MATH70042: Algebraic Number Theory

Lecturer: Margherita Pagano

Scribe: Sidharth Hariharan

Imperial College London - Spring 2025

Contents

Chapter 1

Preliminary Examples

One of the main goals of number theory is to solve **Diophantine Equations**. Diophantine Equations essentially involve solving the following problem: given some $p \in \mathbb{Z}[X_1, \ldots, X_n]$, how can one describe the set

$$\{(x_1, \ldots, x_n) \in \mathbb{Z}^n \mid p(x_1, \ldots, x_n) = 0\}$$

of **integer** solutions of p?

1.1 Fermat's Last Theorem

A classic example of this is Fermat's Last Theorem, which studies the Diophantine Equation

$$x^n + y^n = z^n \tag{1.1.1}$$

where $x, y, z \in \mathbb{Z}$ and $n \in \mathbb{N}$. We motivate our study of algebraic number theory by studying the specific case of (1.1.1) when $n = 2$.

1.1.1 The Pythagorean Case: $n = 2$

When $n = 2$, finding $x, y, z \in \mathbb{Z}$ such that (1.1.1) holds is tantamount to finding Pythagorean triples x, y, z. We begin by making a few simplifications of the problem.

Reduction 1. We can assume $x, y, z > 0$. Clearly, if (x, y, z) is a solution, so is $(\pm x, \pm y, \pm z)$, for any $x, y, z \in \mathbb{Z}$. Furthermore, if one of the three variables is zero, the problem is easily solved, so we will disregard these cases.

Reduction 2. We can assume that x, y, z are pairwise coprime. The reason for this is that if p is any common prime divisor of x, y, z then $\left(\frac{x}{p}, \frac{y}{p}, \frac{z}{p}\right) \in \mathbb{Z}^3$, and basic algebraic manipulation shows that this is still a solution. Indeed, if p divides any two of them, then one can show, without much difficulty, that p must also divide the third.

Reduction 3. For primitive solutions[1], we can assume that not all x, y, z are odd. The reason for this is that if both x and y are odd, then both x and y are congruent to either 1 or 3 modulo 4. Either way, their square must be congruent to 1 modulo 4, making the sum of their squares congruent to 2 modulo 4. However, $2 \in \mathbb{Z}/4\mathbb{Z}$ is not a square, meaning that if x and y are both odd, then there cannot be a z satisfying the desired equation. Therefore, one of x and y must be even.

Given these reductions, the idea is to rewrite (1.1.1) as

$$y^2 = z^2 - x^2 = (z + x)(z - x)$$

where we assume x to be even (we need to assume that one of x and y is even, and it does not matter which of them we pick to be even).

First, we note that $\gcd(z + x, z - x) = 1$. Indeed, if p divides both $z + x$ and $z - x$, then p must divide $2z$, which is the sum of these two quantities. p cannot divide z, as that would mean $p|x$, which contradicts the fact that x and z have no common factors. But p cannot equal 2, either, as that would again imply that p divides x and therefore that p also divides z, resulting in the same contradiction. Therefore, $z + x$ and $z - x$ must be coprime.

We will now apply the fact that $\mathbb{Z}$ is a UFD. Since $x, z > 0$, it is immediate that $x + z > 0$. Furthermore, we know that $z^2 \geq x^2$, because z^2 is the sum of x^2 and a nonnegative quantity, namely, y^2. Then, since $x, z > 0$, we can conclude that $z > x$, meaning that $z - x > 0$. Finally, we know that the product of $z - x$ and $z + x$ is a square. From this, we can conclude that there

[1] ie, solutions where x, y, z are pairwise coprime

exist $\alpha, \beta \in \mathbb{Z}$ such that $z - x = \alpha^2$ and $z + x = \beta^2$. We can therefore write

$$x = \frac{(z+x)-(z-x)}{2} = \frac{\beta^2 - \alpha^2}{2}$$
$$z = \frac{(z-x)+(z+z)}{2} = \frac{\beta^2 + \alpha^2}{2}$$
$$y = \alpha\beta \qquad \left(\text{because} y^2 = \alpha^2\beta^2\right)$$

1.1.2 Generalising this Argument

A crucial step in the above argument was the so-called **separating powers trick** for $n = 2$.

