抽象代数笔记
多项式

EndlieDownAHell

2023 年 7 月 31 日

Definition

定义 1 同时具有 R 模结构与环结构的集合 B 被称为一个 R 代数, 这 R 代数, 换言之, 也便是装配了如下形式的环同态 f 的环:

$$f : R \to B, rb := f(r)b$$

例 1 取定环 R, 由于存在自然的环同态 $\mathbb{Z} \to R, n \to n \cdot 1$, 于是 R 为一 $\mathbb{Z}$ 代数.

取定域 K, 为 $M_n(K)$ 生成环同态 $K \to M_n(K), k \to (k\delta_{i,j})_{n\times n}$, 则 $M_n(K)$ 成一 K 代数.

取乘法幺半群 G 与交换环 R, 生成如下的集合:

$$R[G] = \{\alpha : G \to R \mid 使得\alpha(x)非零的x有限\}$$

$R[G]$ 中加法为普通的映射加法, 对于乘法, 则记

$$(\alpha\beta)(t) = \sum_{xy=t} \alpha(x)\beta(y)$$

不难验证这样的 $R[G]$ 生成一个环, 这环中的恒等元只将 G 的幺元映射入 R 中的恒等元, 其他元素则被映为 0.

我们再追加函数 ax, 这函数只将 x 映射为 a, 其余元素则映为 0, 于是 $\alpha \in R[G]$ 又有表示:

$$\alpha = \sum_{x\in G} \alpha(x)x$$

不难确定这表法的唯一性, 简记 $\alpha(x) = a_x$, 我们利用下式使得 $R[G]$ 构成一个 R 模:

$$r\left(\sum_{x\in G} a_x x\right) = \sum_{x\in G} r a_x x$$

这模的基便是 $\{1x\}_{x\in G}$. 模中成员的乘法按现在的记法便是

$$\left(\sum_{x\in G} a_x x\right)\left(\sum_{y\in G} b_y y\right) = \sum_{x,y} a_x b_y xy$$

如下两个同态均为嵌入:

$$G \to R[G], x \to 1x, R \to R[G], a \to ae$$

取 S 为集合, $\mathbb{N}$ 为自然数的加法幺半群, 取定

$$\mathbb{N}\langle S\rangle = \{\alpha : S \to \mathbb{N} \mid 使得\alpha非零的x \in S有限\}$$

在其中额外定义运算 $(\varphi\psi)(x) = \varphi(x) + \psi(x)$, 取函数 $x^i : S \to \mathbb{N}$ 仅为将 x 映为 i 的映射, 这是对字符 $x \in S$ 的次数的指派, 于是 $\alpha \in N\langle S\rangle$ 具有表出

$$\prod_{x \in S} x^{v(x)}$$

我们称这样的积为基本单项式, 记作 $M_{(v)}$, 对基本单项式, 我们定义其积为:

$$\prod_{x \in S} x^{v(x)} \cdot \prod_{x \in S} x^{u(x)} = \prod_{x \in S} x^{u(x)+v(x)}$$

不难证明其在 $\mathrm{Hom}(S, G)$ 中具有如下的泛性质:

$$\begin{tikzcd} S \arrow[r, "j_s"] \arrow[d, "\gamma"'] & \mathbb{N}\langle S\rangle \arrow[dl, dashed] \\ G & \end{tikzcd}$$

定义 2 R 上的幺半群代数 $R[\mathbb{N}\langle S\rangle]$ 被称为 R 上的多项式环, 其上元素便有唯一表出:

$$\sum_{(v)} a_{(v)} \prod_{x \in S} x^{v(x)}$$

针对 S 有限的情形, 我们设定其为文字集 $\{x_1, \cdots, x_n\}$, 以防止多项式他妈来了都要问 "这谁? ", 相应的多项式环便有记法 $R[x_1, \cdots, x_n]$, 此时, 这环中的元素便有表出

$$\sum_{(v)} a_{(v)} x_1^{v(x_1)} \cdots x_n^{v(x_n)}$$

特别的, 对 $R[x]$ 的情形, 我们便对其元素有了如下能拉出来见人的表示:

$$\sum_{k=0}^{n} a_k x^k$$

取定交换环 R 上的交换代数 B, 其中相应的环同态是 f_0, 取定 $S \subset B$, 若单项式族

$$M_{(v)}(S) = \prod_{x \in S} x^{v(x)}$$

在 R 上线性无关, 则称 S 在 R 上是代数无关的.

