零知识证明笔记

谢文进

2023 年 4 月 18 日

目录

1 TO-DO

- 线性变换
- 不可约多项式

2 基本概念

2.1 数学概念

2.1.1 抽象代数

参考资料

- 《抽象代数》张贤科 清华大学出版社
- 《高等代数》(第三版) 北京大学数学系几何与代数教研室

定理 1 (古典代数学基本定理) *任意 n 次方程 $x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ 一定有复数解 (这里 $a_1, \cdots, a_n$ 为任意复数, 整数 $n \geq 1$).*

一个**集合**就是一些互异的确定的对象全体, 其中每个对象称为一个成员或元素, 简称为元, 有时也称为点。
映射三要素: 定义域、值域、对应规则。对任意两个不同的原像, 它们有不同的像, 则为**单射**。
以 (a, b) 或 $\gcd(a, b)$ 记 a, b 的正的最大公因子。

引理 1 *若 $a = bq + r$, 其中 a, b, r 为整数 (不全为 0), 则*

$$(a, b) = (r, b).$$

《高等代数》中有类似引理。

引理 2 (《高等代数》P13) 如果有等式

$$f(x) = q(x)g(x) + r(x) \tag{1}$$

成立，那么 $f(x), g(x)$ 和 $g(x), r(x)$ 有相同的公因式。

引理1中的公式 $(a, b) = (r, b)$ 说明：余数 r 可作为原数 a 的“替身”去参与求最大公因子，以此类推，引出著名的**“辗转相除法”**。

定理 2 任意两个整数 $a, b(b \neq 0)$ 的最大公因子 $d = (a, b)$ 是唯一存在的，即 $d = r_s$（就是 a 与 b 辗转相除的最后非零余数），而且存在整数 u, v 使

$$ua + vb = d \quad (\textbf{贝祖等式}, \textit{Bézout's identity}).$$

定义 1 (《抽象代数》张贤科 P17) 一个群就是一个非空集合 G，且其元素之间有一种运算，此运算将 G 中任意元素 a，b（可以相等）对应于 G 中的一个元素（记为 $a \cdot b$ 或 ab），而且满足如下 4 个条件（称为**群的公理**）：

($G1$) （封闭性）ab 仍然在 G 中（对任意 a，$b \in G$）；

($G2$) （结合律）$a(bc) = (ab)c$（对任意 $a, b, c \in G$）；

($G3$) （存在单位元）存在元素 $e \in G$ 使 $ea = ae = a$（对任意 $a \in G$）；

($G4$) （可逆性）对每个元素 $a \in G$，存在 $a' \in G$ 使 $a'a = aa' = e$.

满足交换律的群称为**交换群**，或 **Abel 群**。

由一个元素 a 生成的子群，称为**循环子群**，记为 $\langle a \rangle$. 如果群 $G = \langle a \rangle$，则 G 称为**循环群**.

定理 3 (算术基本定理，参考维基百科) 算术基本定理，又称为正整数的唯一分解定理，即：每个大于 1 的自然数，要么本身就是质数，要么可以写为 2 个或以上的质数的积，而且这些质因子按大小排列之后，写法仅有一种方式。

充分条件与必要条件

- 由条件能推出结论，但由结论推不出这个条件，这个条件就是充分条件。
- 如果能由结论推出条件，但由条件推不出结论，此条件为必要条件。
- 如果既能由结论推出条件，又能有条件推出结论，此条件为充要条件。

2.1.2 原根

参考oi-wiki 原根，一些数学概念如下：

定义 2 阶：由欧拉定理可知，对 $a \in \mathbb{Z}$，$m \in \mathbb{N}^*$，若 $\gcd(a, m) = 1$，则 $a^{\varphi(m)} \equiv 1 \pmod{m}$。因此满足同余式 $a^n \equiv 1 \pmod{m}$ 的最小正整数 n 存在，这个 n 称作 a 模 m 的阶，记作 $\delta_m(a)$。

定义 3 原根：设 $m \in \mathbb{N}^*$，$a \in \mathbb{Z}$。若 $\gcd(a, m) = 1$，且 $\delta_m(a) = \varphi(m)$，则称 a 为模 m 的原根。

定理 4 (原根判定定理) 设 $m \geqslant 3$, $\gcd(a, m) = 1$，则 a 是模 m 的原根的充要条件是，对于 $\varphi(m)$ 的每个素因数 p，都有 $a^{\frac{\varphi(m)}{p}} \neq 1 \pmod{m}$。

定理 5 (原根存在定理) 一个数 m 存在原根当且仅当 $m = 2, 4, p^\alpha, 2p^\alpha$，其中 p 为奇素数，$\alpha \in \mathbb{N}^*$。

2.2 计算复杂度

参考P/NP 问题:

- P 问题：复杂度类 P 即为所有可以由一个确定型图灵机在多项式表达的时间内解决的问题。
- NP 问题：类 NP 由所有可以在多项式时间内验证它的解是否正确的决定问题组成，或者等效的说，那些可以在非确定型图灵机上在多项式时间内找出解的问题的集合。