Lemma 1.1.1. *Let $a, b, c \in \mathbb{Z} \setminus \{0\}$, and let $n > 0$ be such that $a^n = bc$. If b and c are coprime, then there exist $b_1, c_1 \in \mathbb{Z}$ such that $b = \pm b_1^n$ and $c = \pm c_1^n$.*

We can try and generalise this argument to when $n = p$ is an odd prime. Denote by ζ_p a primitive pth root of unity. We can factorise the expression $x^p + y^p$ as follows:

$$z^p = x^p + y^p = (x+y)(x+\zeta_p y)\cdots\left(x+\zeta_p^{p-1}y\right)$$

The problem is, the factors of z^p no longer lie in $\mathbb{Z}$: rather, they lie in the ring

$$\mathbb{Z}[\zeta_p] = \left\{ \sum_{i=0}^{p-1} a_i \zeta_p^i \;\middle|\; a_i \in \mathbb{Z} \right\}$$

One can check that this is, in fact, a subring of $\mathbb{C}$. A very natural question we can ask ourselves is whether this is a UFD. Similarly, we can ask whether the separating powers trick applies in this setting as well. It turns out that it does in the case where p is a **regular prime**, and we will see exactly what this means later on.

The goal of this module is to study rings "similar" to $\mathbb{Z}[\zeta_p]$. We will eventually be more precise about what similarities we are interested in.

1.2 Mordell's Equation

In this section, we study the Diophantine equation

$$y^2 = x^3 + 16 \tag{1.2.1}$$

We begin by observing that there is a trivial case: when $x = 0$, we can see that $y = \pm 4$.

1.2.1 The Case where $x \neq 0$ and y is Odd

We begin by rewriting (1.2.1) and factoring: we have

$$x^3 = y^2 - 16 = (y + 4)(y - 4)$$

It turns out that $\gcd(y - 4, y + 4) = 1$: one can show that if $y - 4$ and $y + 4$ have a prime divisor, then that prime would have to be 2, making y even, a contradiction.

Chapter 2

Important Fundamentals from Algebra

We begin by mentioning that in this module, all rings will be commutative with unity.

The primary reference for this chapter will be the lecture notes by Ambrus Pál [2].

2.1 Important Classes of Rings

We begin by stating basic properties about rings.Let R be a ring.

Definition 2.1.1 (Group of Units). The **group of units** of R is defined ot be the set

$$R^\times := \{a \in R \mid \exists b \in R \text{ s.t. } ab = 1\}$$

which forms a group under the ring's multiplication operation. Elements of $R^\times$ are called **units**.

The first property of the integers we can generalise is that of divisors.

Definition 2.1.2. For every $a, b \in R$, we say that a **divides** b if $\exists c \in R$ such that $ac = b$. We denote this property as $a|b$.

Definition 2.1.3 (Irreducibility). We say that $a \in R \setminus \{0\}$ is **irreducible** if a is not a unit and for every $b, c \in R$ such that $a = bc$, we have that either b or c is a unit.

2.1.1 Integral Domains

For the remainder of this subsection, assume that R is an integral domain.

Definition 2.1.4 (Prime Elements). We say an element $a \in R \setminus \{0\}$ is prime if a is not a unit and if for all $b, c \in R$, if $a|bc$ then either $a|b$ or $a|c$.

We have the following relationship between irreducible and prime elements.

Lemma 2.1.5. *Every prime element of R is irreducible.*

Example 2.1.6. For $k \in \mathbb{Z}_{\geq 0}$, denote by $\sqrt{k}$ the *positive* square root of k. Consider the set

$$\mathbb{Z}\left[i\sqrt{k}\right] = \left\{a + i\sqrt{k} \in \mathbb{C} \;\middle|\; a, b \in \mathbb{Z}\right\} \tag{2.1.1}$$

where $i = \sqrt{-1}$ is the imaginary unit. It is easy to show that $\mathbb{Z}\left[i\sqrt{k}\right]$ is a subring of $\mathbb{C}$.

