

第一章 集合、映射与逻辑初步

1.7 从解方程到一元多项式环

本章简介 我们从初中一年级开始就体会到,用字母 x 或 y 表示未知数,通过列方程和解方程求出未知数的值,对于解决实际问题非常有用。解方程是古典代数研究的中心问题,一次方程与二次方程自不必多言,初中阶段的课本已给出其求解公式与诸情况的讨论。我们一般认为,对于三次及以上的方程的基本方法是把方程左端的多项式因式分解。例如在复数域中解四次方程 $x^4 + 1 = 0$ 。先把方程左端的多项式因式分解为 $(x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$ 。于是 $x^4 + 1 = 0$ 的全部解是 $x_1 = \frac{\sqrt{2}}{2}(-1 + i)$, $x_2 = -\frac{\sqrt{2}}{2}(1 + i)$, $x_3 = \frac{\sqrt{2}}{2}(1 + i)$, $x_4 = \frac{\sqrt{2}}{2}(1 - i)$ 。为了把多项式因式分解,就需要研究多项式组成的集合,对于加法和乘法运算,它的结构是怎样的?

1.7.1 一元多项式环的概念

同学们熟悉的多项式,它的系数是实数。例如 $x^4 + 1, x^2 + \sqrt{2}x + 1, x^2 - 2x + 1, \dots$ 。同学们还知道,在多项式的等式中, x 可以用任一实数代入,例如 $(x-1)^2 = x^2 - 2x + 1$, x 用 200 代入,从而 $(200-1)^2 = 200^2 - 2 \cdot 200 + 1$, 由此简便地计算出 $199^2 = 40000 - 400 + 1 = 39601$ 。

为了使多项式的应用更广,我们来考虑系数属于任一数域 K (或任一域 F) 的多项式,并且使得在多项式的等式中, x 不仅可以用数域 K 中的数 (或域 F 中的元素) 代入,而且还可以用数域 K (或域 F) 上的 m 级矩阵 A 等代入。为此对于多项式的概念作如下的定义。

定义 1.7.1. 设 F 是一个域, x 是一个不属于 F 的符号。域 F 上的一元多项式是指形如 $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ 的表达式,其中 $n \in \mathbb{N}$, $a_i \in F$, $i = 0, 1, \dots, n$, 并且 $a_n \neq 0$, 或者 $a_n = a_{n-1} = \dots = a_0 = 0$ 。两个这样的表达式相等,规定为它们除去系数为零的项外其余项的系数都相等。此时,符号 x^k 称为第 k 次项, a_0 称为零次项,也称为常数项。系数全为 0 的多项式称为零多项式,记为 0。

在多项式 $f(x) = a_n x^n + \dots + a_0$ 中,如果 $a_n \neq 0$, 那么称 $a_n x^n$ 为 $f(x)$ 的首项,称 n 为 $f(x)$ 的次数,记做 $\deg f(x)$ 。零多项式的次数定义为 $-\infty$, 并规定 $-\infty < n$, $(-\infty) + n = -\infty$, $(-\infty) + (-\infty) = -\infty$, 其中 n 是任意非负整数。

零次多项式如 a , 其中 $a \in F$ 且 $a \neq 0$ (即 $a \in F^*$), 可以把零次多项式 a 与 F 中的非零元 a 等同看待。域 F 上的所有一元多项式组成的集合记做 $F[x]$ 。

类似于初中数学讲的多项式的加法和乘法,在 $F[x]$ 中规定加法和乘法运算如下: 设 $f(x) = \sum_{i=0}^n a_i x^i$, $g(x) = \sum_{i=0}^m b_i x^i$, 不妨设 $n \geq m$, 则 $f(x) + g(x) := \sum_{i=0}^n (a_i + b_i) x^i$, $f(x)g(x) := \sum_{s=0}^{n+m} f_t \left(\sum_{i+j=s} a_i b_j \right) x^s$ 。

容易验证,上面所定义的多项式的加法与乘法满足下列运算规则:

1. $f(x) + g(x) = g(x) + f(x)$ (加法交换律);
2. $(f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x))$ (加法结合律);

3. $0 + f(x) = f(x) + 0 = f(x)$;
4. 若 $f(x) = \sum_{i=0}^n a_i x^i$, 定义 $-f(x) = \sum_{i=0}^n (-a_i) x^i$, 则 $f(x) + (-f(x)) = (-f(x)) + f(x) = 0$, 称 $-f(x)$ 是 $f(x)$ 的负元素;
5. $f(x)g(x) = g(x)f(x)$ (乘法交换律);
6. $f(x)(g(x)h(x)) = (f(x)g(x))h(x)$ (乘法结合律);
7. $1f(x) = f(x)1 = f(x)$, 其中 1 是域 F 的单位元;
8. $f(x)(g(x) + h(x)) = f(x)g(x) + f(x)h(x)$, $(g(x) + h(x))f(x) = g(x)f(x) + h(x)f(x)$ (左分配律、右分配律)。

因此, $F[x]$ 成为一个有单位元的交换环, 称为域 F 上的一元多项式环。一元多项式的减法运算规定如下: $f(x) - g(x) := f(x) + (-g(x))$ 。

一元多项式的重要特点是它有次数的概念。多项式的运算与次数的关系如下。

命题 1.7.2. 设 $f(x), g(x) \in F[x]$, 则 $\deg(f(x)+g(x)) \leq \max\{\deg f(x), \deg g(x)\}$, $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$ 。

证明. 如果 $f(x)$ 或 $g(x)$ 是零多项式, 结论显然。设 $f(x) = \sum_{i=0}^n a_i x^i$, $g(x) = \sum_{i=0}^m b_i x^i$, 其中 $a_n \neq 0, b_m \neq 0$, 不妨设 $n \geq m$ 。由加法公式, $\deg(f(x) \pm g(x)) \leq n = \max\{\deg f(x), \deg g(x)\}$ 。又因为 $a_n b_m \neq 0$, $a_n b_m x^{n+m}$ 是 $f(x)g(x)$ 的首项, 所以 $\deg(f(x)g(x)) = n + m$ 。□

由命题 1 的证明可看出, 如果 $f(x) \neq 0, g(x) \neq 0$, 那么 $f(x)g(x) \neq 0$ 。因此 $F[x]$ 没有非零的零因子, 并且可以得到一元多项式的乘法满足消去律, 即

命题 1.7.3. 若 $f(x)g(x) = f(x)h(x)$, 且 $f(x) \neq 0$, 则 $g(x) = h(x)$ 。

证明.

由 $f(x)g(x) = f(x)h(x)$ 可得 $f(x)(g(x) - h(x)) = 0$ 。由于 $f(x) \neq 0$, 所以 $g(x) - h(x) = 0$, 即 $g(x) = h(x)$ 。□

在 $F[x]$ 中, $(x-1)^2 = x^2 - 2x + 1$, 设 A 是域 F 上的 r 级矩阵, I 是域 F 上的 r 级单位矩阵, 则 $(A-I)^2 = A^2 - 2A + I$ 。由此看出, 在 $F[x]$ 中, 不定元 x 可以用域 F 上的 r 级矩阵 A 代入。

定理 1.7.4. 设 A 是域 F 上的任一个 r 级矩阵。如果在 $F[x]$ 中有下列等式: $f(x)+g(x)=h(x)$, $f(x)g(x)=p(x)$, 那么用矩阵 A 代入后仍有 $f(A)+g(A)=h(A)$, $f(A)g(A)=p(A)$ 。

证明.

设 $f(x) = \sum_{i=0}^n a_i x^i$, $g(x) = \sum_{i=0}^m b_i x^i$, 不妨设 $n \geq m$ 。按定义, $h(x) = \sum_{i=0}^n (a_i + b_i) x^i$, $p(x) = \sum_{s=0}^{n+m} (\sum_{i+j=s} a_i b_j) x^s$ 。又 $f(A) = \sum_{i=0}^n a_i A^i$, $g(A) = \sum_{i=0}^m b_i A^i$, 所以 $h(A) = \sum_{i=0}^n (a_i + b_i) A^i$, $p(A) = \sum_{s=0}^{n+m} (\sum_{i+j=s} a_i b_j) A^s$ 。根据矩阵的加法、数乘和乘法的运算法则, 立即得到 $f(A) + g(A) = h(A)$ 及 $f(A)g(A) = p(A)$ 。□

类似地, 如果 $F[x]$ 中有等式 $f(x) + g(x) = h(x)$ 、 $f(x)g(x) = p(x)$, 则 $x + c$ 、 x^m 以及 $q(x)$ 都可以分别代入, 得到相应的等式。这种性质是一元多项式环 $F[x]$ 的通用性质。

习题 2.1

1. 在 $F[x]$ 中, 如果 $f(x) = cg(x)$, 其中 $c \in F^*$, 试问: $f(x)$ 与 $g(x)$ 的次数有什么关系?
2. 在 $F[x]$ 中, 如果 $f(x)g(x) = c$, 其中 $c \in F^*$, 试问: $f(x)$ 与 $g(x)$ 的次数有什么关系?
3. 在 $F[x]$ 中, 如果 $f(x)$ 与 $g(x)$ 的次数都是 3, 试问: $f(x) + g(x)$ 的次数一定是 3 吗?
4. 证明: $F[x]$ 中一个元素 $f(x)$ 是可逆当且仅当 $f(x)$ 是零次多项式, 即 $f(x) = a$, 其中 $a \in F^*$ 。
5. 在复数域中解下列方程:

$$(1) x^4 - 4 = 0;$$

$$(2) x^3 + 1 = 0.$$

6. 在 $\mathbb{Z}_2[x]$ 中, 计算:

$$(1) (x + \bar{1})^2;$$

$$(2) x(x + \bar{1})(x^2 + x + \bar{1}).$$

7. 在 $\mathbb{Z}_2[x]$ 中, 把下列多项式因式分解:

$$(1) x^2 + \bar{1};$$

$$(2) x^4 + x;$$

$$(3) x^3 + x^2 + x + \bar{1}.$$

1.7.2 带余除法, 整除关系

在域 F 上的一元多项式环 $F[x]$ 中, 可以做加法、减法、乘法运算, 但不能做除法。例如在 $\mathbb{R}[x]$ 中, 用 $g(x) = x^2 + 2x - 1$ 去除 $f(x) = 2x^3 + 3x^2 + 5$ 是除不尽的, 结果为 $2x^3 + 3x^2 + 5 = (2x - 1)(x^2 + 2x - 1) + (4x + 4)$ 。

从这个例子受到启发, 类比上一章整数带余除法的相关定理, 猜想有下述定理:

定理 1.7.5. 设 $f(x), g(x) \in F[x]$, 且 $g(x) \neq 0$, 则在 $F[x]$ 中存在唯一的一对多项式 $h(x), r(x)$, 使得 $f(x) = h(x)g(x) + r(x)$, $\deg r(x) < \deg g(x)$ 。

式中的 $h(x), r(x)$ 分别称为 $g(x)$ 除 $f(x)$ 所得的商式、余式。

既然域 F 上一元多项式环 $F[x]$ 也有带余除法, 这使我们直觉判断 $F[x]$ 与整数环 $\mathbb{Z}$ 有类似的结构。下面我们运用类比推理研究 $F[x]$ 的结构。类比推理在日常生活中经常运用, 而数学的思维方式告诉我们, 类比推理的结果是真是假, 必须进行论证。

若余式 $r(x) = 0$, 则称 $g(x)$ 整除 $f(x)$, 类比整数环中的整除概念, 得到下述定义。

定义 1.7.6. 设 $f(x), g(x) \in F[x]$, 如果存在 $h(x) \in F[x]$, 使得 $f(x) = h(x)g(x)$, 那么称 $g(x)$ 整除 $f(x)$, 记做 $g(x) \mid f(x)$; 否则称 $g(x)$ 不能整除 $f(x)$, 记做 $g(x) \nmid f(x)$. 当 $g(x) \mid f(x)$ 时称 $g(x)$ 是 $f(x)$ 的一个因式, 称 $f(x)$ 是 $g(x)$ 的一个倍式。

特别地, $0 \mid 0$, 因为 $0 = 0 \cdot f(x)$. 对任意 $b \in F^*$, $b \mid f(x)$, $\forall f(x) \in F[x]$, 即任意一个零次多项式都是任一多项式的因式。

问题 1.1 判断整除关系是否具有反身性、对称性、传递性。

定义 1.7.7 (相伴). 在 $F[x]$ 中, 如果 $g(x) \mid f(x)$ 且 $f(x) \mid g(x)$, 那么称 $f(x)$ 与 $g(x)$ 相伴, 记做 $f(x) \sim g(x)$ 。

在 $F[x]$ 中, 怎样的两个多项式才相伴呢? 首先探索 $f(x)$ 与 $g(x)$ 相伴的必要条件. 设 $f(x) \sim g(x)$, 则 $g(x) \mid f(x)$ 且 $f(x) \mid g(x)$. 于是存在 $h_1(x), h_2(x) \in F[x]$, 使得 $f(x) = h_1(x)g(x)$, $g(x) = h_2(x)f(x)$. 由此得出 $f(x) = h_1(x)h_2(x)f(x)$. 若 $f(x) \neq 0$, 则两边消去 $f(x)$ 得 $1 = h_1(x)h_2(x)$ 。

于是 $0 = \deg h_1(x) + \deg h_2(x)$. 从而 $\deg h_1(x) = \deg h_2(x) = 0$. 因此 $h_1(x) = c$, 对某个 $c \in F^*$, 于是 $f(x) = cg(x)$. 若 $f(x) = 0$, 则 $g(x) = 0$. 从而相伴的必要条件是: 存在 $c \in F^*$, 使得 $f(x) = cg(x)$ 。

显然, (3) 式也是 $f(x)$ 与 $g(x)$ 相伴的充分条件. 于是我们证明了下述命题:

命题 1.7.8. 在 $F[x]$ 中, $f(x) \sim g(x)$ 当且仅当存在 $c \in F^*$, 使得 $f(x) = cg(x)$ 。

类似于整数环的情形, 在 $F[x]$ 中, 整除关系还具有下述性质:

命题 1.7.9. 在 $F[x]$ 中, 如果 $g(x) \mid f_i(x)$, $i = 1, 2, \dots, s$, 那么对于任意 $u_i(x) \in F[x]$, 有 $g(x) \mid u_1(x)f_1(x) + u_2(x)f_2(x) + \dots + u_s(x)f_s(x)$ 。

留做习题。

本节开始举的例子, 在 $\mathbb{R}[x]$ 中, $g(x) \nmid f(x)$. 试问: 在 $\mathbb{C}[x]$ 中, $g(x)$ 能否整除 $f(x)$ 呢? 假如在 $\mathbb{C}[x]$ 中, $g(x) \mid f(x)$, 则 $g(x)$ 去除 $f(x)$ 所得的余式为 0. 在本节开始已知道, 在 $\mathbb{R}[x]$ 中, $f(x) = (2x - 1)g(x) + (4x + 4)$. 由于 $f(x), g(x), 2x - 1, 4x + 4 \in \mathbb{C}[x]$, 因此也可看成是在 $\mathbb{C}[x]$ 中做的带余除法, 余式为 $4x + 4$, 这与带余除法中余式的唯一性矛盾. 因此在 $\mathbb{C}[x]$ 中也有 $g(x) \nmid f(x)$. 这一推理过程一样, 可证得下述命题:

命题 1.7.10. 设 $f(x), g(x) \in F[x]$, 域 $E \supset F$, 则在 $F[x]$ 中, $g(x) \mid f(x) \iff$ 在 $E[x]$ 中, $g(x) \mid f(x)$ 。

这一个性质称为整除关系不随域的扩大而改变。

例题 1.7.1. 在 $\mathbb{Z}_2[x]$ 中, 用 $g(x) = x^4 + x^3 + \bar{1}$ 去除 $f(x) = x^6 + x^4 + x^2 + \bar{1}$, 求商式和余式。

$x^4 + x^3 + \bar{1} \mid x^6 + x^4 + x^2 + \bar{1}$, 带余除法所得商式为 $x^2 + x$, 余式为 $x + \bar{1}$. 因此 $x^6 + x^4 + x^2 + \bar{1} = (x^2 + x)(x^4 + x^3 + \bar{1}) + (x + \bar{1})$ 。

设 K 是数域, 在 $K[x]$ 中作带余除法, 如果除式是一次多项式 $x + b$, 那么可以采用如下所示的综合除法。

例题 1.7.2. 在 $K[x]$ 中, 用 $x - 2$ 去除 $f(x) = 2x^4 - 6x^3 + 3x^2 - 2x + 5$, 求商式和余式。

综合除法的计算得到商式 $2x^3 - 2x^2 - x - 4$, 余式是 -3 。因此 $f(x) = (2x^3 - 2x^2 - x - 4)(x - 2) - 3$ 。

习题 1.8.2

1. 在 $\mathbb{R}[x]$ 中, 用 $g(x) = x^2 - 2x + 5$ 去除 $f(x) = x^4 - 3x^2 - 2x - 1$, 求商式和余式。
2. 在 $\mathbb{Z}_2[x]$ 中, 用 $g(x) = x^4 + x^2 + \bar{1}$ 去除 $f(x) = x^{10} + x^5 + \bar{1}$, 求商式和余式。
3. 证明 $F[x]$ 中整除关系的传递性, 即若 $h(x) \mid g(x)$, 且 $g(x) \mid f(x)$, 则 $h(x) \mid f(x)$ 。
4. 证明本节的命题 2。
5. 用综合除法求一次多项式 $g(x)$ 除 $f(x)$ 所得的商式和余式:
 - (1) $f(x) = 3x^4 - 5x^2 + 2x - 1$, $g(x) = x - 4$;
 - (2) $f(x) = 5x^3 - 3x + 4$, $g(x) = x + 2$ 。

- 1.
- 2.
- 3.
- 4.
- 5.