定理 1 沿用上文符号, 假定 R' 为另一交换代数, $f : R \to R'$ 为环同态, 且有映射 $\lambda : S \to R'$, 则

$$\begin{tikzcd} B \arrow[r, dashed, "h"] & R' \\ R \arrow[u, "f_0"] \arrow[ur, "f"'] & \end{tikzcd}$$

且 $h|_S = \lambda$.

Proof. 取定 G 为 B 中全体 $M_v(S)$ 组成的乘法幺半群, 自然, 若 $v \neq \mu$, 则 $M_v(S) \neq M_\mu(S)$, 否则 S 将要是代数相关的, 进而

$$\varphi\left(\prod_{x\in S} x^{v(x)}\right) = \prod_{x\in S} \lambda(x)^{v(x)}$$

是幺半群同态. 再定义

$$h\left(\sum_{(v)} a_{(v)} \prod_{x\in S} x^{v(x)}\right) = \sum_{(v)} f(a_{(v)}) \prod_{x\in S} \lambda(x)^{v(x)}$$

不难验证其满足所需的条件. □

当 S 为有限集合时, 不难建立环同构

$$R[x_1, \cdots, x_n] \to R[t_1, \cdots, x_n]$$

因而 n 个 R 上代数无关元生成的环同构.

假若 $S \subset S'$, 不难建立 $R[S] \to R[S']$ 的嵌入映射, 同样的, 若 R 是 R' 的子环, 将有 $R[S] \to R'[S]$ 的嵌入.

取定交换环同态 $f : R \to R'$, 其可导出如下的环同态:

$$\bar{f} : R[S] \to R'[S]$$

其中 $\bar{f}\ |_R = f$.

另外的, 取 P 为 R 的素理想, 自然同态 $R \to R/P$ 诱导出了 $R[x] \to R/P[x]$, $\lambda(x) \in R[x]$ 在 $R/P[x]$ 下的像被称为 $\lambda(x)$ 模 P 的约化.

多项式的基本性质

取定交换环 R 与文字集 $X = \{x_1, \cdots, x_n\}$ 生成的多项式, $\{x_1, \cdots, x_m\}$ 自然在 R 上是代数无关的, 称其为代数无关的变量, 进而也称 $R[X]$ 为 n 个变量的多项式, 其中成员有唯一的表示

$$\sum_{k=1}^{n} a_{(v)} x_1^{v_1} \cdots x_n^{v_n}$$

取定 $(b_1, \cdots, b_n) \in R^n$, 从定理 1 能够得到同态

$$h : R[x_1, \cdots, x_n] \to R$$

这同态将保证 $h(x_i) = b_i$ 且 R 中元素保持不变, 从而得到

$$h(\alpha) = \sum_{(v)} a_{(v)} b_1^{v_1} \cdots b_n^{v_n}$$

反将结果记为 $\alpha(b_1, \cdots, b_n)$, 则我们得到了 $R^n \to R$ 的一个函数.

在交换环上代数 $R[X]$ 中, 基本单项式 $\prod_{k=1}^{n} x_k^{v_k}$ 的次数是 $\sum_{k=1}^{n} v_k$, $r\prod_{k=1}^{n} x_k^{v_k}$ 被称为单项式.

对于多项式 $\sum_{(v)} a_(v) x_1^{v_1} \cdots x_n^{v_n}$, 其若为 0, 多项式次数为 $-\infty$, 其若非零, 将次数定义为各组分多项式的最大次数.