2.1.2 Unique Factorisation Domains

A UFD is exactly what it sounds like.

Definition 2.1.7 (Unique Factorisation Domain). We say that an integral domain R is a **unique factorisation domain**, or a **UFD**, if every element of R is uniquely expressible as a product of prime elements, up to reordering of primes and multiplication by a unit.

In a UFD, the converse of Lemma 2.1.5 is true. We sketch the proof below.

Lemma 2.1.8. *If R is a UFD, then every irreducible element of R is prime.*

Proof. Assume that $a \in R \setminus \{0\}$ is irreducible. Let $b, c \in R$ be such that $a|bc$. Then, there exists some $d \in R$ such that $ad = bc$. We can then use the fact that ad and bc must admit the same unique factorisation into irreducibles to see that a must appear in the unique factorisation of bc, making it a divisor of either b or c. □

We give a non-trivial example of a ring that is **not** a unique factorisation domain in Section 2.2.

2.1.3 Principal Ideal Domains

PIDs, too, are exactly what they sound like.

Definition 2.1.9 (Principal Ideal Domain)**.** An integral domain R is called a **Principal Ideal Domain**, or **PID**, if every ideal of R is generated by a single element.

We have an important relationship between PIDs and UFDs.

Theorem 2.1.10. *Every PID is a UFD.*

For the proof of this result, see [2, Theorem 1.2].

2.1.4 Euclidean Domains

Euclidean Domains are essentially Integral Domains in which we can perform long division using the Euclidean Algortihm.

Definition 2.1.11 (Euclidean Domain)**.** We say that an integral domain R is a **Euclidean Domain** if there exists a function $N : R \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ such that for all $a, b \in R \setminus \{0\}$,

1. $N(a) \leq N(ab)$.
2. There exist $q, r \in R$ such that $a = qb + r$ with either $r = 0$ or $N(r) < N(b)$.

There are many examples of Euclidean Domains.

Example 2.1.12 (Polynomial Rings over Fields). Let k be a field. Then, the polynomial ring $k[X]$ is a Euclidean Domain with size function $2^{\deg}$ (or $n^{\deg}$ for any $n \in \mathbb{N}_{>1}$).

We have an important relationship between Euclidean Domains and PIDs (and, by extension, UFDs).

Proposition 2.1.13. *Every Euclidean Domain is a PID.*

We again skip the proof and refer the reader to []

2.1.5 Integrally Closed Rings

In this subsection, we will assume nothing about R beyond that it is an integral domain. We denote its field of fractions by $K = \text{Frac}(R)$.

Definition 2.1.14 (Integrally Closed). R is **integrally closed** if for every monic polynomial $f \in R[X]$ and every $\frac{a}{b} \in K$, we have the implication

$$f\left(\frac{a}{b}\right) = 0 \implies \frac{a}{b} \in K$$

It turns out there is a simple criterion for being integrally closed.

Proposition 2.1.15. *If R is a UFD, then R is integrally closed.*

Proof. Let $f \in R[X]$ be a monic polynomial. Write

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

Fix some $\frac{\alpha}{\beta} \in K$. Assume that $f\left(\frac{\alpha}{\beta}\right) = 0$. We can assume, without loss of generality, that α and β have no common factors that are not units: if they do, then we can write out both of their *unique* factorisations into irreducibles and perform the necessary cancellations in K to reduce $\frac{\alpha}{\beta}$ to a fraction whose numerator and denominator have no common factors.

We have that

$$\frac{\alpha^n}{\beta^n} = -\left(a_{n-1}\frac{\alpha^{n-1}}{\beta^{n-1}} + \cdots + a_0\right)$$
$$\implies \alpha^n = -\beta\left(a_{n-1}\alpha^{n-1} + \cdots + a_0\beta^{n-1}\right)$$

sorry □

2.2 Normed Rings

2.2.1 Norm Functions

Let R be a ring.