1.7.3 最大公因式

类比两个整数的最大公因数, 我们得到一元多项式的最大公因式的概念。

定义 1.7.11 (最大公因式). 设 $f(x), g(x) \in F[x]$, 如果存在 $d(x) \in F[x]$ 满足 $d(x) \mid f(x)$ 且 $d(x) \mid g(x)$ (此时称 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的一个公因式) 且对于 $f(x)$ 与 $g(x)$ 的任一个公因式 $c(x)$, 都有 $c(x) \mid d(x)$, 那么称 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的一个最大公因式。

设 $f(x) \in F[x]$, 可知 $f(x)$ 是 $f(x)$ 与 0 的一个公因式。特别地, 0 是 0 与 0 的最大公因式。

对于 $F[x]$ 中任意两个非零多项式 $f(x)$ 与 $g(x)$, 它们的最大公因式是否存在? 如果存在, 如何求出来? 是两题一起解决这些问题的出发点。从带余除法的算式要启发, 在 $F[x]$ 中, 如果有下式成立: $f(x) = h(x)g(x) + r(x)$, 那么根据上一节的命题 2, 容易得出 $c(x) \mid f(x)$ 且 $c(x) \mid g(x) \iff c(x) \mid g(x)$ 且 $c(x) \mid r(x)$, 从而得出: $d(x)$ 是 $f(x)$ 与 $g(x)$ 的最大公因式 $\iff d(x)$ 是 $g(x)$ 与 $r(x)$ 的最大公因式。

这表明: 利用带余除法可以把被除式与除式的最大公因式转化为求除式与余式的最大公因式。沿着这一思路, 对于 $F[x]$ 中任意两个多项式 $f(x), g(x) \neq 0$, 有 $f(x) = h_1(x)g(x) + r_1(x)$, $\deg r_1(x) < \deg g(x)$; 若 $r_1(x) \neq 0$, 则有 $g(x) = h_2(x)r_1(x) + r_2(x)$, $\deg r_2(x) < \deg r_1(x)$; 若 $r_2(x) \neq 0$, 则有 $r_1(x) = h_3(x)r_2(x) + r_3(x)$, $\deg r_3(x) < \deg r_2(x)$; 只要余式不为 0, 就可以用余式去除除式, 作带余除法。注意到每作一次带余除法, 余式的次数在降低。由于非零多项式的次数是自然数, 因此在有限步之后, 必有余式为 0。于是最后几步为 $r_{s-2}(x) = h_s(x)r_{s-1}(x) + r_s(x)$, $\deg r_s(x) < \deg r_{s-1}(x)$; $r_{s-1}(x) = h_{s+1}(x)r_s(x) + 0$ 。

由于 $r_s(x)$ 是 $r_s(x)$ 与 0 的一个最大公因式, 因此 $r_s(x)$ 是 $r_{s-1}(x)$ 与 $r_s(x)$ 的一个最大公因式, 依次往上推, 最后得 $r_s(x)$ 是 $f(x)$ 与 $g(x)$ 的一个最大公因式。这种方法为辗转相除法。

从上述一系列等式中的倒数第二个等式开始可得 $r_s(x) = r_{s-2}(x) - h_s(x)r_{s-1}(x) = r_{s-2}(x) - h_s(x)(r_{s-3}(x) - h_{s-1}(x)r_{s-2}(x)) = -h_s(x)r_{s-3}(x) + (1 + h_s(x)h_{s-1}(x))r_{s-2}(x) = \dots = u(x)f(x) + v(x)g(x)$, 其中 $u(x), v(x) \in F[x]$ 。

从上述推导过程得到下述重要定理:

定理 1.7.12. 对于 $F[x]$ 中任意两个多项式 $f(x), g(x)$, 存在它们的一个最大公因式 $d(x)$, 并且 $d(x)$ 可以表示成 $f(x)$ 与 $g(x)$ 的倍式和, 即存在 $u(x), v(x) \in F[x]$, 使得 $u(x)f(x) + v(x)g(x) = d(x)$ 。

证明. 若 $g(x) = 0$, 则 $f(x)$ 是 $f(x)$ 与 0 的一个最大公因式, 并且 $f(x) = 1 \cdot f(x) + 1 \cdot 0$ 。若 $g(x) \neq 0$, 则用 $g(x)$ 去除 $f(x)$, 作带余除法。上面的推导过程已证明了定理 1 的结论。□

若 $d_1(x)$ 和 $d_2(x)$ 都是 $f(x)$ 与 $g(x)$ 的最大公因式, 则 $d_1(x) \mid d_2(x)$ 且 $d_2(x) \mid d_1(x)$, 因此 $d_1(x) \sim d_2(x)$ 。这表明 $f(x)$ 与 $g(x)$ 的最大公因式不唯一, 但是在相伴的意义下是唯一的。

设 $f(x)$ 与 $g(x)$ 不全为 0, 则它们的最大公因式一定是非零多项式, 用 $(f(x), g(x))$ 表示首项系数为 1 的那个最大公因式, 简称首一最大公因式。

例题 1.7.3. 设 $f(x) = x^3 + x^2 - 7x + 2$, $g(x) = 3x^2 - 5x - 2$, 求 $(f(x), g(x))$, 并且把它表示成 $f(x)$ 与 $g(x)$ 的倍式和。

在作辗转相除法时, 可以用适当的非零数去乘被除式或除式, 以便使计算简单一些。具体的算式如下:

$3f(x)$	$g(x)$	$x + \frac{8}{3} = h_1(x)$
$3x^2 - 5x - 2$	$3x^3 + 3x^2 - 21x + 6$	
$3x^3 - 6x^2 - 2x$	$3x^3 - 5x^2 - 2x$	
$x - 2$	$8x^2 - 19x + 6$	
$x - 2$	$8x^2 - \frac{40}{3}x - \frac{16}{3}$	
0	$\frac{3}{17}$	$\frac{34}{17}$
0	$r_1(x) = -\frac{17}{17}x + \frac{17}{17}$	
0	$-\frac{3}{17}r_1(x) = x - 2$	

因为最后一个不等于零的余式是 $r_1(x)$, 所以 $(f(x), g(x)) = x - 2$ 。把上述辗转相除过程写出来就是 $3f(x) = (x + \frac{8}{3})g(x) + r_1(x)$, $g(x) = (3x + 1)(-\frac{3}{17}r_1(x)) + 0$ 。于是 $(f(x), g(x)) = -\frac{3}{17}r_1(x) = -\frac{3}{17}[3f(x) - (x + \frac{8}{3})g(x)] = -\frac{9}{17}f(x) + \frac{1}{17}(3x + 8)g(x)$ 。

1.7.4 互素的多项式

两个多项式的最大公因式是零次多项式特别重要, 这与整数环类似。

定义 1.7.13 (互素). 设 $f(x), g(x) \in F[x]$, 如果 $(f(x), g(x)) = 1$, 那么称 $f(x)$ 与 $g(x)$ 互素。

由定义 2 立即得到: $f(x)$ 与 $g(x)$ 互素 $\iff f(x)$ 与 $g(x)$ 的公因式都是零次多项式。由定理 1 立即得到, $f(x)$ 与 $g(x)$ 互素的必要条件是: 存在 $u(x), v(x) \in F[x]$, 使得 $u(x)f(x) + v(x)g(x) = 1$ 。反之, 如果这个等式成立, 那么对于 $f(x)$ 与 $g(x)$ 的任一公因式 $c(x)$, 有 $c(x) \mid 1$ 。从而 $c(x)$ 是零次多项式, 因此 $(f(x), g(x)) = 1$ 。这证明了下述重要定理:

定理 1.7.14. 在 $F[x]$ 中两个多项式 $f(x)$ 与 $g(x)$ 互素的充分必要条件是: 存在 $u(x), v(x) \in F[x]$, 使得 $u(x)f(x) + v(x)g(x) = 1$ 。

类似于整数环的情形, 利用定理 2 可以证明关于互素的多项式的一些重要性质:

1. 若 $f(x) \mid g(x)h(x)$, 且 $(f(x), g(x)) = 1$, 则 $f(x) \mid h(x)$ 。
2. 若 $f(x) \mid h(x)$, $g(x) \mid h(x)$, 且 $(f(x), g(x)) = 1$, 则 $f(x)g(x) \mid h(x)$ 。
3. 若 $(f(x), h(x)) = 1$, 且 $(g(x), h(x)) = 1$, 则 $(f(x)g(x), h(x)) = 1$ 。
4. 可以推广成: 若 $(f_i(x), h(x)) = 1$, $i = 1, 2, \dots, s$, 则 $(f_1(x)f_2(x) \cdots f_s(x), h(x)) = 1$ 。

上述性质的证明留作习题。

与证明整除关系不随域的扩大而改变的方法类似, 可证明:

命题 1.7.15. 设 $f(x), g(x) \in F[x]$, 域 $E \supset F$, 则在 $F[x]$ 中 $f(x)$ 与 $g(x)$ 的首一最大公因式也是它们在 $E[x]$ 中的首一最大公因式, 称为 $f(x)$ 与 $g(x)$ 的首一最大公因式不随域的扩大而改变。

由命题 1 立即得到: 设 $f(x), g(x) \in F[x]$, 域 $E \supset F$, 则在 $F[x]$ 中, $(f(x), g(x)) = 1 \iff$ 在 $E[x]$ 中, $(f(x), g(x)) = 1$, 即互素性不随域的扩大而改变。

习题

1. 求 $(f(x), g(x))$, 并且把 $(f(x), g(x))$ 表示成 $f(x)$ 与 $g(x)$ 的倍式和:
2. $f(x) = x^4 + 6x^3 - 6x^2 + 6x - 7$, $g(x) = x^3 + x^2 - 7x + 5$;
3. $f(x) = x^4 + 3x^3 - x^2 + 4x - 3$, $g(x) = 3x^3 + 10x^2 + 2x - 3$ 。
4. 证明: 在 $F[x]$ 中, 若 $u(x)f(x) + v(x)g(x) = d(x)$, 且 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的一个公因式, 则 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的一个最大公因式。
5. 设 $f(x), g(x), h(x) \in F[x]$, 且 $h(x)$ 的首项系数为 1, 证明: $(f(x)h(x), g(x)h(x)) = (f(x), g(x))h(x)$ 。
6. 证明关于互素的多项式的三条性质。
7. 证明: 在 $F[x]$ 中, 如果 $f(x)$ 与 $g(x)$ 不全为 0, 那么 $\leq \left(\frac{f(x)}{(f(x), g(x))}, \frac{g(x)}{(f(x), g(x))} \right) = 1$ 。
8. 证明: 在 $F[x]$ 中, 如果 $(f(x), g(x)) = 1$, 那么 $((f(x)g(x)), f(x) + g(x)) = 1$ 。

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.

1.7.5 不可约多项式, 唯一因式分解定理

研究整数环的结构, 我们抓住了素数的特征。素数的特征是它的正因数最少: 只有 1 和它自身。类比地, 研究域 F 上一元多项式环 $F[x]$ 的结构, 应当抓住多项式的特征。我们知道, 零次多项式是任一多项式的因式, $f(x)$ 的相伴就是 $f(x)$ 的因式。由此引出了下述重要概念:

定义 1.7.16 (可约, 不可约). $F[x]$ 中一个次数大于 0 的多项式 $f(x)$, 如果它在 $F[x]$ 中的因式只有零次多项式和 $f(x)$ 的相伴, 称 $f(x)$ 是域 F 上的一个不可约多项式; 否则, 称 $f(x)$ 在域 F 上是可约的。

域 F 上的不可约多项式起着基本建筑块的作用。为此需要进一步研究不可约多项式的特征性质。类似于对素数的各种刻画, 对不可约多项式也有各种刻画:

定理 1.7.17. 设 $p(x)$ 是 $F[x]$ 中的一个次数大于 0 的多项式, 则下列命题等价:

1. $p(x)$ 是域 F 上的不可约多项式;
2. 对于 $F[x]$ 中任一多项式 $f(x)$ 都有 $(p(x), f(x)) = 1$ 或 $p(x) \mid f(x)$;
3. 在 $F[x]$ 中, 从 $p(x) \mid f(x)g(x)$ 可推出 $p(x) \mid f(x)$ 或 $p(x) \mid g(x)$;
4. 在 $F[x]$ 中, $p(x)$ 不能分解成两个次数都低于 $p(x)$ 的次数的多项式的乘积。

证明. (1) $\Rightarrow$ (2): 设 $p(x)$ 是域 F 上的不可约多项式。对于任意 $f(x) \in F[x]$, 由于 $(p(x), f(x))$ 是 $p(x)$ 的一个因式, 因此 $(p(x), f(x)) = 1$ 或 $(p(x), f(x)) \sim p(x)$ 。从而得出, $(p(x), f(x)) = 1$ 或 $p(x) \mid f(x)$ 。

(2) $\Rightarrow$ (3): 设在 $F[x]$ 中, $p(x) \mid f(x)g(x)$ 。若 $p(x) \nmid f(x)$, 则据 (2) 得 $(p(x), f(x)) = 1$ 。从而 $p(x) \mid g(x)$ 。

(3) $\Rightarrow$ (4): 假如 $p(x) = p_1(x)p_2(x)$, 且 $\deg p_i(x) < \deg p(x)$, $i = 1, 2$, 则 $p(x) \mid p_1(x)p_2(x)$ 。据 (3) 得 $p(x) \mid p_1(x)$ 或 $p(x) \mid p_2(x)$ 。于是有 $\deg p_1(x) \geq \deg p(x)$ 或 $\deg p_2(x) \geq \deg p(x)$, 矛盾。因此 $p(x)$ 不能分解成两个次数都低于 $p(x)$ 的次数的多项式的乘积。

