MATH 6122: Algebra II

Frank Qiang
Instructor: Matthew Baker

Georgia Institute of Technology
Spring 2025

Contents

Lecture 1

Jan. 7 — Motivation for Algebraic Number Theory

1.1 Motivation: Fermat's Last Theorem

Theorem 1.1 (Fermat's last theorem[1]). *$x^n + y^n = z^n$ has no nonzero integer solutions when $n \geq 3$.*

Remark. The $n = 3$ case was likely solved by Fermat, and Euler and Gauss had work for $n = 4$. So we will assume $n \geq 5$. We can also assume n is prime, since if $n = pm$, then we can instead consider

$$(x^m)^p + (y^m)^p = (z^m)^p.$$

Thus any nonzero solution to $x^n + y^n = z^n$ also yields a nonzero solution to $x^p + y^p = z^p$. So let $p \geq 5$ be prime, and let $\zeta = \zeta_p$ be a primitive pth root of 1. Then consider

$$x^p + y^p = (x + y)(x + \zeta y)(x + \zeta^2 y) \dots (x + \zeta^{p-1} y) = z^p.$$

Note that $x + \zeta^j y \in \mathbb{Z}[\zeta] \subseteq \mathbb{C}$. Let us pretend for the moment that $\mathbb{Z}[\zeta]$ is a UFD.[2] One can check that

$$\gcd(x + \zeta^j y, x + \zeta^k y) = 1$$

whenever $j \neq k$. If $\mathbb{Z}[\zeta]$ were a UFD, then we could conclude that

$$x + y\zeta = u\alpha^p$$

for some $u \in \mathbb{Z}[\zeta]^\times$ and $\alpha \in \mathbb{Z}[\zeta]$.[3] For the sake of illustration, suppose $u = \pm\zeta^j$ for some j. Then

$$\alpha = a_0 + a_1\zeta + \dots + a_{p-2}\zeta^{p-2}$$

for $a_i \in \mathbb{Z}$. This gives

$$\alpha^p = a_0 + a_1 + \dots + a_{p-2} \pmod{p},$$

using Fermat's little theorem, $\zeta^p = 1$, and the binomial theorem. So $\alpha^p = a \pmod{p}$ with $z \in \mathbb{Z}$, and

$$x + y\zeta = \pm a\zeta^j \pmod{p}$$

for some $0 \leq j \leq p - 1$. Note that $\zeta^{p-1} = -(1 + \zeta + \dots + \zeta^{p-2})$, and one can check as an exercise that this implies $p|x$ or $p|y$. This would have proved the "first case" of Fermat's last theorem.

[1] This problem was finally resolved by Wiles-Taylor in 1995.
[2] It is far from it, and this is likely the mistake that Fermat originally made.
[3] In a UFD, if a product of relatively prime elements is a pth power, then each factor must itself be a pth power.

Remark. However, Kummer (c. 1850) observed that $\mathbb{Z}[\zeta]$ is rarely a UFD (in fact, $\mathbb{Z}[\zeta]$ is a UFD if and only if $p \leq 19$).[4] Also, when $p \geq 5$, the unit group of $\mathbb{Z}[\zeta]$ is always infinite (so that $\mathbb{Z}[\zeta]^\times \neq \{\pm\zeta^j\}$).

Theorem 1.2 (Kummer)**.** *Fermat's last theorem holds for all "regular" primes.*[5]

Remark. The first irregular prime is 37, so Kummer's method works for $3 \leq n \leq 36$.

1.2 Algebraic Integers

Remark. To resolve these issues, Kummer realized that one can replace elements of $\mathbb{Z}[\zeta]$ by "ideal elements." Later on, Dedekind look at Kummer's work and introduced the modern notion of an ideal. We will be working towards the *unique factorization of ideals into prime ideals* in certain cases.

Remark. We will work at the level of generality of Dedekind rings (as opposed to just number rings). This is because there is an analogue of such a unique factorization of ideals for function fields of curves in algebraic geometry, and this framework is general enough to capture both cases.

Definition 1.1. Let $K/\mathbb{Q}$ be a finite extension (i.e. a *number field*). Then $\alpha \in K$ is an *algebraic integer* if there exists a monic polynomial $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

Theorem 1.3. *Let $A \subseteq B$ be rings and let $b \in B$. Then the following are equivalent:*

1. *b is integral over A (i.e. there exists a monic $f \in A[x]$ such that $f(b) = 0$).*
2. *$A[b]$ is a finitely generated A-module.*[6]
3. *$A[b]$ is contained in a subring $C \subseteq B$ which is finitely generated as an A-module.*

Proof. $(1 \Rightarrow 2)$ This direction is standard, one only needs powers up to $\deg f$ since $f(b) = 0$.