Definition 2.2.1 (Norm)**.** We say that $N : R \to \mathbb{R}$ is a **norm** if for all $\alpha, \beta \in R$,

1. $N(\alpha) \geq 0$ and $N(\alpha) = 0 \iff \alpha = 0$.
2. $N(\alpha\beta) = N(\alpha)N(\beta)$.
3. $N(\alpha) = 1 \iff \alpha \in R^\times$.

A normed ring is then exactly what we would expect it to be.

Definition 2.2.2 (Normed Ring)**.** We say that R is a **normed ring** if there exists a norm function on R.

There are many examples of normed rings that we have encountered before.

Example 2.2.3. $\mathbb{Z}$ is a normed ring under the Euclidean norm on $\mathbb{R}$ restricted to $\mathbb{Z}$.

In the case of $\mathbb{Z}$, the Euclidean norm acts as a **size function** that we can use to show $\mathbb{Z}$ is a Eucldiean Domain. However, in general, admitting a norm does not make a ring a Euclidean Domain—indeed, there are normed rings that are not even UFDs. In the next few subsections, we will explore important normed rings.

2.2.2 The Gaussian Integers

Definition 2.2.4 (The Gaussian Integers). The **Gaussian Integers** are the subring $\mathbb{Z}[i]$ of $\mathbb{C}$, where $i = \sqrt{-1}$ is the imaginary constant.

The Gaussian Integers are normed.

Proposition 2.2.5. *The function $N : \mathbb{Z}[i] \to \mathbb{R} : a + bi \mapsto a^2 + b^2$ is a norm on $\mathbb{Z}[i]$.*

In fact, we can go a step further.

Theorem 2.2.6. *Under the restriction of the above function N to the set $\mathbb{Z}[i] \setminus \{0\}$, the Gaussian Integers form a Euclidean Domain.*

The proof depends strongly on a geometric result that states that for any point in $\mathbb{C}$, there exists a point on $\mathbb{Z}[i]$ that is at a distance of most $\frac{\sqrt{2}}{2}$ from it (cf. [2, Proposition 2.4]). For the proof of Theorem 2.2.6, see [2, Theorem 2.3].

2.2.3 The Rings $\mathbb{Z}\left[i\sqrt{k}\right]$

The Gaussian Integers are one example of a very broad family of rings.

Definition 2.2.7. For $k \in \mathbb{Z}_{\geq 0}$, denote by $\sqrt{k}$ the *positive* square root of k. Consider the set

$$\mathbb{Z}\left[i\sqrt{k}\right] = \left\{a + i\sqrt{k} \in \mathbb{C} \;\middle|\; a, b \in \mathbb{Z}\right\} \tag{2.2.1}$$

where $i = \sqrt{-1}$ is the imaginary unit. It is easy to show that $\mathbb{Z}\left[i\sqrt{k}\right]$ is a subring of $\mathbb{C}$.

2.3 Algebraic Integers

The primary reference for this section is the lecture notes by George Boxer [1, §2].

We begin by stating a general result.

Proposition 2.3.1 (Gauss's Lemma). *Let $g, h \in \mathbb{Q}[X]$ be monic polynomials such that their product gh is in $\mathbb{Z}[X]$. Then, g and h are in $\mathbb{Z}[X]$.*

For the proof, see [1, Lemma 2.2].

Definition 2.3.2 (Algebraic Element). A Complex number α is **algebraic** if it is the root of a polynomial over $\mathbb{Q}$.

Recall an important result.

Lemma 2.3.3. *Given an algebraic element $\alpha \in \mathbb{C}$, the set*

$$I_\alpha := \{f \in \mathbb{Q}[X] \mid f(\alpha) = 0\}$$

is an ideal in $\mathbb{Q}[X]$.