(4) $\Rightarrow$ (1): 任取 $p(x)$ 在 $F[x]$ 中的一个因式 $g(x)$, 则存在 $h(x) \in F[x]$, 使得 $p(x) = h(x)g(x)$ 。于是 $\deg p(x) = \deg h(x) + \deg g(x)$ 。据 (4) 得, $\deg h(x) = \deg p(x)$ 或 $\deg g(x) = \deg p(x)$, 从而 $\deg g(x) = 0$ 或 $\deg h(x) = 0$ 。从后者推出 $p(x) \sim g(x)$, 对于某个 $c \in F^*$, 于是 $p(x) \sim g(x)$ 。因此 $p(x)$ 在域 F 上不可约。 $\square$

从定理 1 中命题 (3) 与命题 (1) 等价, 运用数学归纳法可证明:

推论 1.7.18. 在 $F[x]$ 中, 若 $p(x)$ 不可约, 且 $p(x) \mid f_1(x)f_2(x)\cdots f_s(x)$, 则 $p(x) \mid f_j(x)$, 对于某个 $j \in \{1, 2, \dots, s\}$ 。

从定理 1 中命题 (4) 与命题 (1) 等价, 立即得出:

推论 1.7.19. $F[x]$ 中每一个一次多项式都是不可约的。

推论 3: $F[x]$ 中每一个次数大于 0 的多项式 $f(x)$ 都可以分解成域 F 上有限多个不可约多项式的乘积。

进一步可以证明这样的分解是唯一的。唯一性是指, 如果 $f(x)$ 有两个这样的分解: $f(x) = p_1(x)p_2(x)\cdots p_s(x) = q_1(x)q_2(x)\cdots q_t(x)$, 其中 $p_1(x), \dots, p_s(x), q_1(x), \dots, q_t(x)$ 都是域 F 上的不可约多项式, 我们对 $f(x)$ 的第一个分解中不可约多项式的个数 s 作数学归纳法。

当 $s = 1$ 时, $f(x) = p_1(x)$, 于是 $p_1(x) = q_1(x)q_2(x)\cdots q_t(x)$ 。由推论 1, $p_1(x) \mid q_j(x)$, 对于某个 j 。不妨设 $j = 1$, 则 $p_1(x) \sim q_1(x)$ 。从而 $t = 1$, 且适当排列因式的次序后, 有 $p_1(x) \sim q_1(x)$ 。

假设当 $s-1$ 时, 唯一性成立。现在来看 s 的情形。由上面的推论, $p_1(x) \mid q_1(x)q_2(x)\cdots q_t(x)$ 。不妨设 $p_1(x) \mid q_1(x)$ 。由于 $q_1(x)$ 不可约, 因此 $p_1(x) \sim q_1(x)$ 。从而由 (1) 式得 $p_2(x)\cdots p_s(x) \sim q_2(x)\cdots q_t(x)$ 。归纳假设, $s = t$, 且适当排列因式的次序后, 有 $p_i(x) \sim q_i(x)$, $i = 1, 2, \dots, s$ 。
□

定理 1.7.20 (唯一因式分解定理). $F[x]$ 中每一个次数大于 0 的多项式 $f(x)$ 都能唯一地分解成域 F 上不可约多项式的乘积。唯一性是指: 如果 $f(x) = p_1(x)p_2(x)\cdots p_s(x) = q_1(x)q_2(x)\cdots q_s(x)$, 其中各 $p_i(x), q_i(x)$ 都是域 F 上的不可约多项式, 则适当排列因式的次序后, 有 $p_i(x) \sim q_i(x)$, $i = 1, 2, \dots, s$ 。

在 $F[x]$ 中, 次数大于 0 的多项式 $f(x)$ 的分解式可以写成 $f(x) = ap_1^{r_1}(x)p_2^{r_2}(x)\cdots p_m^{r_m}(x)$, 其中 a 是 $f(x)$ 的首项系数; $p_1(x), p_2(x), \dots, p_m(x)$ 是两两不等的首一不可约多项式, $r_i > 0$ ($i = 1, 2, \dots, m$), $p_i^{r_i}(x) = [p_i(x)]^{r_i}$ 。式 (3) 称为 $f(x)$ 的标准分解。

在 $F[x]$ 中, 设次数大于 0 的多项式 $f(x), g(x)$ 的标准分解式分别为 $f(x) = ap_1^{r_1}(x)\cdots p_t^{r_t}(x)p_{t+1}^{r_{t+1}}(x)\cdots p_s^{r_s}(x)$, $g(x) = bp_1^{s_1}(x)\cdots p_t^{s_t}(x)q_{t+1}^{s_{t+1}}(x)\cdots q_l^{s_l}(x)$, 则 $f(x)$ 与 $g(x)$ 的首一最大公因式为 $(f(x), g(x)) = p_1^{\min\{r_1, s_1\}}(x)\cdots p_t^{\min\{r_t, s_t\}}(x)$; $f(x)$ 与 $g(x)$ 的首一最小公倍式为 $[f(x), g(x)] = p_1^{\max\{r_1, s_1\}}(x)\cdots p_t^{\max\{r_t, s_t\}}(x)\cdots q_{t+1}^{s_{t+1}}(x)\cdots q_l^{s_l}(x)$ 。

由于把一个多项式的标准分解式写出来比较困难, 因此实际求 $f(x)$ 与 $g(x)$ 的最大公因式时最常用的方法是辗转相除法。

在 $f(x)$ 的标准分解式 (3) 中, 称 $p_i(x)$ 是 $f(x)$ 的 r_i 重因式。由于把多项式因式分解是比较困难的, 因此我们不通过标准分解式来定义重因式, 而采取下面方法定义重因式:

定义 1.7.21. 在 $F[x]$ 中, 不可约多项式 $p(x)$ 称为多项式 $f(x)$ 的 k 重因式, 如果 $p^k(x) \mid f(x)$, 而 $p^{k+1}(x) \nmid f(x)$ 。当 $k = 0$ 时, $p(x)$ 不是 $f(x)$ 的因式; 当 $k = 1$ 时, $p(x)$ 称为 $f(x)$ 的单因式; 当 $k \geq 2$ 时, $p(x)$ 称为 $f(x)$ 的 k 重因式。若 $k > 1$, 则 $p(x)$ 称为 $f(x)$ 的重因式。

习题 2.4

1. 分别在实数域 $\mathbb{R}$ 、复数域 $\mathbb{C}$ 上把下列多项式分解成不可约式的乘积:

(1) $x^4 + x^2 + 1$;

(2) $x^3 - 1$;

(3) $x^6 - 1$;

(4) $x^4 + 4$;

(5) $x^6 + 1$;

$$(6) x^{12} - 1.$$

2. 下列多项式在有理数域 $\mathbb{Q}$ 上是否可约?

$$(1) x^3 + x^2 + x + 1;$$

$$(2) x^5 + x^4 + x^3 + x^2 + x + 1.$$

$$(3) x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1;$$

$$(4) x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

3. 从第 2 题受到启发, 你能猜出当 n 是什么样的大于 1 的整数时, $x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1$ 在 $\mathbb{Q}$ 上可约? 你能证明这个猜测是真的吗?

1.7.6 多项式的根, 多项式函数, 复数域上的不可约多项式

在 $F[x]$ 中, 如何判别一个次数大于 0 的多项式是否可约? 如何把域 F 上的所有不可约多项式都求出来? 我们知道, $F[x]$ 中一次多项式都是不可约的。二次和二次以上的多项式呢? 据不可约多项式的定义, 次数大于 1 的多项式 $f(x)$ 如果有一次因式, 那么 $f(x)$ 必是可约的。因此次数大于 1 的多项式 $f(x)$ 在域 F 上不可约的必要条件是它没有一次因式。如何判断 $f(x)$ 有没有一次因式? 首先要研究用一次多项式 $x - c$ 去除 $f(x)$, 它的余式 $r(x)$ 是什么样的。由于 $\deg r(x) < \deg(x - c) = 1$, 因此 $r(x)$ 是零次多项式或零多项式, 把它们等同于 F 中的元素, 记做 r 。于是有 $f(x) = h(x)(x - c) + r$ 。

x 用 c 代入, 从 (1) 式得 $f(c) = r$ 。于是得到下述结论:

定理 1.7.22 (余数定理). 在 $F[x]$ 中, 用 $x - c$ 去除 $f(x)$ 所得的余式是 $f(c)$ 。

由余数定理立即得到:

推论 1.7.23. 在 $F[x]$ 中, $x - c$ 整除 $f(x)$ 当且仅当 $f(c) = 0$ 。

从推论 1 看到了, 为了研究 $f(x)$ 有没有一次因式, 需要引进多项式的根的概念。

1.8 多项式的根

定义 1.8.1. 设 $f(x) \in F[x]$, 如果有 $c \in F$, 使得 $f(c) = 0$, 那么称 c 是 $f(x)$ 在 F 中的一个根。设域 $E \supset F$, 如果有 $\alpha \in E$, 使得 $f(\alpha) = 0$, 那么称 α 是 $f(x)$ 在 E 中的一个根。

例如, 实数域 $\mathbb{R}$ 上的多项式 $f(x) = x^2 + 1$ 没有实根, 但是有一对复根: i 和 $-i$ 。

从推论 1 立即得到下述重要定理:

定理 1.8.2 (Bezout 定理). 在 $F[x]$ 中, $x - c$ 整除 $f(x)$ 当且仅当 c 是 $f(x)$ 在 F 中的一个根。

Bezout 定理把 $F[x]$ 中一个次数大于 1 的多项式 $f(x)$ 有没有一次因式转化为 $f(x)$ 在 F 中有没有根, 这是一个创新点。有关 $F[x]$ 中的不可约多项式就开辟了新的方法。

如果 $x - c$ 是 $f(x)$ 的 k 重因式, 那么称 c 是 $f(x)$ 的 k 重根。当 $k = 0$ 时, c 不是 $f(x)$ 的根; 当 $k = 1$ 时, 称 c 是 $f(x)$ 的单根; 当 $k > 1$ 时, 称 c 是 $f(x)$ 的重根。

$F[x]$ 中的多项式 $f(x)$ 在 F 中有多少个根?由唯一因式分解定理得 $f(x) = a(x-c_1)^{r_1} \cdots (x-c_s)^{r_s} p_1^{t_1}(x) \cdots p_l^{t_l}(x)$, 其中 $c_1, c_2, \dots, c_s$ 两两不等; $p_1(x), \dots, p_l(x)$ 是域 F 上的两两不等的次数大于 1 的首一不可约多项式; $r_i > 0$ ($i = 1, 2, \dots, s$), $t_j \geq 0$ ($j = 1, 2, \dots, l$)。于是根据 Bezout 定理, $c_1, \dots, c_s$ 分别是 $f(x)$ 的 $r_1, \dots, r_s$ 重根。从 (2) 式得 $\deg f(x) \geq r_1 + \cdots + r_s$ 。

因此得到下述结论:

定理 1.8.3. 在 $F[x]$ 中, $n(n > 0)$ 次多项式 $f(x)$ 在 F 中至多有 n 个根 (重根按重数计算)。

显然, 零次多项式没有根。因此定理 3 对次数 $n = 0$ 也成立。由定理 3 立即得到下述结论:

推论 1.8.4. 在 $F[x]$ 中, 一个次数不超过 n 的多项式 $h(x)$ 如果在 F 中有 $n+1$ 个根 (重根按重数计算), 那么 $h(x) = 0$ 。

利用推论 2 可以给出两个多项式相等的一个充分条件:

定理 1.8.5. 设 $f(x), g(x) \in F[x]$, $\deg f(x) \leq n, \deg g(x) \leq n$ 。如果在 F 中有 $n+1$ 个不同的元素 $c_1, c_2, \dots, c_{n+1}$, 使得 $f(c_i) = g(c_i)$, $i = 1, 2, \dots, n+1$, 那么 $f(x) = g(x)$ 。

证明. 设 $h(x) = f(x) - g(x)$, 则 $\deg h(x) \leq \max\{\deg f(x), \deg g(x)\} \leq n$, 且 $h(c_i) = f(c_i) - g(c_i) = 0$, $i = 1, 2, \dots, n+1$ 。于是 $h(x)$ 至少有 $n+1$ 个根。据推论 2 得, $h(x) = 0$, 从而 $f(x) = g(x)$ 。□

例题 1.8.1. 在 $\mathbb{Z}_2[x]$ 中, $f(x) = x^3 + x + \bar{1}$ 是否可约?

**** 解 **** 3 次多项式 $f(x)$ 如果可约, 那么它必有一次因式。由于 $f(\bar{0}) = \bar{1}$, $f(\bar{1}) = \bar{1} + \bar{1} + \bar{1} = \bar{1}$, 因此 $f(x)$ 在 $\mathbb{Z}_2$ 中没有根。根据 Bezout 定理, $f(x)$ 在 $\mathbb{Z}_2[x]$ 中没有一次因式。因此 $f(x)$ 在 $\mathbb{Z}_2$ 上不可约。

从例 1 初步体会到: 利用多项式的根可以有助于判断一个多项式是否可约。

如何研究数域 K 上的一个多项式 $f(x)$ 在 K 中有没有根呢? 实系数多项式 $f(x) = x^2 - 1$ 有两个实根: $1, -1$ 。还可以把 $f(x) = x^2 - 1$ 的函数值取为 0。由此受到启发, 可以利用多项式函数是否在某些点的函数值为 0 来研究多项式有没有根。为此要从多项式导出多项式函数。

1.8.1 多项式函数

定义 1.8.6. 设 $f(x) \in F[x]$, 它诱导了 F 到 F 的一个映射: $f: F \rightarrow F, c \mapsto f(c), \forall c \in F$, 称 f 是多项式 $f(x)$ 诱导的域 F 上的一元多项式函数。

显然, 若多项式 $f(x) = g(x)$, 则它们诱导的多项式函数 f 与 g 相等。反之如何?