$(2 \Rightarrow 3)$ This direction is clear since $A[b]$ itself satisfies the desired conditions.

$(3 \Rightarrow 1)$ The idea is to argue via determinants and use the Cayley-Hamilton theorem for modules. □

Corollary 1.3.1. *Integrality is transitive, i.e. if B is integral over A and C is integral over B, then C is integral over A.*[7]

Proof. A finitely generated module over a finitely generated module is finitely generated. □

Corollary 1.3.2. *If α, β are integral over A, then $\alpha \pm \beta, \alpha\beta$ are also integral over A.*

Proof. This is because $\alpha \pm \beta, \alpha\beta \subseteq C = A[\alpha][\beta]$. □

Theorem 1.4. *The set of all algebraic integers in K (denoted $\mathcal{O}_K$) forms a subring of K.*[8]

Remark. This theorem is not obvious: Given $f(\alpha) = 0$ and $g(\beta) = 0$, one must find a polynomial h such that $h(\alpha + \beta) = 0$. It is not immediately obvious how to do this.

---

[4] Kummer made the first real progress on Fermat's last theorem in a long time.

[5] A prime p is *regular* if p does not divide the order of the *ideal class group* of $\mathbb{Z}[\zeta]$.

[6] Here $A[b]$ is the smallest subring of B containing A and b, so $A[b] = \{a_0 + a_1 b + a_2 b^2 + \cdots + a_k b_k : a_i \in A\}$.

[7] We say that B is *integral over A* if every $b \in B$ is integral over A.

[8] The ring of algebraic integers $\mathcal{O}_K$ of a number field K is called a *number ring*.

Lecture 2

Jan. 9 — Algebraic Integers and Dedekind Domains

2.1 More on Algebraic Integers

Proposition 2.1. *Suppose $\alpha, \beta \in \overline{\mathbb{Z}} \subseteq \mathbb{C}$, then $\alpha + \beta, \alpha\beta \in \overline{\mathbb{Z}}$.*[1]

Proof. First, note that every algebraic integer is an eigenvalue of some integer matrix (e.g. take the companion matrix for the minimal polynomial). So take linear maps $T_\alpha : V_\alpha\, to V_\alpha$ and $T_\beta : V_\beta \to V_\beta$ which have α and β as eigenvalues, respectively. Then one can check that the map on the direct sum

$$T_\alpha \oplus T_\beta : V_\alpha \oplus V_\beta \to V_\alpha \oplus V_\beta$$

has $\alpha + \beta$ as an eigenvalue. Similarly, by looking at the map on the tensor product

$$T_\alpha \otimes T_\beta : V_\alpha \otimes V_\beta \to V_\alpha \otimes V_\beta$$

has $\alpha\beta$ as an eigenvalue. Hence we see that $\alpha + \beta, \alpha\beta \in \overline{\mathbb{Z}}$ as well. □

Remark. This is a constructive proof of what we showed via finitely generated modules last time.

Lemma 2.1. *Let $\alpha \in K$ be an algebraic number. Then α is an algebraic integer, i.e. $\alpha \in \mathcal{O}_K$, if and only if the minimal polynomial of α over $\mathbb{Q}$, call it $f_\alpha \in \mathbb{Q}[x]$, has integer coefficients.*

Proof. ($\Leftarrow$) This direction is clear by the definition of an algebraic integer.

($\Rightarrow$) We need to show that if $\alpha \in \mathcal{O}_K$, then $f_\alpha \in \mathbb{Z}[x]$. By assumption, there exists some monic integer polynomial $h \in \mathbb{Z}[x]$ such that $h(\alpha) = 0$. From this, we know that $f_\alpha | h$ in $\mathbb{Q}[x]$.[2] Let $\alpha_1, \ldots, \alpha_n$ be the roots of f_α with $\alpha_1 = \alpha$. Since $f_\alpha | h$, we know that $h(\alpha_i) = 0$ for every i, so $h \in \mathbb{Z}[x]$ implies that $\alpha_i \in \overline{\mathbb{Z}}$ for each i. Thus the coefficients of f_α are elementary symmetric functions of the α_i,[3] so

$$f_\alpha \in (\overline{Z} \cap \mathbb{Q})[x].$$

Thus it suffices to show that $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$ to conclude the result. For this, suppose $r/s \in \mathbb{Q}$ is the root of

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

[1]Here $\overline{\mathbb{Z}}$ is the set of algebraic integers.