另外的, 多项式 $R[x_1,\cdots,x_n]$ 可视为系数为 $R[x_1,\cdots,x_{n-1}]$ 的多项式环, 其上的同态便是

$$f:R[x_1,\cdots,x_n]\to R[x_1,\cdots,x_n][x_n]$$

$$\sum_{(v)}a_{(v)}x_1^{v_1}\cdots x_n^{v_n}\to\sum_{j=1}^{d}\alpha_j(x_1,\cdots,x_{n-1})x_n^j$$

其中 d 便是左边各单项式中中 x_n 的最大次数, 称为 x_n 左边的多项式中的次数.

现在我们回头来关注一元多项式.

定理 2 R 为整环时, $R[x_1,\cdots,x_n]$ 也为整环, 且其中的可逆元都是 R 中的可逆元.

Proof. 注意到式子 $\deg(fg)=\deg f+\deg g$ 在整环中总成立, 于是当 $fg=0\Rightarrow\deg(fg)=-\infty$ 时, 自然能够断言 $f=0$ 或 $g=0$.

当 $fg=1$ 时, 即得 $\deg f+\deg g=0$, 则只能 $\deg f,\deg g=0$, 这便导出了 $f,g\in R$ 且可逆. □

下面几个命题, 还想看我写证明的让高代老师把你高代挂了吧.

定理 3 取定交换环 R 上一元多项式 f,g, 当 g 的首项系数可逆时, 存在唯一一对多项式 q,r 使得

$$f=gq+r,\deg r<\deg g$$

推论 4 存在唯一的 $q\in R[x]$ 使得下式成立:

$$f(x)=(x-a)q(x)+f(a)$$

推论 5 $(x-a)\mid f$ 当且仅当 $f(a)=0$.

定理 6 取定 $F[x]$ 为域上一元多项式环, 其是主理想整环.

例 2 多元多项式环 $F[x_1,\cdots,x_n]$ 不是主理想整环.

Proof. 考虑 $F[x_1,\cdots,x_n]$ 中 $x_1,\cdots,x_n$ 生成的理想 I, 其若具有形式 $\langle a\rangle$, 立即成立

$$x_k=af_k,k=1,\cdots,n$$

显然 a 不可逆, 否则 $I=R$, 于是 a 具有表出 $a=u_kx_k,u_k\in F^*$, 进而我们将宣称 $u_ix_i=u_jx_j$ 对 $i\neq j$ 成立, 这与 $\{x_n\}$ 的代数无关性矛盾. □

定理 7 任一域的有限乘法子群总为循环群.

Proof. 取 m 是使得 $a^m=1$ 恒成立的最小整数, 我们来证明其就是 $|G|$, 考虑到 $\forall g\in G,g^{|G|}=1$, 显然 $m\leq G$. 又方程 $x^m-1=0$ 至多有 m 个根, 则还需有 $|G|\leq m$, 从而 $m=|G|$, 则 G 是循环群. □

定理 8 取域 F 上 n 个变量的多项式 $f(x_1,\cdots,x_n)$, 假若 $f(a_1,\cdots,a_n)=0$ 对 $a_i\in I_i(\{T_n\}$ 为 F 的一组无穷子集) 恒成立, $f=0$.

Proof. 采取归纳法证明, 针对 $n=1$ 的情形, 这是不知道就把高代挂掉的结论, 现在查看 $n+1$ 的情况, 为此改写 $R[x_1,\cdots,x_{n+1}]$ 为 $R[x_1,\cdots,x_n][x_{n+1}]$, 于是

$$f(X)=\sum_j f_j(x_1,\cdots,x_n)x_{n+1}^j$$

假若能够取得 $b_1,\cdots,b_n$ 使得有 $f_j(b_1,\cdots,b_n)\neq 0$, 为使得条件成立, 将有 T_n 上无限点使得

$$\sum_j f_j(x_1,\cdots,x_n)b_{n+1}^j=0$$

这与 $n=1$ 的情形是矛盾的, 故而必然 $f_j(b_1,\cdots,b_n)=0$ 恒成立, 于是 $f\equiv 0$. □

R 上多项式环的根被认为是在 R 上"代数"的.

因式分解

定义 3 整环 R 中, 若对非零元素 a 而言, $a=bc$ 必然导出 b,c 中一个为可逆元, 称 a 为既约元.