定理 1.8.7. 设 K 是数域, $K[x]$ 中的多项式 $f(x) \sim g(x)$, 如果它们诱导的多项式函数 f 与 g 相等, 那么 $f(x) = g(x)$ 。

**** 证明 **** 设 $f(x) = g(x)$, 由于数域 K 有无穷多个数, 因此据定理 4, $f(x) = g(x)$ 。□

在定理 5 的证明中, “数域 K 有无穷多个数”起了关键作用。由此猜测: 对于有限域上的多项式, 定理 5 的结论不成立。事实上果真如此, 例如在 $\mathbb{Z}_2[x]$ 中, $f(x) = x^2 + \bar{1}, g(x) = x + \bar{1}$, 显然 $f(x) \neq g(x)$ 。但是 $f(\bar{0}) = g(\bar{0}) = \bar{1}, f(\bar{1}) = g(\bar{1}) = \bar{0}$ 。这表明: 域 F 上的一元多项式

(作为一种表达式)与域 F 上的一元多项式函数(作为 F 到 F 的一个映射)是不同的两个概念。这开拓了人们的眼界。

用 K_{pol} 表示数域 K 上所有一元多项式函数组成的集合,在这个集合中规定加法和乘法运算如下:对于 $f, g \in K_{pol}$, $(f+g)(c) := f(c) + g(c)$, $\forall c \in K$; $(fg)(c) := f(c)g(c)$, $\forall c \in K$ 。

容易看出, (4) 式定义的函数 $f+g$ 是多项式 $f(x) + g(x)$ 诱导的多项式函数, (5) 式定义的函数 fg 是多项式 $f(x)g(x)$ 诱导的多项式函数, 从而 $(K_{pol}, +, \cdot)$ 的确是域 K 上的多项式函数构成的环。加法和乘法运算后, 容易验证 K_{pol} 成为一个有单位元的交换环, 其中的零元是零多项式 0 确定的函数, 称为零函数, 显然, $0(c) = 0$, $\forall c \in K$; 单位元是多项式 1 确定的函数, 是一个常值函数, 显然, $1(c) = 1$, $\forall c \in K$ 。

把数域 K 上的任一多项式 $f(x)$ 对应到它诱导的多项式函数 f , 这是 $K[x]$ 到 K_{pol} 的一个映射, 记做 σ 。显然, σ 是满射。根据定理 5 得, σ 是单射。从而是双射。由于 $f+g$ 是多项式 $f(x) + g(x)$ 诱导的多项式函数, 因此 σ 保持加法运算。由于 fg 是多项式 $f(x)g(x)$ 诱导的多项式函数, 因此 σ 保持乘法运算。这样我们证明了下述定理:

定理 1.8.8. 把数域 K 上的任一多项式 $f(x)$ 对应到它诱导的多项式函数 f , 这是 $K[x]$ 到环 K_{pol} 的一个同构映射, 从而 $K[x] \cong K_{pol}$ 。

根据定理 6, 可以把数域 K 上的一元多项式 $f(x)$ 与它诱导的一元多项式函数 f 等同。于是 $c \in K$ 是 $K[x]$ 中多项式 $f(x)$ 的根 $\iff$ 函数 f 在 c 处的函数值 $f(c) = 0$ 。这使得我们可以利用函数论的知识来研究复数域上的多项式 $f(x)$ 是否有复根的问题, 进而找出复数域上的全部不可约多项式。

1.8.2 复数域上的不可约多项式

设 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$, $\deg f(x) = n > 0$ 。假如 $f(x)$ 没有复根, 则对任意 $z \in \mathbb{C}$, 有 $f(z) \neq 0$ 。于是函数 $\varphi(z) = \frac{1}{f(z)}$ 的定义域为 $\mathbb{C}$ 。类似于实变量复数, 复变量的多项式函数有导数, 且复变量函数的导数与四则运算的关系, 以及复合函数的求导法则, 都像实变量函数那样, 因此 $\varphi'(z) = -\frac{f'(z)}{[f(z)]^2}$, $\forall z \in \mathbb{C}$ 。

这表明 $\varphi(z)$ 在复平面 $\mathbb{C}$ 上解析。

类比实变量多项式函数值的倒数的极限, 我们猜测 $\lim_{|z| \rightarrow +\infty} |\varphi(z)| = \lim_{|z| \rightarrow +\infty} \frac{1}{|f(z)|} = 0$ 。下面来探索这一猜想是否真实。我们有 $|f(z)| = |a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0| \geq |a_n z^n| - |a_{n-1} z^{n-1} + \cdots + a_1 z + a_0| \geq |a_n||z|^n - (|a_{n-1}||z|^{n-1} + \cdots + |a_1||z| + |a_0|)$ 。

当 $|z| > 1$ 时, 令 $M = \max\{|a_{n-1}|, |a_{n-2}|, \dots, |a_1|, |a_0|\}$, 于是 $|a_{n-1}||z|^{n-1} + \cdots + |a_1||z| + |a_0| \leq M(|z|^{n-1} + \cdots + |z| + 1) = M \frac{|z|^n - 1}{|z| - 1} < \frac{M|z|^n}{|z| - 1}$ 。

又当 $|z| > 1$ 时, $\frac{M|z|^n}{|z| - 1} \leq |a_n||z|^n \iff |z| \geq 1 + \frac{M}{|a_n|}$ 。因此当 $|z| \geq 1 + \frac{M}{|a_n|}$ 时, 有 $|a_n||z|^n - (|a_{n-1}||z|^{n-1} + \cdots + |a_1||z| + |a_0|) > |a_n||z|^n - \frac{M|z|^n}{|z| - 1} \geq 0$ 。

于是当 $|z| \geq 1 + \frac{M}{|a_n|}$ 时, 有 $|\varphi(z)| = \frac{1}{|f(z)|} \leq \frac{1}{|a_n||z|^n - (|a_{n-1}||z|^{n-1} + \cdots + |a_1||z| + |a_0|)} \leq$

$$\frac{1}{|z|^n} \leq \left(|a_n| - \left(\frac{|a_{n-1}|}{|z|} + \cdots + \frac{|a_1|}{|z|^{n-1}} + \frac{|a_0|}{|z|^n} \right) \right) \rightarrow 0, \text{ 当 } |z| \rightarrow +\infty. \text{ 所以 } \lim_{|z| \rightarrow +\infty} |\varphi(z)| = 0.$$

于是存在 $r > 0, M_1 > 0$, 使得当 $|z| > r$ 时, 有 $|\varphi(z)| < M_1$. 显然, $\varphi(z)$ 在圆盘 $|z| \leq r$ 上连续. 由于有界闭集上的连续函数必有界 (指它的模), 因此存在 $M_2 > 0$, 使得当 $|z| \leq r$ 时, 有 $|\varphi(z)| \leq M_2$. 从而 $\forall z \in \mathbb{C}$, 有 $|\varphi(z)| \leq \max\{M_1, M_2\}$. 这表明 $\varphi(z)$ 在复平面 $\mathbb{C}$ 上有界.

根据复变函数论的 Liouville 定理 (在复平面 $\mathbb{C}$ 上解析且有界的函数必为常值函数), 存在非零复数 b , 使得 $\varphi(z) = b, \forall z \in \mathbb{C}$. 从而 $f(z) = \frac{1}{b}, \forall z \in \mathbb{C}$. 因此得出, $f(x) = \frac{1}{b}$. 这与 $\deg f(x) = n > 0$ 矛盾. 于是我们证明了下述著名定理:

定理 1.8.9 (代数基本定理). 每一个次数大于 0 的复系数多项式都有复根.

高斯于 1799 年给出了代数基本定理的第一个严格证明, 后来他又给出了四个证明. 若尔当 (Jordan)、外尔 (Weyl) 等人也给出过证明.

由定理 7 和 Bezout 定理立即得到: 每一个次数大于 1 的复系数多项式都有一次因式, 从而可约. 于是得到:

推论 1.8.10. 复数域上的不可约多项式只有一次多项式.

这样我们完全决定了复数域上的不可约多项式, 这是数学上的一个创新点. 其中创造性的思维有: 把数域 K 上的多项式 $f(x)$ 有没有一次因式转化为它在 K 中有没有复根; 进一步转化为多项式 $f(x)$ 诱导的多项式函数 f 有没有在某些点为 0, 借此利用函数论的知识证明了代数基本定理, 证明的关键是证 $\varphi(z)$ 在复平面 $\mathbb{C}$ 上有界, 而这需要利用复数域的完备性或者说连续性.

从推论 3 立即得到:

推论 1.8.11. 每一个次数大于 0 的复系数多项式 $f(x)$ 都可以唯一地分解成有限多个一次因式的乘积.

据推论 4, $f(x)$ 的标准分解式为 $f(x) = a(x - c_1)^{r_1}(x - c_2)^{r_2} \cdots (x - c_s)^{r_s}$. 其中 $c_1, c_2, \dots, c_s$ 是两两不等的复数, $r_i > 0, i = 1, 2, \dots, s$, 因此在 $\mathbb{C}[x]$ 中进行因式分解一定要分解到都是一次因式的乘积为止.

推论 1.8.12. 每一个 $n(n > 0)$ 次复系数多项式恰有 n 个复根 (重根按重数计算).

对于 n 次复系数多项式 $f(x)$, 只要把它的 n 个复根都求出来了, 就可以写出它的标准分解式.

例题 1.8.2. 求多项式 $x^n - 1$ 在复数域上的标准分解式.

**** 解 **** 为了求 $x^n - 1$ 在复数域上的标准分解式, 先求出 $x^n - 1$ 的全部复根. 设 $x = r(\cos \theta + i \sin \theta)$ 是 $x^n - 1$ 的复根, 则 $x^n - 1 = 0 \iff r^n(\cos n\theta + i \sin n\theta) = 1 \iff r^n = 1$ 且 $n\theta = 0 + 2k\pi, k \in \mathbb{Z} \iff r = 1$ 且 $\theta = \frac{2k\pi}{n}, k \in \mathbb{Z} \iff x = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} = e^{2ki\pi/n}, k \in \mathbb{Z}$.

记 $\xi = e^{2\pi i/n}$, 则 $1, \xi, \xi^2, \dots, \xi^{n-1}$ 都是 $x^n - 1$ 的根, 且容易证明它们两两不相等, 因此它们是 $x^n - 1$ 的全部复根, 称它们为 n 次单位根。根据 Bezout 定理, $x^n - 1 = (x - 1)(x - \xi)(x - \xi^2) \cdots (x - \xi^{n-1})$ 。

习题

1. 设 $f(x) = x^5 + 7x^4 + 19x^3 + 26x^2 + 20x + 8 \in \mathbb{Q}[x]$, 判断 -2 是否是 $f(x)$ 的根, 如果是的话, 它是几重根? (提示: 用综合除法看 $x+2$ 能否整除 $f(x)$ 。)
2. 写出 $\mathbb{Z}_2[x]$ 中所有一次多项式和二次多项式, 并且找出不可约的二次多项式。
3. 在 $\mathbb{Z}_2[x]$ 中, $f(x) = x^3 + x^2 + \bar{1}$ 是否不可约?
4. 在 $\mathbb{Z}_3[x]$ 中, $f(x) = x^3$, $g(x) = x$ 。试问: 它们诱导的多项式函数 f 与 g 是否相等?
5. 在 $\mathbb{Z}_3[x]$ 中, $f(x) = x^4 + x^3 + x + \bar{1}$, $g(x) = x^2 + \bar{2}x + \bar{1}$ 。试问: 它们诱导的多项式函数 f 与 g 是否相等?
6. 从第 4 题和第 5 题受到启发, 你能猜测 $\mathbb{Z}_3$ 上的多项式函数可以由 $\mathbb{Z}_3$ 上的次数小于多少的多项式诱导出来吗? 你能证明这个猜测为真吗?
7. 利用第 6 题的结果, 你能进一步猜测 $\mathbb{Z}_p$ 上的多项式函数 (即 $\mathbb{Z}_p$ 到 $\mathbb{Z}_p$ 的映射) 都是些什么样的函数吗? 你能证明这个猜测为真吗?
8. 从第 7 题受到启发, 对于素数 p , 你能猜测 $\mathbb{Z}_p$ 上的 $\mathbb{Z}_p$ 值函数 (即 $\mathbb{Z}_p$ 到 $\mathbb{Z}_p$ 的映射) 的解析式都是些什么样子吗? 你能证明这个猜测是真的吗?
9. 求多项式 $x^n + 1$ 在复数域上的标准分解式。

1.

2.

3.

4.

5.

6.

7.

8.

9.

1.8.3 实数域上的不可约多项式

实数域上的不可约多项式有哪些？

一次多项式都是不可约的。

二次多项式 $f(x) = ax^2 + bx + c (a \neq 0)$ ，若判别式 $\Delta \geq 0$ ，则 $f(x)$ 有两个实根，从而 $f(x)$ 在 $\mathbb{R}[x]$ 中有一次因式，于是 $f(x)$ 在 $\mathbb{R}$ 上可约。若判别式 $\Delta < 0$ ，则 $f(x)$ 没有实根，从而 $f(x)$ 在 $\mathbb{R}[x]$ 中没有一次因式，于是 $f(x)$ 在 $\mathbb{R}$ 上不可约。

三次和三次以上的多项式是否都有在 $\mathbb{R}$ 上不可约的？如果对于次数 n 从 3 逐一进行研究，显然不能解决问题。因此我们要换一个思路，研究实数域上的次数大于 0 的多项式不可约的必要条件是什么？又如何研究这个必要条件？注意到实数与复数的联系很简单：任一复数 $z = a + bi$ ，其中 $a, b \in \mathbb{R}$ 。因此首先对实数域上的多项式 $f(x)$ 的复根有什么性质进行研究。

引理 1.8.13. 设 $f(x) \in \mathbb{R}[x]$ ，如果 c 是 $f(x)$ 的一个复根，那么它的共轭 $\bar{c}$ 也是 $f(x)$ 的一个复根。

证明. 设 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$ 。若 c 是 $f(x)$ 的一个复根，则 $0 = f(c) = a_n c^n + \cdots + a_1 c + a_0$ 。两边取其共轭，得 $0 = a_n \bar{c}^n + \cdots + a_1 \bar{c} + a_0 = f(\bar{c})$ 。因此， $\bar{c}$ 是 $f(x)$ 的一个复根。 $\square$

现在我们来探索实系数多项式不可约的必要条件。

设 $p(x)$ 是 $\mathbb{R}[x]$ 中一个不可约多项式，把它看成复系数多项式，它有一个复根 c 。情形 1: c 是实数。此时据 Bezout 定理，在 $\mathbb{R}[x]$ 中， $p(x)$ 有一次因式 $x - c$ 。由于 $p(x)$ 不可约，因此 $p(x) \sim x - c$ 。于是 $p(x) = a(x - c)$ ， a 是某个非零实数。

情形 2: c 是虚数。据命题 1 得， $\bar{c}$ 也是 $p(x)$ 的一个虚根。从而在 $\mathbb{C}[x]$ 中， $x - c \mid p(x)$ ， $x - \bar{c} \mid p(x)$ 。由于 $c \neq \bar{c}$ ，因此 $x - c$ 与 $x - \bar{c}$ 互素。互素多项式的性质 2 得 $(x - c)(x - \bar{c}) \mid p(x)$ 。

由于 $(x - c)(x - \bar{c}) = x^2 - (c + \bar{c})x + c\bar{c} \in \mathbb{R}[x]$ ，并且整除关系不随域的扩大而改变，因此在 $\mathbb{R}[x]$ 中有 $x^2 - (c + \bar{c})x + c\bar{c} \mid p(x)$ 。由于 $p(x)$ 不可约，因此 $x^2 - (c + \bar{c})x + c\bar{c} \sim p(x)$ 。从而 $p(x) = a[x^2 - (c + \bar{c})x + c\bar{c}]$ ， a 是某个非零实数。

由此表明：如果 $p(x)$ 是 $\mathbb{R}$ 上的不可约多项式，那么 $p(x)$ 或者是一次多项式，或者是判别式小于 0 的二次多项式。这就把寻找实数域上不可约多项式的范围大大缩小了。剩下还需检查在这个范围内的多项式是否都是不可约的。显然，一次多项式都是不可约的。上面已指出，判别式小于 0 的二次多项式是不可约的。这样我们证明了下述定理：

定理 1.8.14. 实数域上的不可约多项式只有一次多项式和判别式小于 0 的二次多项式。

这样我们完全决定了实数域上的不可约多项式。由此立即得到：

定理 1.8.15 (实系数多项式唯一因式分解定理)。每一个次数大于 0 的实系数多项式 $f(x)$ 在实数域上都可以唯一地分解成一次因式与判别式小于 0 的二次因式的乘积。

定理 2 告诉我们：在 $\mathbb{R}[x]$ 中对多项式 $f(x)$ 因式分解一定要分解到一次因式与判别式小于 0 的二次因式的乘积为止。一种做法是可以先把 $f(x)$ 在复数域中因式分解，然后利用 $f(x)$ 的复根一共轭成对出现，把 $x - c$ 与 $x - \bar{c}$ 相乘得到实系数二次式 $x^2 - (c + \bar{c})x + c\bar{c}$ 。下面的例子说明这种做法。

例题 1.8.3. 求多项式 $x^n - 1$ 在实数域上的标准分解式。

**** 解 **** 我们已求出 $x^n - 1$ 在复数域上的标准分解式为 $x^n - 1 = (x - 1)(x - \xi)(x - \xi^2) \cdots (x - \xi^{n-1})$, 其中 $\xi = e^{2\pi i/n}$. 由于对于 $1 \leq k < n$, 有 $\xi^k \xi^{n-k} = \xi^n = 1$, $\bar{\xi^k} = \xi^{n-k}$, $|\xi^k| = 1$, 因此 $\xi^k = \overline{\xi^{n-k}}$, $1 \leq k < n$. 于是 $\xi^k + \xi^{n-k} = \xi^k + \bar{\xi^k} = 2 \cos \frac{2k\pi}{n}$, $1 \leq k < n$.

情形 1: $n = 2m + 1$. 此时有 $x^{2m+1} - 1 = (x - 1)(x - \xi)(x - \xi^2) \cdots (x - \xi^m)(x - \xi^{m+1}) \cdots (x - \xi^{2m}) = (x - 1) \prod_{k=1}^m \left(x^2 - 2x \cos \frac{2k\pi}{2m+1} + 1 \right)$.

