observed in the 1700s and early 1800s that many of these same ideas extend in fundamentally similar ways to other kinds of numbers beyond the integers – various natural examples being the Gaussian integers, other kinds of algebraic numbers such as the nth roots of unity, and polynomials with coefficients in the field $\mathbb{F}_p$.
  - ○ However, it was not until some of the fundamental constructions from abstract algebra were better understood that these ideas coalesced into an understandable form – precisely, the central ideas are the closely-related notions of a ring, a module, and of an integral extension – which arose between the 1860s and 1880s in the work of Dedekind and Kronecker, and were extended greatly over the subsequent decades by Noether, Hilbert, Krull, and others.
  - ○ As a matter of history, the questions we will study about unique factorization and algebraic number fields motivated the development of a great deal of abstract algebra, but we will reverse the historical trend and start by developing the needed algebraic facts before applying them to study number theory.
- Our general goal is to study the problem of unique factorization (and quite often its failure!) in the ring of integers of a number field.
  - ○ Now, one may certainly adopt the position that the existence or nonexistence of unique factorization in an integral domain is already an intrinsically interesting question by itself, but the question is rather trivialized simply by noting that such rings are, by definition, unique factorization domains.
  - ○ The more specific question of whether we can tell if a particular ring has unique factorization is more interesting, but still, we are really interested only in rings of interest for their utility in answering questions about number theory.
  - ○ So let us first formulate the proper class of rings that we will study.
- Definition: A number field is a field extension $K/\mathbb{Q}$ whose vector space dimension over $\mathbb{Q}$ is finite.
  - ○ Equivalently, a number field is a finite-degree extension of $\mathbb{Q}$.
  - ○ Since the complex field $\mathbb{C}$ is algebraically closed and contains $\mathbb{Q}$, by standard facts about algebraic field extensions, K can be embedded into $\mathbb{C}$.

- ○ As such, we may equivalently think of a number field as a subfield of $\mathbb{C}$ that has finite degree over $\mathbb{Q}$.

- Example: The quadratic field $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$ for any squarefree integer $D \neq 1$ is a number field of degree 2 over $\mathbb{Q}$.
  - ○ For positive D the field $\mathbb{Q}(\sqrt{D})$ is a real quadratic field, while for negative D the field $\mathbb{Q}(\sqrt{D})$ is an imaginary quadratic field.
  - ○ We could spend a tremendous amount of time just studying properties of factorization in quadratic fields, since even by themselves they already provide interesting examples of unique and non-unique factorization.
  - ○ As is well known (and which we will prove properly later), the ring $\mathbb{Z}[i]$ of Gaussian integers, which is a subring of the quadratic field $\mathbb{Q}(i)$, has unique factorization.
  - ○ On the other hand, in $\mathbb{Z}[\sqrt{-3}]$, a subring of $\mathbb{Q}(\sqrt{-3})$, we have $4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$, and these two factorizations are inequivalent because the terms are all irreducible but are not associates of one another.
  - ○ However, this "example" is not really so interesting, because inside the corresponding field $\mathbb{Q}(\sqrt{-3})$ there does exist a subring where these two factorizations are equivalent up to unit factors: namely, the subring $\mathbb{Z}[\omega] = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$.
  - ○ More interestingly, in the ring $\mathbb{Z}[\sqrt{-5}]$, a subring of $\mathbb{Q}(\sqrt{-5})$, we have a similar lack of unique factorization: $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. Yet as we will see, there is no similar way to "enlarge" this subring (while still maintaining the desired kind of integrality of the elements) in order to salvage unique factorization of elements.

- Example: For a primitive nth root of unity ζ_n such as $\zeta_n = e^{2\pi i/n}$, the cyclotomic field $\mathbb{Q}(\zeta_n)$ is a number field of degree $\varphi(n)$ over $\mathbb{Q}$, since the minimal polynomial of ζ_n over $\mathbb{Q}$ is the nth cyclotomic polynomial which has degree $\varphi(n)$.
  - ○ There are many properties of the roots of unity, and some simple ones lead to relations among the cyclotomic fields.
  - ○ Exercise: If a and b are relatively prime, show that $\mathbb{Q}(\zeta_{ab}) = \mathbb{Q}(\zeta_a, \zeta_b)$. Deduce that $\mathbb{Q}(\zeta_{2n}) = \mathbb{Q}(\zeta_n)$ for odd integers n. Do there exist distinct even integers $2m$ and $2n$ such that $\mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_{2n})$?