自然, 若 $\langle a\rangle$ 为素理想, a 便是既约元.

注意到对既约元 p 与可逆元 u 而言 up 也是既约的, 故而对于与 p 相差一个可逆元的 q, 我们称 p,q 相伴.

例 3 考虑环 $\mathbb{Z}(\sqrt{-5})$, 不难发现 $2\in\mathbb{Z}(\sqrt{-5})$ 是既约的, 然而注意到

$$6=(1+\sqrt{-5})(1=\sqrt{-5})\in\langle 2\rangle$$

于是 $\langle 2\rangle$ 非素理想.

定义 4 环 R 中元素 a 被称为有唯一因子分解的, 若 R 中存在可逆元 u 与既约元 $\{p_i\}$ 使得

$$a=u\prod_{i=1}^r p_i$$

且若存在两种表出

$$a=u\prod_{i=1}^r p_i=u'\prod_{i=1}^s p_i$$

将成立 $r=s$, 且调整后诸多 p_i,q_i 相伴.

整环 R 被称为是 Gauss(唯一分解) 的, 若其中非零元素均可唯一分解为既约元的乘积.

取定 $a,b\in R$, 若存在 c 使得 $b=ac$, 称 $a\mid b$, 若 $d\mid a,b$, 称 d 是 a,b 的公因子, 若对 a,b 的任意公因子 e 成立 $e\mid d$, 称 d 是 a,b 的最大公因子.

命题 9 主理想整环是 Gauss 环.

Proof. 先来指明 R 的非零元均具有既约元的分解, 为此取 R 是生成元无既约分解的主理想的全体 S, 若其不空, 取 $\langle a_1\rangle\in R$, 构作如下理想升链:

$$\langle a_1\rangle\subset\langle a_2\rangle\subset\cdots\subset\langle a_n\rangle\subset\cdots$$

取 $\langle a\rangle=\bigcup_k\langle a_k\rangle$, 则其必然落在某个 $\langle a_n\rangle$ 中, 使得 $\langle a\rangle\subset\langle a_n\rangle\subset\langle a\rangle$, 则这链是有限的, 于是, R 的任意理想只要能够将 $\langle a_n\rangle$ 真包含, 其生成元是可既约分解的.

另外的, a_n 又不能是既约的, 否则其既约分解便是其自身, 假定 $a_n = bc$, 则 b, c 同时不是既约的, 然而又成立 $\langle b\rangle, \langle c\rangle \supset \langle a_n\rangle$, 于是 b, c 又同时有着既约分解, 这便导致矛盾, 从而 S 只能为空.

对于唯一性, 仿照整数环中情形即可. □

定义 5 借助唯一析因的表出, 不难为 Gauss 环 R 中成员取得最大公因子, 进而若 p 是 R 中整除 ab 的既约元素, 能取 d 为 a, p 的最大公因子.

假若 $d \sim p$, 则 $p \mid a$, 假若 $d = 1$, 则 $b = bd$ 是 bp, ba 的最大公因子, 考虑到 p 将 bp, ab 整除, 于是 $p \mid b$.

于是, 若 $p \mid ab$, 要么 $p \mid a$, 要么 $p \mid b$, 这又指出了 $\langle p\rangle$ 是一个素理想, 从而我们也将 Gauss 环中的既约元称为素元.

若 R 中 a, b 彼此仅差一个可逆元, 称 a, b 等价, 将诸多既约元 p 的等价类记为 P, 并以 p 为代表元, 若 R 是 Gauss 环, 对非零的 a, 我们便有如下的表出:

$$a = u \prod_{p \in P} p^{v(p)}$$

其中 $v(p)$ 是由 a 确定的, 我们记其为 $\mathrm{ord}_p a$, 称作 a 在 p 的阶.