情形 2: $n = 2m$. 此时 $\xi^m = e^{2\pi i m/(2m)} = e^{\pi i} = -1$. 从而 $x^{2m} - 1 = (x - 1)(x + 1)(x - \xi)(x - \xi^2) \cdots (x - \xi^{m-1})(x - \xi^{m+1}) \cdots (x - \xi^{2m-1}) = (x - 1)(x + 1) \prod_{k=1}^{m-1} \left(x^2 - 2x \cos \frac{k\pi}{m} + 1 \right)$.

上面两个式子分别是 $x^{2m+1} - 1$ 和 $x^{2m} - 1$ 在实数域上的标准分解式。

例题 1.8.4. 证明: $\prod_{k=1}^m \cos \frac{k\pi}{2m+1} = \frac{1}{2^m}$; $\prod_{k=1}^{m-1} \sin \frac{k\pi}{2m} = \frac{\sqrt{m}}{2^{m-1}}$.

**** 证明 **** (1) 在等式 $x^{2m+1} - 1 = (x - 1) \prod_{k=1}^m \left(x^2 - 2x \cos \frac{2k\pi}{2m+1} + 1 \right)$ 的左端出现杂弦的连乘积, 而右端也有这些杂弦, 于是想到在这个等式中令 $x = -1$, 得 $-2 = -2 \prod_{k=1}^m \left(1 + 2 \cos \frac{2k\pi}{2m+1} + 1 \right)$, 从而 $\frac{1}{2^m} = \prod_{k=1}^m \left(1 + \cos \frac{2k\pi}{2m+1} \right)$. 利用 $\cos 2\alpha = 2 \cos^2 \alpha - 1$, 上式右端可化简, 于是有 $\frac{1}{2^m} = \prod_{k=1}^m 2 \cos^2 \frac{k\pi}{2m+1}$, 从而 $\frac{1}{(2^m)^2} = \left(\prod_{k=1}^m \cos \frac{k\pi}{2m+1} \right)^2$. 因此 $\frac{1}{2^m} = \prod_{k=1}^m \cos \frac{k\pi}{2m+1}$.

(2) 直接计算可验证有下述公式: $x^{2m} - 1 = (x^m)^2 - 1 = (x^m - 1)(x^{m-1} + x^{m-2} + \cdots + x^4 + x^3 + x^2 + 1)$. 与上式的左端相等, 从而右端也相等, 消去 $x^2 - 1$, 得 $x^{2(m-1)} + x^{2(m-2)} + \cdots + x^4 + x^2 + 1 = \prod_{k=1}^{m-1} \left(x^2 - 2x \cos \frac{k\pi}{m} + 1 \right)$. 令 $x = 1$, 得 $m = \prod_{k=1}^{m-1} \left(2 - 2 \cos \frac{k\pi}{m} \right)$.

两边除以 2^m , 并利用 $\cos 2\alpha = 1 - 2 \sin^2 \alpha$ 可得 $\frac{m}{2^{m-1}} = \prod_{k=1}^{m-1} \left(1 - \cos \frac{k\pi}{m} \right) = \prod_{k=1}^{m-1} \left(1 - \cos \frac{2k\pi}{2m} \right) = \prod_{k=1}^{m-1} 2 \sin^2 \frac{k\pi}{2m}$. 由此得出 $\frac{\sqrt{m}}{2^{m-1}} = \prod_{k=1}^{m-1} \sin \frac{k\pi}{2m}$.

例题 1.8.5. 求多项式 $x^n - a^n$ 在实数域上的标准分解式, 其中 $a \in \mathbb{R}$ 且 $a \neq 0$.

**** 解 **** 在例 1 的 (6) 式中, x 用 $\frac{x}{a}$ 代入, 得 $\left(\frac{x}{a} \right)^{2m+1} - 1 = \left(\frac{x}{a} - 1 \right) \prod_{k=1}^m \left[\left(\frac{x}{a} \right)^2 - 2 \frac{x}{a} \cos \frac{2k\pi}{2m+1} + 1 \right]$. 两边乘以 a^{2m+1} , 得 $x^{2m+1} - a^{2m+1} = (x - a) \prod_{k=1}^m \left(x^2 - 2ax \cos \frac{2k\pi}{2m+1} + a^2 \right)$.

在例 1 的 (7) 式中, x 用 $\frac{x}{a}$ 代入, 得 $\left(\frac{x}{a} \right)^{2m} - 1 = \left(\frac{x}{a} - 1 \right) \left(\frac{x}{a} + 1 \right) \prod_{k=1}^{m-1} \left[\left(\frac{x}{a} \right)^2 - 2 \frac{x}{a} \cos \frac{k\pi}{m} + 1 \right]$. 两边乘以 a^{2m} , 得 $x^{2m} - a^{2m} = (x - a)(x + a) \prod_{k=1}^{m-1} \left[\left(\frac{x}{a} \right)^2 - 2 \frac{x}{a} \cos \frac{k\pi}{m} + 1 \right]$.

$$\left(x^2 - 2ax \cos \frac{k\pi}{m} + a^2\right).$$

从例 1、例 2、例 3 看到了，研究清楚了 $x^n - 1$ 在复数域上的标准分解式，就容易求出它在实数域上的标准分解式。进而可求出 $x^n - a^n$ 在实数域上的标准分解式，其中 a 是任意一个非零实数；并且可以证明有关弦或正弦的连乘积的恒等式。这说明研究数学要抓住最根本的东西，根深才能叶茂。

习题 2.6

习题

1. 证明实系数的奇次多项式至少有一个实根。
2. 求多项式 $x^n + 1$ 在实数域上的标准分解式。
3. 求多项式 $x^n - a^n$ 在实数域上的标准分解式，其中 $a \in \mathbb{R}$ 且 $a \neq 0$ 。
4. 证明：
$$\prod_{k=1}^m \cos \frac{(2k-1)\pi}{4m} = \frac{\sqrt{2}}{2^m}.$$

1.

2.

3.

4.

1.8.4 有理数域上的不可约多项式

有理数域上的不可约多项式有哪些？如何判别一个有理系数多项式是否可约？

任意一个次数大于 0 的有理系数多项式都可以表示成一个有理数乘以一个整数系数多项式，其中整数系数多项式的各项系数的最大公因数只有 ± 1 。例如 $f(x) = \frac{1}{2}x^4 + \frac{1}{3}x^3 - 2x + 1 = \frac{1}{6}(3x^4 + 2x^3 - 12x + 6)$ 。

由此抽象出下述概念：

定义 1.8.16 (本原多项式). 一个非零的整数系数多项式 $g(x)$ ，如果它的各项系数的最大公因数只有 ± 1 ，那么称 $g(x)$ 是一个本原多项式。

从上述例子看出，任意一个次数大于 0 的有理系数多项式 $f(x)$ 都与一个本原多项式 $g(x)$ 相伴，而相伴的多项式其可约性是一样的。因此我们可以把研究有理数域上的不可约多项式的问题简化为研究本原多项式是否可约的问题。这样做的好处是可以利用整数环的结构。我们首先来研究本原多项式的性质。

性质 1 两个本原多项式 $g(x)$ 与 $h(x)$ 在 $\mathbb{Q}[x]$ 中相伴当且仅当 $g(x) = \pm h(x)$ 。

证明. 充分性是显然的。下面证必要性。由已知条件得 $g(x) = ch(x)$ ，其中 $c \in \mathbb{Q}$ 且 $c \neq 0$ 。设 $c = \frac{q}{p}$ ，其中 p 与 q 是互素的整数。假如 $c \neq \pm 1$ ，则 p 与 q 至少有一个不等于 ± 1 。不妨

设 $p \neq \pm 1$ 。设 $h(x) = \sum_{i=0}^n b_i x^i$ ，则 $g(x) = \frac{q}{p} \sum_{i=0}^n b_i x^i$ 。由于 $\frac{qb_i}{p} \in \mathbb{Z}$ ，因此 $p \mid qb_i$ 。由于 $(p, q) = 1$ ，因此 $p \mid b_i$ ， $i = 0, 1, \dots, n$ ，这与 $h(x)$ 是本原多项式矛盾。所以 $c = \pm 1$ ，即 $g(x) = \pm h(x)$ 。 $\square$

性质 2 (高斯引理) 两个本原多项式的乘积还是本原多项式。

证明. 设 $f(x) = \sum_{i=0}^n a_i x^i$ ， $g(x) = \sum_{j=0}^m b_j x^j$ 都是本原多项式。设 $h(x) = f(x)g(x) = c_{n+m}x^{n+m} + \dots + c_1x + c_0$ ，其中 $c_s = \sum_{i+j=s} a_i b_j$ ， $s = 0, 1, \dots, n+m$ 。

假如 $h(x)$ 不是本原多项式，则存在一个素数 p ，使得 $p \mid c_s$ ， $s = 0, 1, \dots, n+m$ 。因为 $f(x)$ 是本原多项式，所以存在 $k(0 \leq k \leq n)$ 满足 $p \mid a_0, p \mid a_1, \dots, p \mid a_{k-1}, p \nmid a_k$ 。同理，由于 $g(x)$ 本原，因此存在 $l(0 \leq l \leq m)$ 满足 $p \mid b_0, p \mid b_1, \dots, p \mid b_{l-1}, p \nmid b_l$ 。

考虑 $h(x)$ 的 $k+l$ 次项的系数 $c_{k+l} = a_k b_l + a_{k+1} b_{l-1} + \dots + a_{k+l} b_0$ 。从而 $p \mid c_{k+l}$ 。但 $p \mid a_{k+1}, \dots, a_{k+l}$ 或 $p \mid b_{l-1}, \dots, b_0$ ，于是 $p \mid a_k b_l$ ，矛盾。因此 $h(x)$ 是本原多项式。 $\square$

为了研究本原多项式在 $\mathbb{Q}$ 上不可约的判定，我们首先来研究本原多项式在 $\mathbb{Q}$ 上可约的充分必要条件。

定理 1.8.17. 一个次数大于 0 的本原多项式 $g(x)$ 在 $\mathbb{Q}$ 上可约当且仅当 $g(x)$ 能分解成两个次数比 $g(x)$ 的次数低的本原多项式的乘积。

证明. 充分性是显然的。下面证必要性。设本原多项式 $g(x)$ 在 $\mathbb{Q}$ 上可约，则存在 $g_1(x), g_2(x) \in \mathbb{Q}[x]$ ，使得 $g(x) = g_1(x)g_2(x)$ ， $\deg g_i(x) < \deg g(x)$ ， $i = 1, 2$ 。设 $g_i(x) = r_i h_i(x)$ ，其中 $r_i \in \mathbb{Q}$ 且 $r_i \neq 0$ ， $h_i(x)$ 是本原多项式， $i = 1, 2$ ，则 $g(x) = r_1 r_2 h_1(x) h_2(x)$ 。由于性质 1 得 $g(x) = \pm h_1(x) h_2(x)$ ， $\deg h_i(x) = \deg g_i(x) < \deg g(x)$ ， $i = 1, 2$ 。于是 $g(x)$ 分解成了两个次数比 $g(x)$ 的次数低的本原多项式的乘积。 $\square$

由定理 1 立即得到：

定理 1.8.18. 一个次数大于 0 的本原多项式 $g(x)$ 可以分解成有限多个在 $\mathbb{Q}$ 上不可约的本原多项式的乘积。

由定理 1 还可以得到：

推论 1.8.19. 一个次数大于 0 的整数系数多项式 $f(x)$ 在 $\mathbb{Q}$ 上可约当且仅当 $f(x)$ 能分解成两个次数比 $f(x)$ 的次数低的整数系数多项式的乘积。

证明. 必要性：设 $f(x) = mg(x)$ ，其中 $g(x)$ 是本原多项式， $m \in \mathbb{Z}$ ，且 $m \neq 0$ 。由于 $f(x)$ 在 $\mathbb{Q}$ 上可约，因此 $g(x)$ 也在 $\mathbb{Q}$ 上可约。据定理 1 得， $g(x) = h_1(x)h_2(x)$ ，其中 $h_i(x)$ 是本原多项式，且 $\deg h_i(x) < \deg g(x) = \deg f(x)$ ， $i = 1, 2$ 。于是 $f(x) = (mh_1(x))h_2(x)$ 。这证明了 $f(x)$ 分解成两个次数比 $f(x)$ 的次数低的整数系数多项式的乘积。

充分性是显然的。 $\square$

现在我们来探寻本原多项式在 $\mathbb{Q}$ 上不可约的判别方法。次数大于 1 的本原多项式 $f(x)$ 如果在 $\mathbb{Q}[x]$ 中有一次因式，那么它一定可约。而 $f(x)$ 在 $\mathbb{Q}[x]$ 中有一次因式当且仅当 $f(x)$ 在 $\mathbb{Q}$ 中有根，因此本节的重点是判断 $f(x)$ 有没有有理根的问题。

定理 1.8.20. 设 $f(x) = a_n x^n + \cdots + a_1 x + a_0$ 是一个次数 n 大于 0 的本原多项式。如果 $\frac{q}{p}$ 是 $f(x)$ 的一个有理根，其中 p 与 q 互素，那么 $p \mid a_n$ ， $q \mid a_0$ 。

证明. 由于 $\frac{q}{p}$ 是 $f(x)$ 的根，因此在 $\mathbb{Q}[x]$ 中， $x - \frac{q}{p} \mid f(x)$ 。由于 $\frac{q}{p}$ 与 $x - \frac{q}{p}$ 互素，故据定理 2 和性质 2 得， $f(x) = (px - q)g(x)$ ，其中 $g(x)$ 是本原多项式。设 $g(x) = \sum_{i=0}^{n-1} b_i x^i$ ，则 $f(x) = (px - q) \sum_{i=0}^{n-1} b_i x^i$ 。分别比较 (4) 式两边的多项式的首项系数和常数项，得 $a_n = pb_{n-1}$ ， $a_0 = -qb_0$ 。因此 $p \mid a_n$ ， $q \mid a_0$ 。 $\square$

在定理 3 的证明过程中看到：若 $\frac{q}{p}$ 是 $f(x)$ 的根，且 $(p, q) = 1$ ，则 $f(x) = (px - q)g(x)$ 。

于是 $f(1) = (p - q)g(1)$ ， $f(-1) = -(p + q)g(-1)$ 。当 $\frac{q}{p} \neq \pm 1$ 时，有 $\frac{f(1)}{p - q} = g(1) \in \mathbb{Z}$ ， $\frac{f(-1)}{p + q} = -g(-1) \in \mathbb{Z}$ 。因此如果计算出 $\frac{f(1)}{p - q} \notin \mathbb{Z}$ 或 $\frac{f(-1)}{p + q} \notin \mathbb{Z}$ ，那么 $\frac{q}{p}$ 不是 $f(x)$ 的根。

例题 1.8.6. 设 $f(x) = x^4 + 5x^3 - 3x^2 + 9$ ，试问： $f(x)$ 有没有有理根？

**** 解 **** 据定理 3，若 $\frac{q}{p}$ 是 $f(x)$ 的根，则 $p \mid 1$ ， $q \mid 9$ ，从而 $p = \pm 1$ ， $q = \pm 1$ 或 ± 3 或 ± 9 。于是 $f(x)$ 的有理根只可能是 $\pm 1, \pm 3, \pm 9$ 。由于 $f(1) = 1 + 5 - 3 + 9 = 12 \neq 0$ ， $f(-1) = 1 - 5 - 3 + 9 = 2 \neq 0$ ，因此 ± 1 都不是 $f(x)$ 的根。

对于 $\frac{q}{p} = 3$ ，计算 $\frac{f(1)}{p - q} = \frac{12}{1 - 3} = -6$ ， $\frac{f(-1)}{p + q} = \frac{2}{1 + 3} = \frac{1}{2} \notin \mathbb{Z}$ 。因此 3 不是 $f(x)$ 的根。

对于 $\frac{q}{p} = -3$ ，计算 $\frac{f(1)}{p - q} = \frac{12}{1 - (-3)} = 3$ ， $\frac{f(-1)}{p + q} = \frac{2}{1 + (-3)} = -1$ 。为进一步讨论 -3 是否为 $f(x)$ 的根，用 $x - (-3)$ 去除 $f(x)$ ，采用综合除法的格式，得到余式为 -72，所以 $x + 3 \nmid f(x)$ ，从而 -3 不是 $f(x)$ 的根。

对于 $\frac{q}{p} = 9$ ，计算 $\frac{f(1)}{p - q} = \frac{12}{1 - 9} = -\frac{3}{2} \notin \mathbb{Z}$ ，因此 9 不是 $f(x)$ 的根。对于 $\frac{q}{p} = -9$ ，计算 $\frac{f(1)}{p - q} = \frac{12}{1 - (-9)} = \frac{6}{5} \notin \mathbb{Z}$ ，因此 -9 不是 $f(x)$ 的根。综上所述， $f(x)$ 没有有理根。

在例 1 中, $f(x)$ 没有有理根, 因此 $f(x)$ 没有一次因式。但是还不能判定 $f(x)$ 在 $\mathbb{Q}$ 上不可约。这是因为 4 次多项式 $f(x)$ 虽然没有一次因式, 但有可能含有二次因式。只有证明了 $f(x)$ 也没有二次因式, 才能断定 $f(x)$ 在 $\mathbb{Q}$ 上不可约。证明 $f(x)$ 没有二次因式可以采用反证法, 还可以有其他的方法, 这将在本小节最后一部分的例 5 中讨论。

对于 2 次或 3 次本原多项式, 如果它没有有理根, 那么它在 $\mathbb{Q}[x]$ 中没有一次因式, 从而它在 $\mathbb{Q}[x]$ 中不能分解成两个次数较低的多项式的乘积, 于是它在 $\mathbb{Q}$ 上不可约。

例题 1.8.7. 判断 $f(x) = x^3 + x + 3$ 在 $\mathbb{Q}$ 上是否可约?