- We can generalize the two examples above rather substantially:

- Example: For any irreducible polynomial $p(x) \in \mathbb{Q}[x]$ of degree n with a complex root α, the field $\mathbb{Q}(\alpha) = \{c_0\alpha + \cdots + c_{n-1}\alpha^{n-1} : c_i \in \mathbb{Q}\}$ generated by α over $\mathbb{Q}$ is a number field of degree n.
  - ○ In fact, every number field is really of this form:
  - ○ Exercise: Suppose $K/\mathbb{Q}$ is a number field. Show that $K = \mathbb{Q}(\alpha)$ for some complex number α. [Hint: Apply the primitive element theorem.]

- Now, in order to discuss unique factorization fruitfully, we need to identify the analogue of the integers $\mathbb{Z}$ inside our number field K, which will give us (in a very strong sense) the "proper" subring of K in which to consider factorizations:

- Definition: For a number field K, an algebraic number $\alpha \in K$ is an algebraic integer if there exists a monic polynomial $p(x)$ with integer coefficients such that $p(\alpha) = 0$.
  - ○ Examples: Integers are algebraic integers, as are $\sqrt{2}$ and i, and more generally $a^{1/n}$ for any integer a and positive integer n. The roots of $x^3 - x - 1 = 0$ are algebraic integers.
  - ○ Indeed, it is not so trivial to show that a given complex number is *not* an algebraic integer using this definition, since it would require showing that there is no monic polynomial with integer coefficients of which it is a root.
  - ○ Let us give a better way to determine whether an algebraic number is an algebraic integer, while also reviewing some properties of algebraic numbers in general:

- Proposition (Algebraic Integers I): Suppose α is an algebraic number, so that α is the root of some nonzero polynomial $q(x) \in \mathbb{Q}[x]$.

  1. The set of all polynomials $p(x) \in \mathbb{Q}[x]$ for which $p(\alpha) = 0$ is an ideal of $\mathbb{Q}[x]$. The unique monic generator $m(x)$ of this ideal is the minimal polynomial of α, and is the unique monic polynomial in $\mathbb{Q}[x]$ of smallest degree having α as a root.
     - Proof: It is easy to see that the set of $p(x)$ with $p(\alpha) = 0$ is an ideal. Since $\mathbb{Q}[x]$ is a principal ideal domain, this ideal is principal, and therefore has a unique monic generator.
     - Since $m(x)$ divides all elements of this ideal, its degree is smallest among all nonzero elements of the ideal.
     - Exercise: Show that the minimal polynomial $m(x)$ is irreducible in $\mathbb{Q}[x]$.
  2. The algebraic number α is an algebraic integer if and only if its minimal polynomial (over $\mathbb{Q}$) has integer coefficients.
     - Proof: If the minimal polynomial $m(x)$ has integer coefficients, then $m(x)$ itself is a monic polynomial with integer coefficients of which α is a root, so obviously α is an algebraic integer.
     - Conversely, suppose α is an algebraic integer. Let $p(x)$ be the monic polynomial of minimal degree such that $p(\alpha) = 0$ and $p(x)$ has integer coefficients. If $p(x)$ were reducible in $\mathbb{Q}[x]$, then by Gauss's lemma[1] $p(x)$ would have a factorization in $\mathbb{Z}[x]$: say $p(x) = f(x)g(x)$. But then at least one of f and g would have α as a root, contradicting the minimality of p.
     - Thus p is irreducible. Now, since $p(\alpha) = 0$, we see that $m(x)$ divides $p(x)$, so since p is irreducible we must have $p(x) = c \cdot m(x)$ for some $c \in \mathbb{Q}$, but as both p and m are monic, we have $c = 1$. Thus, $m(x) \in \mathbb{Z}[x]$ as claimed.

- Using the criterion in (2) above we may compute the algebraic integers in a number field K by finding the elements of K whose minimal polynomials have integer coefficients.
  - Exercise: Show that the set of algebraic integers of $\mathbb{Q}$ is $\mathbb{Z}$.
  - Exercise: Suppose D is squarefree. Show that the set of algebraic integers of $\mathbb{Q}(\sqrt{D})$ is $\mathbb{Z}[\sqrt{D}]$ when $D \equiv 2, 3 \pmod 4$ and that it is $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ when $D \equiv 1 \pmod 4$. [Hint: First verify that for $b \neq 0$ the minimal polynomial of $a + b\sqrt{D}$ is $m(x) = x^2 - 2a + (a^2 - Db^2)$, and then classify when the coefficients are integers.]