取 Gauss 环 R 与其商域 K, 对于 $a \in K$, 我们可写如下的表示:

$$a = \frac{q}{x}, q \perp x \Rightarrow a = p^r b, b \in K, p \text{ 是素元, 且不整除} b \text{ 的分子分母.}$$

r 的唯一性不难验证, 于是类似的我们也可以定义 $\mathrm{Ord}_p a = r$, 规定 $\mathrm{Ord}_p 0 = -\infty$, 于是成立式子

$$\mathrm{Ord}_p(a_1 a_2) = \mathrm{Ord}_p(a_1) + \mathrm{Ord}_p(a_2)$$

取 $f = \sum_{k=0}^{n} a_k x^k \in R[x]$, 当 $f = 0$ 时, 定义 $\mathrm{Ord}_p f = -\infty$, 其余情形

$$\mathrm{Ord}_p f = \min_{a_k \neq 0} \{\mathrm{Ord}_p a_k\}$$

称 $up^{\mathrm{Ord}_p f}$(u 可逆) 为 f 的 p-容度, 进而定义

$$\mathrm{Cont} f = \prod_{\mathrm{Ord}_p f \neq 0} p^{\mathrm{Ord}_p f}$$

为 f 的容度, 则在相差一个可逆员的意义上, f 的容度是确定的.

对非零的 $b \in K$, 我们能够断言 $\mathrm{Cont}(bf) = b\mathrm{Cont} f$, 进而我们有式子

$$f = \mathrm{Cont}(f) f_0$$

其中 $\mathrm{Cont}(f_0) = 1$, 特殊的 f_1 的系数仍然在 R 中, 且其最大公因子为 1, 这样的多项式被我们称为本原多项式.

命题 10 取定 Gauss 环 R 与 $f, g \in R[x]$, 则

$$\mathrm{Cont}(fg) = \mathrm{Cont}(f)\mathrm{Cont}(g)$$

结合上文的论断, 所需证明的只是本原多项式的积为本原多项式, 这种事情问你高代老师.

引理 11 取定 Gauss 环 R 与其相应的商域 K, 则非零的本原多项式 f 在 $R[x]$ 中既约当且仅当其在 $K[x]$ 中既约.

Proof. 若 f 在 K 上既约, 自然在 R 上既约.

现在反设 f 在 K 上可约, 对于分解式 $f = gh$, 通过一段你要是不会就去问问你高代老师的变换, 我们不难确信如下一个式子:

$$f = \frac{ac}{bd} g_0 h_0 \Rightarrow bdf = acg_0 h_0$$

其中 g_0, h_0 本原, 又 f 本原, 于是马上确信 $ac = bd$, 因而 f 与 $g_0 h_0$ 至多相差一个可逆元, 从而 f 在 R 上可约, 等价性便得到了论证. □

定理 12 若 R 是 Gauss 环, $R[x]$ 也是 Gauss 环, 且其中的素元要么是 R 的素元, 要么是容度为 1 的既约多项式.

Proof. 取 $f \in R[x]$, 改写为 $f = \mathrm{Cont}(f) f_0$, 其中 f_0 是本原多项式, 在 $K[x]$ 中分解 f_0 为既约多项式 $\prod_{k=1}^{n} p_k^*(x)$, 进而能够断言 $f_1 = ua_1 \cdots a_r \prod_{k=1}^{n} p_k(x)$ 其中 $u \in R^*, a_k$ 既约, $p_k(x)$ 是既约且本原的, 这便是所需的分解式.

对于唯一性, 假若 f 还有分解

$$f = vd_1 \cdots d_s \prod_{k=1}^{m} q_k(x)$$

则由于上下两式的本原属性, 不难断定 $ua_1 \cdots a_r \sim vd_1 \cdots d_s$, 再从 R 是 Gauss 环, 则 $r = s, a_k \sim d_k$.

再从 $K[x]$ 中观照如上诸多多项式, 即得 $k = t, b_k p_k = c_k q_k$ 的成立, p_k, q_k 的本原属性表明了 $c_k = d_k$, 于是分解的唯一性得证.

另外的, 若 $p \in R[x]$ 是次数大于 1 的既约多项式, 为了防止出现既约分解 $p = \mathrm{Cont}(p) p_0$, 只能是 $\mathrm{Cont}(p) = 1$. □

推论 13 Gauss 环上的多元多项式环 $R[x_1, \cdots, x_n]$ 是 Gauss 环.