Indeed, since $\mathbb{Q}[X]$ is a PID, we can see that $\exists m_\alpha \in \mathbb{Q}[X]$ such that $I_\alpha = (m_\alpha)$. Furthermore, we will assume, without loss of generality, that m_α is monic (we can do this because $\mathbb{Q}$ is a field and we can clear numerators).

Definition 2.3.4 (Minimal Polynomial). The polynomial m_α as defined in Lemma 2.3.3 is called the **minimal polynomial** of α.

In this section, we will study a specific class of algebraic elements.

Definition 2.3.5 (Algebraic Integer). We say that a Complex number is an **algebraic integer** if it is the root of a monic polynomial over $\mathbb{Z}$.

2.3.1 Minimal Polynomials

Proposition 2.3.6. *Let $\alpha \in \mathbb{C}$ be an algebraic number. Denote by $m_\alpha \in \mathbb{Q}[X]$ its minimal (monic) polynomial over $\mathbb{Q}$. Then, α is an algebraic integer if and only if $m_\alpha \in \mathbb{Z}[X]$.*

Proof. We only need to prove the forward direction, as the converse is an immediate consequence of the fact that $\mathbb{Z}[X]$ embeds into $\mathbb{Q}[X]$ in a degree-preserving manner.

Suppose that α is an algebraic integer. Let $f \in \mathbb{Z}[X]$ be monic such that $f(x) = 0$. We know that such an f exists because we are assuming that α is an algebraic integer. Then, by the definition of a minimal polynomial, we have that $\exists g \in \mathbb{Q}[X]$ such that $m_\alpha \cdot g = f \in \mathbb{Z}[X]$. Since f and m_α are monic, so is g. Therefore, by Gauss's Lemma, it must be that $g, m_\alpha \in \mathbb{Z}[X]$. □

Example 2.3.7. For any $\alpha \in \mathbb{Q}$, we have that α is an algebraic integer if and only if $m_\alpha \in \mathbb{Z}[X]$. This is equivalent to $m_\alpha(X) = X - \alpha$ lying in $\mathbb{Z}[X]$, which is true if and only if $\alpha \in \mathbb{Z}$.

2.3.2 Quadratic Integer Rings

This material comes from [1, §2.1].

Definition 2.3.8 (Quadratic Number)**.** We say that $\alpha \in \mathbb{C}$ is a quadratic number if $m_\alpha \in \mathbb{Z}[X]$ has degree 2.

Indeed, by Galois Theory, we know that any algebraic integer will lie in a quadratic field.

Lemma 2.3.9. *If $\alpha \in \mathbb{C}$ is a quadratic number, then there exists some $d \in \mathbb{Z}$ such that*

$$\alpha \in \mathbb{Q}\left[\sqrt{d}\right] = \left\{a + b\sqrt{d} \;\middle|\; a, b \in \mathbb{Q}\right\}$$

We define a trace and a norm on $\mathbb{Q}\left[\sqrt{d}\right]$.

Definition 2.3.10 (Trace). The **trace** of a quadratic field is the map

$$\mathrm{Tr} : \mathbb{Q}\left[\sqrt{d}\right] \to \mathbb{Q} : a + b\sqrt{d} \mapsto 2a$$

Definition 2.3.11 (Norm). The **norm** of a quadratic field is the map

$$N : \mathbb{Q}\left[\sqrt{d}\right] \to \mathbb{Q} : a + b\sqrt{d} \mapsto a^2 - db^2$$

Indeed, we can show that α is always a root of the polynomial

$$p(x) = x^2 - \mathrm{Tr}(\alpha)x + N(\alpha) \in \mathbb{Q}[X]$$

Furthermore, when $\alpha \notin \mathbb{Q}$, we can show that the polynomial p defined above is precisely m_α.

Proposition 2.3.12. *Let $\alpha \notin \mathbb{Q}$ be an algebraic number. Then, α is an algebraic integer if and only if* $\mathrm{Tr}(\alpha), N(\alpha) \in \mathbb{Z}$.

