Supplementary Materials for Chapter III

Xu Gao

MATH 110 | Introduction to Number Theory | Summer 2023

June 29, 2023

Prerequisites

In order to succeed in this course, it is important to meet the following prerequisites:

(a). familiar with the style of proof-based mathematics;

(b). have a good understanding of proof formats and methods;

(c). have basic knowledge of set theory and combinatorics, which are covered in Math 100;

(d). solid grasp of lower division math courses, such as calculus and linear algebra.

In addition, you will meet some concepts which will be explored in greater depth in later courses. They will be used as terminology, and you should have ability to unpackage the abstract definitions.

What to expect in this document?

Definition important concepts which are not explicitly covered in the lectures. You are expected to be proficient in them.

Convenience conveniences used in this course. You should be able to reconginize them without mention.

Terminology useful terminology which are concepts from other courses. You are expected to be able to translate these terms into your own words, even without an in-depth understanding of the relevant theory.

Exercise non-mandatory exercises for practice and self-assessment. Highly recommended.

Further reading reading materials for further interest.

Problem homework problems and challenge problems.

† contents with † mark may be too deep or too off-topics.

Chapter III

Rational Numbers and Algebraic Numbers

1 Irrational numbers

Exercise 1.1. Show that $\mathbb{Q}$ is closed under addition, multiplication, and (nonzero) division. More precisely, for any rational numbers a, b, show that $a+b \in \mathbb{Q}$, $ab \in \mathbb{Q}$, and when $b \neq 0$, $\frac{a}{b} \in \mathbb{Q}$.

Remark. Although it is true that the set of algebraic numbers is closed under addition, multiplication, and (nonzero) division, it is hard to directly verify this. For instance, you can take two irrational algebraic numbers and try to show their sum/product/fraction gives an algebraic number. Then you will realize the difficulty of this problem. A more feasible way is to consider the structure of the entire set rather than specific elements. Following this approach, the statement is a simple consequence of the *Galois theory*, which will be a content in later math course (Math 111).

Terminology 1.1. A $\mathbb{Q}$-*module* is an abelian group $(M, +, e)$ together with an action of integers $\rho\colon \mathbb{Q} \times M \to M$ satisfying

- (*associativity*) $\rho(ab, x) = \rho(a, \rho(b, x))$ for all $a, b \in \mathbb{Q}$ and $x \in M$;
- (*neutrality*) $\rho(a, e) = e$ for all $a \in \mathbb{Q}$.

The notion of $\mathbb{Q}$-*modules* is very similar to *vector spaces*. In fact, some authors may also call them $\mathbb{Q}$-*vector spaces*.

Example 1.2. $(\mathbb{F}, +, 0)$ (where $\mathbb{F}$ is one of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) is a $\mathbb{Q}$-module under the action of left multiplications.

Terminology 1.3. Let $x_1, \cdots, x_n$ be elements in a $\mathbb{Q}$-module M. We say they are $\mathbb{Q}$-*linearly independent* if the only $\mathbb{Q}$-linear combination

$$a_1 x_1 + \cdots + a_n x_n$$

of $x_1, \cdots, x_n$ expressing 0 is the *trivial* one: all coefficients $a_1, \cdots, a_n$ are 0.

Remark. Please compare this notion with *linear independence* in Linear Algebra.

The following theorem connects irrationality and $\mathbb{Q}$-linearly independence.

Theorem 1.4. $\alpha \in \mathbb{C}$ *is irrational if and only if* $1, \alpha$ *are* $\mathbb{Q}$*-linearly independent.*

Proof. ($\Longleftarrow$) If $\alpha \in \mathbb{Q}$, then $\alpha \cdot 1 + (-1) \cdot \alpha$ gives a non-trivial $\mathbb{Q}$-linear combination of $1, \alpha$ expressing 0.