多元多项式

多元多项式

定义 6 取定多项式环 $R[t_1, \cdots, t_n]$ 与 $T = \{t_1, \cdots, t_n\}$ 上的置换 π, 若 π 在作用于 $f \in R[T]$ 后依旧为其本身, 我们称这多项式为对称多项式. 不难验证对称多项式全体是 $R[T]$ 的一个子环, 暂且记之为 σ.

观察如下形式的多项式 $f \in R[x]$:

$$f(x) = \prod_{i=1}^{n} (x - t_i)$$

这多项式在 T 上置换下是不变的, 进而, 表为级数形式时, 相应的系数也是在置换下不变的, 这实际上便向我们告示着如下的 $R[T]$ 中多项式序列是对称不变的:

$$s_1 = \sum_{j=1}^{n} t_j, s_2 = \sum_{i<j} t_i t_j, \cdots, s_n = t_1 \cdots t_n$$

如上的多项式被我们称呼为初等对称多项式.

我们称单项式

$$\prod_{i=1}^{n} x_i^{v_i}$$

的权为 $\sum_{i=1}^{n} iv_i$, 多项式的权则被定义为 g 中单项式的极大权.

定理 14 取定 $f(T) \in R[t_1, \cdots, t_n]$ 是 d 次对称多项式, 则存在权不大于 d 的多项式 $g(s_1, \cdots, s_n) \in R[s_1, \cdots, s_n]$ 使得

$$f(T) = g(S)$$

且 $\{s_n\}$ 在 R 上是代数无关的, $\{t_n\}$ 在 $R[S]$ 上是代数的.

Proof. $n = 1$ 时命题自然成立, 对于 n 的情形, 假设 $n-1$ 的情形下命题成立, 我们现在对 d 进行归纳证明, 为此, 首先注意到 $s_k \mid_{t_n=0}$ 同样是 $t_1, \cdots, t_{n-1}$ 的基本对称多项式, 只需令定义 $6g(x)$ 的表达式里的 $t_n = 0$ 即可, 于是, 针对对称多项式, 我们知道 $f(t_1, \cdots, t_{n-1}, 0)$ 作为关于 $t_1, \cdots, t_{n-1}$ 的对称多项式, 可以表出为

$$f(t_1, \cdots, t_{n-1}, 0) = g_1(s_1 \mid_{t_n=0}, \cdots, s_{n-1} \mid_{t_n=0})$$

注意到 $g_1(s_1, \cdots, s_{n-1})$ 关于 $t_1, \cdots, t_n$ 的次数小于 d, 且对称, 于是

$$f_1(t_1, \cdots, t_n) = f(t_1, \cdots, t_n) - g_1(s_1, \cdots, s_{n-1})$$

关于 $t_1, \cdots, t_n$ 的次数小于 d 且对称, 又 $f_1(t_1, \cdots, t_{n-1}, 0) = 0$, 依据对称性, 知道

$$f_1 = s_n f_2(t_1, \cdots, t_n)$$

其中 f_2 对称, 且其次数不大于 $d-n$, 进而有权不大于 $d-n$ 的多项式 g_2 使得

$$f_2(t_1, \cdots, t_n) = g_2(s_1, \cdots, s_n)$$

从而 $f(T) = g_1(s_1, \cdots, s_{n-1}) + s_n g_2(S)$, 这便是所需的.

对于 $s_1, \cdots, s_n$ 在 R 上代数无关, 反设其不成立, 于是存在多项式 f 使得

$$f(s_1, \cdots, s_n) = 0$$

取 f 是使得上述条件成立的次数最小的非零多项式, 其有表出

$$f(s_1, \cdots, s_n) = \sum_{k=0}^{d} f_k(s_1, \cdots, s_{n-1}) s_n^k$$

于是必然 $f_0(s_1, \cdots, s_{n-1}) \neq 0$, 否则

$$f(S) = s_n \psi(S)$$

成立, 于是, 从 $f(S) = 0$ 中可以导出 $\psi(S) = 0$, 然而已经假定了 f 是满足条件的最小多项式, 则只能是 $\{s_n\}$ 代数无关.