[2]Note that it suffices to show that $f_\alpha | h$ in $\mathbb{Z}[x]$, so from here, a suitable version of Gauss's lemma immediately implies the desired result.

[3]These operations preserve the notion of being an algebraic integer.

We can assume $(r, s) = 1$ without loss of generality.[4] Plugging in, we obtain

$$(r/s)^n + a_{n-1}(r/s)^{n-1} + \cdots + a_1(r/s) + a_0 = 0.$$

Clearly denominators by multiplying by s^n, we obtain

$$r^n + a_{n-1}sr^{n-1} + \cdots + a_1 s^{n-1} r + a_0 s^n = 0$$

The right-hand side is divisible by s and every term on the left-hand side except r^n is divisible by s, so we must have $s | r^n$. Since $(r, s) = 1$, this implies that $s = \pm 1$, i.e. $r/s \in \mathbb{Z}$. $\square$

Example 2.0.1. For $K = \mathbb{Q}$, we have $\mathcal{O}_K = \mathbb{Z}$. This follows from the previous lemma since the minimal polynomial of $a \in \mathbb{Q}$ is $x - a$, which has integer coefficients precisely when $a \in \mathbb{Z}$.

Example 2.0.2. Let $K = \mathbb{Q}(\sqrt{d})$, i.e. K is *quadratic number field*. Clearly $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$, but this is not always an equality. For example,

$$\phi = \frac{1 + \sqrt{5}}{2} \notin \mathbb{Z}[\sqrt{5}],$$

but $x^2 - x - 1$ has ϕ as a root.

Exercise 2.1. Let d be a square-free integer and $K = \mathbb{Q}(\sqrt{d})$. Show that

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \pmod 4, \\ \mathbb{Z}[(1 + \sqrt{d})/2] & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Definition 2.1. Let S be a ring. If $R \subseteq S$ is a subring, then we say that R is *integrally closed* in S if whenever $\alpha \in S$ is integral over R, then $\alpha \in R$.

Remark. Recall that for a domain R, its *field of fractions* K is the localization

$$K = S^{-1}R$$

where $S = R \setminus \{0\}$. There is a natural embedding of R into K via $r \mapsto r/1$.

Lemma 2.2. *The fraction field of $\mathcal{O}_K$ is K. More precisely, for every $\alpha \in K$, there exists $m \in \mathbb{Z}$, $m \neq 0$, such that $m\alpha \in \mathcal{O}_K$.*

Proof. Since α is algebraic, there exists some monic polynomial $f_\alpha \in \mathbb{Q}[x]$ such that $f_\alpha(\alpha)$. By clearing denominators, there exists $m \in \mathbb{Z}$ such that $mf_\alpha \in \mathbb{Z}[x]$. So we have

$$m\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0,$$

and multiplying by m^{n-1} on both sides, we obtain

$$m^n\alpha^n + m^{n-1}b_{n-1}\alpha^{n-1} + \cdots + m^{n-1}b_1\alpha + m^{n-1}b_0 = 0,$$

which implies

$$(m\alpha)^n + b_{n-1}(m\alpha)^{n-1} + \cdots + m^{n-2}b_1(m\alpha) + m^{n-1}b_0 = 0.$$

This shows that $m\alpha$ is integral, i.e. $m\alpha \in \mathcal{O}_K$. $\square$

[4] Here we write (r, s) to denote $\gcd(r, s)$.

Theorem 2.1. *The ring of integers $\mathcal{O}_K$ is integrally closed (in its fraction field).*

Proof. Transitivity of integrality implies that $\mathcal{O}_K$ is integrally closed in K. The theorem then follows from the fact that K is the fraction field of $\mathcal{O}_K$. □

Remark. The theorem says that (it implies the second equality)

$$\mathcal{O}_K = \{\alpha \in K \mid \alpha \text{ is integral over } \mathbb{Z}\} = \{\alpha \in K \mid \alpha \text{ is integral over } \mathcal{O}_K\}.$$

2.2 Dedekind Domains

Definition 2.2. A *Dedekind domain* is a Noetherian integrally closed domain of dimension 1.