($\Longrightarrow$) Suppose there are $\mathbb{Q}$-linear combination $a \cdot 1 + b \cdot \alpha$ is a non-trivial $\mathbb{Q}$-linear combination of $1, \alpha$ expressing 0. Then we must have $b \neq 0$, otherwise $a = a \cdot 1 + 0 \cdot \alpha = 0$ and hence this is a trivial combination. Then we have $\alpha = -\frac{a}{b}$. Hence, $\alpha \in \mathbb{Q}$. □

2 Ford Circles

- Be aware of the translations between the algebraic language of *reduced fractions* and the geometric language of *Ford circles*.
- Be aware of the translations between the *mediant* of fractions and the *sum* of vectors. Notice how to interpret the relation $\heartsuit$ in terms of the area of rectangle.
- Be aware how we reduce the problem of finding fractions kissing the given $\frac{A}{B}$ to linear Diophantine equations.
- Be aware of the trick of placing the questioned number on the number line divided by multiples of a fixed B.

In the proof of Dirichlet's theorem, if we consider the mesh triangle enclosed by three tangent Ford circles rather than the mesh triangle under two tangent Ford circles, we may have a better bound:

Theorem 2.1. *Let α be an* irrational *number, Then there are infinitely many fractions $\frac{a}{b}$ such that*

$$\left|\alpha - \frac{a}{b}\right| \leqslant \frac{1}{\sqrt{5}b^2}.$$

For details, you can find the paper "*Fractions*" by L. Ford.

3 Higher Diophantine equations

Terminology 3.1. The solution set of a *polynomial* equation (more generally, a system of *polynomial* equations) with coefficients in R is called an *algebraic set defined over R*.

Example 3.2. $\left\{(a,b,c) \in \mathbb{Z}^3 \,\middle|\, a^2+b^2=c^2\right\}$ is an algebraic subset of $\mathbb{Z}^3$ **defined over** $\mathbb{Z}$, while $\left\{(x,y) \in \mathbb{Q}^2 \,\middle|\, x^2+y^2=1\right\}$ is an algebraic subset of $\mathbb{Q}^2$ **defined over** $\mathbb{Z}$.

Terminology 3.3. Let $x_1, \cdots, x_k$ be unknowns. Then the *total degree* of the monomial $C{x_1}^{n_1}\cdots{x_k}^{n_k}$ is $n_1+\cdots+n_k$.

A polynomial is *homogeneous* if the total degrees of its terms are all the same.

Example 3.4. $x^2+y^2=z^2$ is a homogeneous polynomial equation of total degree 2 defined over $\mathbb{Z}$, while $x^2+y^2=1$ is not a homogeneous polynomial equation.

Terminology 3.5. An algebraic set is *projective* if it can be defined by homogeneous polynomial equations. Note that projective algebraic sets are stable under nonzero multiplication.

Example 3.6. The algebraic set $\left\{(a,b,c) \in \mathbb{Z}^3 \,\middle|\, a^2+b^2=c^2\right\}$ is projective.

Usually, we would rather put a projective algebraic set in a *projective space*.

Terminology 3.7. An *equivalence relation* on a set S is a relation $\sim$ satisfying

- (*reflexivity*) for all $a \in S$, $a \sim a$;
- (*symmetry*) for all $a, b \in S$, if $a \sim b$, then $b \sim a$;

- (*transitivity*) for all $a, b, c \in S$, if $a \sim b$ and $b \sim c$, then $a \sim c$.

Remark. Compare the notions of *equivalence relation* and *partial order*. The property *symmetry* is almost the opposite of *antisymmetry*.

Exercise 3.1. If a relation is both an equivalence relation and a partial order, what relation it must be? (Hint: combine the *symmetry* and *antisymmetry* properties.)

Example 3.8. In a vector space V (over a field such as $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$), two vectors $x, y \in V$ are *homothetic* if there is a nonzero number $r \in \mathbb{R}$ such that $y = rx$. "Being homothetic" is an equivalence relation.

Terminology 3.9. Let S be a set and $\sim$ an equivalence relation on it. An *equivalence class* in S is a subset E such that:

- E is nonempty;
- Any two $a, b \in E$ have relation $\sim$;
- For any $a \in S$, if $a \sim b$ for some $b \in E$, then $a \in E$.