$t_1, \cdots, t_n$ 在 $R[s_1, \cdots, s_n]$ 上的代数属性则是定义 6 的直接结果. $\square$

结式

定义 7 定义 $R[t]$ 上多项式 $f(t)=\sum_{i=0}^{n} x_i t^{n-i}, g(t)=\sum_{j=0}^{m} y_j t^{m-j}$ 的结式为

$$\begin{vmatrix} x_0 & x_1 & \cdots & x_n & & & \\ & x_0 & x_1 & \cdots & x_n & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & & x_0 & x_1 & \cdots & x_n \\ y_0 & y_1 & \cdots & \cdots & y_n & & \\ & y_0 & y_1 & \cdots & \cdots & y_n & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & & y_0 & y_1 & \cdots & y_n \end{vmatrix}$$

记其为 $R(f,g)$, 这是一个整系数的多项式, 且满足如下的式子:

$$R(zf,g)=z^n R(f,g), R(f,zg)=z^m R(f,g)$$

则 $R(f,g)$ 是关于 f,g 各自系数组的齐次式, 其中必然存在单项式 $x_0^n y_m^m$.

考虑线性方程组:

$$t^k f(t)=\sum_{i=0}^{n} x_i t^{i+k}, k=0,\cdots,n-1$$

$$t^l g(t)=\sum_{j=0}^{n} y_j t^{j+l}, l=0,\cdots,m-1$$

进而, 取 $C=[f(t),\cdots,t^{n-1}f(t),g(t),\cdots,t^l g(t)]$, 再取右边全体 t^p 的系数生成列向量 C_p, 则我们也得到了新的表出

$$C=\sum_{p=0}^{m+n} t^p C_p$$

对这方程应用 Cramer 法则, 则

$$1=\frac{\det(C_0,\cdots,C_{m+n-1},C)}{R(f,g)}$$

于是存在多项式 $\psi,\varphi\in\mathbb{Z}[x_0,\cdots,x_n,y_0\cdots,y_m][t]$ 使得

$$\varphi(t)f(t)+\psi(t)g(t)=R(f,g)$$

成立.

推论 15 当 f,g 存在公共根 ζ 时, 替换 t 以 ζ, 即得 $R(f,g)=0$.

命题 16 取

$$f(t)=x_0\prod_{i=1}^{n}(t-v_i), g(t)=y_0\prod_{j=1}^{m}(t-u_j)$$

则

$$R(f,g)=x_0^m y_0^m \prod_{i,j}(v_i-u_j)$$

Proof. 从 $R(f,g)$ 的齐次性, 得到

$$R(f,g)=x_0^n y_0^m h(u,v)$$

当我们用某个 u_i 替换 v_j 时, f,g 将有公共根, 进而可以断言 $R(f,g)=0$, 故而作为 u,v 的多项式, $R(f,g)$ 将额外满足

$$u_i - v_j \mid R(f,g), 1 \le i \le n, 1 \le j \le m$$

于是我们已经可以断定 $x_0^m y_0^m \prod_{i,j}(v_i-u_j) \mid R(f,g)$.

另一方面, 下面两个式子能够表明 $x_0^m y_0^m \prod_{i,j}(v_i-u_j)$ 分别是 f,g 的系数的 m,n 次齐次式:

$$x_0^n y_0^m \prod_{i,j}(v_i-u_j) = x_0^n \prod_{i=1}^{n} g(v_i) = (-1)^{mn} y_0^m \prod_{j=1}^{m} f(u_j)$$

于是我们断言 $R(f,g)=c\left[x_0^n y_0^m \prod_{i,j}(v_i-u_j)\right]$, 额外思虑 $x_0^m y_0^n$ 的系数, 即得 $c=1$, 等式即证. □

推论 17 若 f,g 首项系数之积非零, 在 K 上完全可裂, 则 $R(f,g)=0$ 当且仅当两者有公共根.