

Chapter 2: Some Basic Notions of Set Theory

Author: Meng-Gen Tsai

Email: plover@gmail.com

Exercise 2.15. A real number is called algebraic if it is a root of an algebraic equation $f(x) = 0$, where $a_0 + a_1x + \cdots + a_nx^n = 0$ is a polynomial with integer coefficients. Prove that the set of all polynomials with integer coefficients is countable and deduce that the set of algebraic numbers is also countable.

Might assume $a_n \neq 0$.

For example, all rational numbers are algebraic since $p = \frac{\alpha}{\beta}$ (where $\alpha, \beta \in \mathbb{Z}$) is a root of $\beta x - \alpha = 0$.

Besides, $x = \sqrt{2} + \sqrt{3}$ is algebraic since $x^4 - 10x^2 + 1 = 0$. In fact, $x = \pm\sqrt{2} + \pm\sqrt{3}$ are also algebraic since $x^4 - 10x^2 + 1 = (x - \sqrt{2} - \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} + \sqrt{3})$.

Note. Countable set in the sense of Tom M. Apostol is equivalent to *at most countable set* in the sense of Walter Rudin.

Lemma. The set of all polynomials over \mathbb{Z} is countable implies that the set of algebraic numbers is countable.

Proof of Lemma. By definition, we write the set of algebraic numbers as

$$S = \bigcup_{f(x) \in \mathbb{Z}[x]} \{\alpha \in \mathbb{R} : f(\alpha) = 0\}.$$

Since each polynomial of degree n has at most n roots, $\{\alpha \in \mathbb{R} : f(\alpha) = 0\}$ is finite (or countable) for each given $f(x) \in \mathbb{Z}[x]$. So S is a countable union (by assumption) of countable sets, and hence countable by Theorem 2.27. \square

Now we show that *the set of all polynomials over \mathbb{Z} is countable*.

Proof (Walter Rudin). For every positive integer N there are only finitely many equations with $n + |a_0| + |a_1| + \cdots + |a_n| = N$. Write

$$P_N = \{f(x) \in \mathbb{Z}[x] : n + |a_0| + |a_1| + \cdots + |a_n| = N\}$$

where $f(x) = a_0 + a_1x + \cdots + a_nx^n$ with $a_n \neq 0$, and

$$P = \bigcup_{N=1}^{\infty} P_N.$$

P is the set of all polynomials over \mathbb{Z} .

Each P_N is finite (or countable) for given N (since the equation $n + |a_0| + |a_1| + \cdots + |a_n| = N$ has finitely many solutions $(n, a_0, a_1, \dots, a_n) \in \mathbb{Z}^{n+2}$). So P is a countable union of countable sets, and hence countable by Theorem 2.27. \square

Proof (Theorem 2.18).

- (1) \mathbb{Z}^N is countable for any integer $N > 0$. Induction on N and apply the same argument of Theorem 2.18.
- (2) The set of all polynomials over \mathbb{Z} is countable. Let

$$P_n = \{f \in \mathbb{Z}[x] : \deg f = n\},$$

and

$$P = \bigcup_{n=1}^{\infty} P_n = \mathbb{Z}[x].$$

Claim: P_n is countable. Define a one-to-one map $\varphi_n : P_n \rightarrow \mathbb{Z}^{n+1}$ by

$$\varphi_n(a_0 + a_1x + \cdots + a_nx^n) = (a_0, a_1, \dots, a_n).$$

By (1) and Theorem 2.16, P_n is countable. Now P is a countable union of countable sets, and hence countable by Theorem 2.27.

\square

Proof (Unique factorization theorem).

- (1) The set of prime numbers is countable. Write all primes in the ascending order as $p_1, p_2, \dots, p_n, \dots$ where $p_1 = 2, p_2 = 3, \dots, p_{10001} = 104743, \dots$ (See ProjectEuler 7: 10001st prime. Use sieve of Eratosthenes to get p_{10001} .)
- (2) The set of all polynomials over \mathbb{Z} is countable. Let

$$P_n = \{f \in \mathbb{Z}[x] : \deg f = n\},$$

and

$$P = \bigcup_{n=1}^{\infty} P_n = \mathbb{Z}[x].$$

Claim: P_n is countable. Define a map $\varphi_n : P_n \rightarrow \mathbb{Z}^+$ by

$$\varphi_n(a_0 + a_1x + \cdots + a_nx^n) = p_1^{\psi(a_0)} p_2^{\psi(a_1)} \cdots p_{n+1}^{\psi(a_n)},$$

where ψ is a one-to-one correspondence from \mathbb{Z} to \mathbb{Z}^+ . By the unique factorization theorem, φ_n is one-to-one. So P_n is countable by Theorem 2.16. Now P is a countable union of countable sets, and hence countable by Theorem 2.27.

\square