**** 解 **** 先看 $f(x)$ 有没有有理根, $f(x)$ 的有理根可能是 $\pm 1, \pm 3$ 。由于 $f(1) = 1 + 1 + 3 = 5 \neq 0$, $f(-1) = -1 - 1 + 3 = 1 \neq 0$, 因此 ± 1 不是 $f(x)$ 的根。对于 $\frac{q}{p} = 3$, 计算 $\frac{f(1)}{p - q} = \frac{5}{1 - 3} = -\frac{5}{2} \notin \mathbb{Z}$, 因此 3 不是 $f(x)$ 的根; 对于 $\frac{q}{p} = -3$, 计算 $\frac{f(1)}{p - q} = \frac{5}{1 - (-3)} = \frac{5}{4} \notin \mathbb{Z}$, 因此 -3 不是 $f(x)$ 的根。综上所述, $f(x)$ 没有有理根。又 $f(x)$ 是 3 次多项式, 因此 $f(x)$ 在 $\mathbb{Q}$ 上不可约。

从例 2 看到, 在 $\mathbb{Q}$ 上不可约的本原多项式有 3 次的。试问: 在 $\mathbb{Q}$ 上不可约的本原多项式有没有 4 次的, 或更高次的? 如果我们能对于次数大于 3 的本原多项式在 $\mathbb{Q}$ 上可约给出一个判别方法就好了。按照一般的思路去探索本原多项式在 $\mathbb{Q}$ 上不可约的必要条件, 然后讨论这些条件是否也是充分条件。尝试后发现寻找本原多项式在 $\mathbb{Q}$ 上不可约的必要条件是很困难的。我们不妨改变思路, 而应当具体问题具体分析, 换一个角度思考, 我们可以直接探寻本原多项式在 $\mathbb{Q}$ 上不可约的充分条件。既然是探索充分条件, 我们可以事先选择一些条件, 从本原多项式的定义出发, 有时考虑这样的 $n(n > 0)$ 次本原多项式 $f(x) = a_n x^n + \cdots + a_1 x + a_0$, 存在一个素数 p 使得 $p \mid a_0, p \mid a_1, \dots, p \mid a_{n-1}, p \nmid a_n$ 。

除了这些条件外, 还需要添加什么条件才能断定 $f(x)$ 在 $\mathbb{Q}$ 上不可约呢? 我们反过来思考: 假如 $f(x)$ 在 $\mathbb{Q}$ 上可约, 能推出现什么结论。此时据定理 1 得 $f(x) = (b_m x^m + \cdots + b_1 x + b_0)(c_l x^l + \cdots + c_1 x + c_0)$, 其中 $m < n, l < n, m + l = n, b_i, c_j \in \mathbb{Z}, i = 0, 1, \dots, m; j = 0, 1, \dots, l$, 且 $b_m \neq 0, c_l \neq 0$ 。由 (6) 式得 $a_n = b_m c_l, a_0 = b_0 c_0$ 。

由于 $p \mid a_0$, 因此 $p \mid b_0$ 或 $p \mid c_0$ 。不妨设 $p \mid b_0$, 又已知 $p \nmid a_n$, 因此 $p \nmid b_m$ 且 $p \nmid c_l$ 。于是存在 $k(0 \leq k \leq m)$ 使得 $p \mid b_0, p \mid b_1, \dots, p \mid b_{k-1}, p \nmid b_k$ 。由于 $a_k = b_0 c_k + b_1 c_{k-1} + \cdots + b_{k-1} c_1 + b_k c_0$, 且 $p \mid a_k$ (因为 $k \leq m < n$), 因此 $p \mid b_k c_0$ 。由于 $p \nmid b_k$, 因此 $p \mid c_0$ 。又因为 $p \mid b_0$, 从而 $p^2 \mid a_0$ 。于是只要 $p^2 \nmid a_0$, 那么 $f(x)$ 在 $\mathbb{Q}$ 上不可约。这样我们探索且证明了下述定理, 这就是著名的 Eisenstein 判别法:

定理 1.8.21 (Eisenstein 判别法). 设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ 是一个次数 n 大于 0 的本原多项式。如果有一个素数 p 使得 $p \mid a_0, p \mid a_1, \dots, p \mid a_{n-1}, p \nmid a_n$, 且 $p^2 \nmid a_0$, 那么 $f(x)$ 在 $\mathbb{Q}$ 上不可约。

从上述探索过程看到, 对于整数系数多项式 $f(x)$, 若 $f(x)$ 在 $\mathbb{Q}$ 上可约, 则据推论 1 得 (6) 式成立。从而在定理 4 中把本原多项式换成整数系数多项式后, 仍然成立。

推论 1.8.22. 在 $\mathbb{Q}[x]$ 中存在任意次数的不可约多项式。

**** 证明 **** 任取正整数 n , 设 $f(x) = x^n + 3$. 素数 3 符合定理 4 的条件, 因此 $f(x) = x^n + 3$ 在 $\mathbb{Q}$ 上不可约. $\square$

从上述讨论看, 引进本原多项式的概念, 研究本原多项式的性质, 经过探索得到本原多项式在 $\mathbb{Q}$ 上不可约的一个充分条件, 并通过证明在任意次数都有在有理数域上的不可约多项式, 这是研究有理数不可约多项式的创新之路.

有时直接用 Eisenstein 判别法无法判断整数系数多项式 $f(x)$ 在 $\mathbb{Q}$ 上是否不可约, 此时可选择有一个有理数 b (通常选 $b = 1$ 或 -1), 如果用 Eisenstein 判别法能判断 $g(x) = f(x+b)$ 在 $\mathbb{Q}$ 上不可约, 那么原来的 $f(x)$ 在 $\mathbb{Q}$ 上也不可约.

例题 1.8.8. 设 p 是一个素数, 多项式 $f_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ 称为 p 阶分圆多项式. 证明 $f_p(x)$ 在 $\mathbb{Q}$ 上不可约.

**** 证明 **** 直接计算得 $(x-1)f_p(x) = x^p - 1$. x 用 $x+1$ 代入, 从上式得 $xf_p(x+1) = (x+1)^p - 1 = x^p + \binom{p}{1}x^{p-1} + \cdots + \binom{p}{k}x^k + \cdots + \binom{p}{p-1}x$. 于是 $g(x) := f_p(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{k}x^{k-1} + \cdots + \binom{p}{p-1}$.

我们知道, $p \mid \binom{p}{k}$, $1 \leq k < p$, 又 $p \nmid 1, p^2 \nmid \binom{p}{p-1} = p$, 因此 $g(x)$ 在 $\mathbb{Q}$ 上不可约. 从而 $f_p(x)$ 也不能分解成两个次数比 $f_p(x)$ 的次数低的多项式的乘积. 这证明了 $f_p(x)$ 在 $\mathbb{Q}$ 上不可约. $\square$

下面我们来探索判定本原多项式在 $\mathbb{Q}$ 上不可约的另一种方法.

设 $f(x) = \sum_{i=0}^n a_i x^i$ 是一个次数 n 大于 0 且首项系数为奇数的本原多项式, 把它的各项系数模 2 以后得到一个 $\mathbb{Z}_2$ 上的多项式 $\bar{f}(x)$. 由于 a_n 是奇数, 因此 $\bar{a}_n \neq \bar{0}$. 从而 $\deg \bar{f}(x) = \deg f(x)$. 由于 $\mathbb{Z}_2$ 只有两个元素 $\bar{0}$ 和 $\bar{1}$, 因此 $\mathbb{Z}_2$ 上的多项式中每一项的系数只有两种可能: $\bar{0}$ 或 $\bar{1}$, 从而研究起来简便得多. 例如, $\mathbb{Z}_2$ 上的一次多项式只有两个: $x, x + \bar{1}$. $\mathbb{Z}_2$ 上的二次多项式只有四个: $x^2, x^2 + x, x^2 + \bar{1}, x^2 + x + \bar{1}$. 其中 $x^2, x^2 + x$ 显然在 $\mathbb{Z}_2$ 上可约. 关于 $x^2 + \bar{1}$, 由于它在 $\mathbb{Z}_2$ 中有根 1, 因此 $x^2 + \bar{1}$ 在 $\mathbb{Z}_2$ 上可约. 关于 $x^2 + x + \bar{1}$, 由于 $\bar{0}$ 和 $\bar{1}$ 都不是它的根, 因此 $x^2 + x + \bar{1}$ 没有一次因式, 从而它不可约. 这证明了: $\mathbb{Z}_2$ 上的二次不可约多项式只有一个: $x^2 + x + \bar{1}$.

类似的方法可讨论 $\mathbb{Z}_2$ 上的三次不可约多项式有哪些. 由此受到启发, 能不能通过研究 $\mathbb{Z}_2$ 上的多项式 $\bar{f}(x)$ 是否可约, 来研究 $f(x)$ 在 $\mathbb{Q}$ 上是否可约呢? 如果 $f(x)$ 在 $\mathbb{Q}$ 上可约, 那么存在本原多项式 $f_1(x)$ 和 $f_2(x)$, 使得 $f(x) = f_1(x)f_2(x)$, $\deg f_i(x) < \deg f(x)$, $i = 1, 2$. 设 $f_1(x) = \sum_{i=0}^m b_i x^i$, $f_2(x) = \sum_{j=0}^l c_j x^j$, 其中 $m+l = n, b_m c_l = a_n$. 由于 a_n 是奇数, 因此 b_m 和 c_l 都是奇数. 把 $f_1(x)$ 和 $f_2(x)$ 的各项系数都模 2 以后得到 $\mathbb{Z}_2$ 上的多项式分别为 $\bar{f}_1(x) = \sum_{i=0}^m \bar{b}_i x^i$, $\bar{f}_2(x) = \sum_{j=0}^l \bar{c}_j x^j$.

由于 $\bar{b}_m \neq \bar{0}, \bar{c}_l \neq \bar{0}$, 因此 $\deg \bar{f}_i(x) = \deg f_i(x), i = 1, 2$. 由于 $f_1(x)f_2(x) = \sum_{s=0}^{m+l} (\sum_{i+j=s} b_i c_j) x^s$, $\bar{f}_1(x)\bar{f}_2(x) = \sum_{s=0}^{m+l} (\sum_{i+j=s} \bar{b}_i \bar{c}_j) x^s$, 因此把 $f_1(x)f_2(x)$ 的各项系数模 2 以后得到的 $\mathbb{Z}_2$ 上的多项式为 $\bar{f}_1(x)\bar{f}_2(x)$. 于是把 (8) 式两边的多项式的系数模 2 以后, 得 $\bar{f}(x) = \bar{f}_1(x)\bar{f}_2(x)$. 由此 $\bar{f}_i(x)$ 的次数小于 $\bar{f}(x)$ 的次数, $i = 1, 2$, 因此 (9) 式表明 $\bar{f}(x)$ 在 $\mathbb{Z}_2$ 上可约. 这使我们探索并证明了下述定理:

定理 1.8.23. 设 $f(x)$ 是一个次数大于 0 且首项系数为奇数的本原多项式, 把它的各项系数模 2 以后得到 $\mathbb{Z}_2$ 上的多项式 $\bar{f}(x)$. 如果 $f(x)$ 在 $\mathbb{Z}_2$ 上不可约, 那么 $f(x)$ 在 $\mathbb{Q}$ 上不可约.

例題 1.8.9. 设 $f(x) = 3x^4 + 5x - 7$, 判断 $f(x)$ 在 $\mathbb{Q}$ 上是否可约?

**** 解 **** 把 $f(x)$ 的各项系数模 2 以后得到 $\mathbb{Z}_2$ 上的多项式 $\bar{f}(x) = \bar{1}x^4 + \bar{1}x + \bar{1} = x^4 + x + \bar{1} = x(x^3 + \bar{1}) + \bar{1}$. 由于 $a^3 + b^3 = (a+b)(a^2 - ab + b^2)$, 因此 $x^3 + \bar{1} = (x + \bar{1})(x^2 + x + \bar{1})$. 代入得 $\bar{f}(x) = x(x + \bar{1})(x^2 + x + \bar{1}) + \bar{1}$. 从而 $\mathbb{Z}_2$ 上的一次多项式 x 和 $x + \bar{1}$ 都不是 $\bar{f}(x)$ 的因式, $\mathbb{Z}_2$ 上唯一的二次不可约多项式 $x^2 + x + \bar{1}$ 也不是 $\bar{f}(x)$ 的因式. 由于 $\deg \bar{f}(x) = 4$, 因此假如 $\bar{f}(x)$ 在 $\mathbb{Z}_2$ 上可约, 那么它应当有一次因式或二次不可约因式. 所以 $\bar{f}(x)$ 在 $\mathbb{Z}_2$ 上不可约. 从而 $f(x)$ 在 $\mathbb{Q}$ 上不可约.

例題 1.8.10. 设 $f(x) = x^4 + 5x^3 - 3x^2 + 9$, 判断 $f(x)$ 在 $\mathbb{Q}$ 上是否可约?

**** 解 **** 把 $f(x)$ 的各项系数模 2 得到 $\mathbb{Z}_2$ 上的多项式: $\bar{f}(x) = x^4 + x^3 + x^2 + \bar{1} = x^3(x + \bar{1}) + (x + \bar{1})^2 = (x + \bar{1})(x^3 + x + \bar{1})$. 于是 $\bar{f}(x)$ 在 $\mathbb{Z}_2$ 上可约. 据习题 2.5 的例 1, $x^3 + x + \bar{1}$ 在 $\mathbb{Z}_2$ 上不可约, 于是 (12) 式是 $\bar{f}(x)$ 在 $\mathbb{Z}_2[x]$ 中的唯一因式分解.

