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

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

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

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

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 $\zeta^p = -(1 + \zeta + \cdots + \zeta^{p-2})$, 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[2] It is far from it, and this is likely the mistake that Fermat originally made.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]

[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] This theorem is not obvious: Given $f(\alpha) = 0$ and $g(\beta) = 0$, one must find a polynomial h such that $h(\alpha + \beta) = 0$.