2.4 Another Characterisation of the Algebraic Integers

This material comes from [1, §2.2].

Proposition 2.4.1. *The following are equivalent:*

(a) $\alpha \in \mathbb{C}$ *is an algebraic integer.*

(b) $\mathbb{Z}[\alpha]$ *is finitely generated* as an abelian group under addition.

(c) *There exists a non-zero, finitely generated subgroup $M \leq \mathbb{C}$ such that $\alpha \cdot M \subseteq M$.*

Proof.

(a) $\implies$ (b). Suppose that $\alpha \in \mathbb{C}$ is an algebraic integer. Then, $\exists m_\alpha \in \mathbb{Z}[X]$ such that $m_\alpha(\alpha) = 0$. Write

$$m_\alpha(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

We can show that the set

$$\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

generate $\mathbb{Z}[\alpha]$ as an abelian group under addition.

It is easily seen that the set of *all* powers of α is a generating set for $\mathbb{Z}[\alpha]$—indeed, this is by definition of $\mathbb{Z}[\alpha]$. We need to show that for all $k \geq n$, α^k can be expressed as a $\mathbb{Z}$-linear combination of $\{1, \alpha, \ldots, \alpha^{n-1}\}$. We show this by induction on k.

The base case $k = n$ is clear: this follows from the fact that α is a root of m_α. Now, suppose that for some $k \geq n$, we can write α^k as a $\mathbb{Z}$-linear combination of $\{1, \alpha, \ldots, \alpha^{n-1}\}$ with coefficients c_i. Then, we have that

$$\alpha^{k+1} = \alpha \cdot \alpha^k = \alpha \cdot \sum_{i=0}^{n-1} c_i \alpha^i = \sum_{i=0}^{n-1} c_i \alpha^{i+1}$$

This is a linear combination of $\{\alpha, \ldots, \alpha^n\}$ with coefficients c_i, and by the base case, we know that α^n is a linear combination of $\{1, \ldots, \alpha^{n-1}\}$. Therefore, α^{k+1} is a linear combination of $\{1, \ldots, \alpha^{n-1}\}$.

(b) $\implies$ (c). Suppose that $\mathbb{Z}[\alpha]$ is finitely generated as an abelian group under addition. Then, there exists a finite set $\{v_1, \ldots, v_n\}$ such that every element of $\mathbb{Z}[\alpha]$ can be written as a $\mathbb{Z}$-linear combination of the v_i. Let M be the subgroup of $\mathbb{C}$ generated by the v_i. Then, $\alpha \cdot M \subseteq M$.

(c) $\implies$ (a). Suppose that there exists a non-zero, finitely generated subgroup $M \leq \mathbb{C}$ such that $\alpha \cdot M \subseteq M$. Denote its generators by $m_1, \ldots, m_n$ for some $n \in \mathbb{N}$. Then, we know there exist $a_{ij} \in \mathbb{Z}$ such that for all $1 \leq i \leq n$,

$$\alpha \cdot m_i = \sum_{j=1}^{n} a_{ij} m_j$$

Define $A = (a_{ij})_{1 \leq i,j \leq n}$. Clearly, $A \in \mathrm{M}_{n \times n}(\mathbb{Z})$. sorry

□

Bibliography

These lecture notes are based heavily on the following references:

[1] George Boxer. *MATH60042/70042: Algebraic Number Theory*. Lecture Notes. Imperial College London, Spring 2024.

[2] Ambrus Pál. *MATH60042/70042: Algebraic Number Theory*. Lecture Notes. Imperial College London, Spring 2023.

[3] Alexei Skorobogatov. *MATH50005: Groups and Rings*. Lecture Notes. Imperial College London, Autumn 2022.

[4] Matteo Tamiozzo. *Algebraic Number Theory*. Lecture Notes. Imperial College London.

For the latest version of these notes, visit https://github.com/thefundamentaltheor3m/LieAlgebrasNotes. For any suggestions or corrections, please feel free to fork and make a pull request to my repository.