Remark. Recall that all rings in this class are commutative and have a 1. A dimension 1 domain is a domain which is not a field and every nonzero prime ideal is maximal. In general, the dimension of a ring R is the maximum length of a chain of prime ideals of the form

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n.$$

In dimension 1, this corresponds to $(0) \subsetneq \mathfrak{p}$ being the maximum chain for every nonzero prime ideal $\mathfrak{p}$, which is equivalent to the other definition.

Remark. Our goal for now will be to show that $\mathcal{O}_K$ is a Dedekind domain.

Definition 2.3. Let k be either $\mathbb{Q}$ or $\mathbb{R}$ and V be a finite-dimensional k-vector space. A *complete lattice* in V is a discrete additive subgroup Λ of V which spans V, where discrete means that any bounded subset of Λ is finite (equivalent to being discrete in the sense of topology).

Proposition 2.2. *Let V be as above (dimension n over k) and $\Lambda \subseteq V$ an additive subgroup which spans V. Then the following are equivalent:*

1. *Λ is discrete.*
2. *Λ is generated by n elements.*
3. *$\Lambda \cong \mathbb{Z}^n$ as $\mathbb{Z}$-modules.*

Proof. $(2 \Leftrightarrow 3)$ This follows by the structure theorem.

$(1 \Rightarrow 2)$ Suppose Λ is discrete, and let $x_1, \ldots, x_n \in \Lambda$ be a basis for V. Let Λ_0 be the $\mathbb{Z}$-module which is spanned by $x_1, \ldots, x_n$. We claim that Λ/Λ_0 is finite, which implies that Λ is also generated by n elements (exercise). To see the claim, we note that there exists $M > 0$ such that if $x = \sum \lambda_i x_i \in \Lambda$ with $\lambda_i \in k$ and all $|\lambda_i| < 1/M$, then $x = 0$. This is standard and follows from all norms being equivalent in a finite-dimensional vector space and the assumption that Λ is discrete.

Now let $y_1, y_2, \ldots$ be coset representatives for Λ/Λ_0. Without loss of generality (by translating in the coset), assume each $y_i \in C$, where C is the unit cube. Cover C by M^n boxes of the form

$$\frac{m_i}{M} \leq \lambda_i < \frac{m_i + 1}{M}$$

with $m_i \in \mathbb{Z}$ and $0 \leq m_i < M$. We must have $|\Lambda/\Lambda_0| \leq M^n$, since otherwise we end up with two $y_i \neq y_j$ in the same box by the pigeonhole principle, and $y_i - y_j \in C[1/M] \cap \Lambda = \{0\}$ leads to a contradiction.

$(2 \Rightarrow 1)$ This proof is to be finished next class. □

Theorem 2.2. *If I is a nonzero ideal in a number ring $\mathcal{O}_K$, then $\mathcal{O}_K/I$ is finite.*

Proof. The strategy is to show that if $[K:\mathbb{Q}] = n$, then $\mathcal{O}_K \cong \mathbb{Z}^n$ and $I \cong \mathbb{Z}^n$ as $\mathbb{Z}$-modules. This will imply that $\mathcal{O}_K/I$ is finite, which follows from the proof of the structure theorem. In fact, we will show the that I and $\mathcal{O}_K$ are lattices in $K \cong \mathbb{Q}^n \subseteq \mathbb{R}^n$. Note that it suffices to show that $\mathcal{O}_K$ is a lattice, since it immediately follows that $I \subseteq \mathcal{O}_K$ is also discrete, hence also a lattice as I is an additive subgroup.

The proof is to be finished next class. $\square$

Corollary 2.2.1. *A number ring $\mathcal{O}_K$ is Noetherian.*

Proof. Suppose that we have an ascending chain of ideals

$$I = I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots.$$

Suppose without loss of generality that $I_0 \neq 0$. Since $\mathcal{O}_K/I$ is finite, by an isomorphism theorem we see that there are only finitely many ideals in $\mathcal{O}_K$ containing I. This implies that the chain must eventually stabilize, i.e. that $\mathcal{O}_K$ is Noetherian. $\square$

Corollary 2.2.2. *A number ring $\mathcal{O}_K$ is 1-dimensional.*

Proof. Verify as an exercise that $\mathcal{O}_K$ is not a field. Now let $\mathfrak{p}$ be a nonzero prime ideal, so that $\mathcal{O}_K/\mathfrak{p}$ is a finite domain, hence a field. This implies that $\mathfrak{p}$ is maximal, so $\mathcal{O}_K$ is 1-dimensional. $\square$

Theorem 2.3. *A number ring $\mathcal{O}_K$ is a Dedekind domain.*