- In the examples above note that the algebraic integers in these number fields both form rings. In fact, the algebraic numbers in any number field always form a ring, as we will now show.
  - After noting rather obviously that 0 is an algebraic integer and the negative of an algebraic integer is an algebraic integer, the claimed fact is equivalent to proving that the set of algebraic integers is closed under addition and multiplication.
  - This fact can be proven directly from the definition using rather tedious polynomial elimination: the idea is that if α and β are algebraic integers with integer polynomials p, q with $p(\alpha) = q(\beta) = 0$, then one may do polynomial elimination on the sets $\{p(x), q(y), z - x - y\}$ and $\{p(x), q(y), z - xy\}$ to obtain a single monic polynomial in z with integer coefficients in each case, which then establishes that $\alpha + \beta$ and $\alpha\beta$ are algebraic integers.
  - But this approach is very tedious to implement in practice, and is not particularly enlightening. Let us give a much more natural approach using modules.

- Proposition (Rings of Integers): Suppose K is a number field.

  1. For $\alpha \in K$, the following are equivalent:
     (a) α is an algebraic integer.
     (b) The ring $\mathbb{Z}[\alpha]$ is finitely generated as an additive group (i.e., as a $\mathbb{Z}$-module).

[1] The formulation of Gauss's lemma we use here is that if a polynomial with integer coefficients factors in $\mathbb{Q}[x]$, then in fact it factors in $\mathbb{Z}[x]$.

(c) α is an element of some subring of $\mathbb{C}$ that is finitely generated as an additive group.

(d) There exists some finitely generated additive subgroup G of $\mathbb{C}$ with $\alpha G \subseteq G$.

- Proof: $(a) \Rightarrow (b)$: If the minimal polynomial of α is $m(x) = x^n + c_n x^{n-1} + \cdots + c_1 x + c_0$ then we claim $\{1, \alpha, \dots, \alpha^{n-1}\}$ generates $\mathbb{Z}[\alpha]$ as an additive group. To see this it suffices to observe that each power of α is an integral linear combination of $\{1, \alpha, \dots, \alpha^{n-1}\}$, which follows by an easy induction relying on the fact that $\alpha^n = -c_0 - c_1\alpha - \cdots - c_n\alpha^{n-1}$.
- $(b) \Rightarrow (c)$: Obvious, since $\alpha \in \mathbb{Z}[\alpha]$.
- $(c) \Rightarrow (d)$: Obvious by taking L to be the given subring.
- $(d) \Rightarrow (a)$: Suppose G is generated by $\beta_1, \dots, \beta_n$. Then $\alpha\beta_1, \dots, \alpha\beta_n$ are all elements of G hence can be expressed as integral linear combinations of $\beta_1, \dots, \beta_n$. As such, we see that $\alpha \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = M \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}$ for an appropriate $B \in M_{n\times n}(\mathbb{Z})$. Thus, α is an eigenvalue of the matrix M, and so the characteristic polynomial $p(x) = \det(xI - M)$ has α as a root; as M has integer entries, $p(x)$ is then a monic polynomial with integer coefficients having α as a root.

2. The set of all algebraic integers forms a ring. The set of algebraic integers in K also forms a ring, which is called the ring of integers of K and is denoted $\mathcal{O}_K$.

   - Proof: Suppose α and β are algebraic integers. Then $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely-generated $\mathbb{Z}$-modules, hence so is $\mathbb{Z}[\alpha, \beta]$ since it is generated by the pairwise products of the generating sets. Hence so are the submodules $\mathbb{Z}[\alpha - \beta]$ and $\mathbb{Z}[\alpha\beta]$.
   - We deduce that the set of all algebraic integers is closed under subtraction and multiplication, so it is ring. The intersection of it with K is therefore also a ring.

- Remark: All of the argument above can be made completely explicit: if $\mathbb{Z}[\alpha]$ has basis $\{1, \alpha, \dots, \alpha^{n-1}\}$ and $\mathbb{Z}[\beta]$ has basis $\{1, \beta, \dots, \beta^{m-1}\}$ then $\mathbb{Z}[\alpha, \beta]$ is spanned by $\{\alpha^i\beta^j\}_{1 \le i \le n, 1 \le j \le mn}$. Then to compute a polynomial with, say, $\alpha + \beta$ as a root, simply compute the coefficients of multiplication by $\alpha + \beta$ on this spanning set, and evaluate the appropriate determinant.
- Exercise: Use the procedure described above to find a monic integer polynomial satisfied by $\sqrt{2} + \sqrt[3]{3}$ and by $\sqrt{2} \cdot (\sqrt[3]{3} - 1)$.

Well, you're at the end of my handout. Hope it was helpful.