假如 $f(x)$ 在 $\mathbb{Q}$ 上可约, 则有首项系数为 1 的本原多项式 $f_1(x), f_2(x)$ 使得 $f(x) = f_1(x)f_2(x)$, $\deg f_i(x) < \deg f(x)$, $i = 1, 2$. 把 (13) 式两边的多项式系数模 2 后得到 $\bar{f}(x) = \bar{f}_1(x)\bar{f}_2(x)$, $\deg \bar{f}_i(x) = \deg f_i(x) < \deg f(x) = \deg \bar{f}(x)$, $i = 1, 2$. 从 $\bar{f}(x)$ 在 $\mathbb{Z}_2[x]$ 中的唯一因式分解看出, $\bar{f}_1(x)$ 与 $\bar{f}_2(x)$ 中必有一个是一次因式, 从而 $f_1(x)$ 与 $f_2(x)$ 中必有一个是 $f(x)$ 的一次因式, 于是 $f(x)$ 至少有一个有理根. 但是例 1 已经证明了 $f(x)$ 没有有理根. 因此 $f(x)$ 在 $\mathbb{Q}$ 上不可约.

如果 $f(x)$ 的首项系数是偶数但不是 3 的倍数, 那么把它的各项系数模 3 得到 $\mathbb{Z}_3$ 上的多项式 $\bar{f}(x)$. 若 $\bar{f}(x)$ 在 $\mathbb{Z}_3$ 上不可约, 那么 $f(x)$ 在 $\mathbb{Q}$ 上不可约.

例題 1.8.11. 设 $f(x) = 2x^3 + 9x^2 + 7x - 4$, 判断 $f(x)$ 在 $\mathbb{Q}$ 上是否可约?

**** 解 **** 把 $f(x)$ 的各项系数模 3 得到 $\mathbb{Z}_3$ 上的多项式 $\bar{f}(x) = \bar{2}x^3 + x + \bar{2}$. 由于 $\bar{f}(\bar{0}) = \bar{2}$, $\bar{f}(\bar{1}) = \bar{2} + \bar{1} + \bar{2} = \bar{2}$, $\bar{f}(\bar{2}) = \bar{2} \cdot \bar{2}^3 + \bar{2} + \bar{2} = \bar{2}$, 因此 $\bar{f}(x)$ 在 $\mathbb{Z}_3$ 中没有根. 又由于 $\deg \bar{f}(x) = 3$, 因此 $\bar{f}(x)$ 在 $\mathbb{Z}_3$ 上不可约. 从而 $f(x)$ 在 $\mathbb{Q}$ 上不可约.

例 6 也可以直接对 $f(x)$ 讨论, 验证 $\pm 1, \pm 2, \pm 4, \pm \frac{1}{2}$ 都不是 $f(x)$ 的根, 从而 $f(x)$ 在 $\mathbb{Q}$ 上不可约. 显然这样做的计算量比较大.

如果 $f(x)$ 的首项系数是奇数但不是 5 的倍数, 那么可以把 $f(x)$ 的各项系数模 5 得到 $\mathbb{Z}_5$ 上的多项式 $\bar{f}(x)$. 关于 $\mathbb{Z}_p[x]$ 的结论, 对于 $\mathbb{Z}_5[x]$ 也同样成立. 例如, 如果 $\bar{f}(x)$ 在 $\mathbb{Z}_5$ 上不可约, 那么 $f(x)$ 在 $\mathbb{Q}$ 上不可约.

把本原多项式 $f(x)$ 的各项系数模 2 (或模 3) 或模 5, 得到 $\mathbb{Z}_2$ (或 $\mathbb{Z}_3, \mathbb{Z}_5$) 上的多项式 $\bar{f}(x)$, 通过研究 $\bar{f}(x)$ 的不可约性来研究 $f(x)$ 在 $\mathbb{Q}$ 上的不可约性, 这也是数学上的一个创新点.

给了一个本原多项式 $f(x)$, 如果它在 $\mathbb{Q}$ 上不可约, 那么它就不能在 $\mathbb{Q}$ 上作因式分解; 如果它在 $\mathbb{Q}$ 上可约, 那么它就可作因式分解, 一直分解到每个因式都是在 $\mathbb{Q}$ 上不可约为止. 有了这个理论的指导和不可约多项式的判别方法, 就不要对一个在 $\mathbb{Q}$ 上不可约的本原多项式徒劳地、挖空心思地去寻找它因式分解的特殊技巧.

习题 2.7

1. 求下列多项式的全部有理根:

(1) $f(x) = 3x^4 + 8x^3 + 6x^2 + 3x - 2$;

(2) $f(x) = 2x^3 + x^2 - 3x + 1$ 。

2. 判断下列本原多项式在有理数域上是否可约:

(1) $x^3 - 5x^2 + 4x + 3$;

(2) $x^4 - 6x^3 + 2x^2 + 10$;

(3) $7x^5 + 18x^4 + 6x - 6$;

(4) $x^4 - 2x^3 + 2x - 3$;

(5) $x^5 + 5x^3 + \bar{1}$;

(6) $x^p + px^2 + \bar{1}$, p 是奇素数;

(7) $x^6 + x^3 + \bar{1}$ 。

3. 用系数模 2 (或模 3) 的方法判断下列整数系数多项式在有理数域上是否不可约:

(1) $f(x) = x^4 - 5x + 1$;

(2) $f(x) = x^5 - x^2 + 1$;

(3) $f(x) = x^4 + 3x^3 + 3x^2 - 5$;

(4) $f(x) = 4x^3 - 12x^2 + 5x - 7$ 。

4. 在 $\mathbb{Q}[x]$ 中, 把下述多项式完全分解: $x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, $x^6 - 1$, $x^6 + 1$, $x^{12} - 1$ 。

第一章 集合、映射与逻辑初步

1.7 拓展阅读：从星期到模 m 剩余类环

第一章 集合、映射与逻辑初步

1.7 拓展阅读：从星期到模 m 剩余类环

第一章 集合、映射与逻辑初步

1.7 拓展阅读：从星期到模 m 剩余类环

1.8 杂 题

- 【2020 全国 II 卷 12】**若序列 $a_1 a_2 \cdots a_n \cdots$ 满足 $a_i \in \{0, 1\} (i = 1, 2, \cdots)$, 且存在正整数 m , 使得 $a_{i+m} = a_i (i = 1, 2, \cdots)$ 成立, 则称其为 0-1 周期序列. 并称满足 $a_{i+m} = a_i (i = 1, 2, \cdots)$ 的最小正整数 m 为这个序列的周期. 对于周期为 m 的 0-1 序列 $a_1 a_2 \cdots a_n \cdots, C(k) = \frac{1}{m} \sum_{i=1}^m a_i a_{i+k} (k = 1, 2, \cdots, m-1)$ 是描述其性质的重要指标. 下列周期为 5 的 0-1 序列中, 满足 $C(k) \leq \frac{1}{5} (k = 1, 2, 3, 4)$ 的序列是

(A) 11010... (B) 11011... (C) 10001... (D) 11001...
- 【2007 福建文 16 理 16】(多选)**中学数学中存在许多关系, 比如“相等关系”、“平行关系”等, 如果集合 A 中的元素之间的一个关系“ $\sim$ ”满足以下三个条件:

 - (1) 自反性: 对于任意 $a \in A$, 都有 $a \sim a$;
 - (2) 对称性: 对于 $a, b \in A$, 若 $a \sim b$, 则有 $b \sim a$;
 - (3) 传递性: 对于 $a, b, c \in A$, 若 $a \sim b, b \sim c$, 则有 $a \sim c$,

则称“ $\sim$ ”是集合 A 的一个等价关系. 下列关系中, 是等价关系的有

(A) 三角形的全等 (B) 整数的整除 (C) 向量的共线 (D) 整数的同余
- 【2019 命题标准样题 15 改编】(多选)**要合理地刻画三角形三个顶点的“集中程度”, 可以使用

(A) 三角形的周长 (B) 三角形的面积 (C) 三角形的外接圆半径 (D) 三角形的最大边长
- 【2021 新高考 II 卷 12】(多选)**设正整数 $n = a_0 \cdot 2^0 + a_1 \cdot 2^1 + \cdots + a_{k-1} \cdot 2^{k-1} + a_k \cdot 2^k$, 其中 $a_i \in \{0, 1\}, i = 0, 1, 2, \dots, k$. 记 $\omega(n) = a_0 + a_1 + \cdots + a_k$, 则

(A) $\omega(2n) = \omega(n)$ (B) $\omega(2n+3) = \omega(n) + 1$
 (C) $\omega(8n+5) = \omega(4n+3)$ (D) $\omega(2^n - 1) = n$
- 【2014 北京 8】**学生的语文、数学成绩均被评定为三个等级, 依次为“优秀”“合格”“不合格”. 若学生甲的语文、数学成绩都不低于学生乙, 且其中至少有一门成绩高于乙, 则称“学生甲比学生乙成绩好”. 如果一组学生中没有哪位学生比另一位学生成绩好, 并且不存在语文成绩相同、数学成绩也相同的两位学生, 则这一组学生最多有多少个?
- 【2017 北京文 14】**某学习小组由学生和教师组成, 人员构成同时满足以下三个条件:

 - (1) 男学生人数多于女学生人数;
 - (2) 女学生人数多于教师人数;

(3) 教师人数的两倍多于男学生人数.

若教师人数为 4, 则女学生人数的最大值为 (Δ); 该小组人数的最小值为 (Δ).

7. 【2009 江西 3】已知全集 $U = A \cup B$ 中有 m 个元素, $(\complement_U A) \cup (\complement_U B)$ 中有 n 个元素. 若 $A \cap B$ 非空, 求 $A \cap B$ 的元素个数. (用 m, n 表示)

8. 【2015 广东文 10】已知集合

$$E = \{(p, q, r, s) | 0 \leq p < s \leq 4, 0 \leq q < s \leq 4, 0 \leq r < s \leq 4 \text{ 且 } p, q, r, s \in \mathbb{N}\}$$

$$F = \{(t, u, v, w) | 0 \leq t < u \leq 4, 0 \leq v < w \leq 4 \text{ 且 } t, u, v, w \in \mathbb{N}\},$$

求 $|E| + |F|$.

9. 【2012 安徽 10】6 位同学在毕业聚会活动中进行纪念品的交换, 任意两位同学之间最多交换一次, 进行交换的两位同学互赠一份纪念品, 已知 6 位同学之间共进行了 13 次交换, 求收到 4 份纪念品的同学人数.
10. 【2011 陕西 14】植树节某班 20 名同学在一段直线公路一侧植树, 每人植一棵, 相邻两棵树的距离是 10. 开始时需将树苗集中放置在某一树坑旁边, 使每位同学从各自树坑出发前来领取树苗往返所走的路程总和最小, 求该最小值.
11. 【2015 年新题型测试】甲、乙、丙、丁四人商量去看电影. 甲说: 乙去我才去; 乙说: 丙去我才去; 丙说: 甲不去我就不去; 丁说: 乙不去我就不去. 最后有人去看了电影, 有人没去看电影, 去的人是谁?

12. 【2023 四省联考 15】数学家祖冲之曾经给出圆周率 π 的两个近似值: “约率” $\frac{22}{7}$ 与 “密率” $\frac{355}{113}$. 它们可用“调日法”得到: 称小于 3.1415926 的近似值为弱率, 大于 3.1415927 的近似值为强率. 由 $\frac{3}{1} < \pi < \frac{4}{1}$, 取 3 为弱率, 4 为强率, 得 $a_1 = \frac{3+4}{1+1} = \frac{7}{2}$, 故 a_1 为强率, 与上一次的弱率 3 计算得 $a_2 = \frac{3+7}{1+2} = \frac{10}{3}$, 故 a_2 为强率, 继续计算, …… 若某次得到的近似值为强率, 与上一次的弱率继续计算得到新的近似值; 若某次得到的近似值为弱率, 与上一次的强率继续计算得到新的近似值, 以此类推. 已知 $a_m = \frac{22}{7}$, 则 $m = (\Delta)$; $a_8 = (\Delta)$.

13. 【2015 福建理 15】一个二进制是由 0 和 1 组成的数字串 $x_1 x_2 \dots x_n$ ($n \in \mathbb{N}^*$), 其中 x_k ($k = 1, 2, \dots, n$) 称为第 k 位码元. 二进制是通信中常用的码, 但在通信过程中有时会发生码元错误 (即码元 0 变为 1, 或者由 1 变为 0). 已知某种二进制码 $x_1 x_2 \dots x_7$ 的码元满足如下校验方程组:

$$\begin{cases} x_4 \oplus x_5 \oplus x_6 \oplus x_7 = 0 \\ x_2 \oplus x_3 \oplus x_6 \oplus x_7 = 0 \\ x_1 \oplus x_3 \oplus x_5 \oplus x_7 = 0 \end{cases}$$

其中运算 $\oplus$ 定义为: $0 \oplus 0 = 0, 0 \oplus 1 = 1, 1 \oplus 0 = 1, 1 \oplus 1 = 0$.

已知某个符合上述特征的二进制码在通信过程中仅在第 k 位发生码元错误后变成了 1101101, 利用上述校验方程组求出 k .

14. 【2013 湖北文 17】在平面直角坐标系中, 若点 $P(x, y)$ 的坐标 x, y 均为整数, 则称点 P 为格点. 若一个多边形的顶点全是格点, 则称该多边形为格点多边形. 格点多边形的面积记为 S , 其内部的格点数记为 N , 边界上的格点数记为 L . 例如图中 $\triangle ABC$ 是格点三角形, 对应的 $S = 1, N = 0, L = 4$.

- (1) 求图中格点四边形 $DEFG$ 对应的 S, N, L ;
- (2) 已知格点多边形的面积可表示为 $S = aN + bL + c$, 其中 a, b, c 为常数, 若某格点多边形对应的 $N = 71, L = 18$, 求它的 S .
- (3) (选做) 第 (2) 问给出的公式是 Pick 定理, 利用 2.3 习题 B 组中介绍的第二类数学归纳法完成该定理的证明

提示: 关于奠基步骤, 首先对矩形证明定理成立, 然后对直角三角形证明定理成立, 最后注意到: 一个三角形区域是由包含该三角形在内的一个较大的矩形区域减去之多三个角形区域所得到的结果, 关于归纳步骤, 可利用下述引理:

引理: 每个简单的至少四边的多边形都存在一条内部对角线。

15. 【2008 福建文 15】【2009 福建文 16】五位同学围成一圈依序循环报数, 规定:

- (1) 第一位同学首次报出的数为 1, 第二位同学首次报出的数也为 1, 之后每位同学报出的数都是前两位同学所报出的数之和;
- (2) 若报出的数为 3 的倍数, 则报该数的同学需拍手一次,

已知甲同学第一个报数, 当五位同学依序循环报到第 100 个数时, 求五位同学拍手的总次数与甲同学拍手的总次数.

16. 【2012 湖南理 16】设 $N = 2^n$ ($n \in \mathbb{N}^*, n \geq 2$), 将 N 个数 $x_1, x_2, \dots, x_N$ 依次放入编号为 $1, 2, \dots, N$ 的 N 个位置, 得到排列 $P_0 = x_1 x_2 \cdots x_N$. 将该排列中分别位于奇数与偶数位置的数取出, 并按原顺序依次放入对应的前 $\frac{N}{2}$ 和后 $\frac{N}{2}$, 得到排列 $P_1 = x_1 x_3 \cdots x_{N-1} x_2 x_4 \cdots x_N$, 将此操作称为 C 变换. 将 P_1 分成两段, 每段 $\frac{N}{2}$ 个数, 得到 P_2 ; 当 $2 \leq i \leq n-1$ 时, 将 P_i 分成 2^{i-1} 段, 每段 $\frac{N}{2^{i-1}}$ 个数, 对每一段进行 C 变换得到 P_{i+1} . 例如, 当 $N = 8$ 时, $P_2 = x_1 x_5 x_3 x_7 x_2 x_6 x_4 x_8$, 此时 x_7 位于 P_2 中的第 4 个位置.