The set of equivalence classes in S is called the *quotient set of S up to $\sim$*, denoted by $S/\sim$.

We usually use $[a]$ to denote the equivalence class of $a \in S$.

Terminology 3.10. Let R be a field such as $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. The quotient set

$$\mathbf{P}^n(R) := (R^{n+1} \setminus \{(0, \cdots, 0)\})/\text{homothety}$$

is called the *n-dimensional projective space over R*. When $n = 1$, it is also called the *projective line*.

Example 3.11. The projective line $\mathbf{P}^1(\mathbb{Q})$ can be identified with the set $\mathbb{Q} \cup \{\infty\}$. One way to do this is mapping $[a : b]$ $(b \neq 0)$ to $\frac{a}{b}$ and $[1 : 0]$ to ∞. Can you therefore define additions and multiplications on $\mathbf{P}^1(\mathbb{Q})$?

Problems

Problem III.1. Recall that an *integer polynomial* is an expression of the form $P(T) = c_d T^d + \cdots + c_1 T + c_0$, where each c_i is an integer.

(a) **Find** a nonzero integer polynomial $P(T)$ that has $\sqrt{3} + \sqrt[3]{5}$ as a root.
(b) **Prove that** $\sqrt{3} + \sqrt[3]{5}$ is irrational using I.1.(a).

Problem III.2. By evaluating the Taylor series for the exponential function:

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} + \cdots$$

at $x = 1$, we get the formula

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!} + \cdots .$$

In this problem, you will prove that e is *irrational*.

(a) Let $s_n := \sum_{k=0}^{n} \frac{1}{k!}$, the n-th partial sum of above series. **Show that**

$$0 \leq e - s_n \leq \frac{1}{n} \cdot \frac{1}{n!}.$$

(b) Assume e is rational, and say a/b is the reduced fraction representing e. Apply the previous result to $n = b$ and arrive at a contradiction.

Problem III.3. Consider the *Fibonacci numbers*, define recursively by

$$F_0 = 0, F_1 = 1, \text{ and } F_n = F_{n-1} + F_{n-2} \qquad \text{for all} \qquad n \geq 2;$$

so the first few terms are

$$0, 1, 1, 2, 3, 5, 8, 13, \cdots .$$

For all $n \geq 2$, define the rational number r_n by the fraction $\frac{F_n}{F_{n-1}}$; so the first few terms are

$$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \cdots .$$

(a) Prove that for all $n \geq 4$, we have $r_n = r_{n-1} \vee r_{n-2}$.
(b) Prove that the sequence r_n converges (to a real number).
(c) Prove that r_n converges to the *golden ratio*:

$$\phi = \frac{1 + \sqrt{5}}{2}.$$

For this problem, you can use any result that you may have seen in your Calculus classes.

Problem III.4. Let $n > 0$ be any positive integer and p any prime number. Denote by $v_p(n)$ the exponent of p appearing in the prime decomposition of n.

(a) Let $k > 1$ be any natural number. **Prove that** there are exactly $\left\lfloor \frac{n}{p^k} \right\rfloor$ integers between 1 and n (inclusive) that are divisible by p^k.
(b) **Prove that** the series

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor := \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p} \right\rfloor + \cdots$$

is a finite sum and equals $v_p(n!)$.
(c) **Prove that** $v_p(n!) \leqslant \frac{n}{p-1}$.
(d) **Prove that** $v_p(\binom{2n}{n}) \leqslant \left\lfloor \frac{\log(2n)}{\log(p)} \right\rfloor$.

Hint. What are possible values of $\lfloor 2x \rfloor - 2\lfloor x \rfloor$?

(e) **Prove that** there is a constant $C > 0$ such that

$$\pi(x) \leqslant C \frac{x}{\log(x)},$$

where $\pi(x)$ equals the number of primes no larger than x (In this course, $\log = \log_e$ denotes the *natural logarithm*).

Hint. Try to apply above to

$$\log(\binom{2n}{n}) = \sum_{p \leqslant n} v_p(\binom{2n}{n}) \log(p)$$