当 $N = 16$ 时, x_7 位于 P_2 中的第 (Δ) 个位置; 当 $N = 2^n$ ($n \geq 8$) 时, x_{173} 位于 P_4 中的第 (Δ) 个位置.

17. 【2025 深圳一模 14】某次考试共 5 道试题, 均为判断题. 计分的方法是: 每道题答对的给 2 分, 答错或不答的扣 1 分, 每个人的基本分为 10 分. 已知赵、钱、孙、李、周、吴 6 人的作答情况及前 5 个人的得分情况如下表, 则吴的得分为 (Δ) .

题号 \ 人	赵	钱	孙	李	周	吴
1	✓	✓	×	×	✓	✓
2	×	✓	×	✓	✓	✓
3	✓	×	×	✓	×	×
4	✓	×	×	×	✓	×
5	×	×	✓	✓	✓	✓
得分	14	11	14	14	11	

18. 【2015 高联一试 10A】设 a_1, a_2, a_3, a_4 为四个有理数, 使得 $\{a_i a_j \mid 1 \leq i < j \leq 4\} = \left\{-24, -2, -\frac{3}{2}, -\frac{1}{8}, 1, 3\right\}$. 求 $a_1 + a_2 + a_3 + a_4$ 的值.

19. 某次知识竞赛包括甲、乙、丙三个问题, 在所有 25 名参加的学生中, 每名学生至少回答出了一题。在没有答出甲题的学生中, 答出乙题的人数是答出丙题人数的 2 倍; 只答出甲题的人数比余下的学生中答出甲题的人数多 1 人; 只答出 2 题的学生中, 有一半没有答出甲题。求学生的答题情况的所有不同可能数。

20. 【2023“fiddie”模拟考 16】正方形 $ABCD$ 位于平面直角坐标系上, 其中 $A(1,1), B(-1,1), C(-1,-1), D(1,-1)$ 。考虑对这个正方形执行下面三种变换:

(1) L : 逆时针旋转 90° 。(2) R : 顺时针旋转 90° 。(3) S : 关于原点对称。

上述三种操作可以把正方形变换为自身, 但是 A, B, C, D 四个点所在的位置会发生变化。例如, 对原正方形作变换 R 之后, 顶点 A 从 $(1,1)$ 移动到 $(1,-1)$, 然后再作一次变换 S 之后, A 移动到 $(-1,1)$ 。对原来的正方形按 $a_1, a_2, \dots, a_k$ 的顺序作 k 次变换记为 $a_1 a_2 \dots a_k$, 其中 $a_i \in \{L, R, S\}, i = 1, 2, \dots, k$ 。如果经过 k 次变换之后, 顶点的位置恢复为原来的样子, 那么我们称这样的变换是 k -恒等变换。例如, RRS 是一个 3-恒等变换。

则 3-恒等变换共 (Δ) 种; 对于正整数 n , n -恒等变换共 (Δ) 种。

21. 【2024 北京第一次学考 28】已知 $\alpha_0 = (a_0, b_0, c_0, d_0)$ 和数表 $A = \begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \end{pmatrix}$, 其中 $a_i, b_i, c_i, d_i \in \mathbb{N}^*$ ($i = 0, 1, 2, 3$)。若数表 A 满足如下两个性质, 则称数表 A 由 α_0 生成。

(1) 任意 $i \in \{0, 1, 2\}$, $a_{i+1} - a_i, b_{i+1} - b_i, c_{i+1} - c_i, d_{i+1} - d_i$ 中有三个 -1 , 一个 3 ;

(2) 存在 $k \in \{1, 2, 3\}$, 使 a_k, b_k, c_k, d_k 中恰有三个数相等。

(1) 判断数表 $A = \begin{pmatrix} 5 & 6 & 6 & 6 \\ 4 & 5 & 5 & 9 \\ 3 & 8 & 4 & 8 \end{pmatrix}$ 是否由 $\alpha_0 = (6, 7, 7, 3)$ 生成; (结论无需证明)

(2) 是否存在数表 A 由 $\alpha_0 = (6, 7, 7, 4)$ 生成? 说明理由;

(3) 若存在数表 A 由 $\alpha_0 = (7, 12, 3, d_0)$ 生成, 写出 d_0 所有可能的值。

22. 【2025 北京第二次学考 25】给定正整数 $n \geq 3$, 按一定顺序排列的向量 $(x_1, y_1), (x_2, y_2), \dots, (x_m, y_m)$ 记为向量序列 $S: (x_1, y_1), (x_2, y_2), \dots, (x_m, y_m)$, 其中 $x_i \in \{1, 2, \dots, n\}, y_i \in \{1, 2\}, i = 1, 2, \dots, m$ 。

给出两个性质:

i. $x_1 = y_1 = 1, x_m = n$, 且 S 中的向量互不相等;

ii. 已知向量集合 $T = \{(1, 0), (0, 1), (0, -1)\}$ 。记 $\alpha_i = (x_i, y_i)$, 对于 S 中的任意两个向量 α_i, α_j ($i < j$), “ $\alpha_j - \alpha_i \in T$ ” 的充要条件是 “ $j = i + 1$ ”。

(1) 当 $n = 3$ 时, 分别判断向量序列

$$A: (1, 1), (2, 1), (2, 2),$$

$$B: (1, 1), (1, 2), (2, 2), (2, 1), (3, 1)$$

是否满足性质 i; (结论无需证明)

(2) 当 $n = 3$ 时, 写出一个同时满足性质 i 和性质 ii 的向量序列 S ;

- (3) 当 $n = 5$ 时, 若向量 $(4, 1)$, $(4, 2)$ 不同时在向量序列 S 中, 且 S 同时满足性质 i 和性质 ii, 求证: S 的个数为偶数。

1. C.

2.

3. AD.

4. ACD. $\omega(n)$ 指的是 10 进制数 n 对应的二进制序列中 1 的个数, 记十进制数 n 的二进制表示为 $B(n) = (a_0 a_1 \cdots a_k)_2$. 对于 A, $2n$ 的二进制序列相当于将 n 的二进制序列左移一位, 末尾添一个 0, 所以 $\omega(2n) = \omega(n)$, A 正确. 对于 B, 当 $n = 3$ 时, $\omega(2n+3) = 2, \omega(n) + 1 = 3$, 二者不相等, 故 B 错误.

对于 C, 分别将 $8n+5$ 与 $4n+3$ 写成二进制形式:

$$B(8n+5) = (\underbrace{\quad\quad\quad}_{n \text{ 的二进制表示}} 101)_2, \quad B(4n+3) = (\underbrace{\quad\quad\quad}_{n \text{ 的二进制表示}} 11)_2,$$

可知 $\omega(8n+5) = \omega(4n+3) = \omega(n) + 2$. C 正确.

$2^n - 1$ 的二进制表示是 n 个 1, 所以 $\omega(2^n - 1) = n$, D 错误.

5. 3. 为方便起见, 把优秀、合格、不合格记为 3, 2, 1 分. 由于不存在语文成绩相同、数学成绩也相同的学生, 所以最多只可能有 9 个学生, 我们可以把所有可能的学生列出来:

$$\begin{array}{ccc} P_{33} & P_{32} & P_{31} \\ P_{23} & P_{22} & P_{21} \\ P_{13} & P_{12} & P_{11} \end{array}$$

其中学生 P_{ij} 表示语文是 i 分, 数学是 j 分. 我们逐步排除掉不可能出现的学生.

因为一组学生中没有哪位学生比另一位学生成绩好, 所以不可能有 P_{33} 和 P_{11} (一定是最好或最差). 根据对称性, 接下来只需考虑 P_{32} 和 P_{31} 是否存在.

如果有 P_{32} , 则不可能有 $P_{31}, P_{22}, P_{21}, P_{12}$, 必须有 P_{23} 或 P_{13} (不可能都有), 此时这一组学生最多只有 2 个, 为 $\{P_{32}, P_{23}\}$ 或 $\{P_{32}, P_{13}\}$.

如果有 P_{31} , 则不可能有 P_{21} 和 P_{32} . 所以这一组学生人数最多的情况只可能是 $\{P_{31}, P_{22}, P_{13}\}$.

综上, 这一组学生最多有 3 个.

6. 6;12. 设男学生人数为 a , 女学生人数为 b , 教师人数为 c . 由条件, $a \geq b+1, b \geq c+1, 2c \geq a+1$.

若教师人数为 4, 则 $a+1 \leq 2c = 8, a \leq 7, b \leq a-1 = 6$. 而当 $b = 6$ 时, $a = 7, c = 4$ 满足三个条件. 故女学生人数最大值为 6.

$a+b+2c \geq (b+1) + (c+1) + (a+1)$, 因此 $c \geq 3$, 从而 $b \geq 4, a \geq 5$. 当 $c = 3, b = 4, a = 5$ 时, 满足三个条件. 故小组人数最小值为 12.

7. $m-n$ 由德摩根律, $(\complement_U A) \cup (\complement_U B) = \complement_U (A \cap B)$, 因而

$$n = |\complement_U (A \cap B)| = |U| - |A \cap B| = m - |A \cap B|$$

即 $|A \cap B| = m - n$.

8. 200.9. 2 或 4.

10. **2000.** 设树苗放在第 k 棵树下, 用 a_n 表示第 n 棵树与第 k 棵树的距离, 则 $a_n = 10|n - k|$, 其中 $n = 1, 2, \dots, 20$. 所以往返路程总和为

$$\begin{aligned} 2 \sum_{n=1}^{20} 10|n - k| &= 20 \sum_{n=1}^k (k - n) + 20 \sum_{n=k+1}^{20} (n - k) \\ &= 20 \frac{(k-1)k}{2} + 20 \frac{(21-k)(20-k)}{2} \\ &= 10(2k^2 - 42k + 420). \end{aligned}$$

函数 $y = 2x^2 - 42x + 420$ 的对称轴是直线 $x = \frac{21}{2}$, 但是 k 是正整数, 所以当 $k = 10$ 或 $k = 11$ 时往返路程取最小值 2000.

11.

12. **6;47/15**, 列表如下:

序号	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
分数	$\frac{3+4}{1+1}$	$\frac{3+7}{1+2}$	$\frac{3+10}{1+3}$	$\frac{3+13}{1+4}$	$\frac{3+16}{1+5}$	$\frac{3+19}{1+6}$	$\frac{3+22}{1+7}$	$\frac{22+25}{7+8}$
近似值	$\frac{7}{2}$	$\frac{10}{3}$	$\frac{13}{4}$	$\frac{16}{5}$	$\frac{19}{6}$	$\frac{22}{7}$	$\frac{25}{8}$	$\frac{47}{15}$
强弱率	强率	强率	强率	强率	强率	强率	弱率	弱率

13. **5.** 接收码为 1101101, 即 $(x_1, x_2, x_3, x_4, x_5, x_6, x_7) = (1, 1, 0, 1, 1, 0, 1)$, 将其代入三个校验式, 得到校验结果

$$s_1 = x_4 \oplus x_5 \oplus x_6 \oplus x_7 = 1 \oplus 1 \oplus 0 \oplus 1 = 1$$

$$s_2 = x_2 \oplus x_3 \oplus x_6 \oplus x_7 = 1 \oplus 0 \oplus 0 \oplus 1 = 0$$

$$s_3 = x_1 \oplus x_3 \oplus x_5 \oplus x_7 = 1 \oplus 0 \oplus 1 \oplus 1 = 1$$

若只有第 k 位发生错误, 那么所有包含该位的校验式均会变为 1, 根据上述结果, 发生错误的码元应当只出现在第 1 个与第 3 个方程中, 观察得到 $k = 5$.

14. **$S = 3, N = 1, L = 6; S = 79$** 代入格点三角形 ABC 与四边形 $DEFG$ 的数据, 得到方程
$$\begin{cases} 4b + c = 1 \\ a + 6b + c = 3 \end{cases}$$

要解出 a, b, c , 还需再找一个例子: 如果某个格点四边形由两个小正方形构成, 此时 $S = 2, N = 0, L = 6$, 因此 $6b + c = 2$. 结合上述三个方程解得 $a = 1, b = \frac{1}{2}, c = -1$, 因此 $S = N + \frac{1}{2}L - 1$, 代入 $N = 71, L = 18$ 可得 $S = 79$.

15. **25;5.** 报数序列为斐波那契型数列:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \dots$$

模 3 计算得到

$$1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, \dots$$

从第一个数开始每八项循环一次, 且其中有两项为 0, 即每八次报数有两次拍手, 计算得到前 100 次报数中拍手 25 次。

甲在第 1, 6, 11, 16, ... 次报数, 即报数序号模 5 为 1 时拍手, 求甲在前 100 次中拍手的次数等价求满足下述条件的 $x (1 \leq x \leq 100)$ 的个数

$$\begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 0 \pmod{4} \end{cases}$$

解得 $x = 16, 36, 56, 76, 96$, 于是甲在前 100 次中拍手 5 次。

16. $6; 3 \times 2^{N-4} + 11$ 当 $N = 16$ 时, 只考虑每次变换序列的下标, 有

$$P_0: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16$$

$$P_1: 1, 3, 5, 7, 9, 11, 13, 15, 2, 4, 6, 8, 10, 12, 14, 16$$

$$P_2: 1, 5, 9, 13, 3, 7, 11, 15, 2, 6, 10, 14, 4, 8, 12, 16$$

于是 x_7 位于第 6 个位置。

可以发现, 每次进行 C 变换后, 当前的所有段都会按照奇偶编号被平均划分为 2 段, 在下次 C 变换时, 若要考察某个数所处位置的编号, 只需注意它所处的段编号的奇偶性即可。

进行 P_1 变换后, x_{173} 处于第 87 号位置; 进行 P_2 变换后, x_{173} 处于第 44 号位置, 且位于分别含有 2^{N-2} 个元素的 4 个段中的第一段, 进行 P_3 变换后, x_{173} 处于第 $2^{N-3} + 22$ 号位置, 且位于分别含有 2^{N-3} 个元素的 8 个段中的第二段, 进行 P_4 变换后, x_{173} 处于 $2^{N-3} + 2^{N-4} + 11$ 号位置, 即 $3 \times 2^{N-4} + 11$ 号位置。

17.

18. 14. 可知, 得 14 分表示其答对 3 题, 答错 2 题; 得 11 分表示其答对 2 题, 答错 3 题, 现假设: 若赵同学答对第 i 题, 则记 $a_i = 1$, 否则记 $a_i = 0$, 尝试利用已知条件解出 a_1, a_2, a_3, a_4, a_5 , 记 $\overline{a_i} = 1 - a_i$, 于是列出方程组

$$\begin{cases} a_1 + a_2 + a_3 + a_4 + a_5 = 3 & (1) \text{赵同学的答题情况} \\ a_1 + \overline{a_2} + \overline{a_3} + \overline{a_4} + a_5 = 2 & (2) \text{钱同学的答题情况} \\ \overline{a_1} + a_2 + \overline{a_3} + \overline{a_4} + \overline{a_5} = 3 & (3) \text{孙同学的答题情况} \\ \overline{a_1} + \overline{a_2} + a_3 + \overline{a_4} + \overline{a_5} = 3 & (4) \text{李同学的答题情况} \\ a_1 + \overline{a_2} + \overline{a_3} + a_4 + \overline{a_5} = 2 & (5) \text{周同学的答题情况} \end{cases}$$

可知, $a_i + \overline{a_i} = 1$, (1)+(2) 化简得到 $a_1 + a_5 = 1$, (1)+(3) 化简得到 $a_2 = 1$, (1)+(4) 化简得到 $a_3 = 1$, (1)+(5) 化简得到 $a_1 + a_4 = 1$, 同时考虑 (1) 式, 可以解得 $a_1 = a_2 = a_3 = 1, a_4 = a_5 = 0$, 于是 1-5 题的正确答案分别为“对, 错, 对, 错, 对”, 故吴同学答对 3 道, 得分为 14。

19.

20.

21.

22.

23.

第一章 集合、映射与逻辑初步

1.7 拓展阅读：从星期到模 m 剩余类环