# Abstract

(ppwwyyxxc@gmail.com)

July 8, 2013

## 目录



## 1 Structure

一个代数系统(封闭)中有左单位元(左乘任何元素都仍等于那个元素)与右单位元，则必相等且等于单位元,且单位元唯一.

一个有单位元的代数系统，若某 $x, \exists x', x'x = e$,则称 $x$ 左可逆. 若此代数系统适合结合律，则左右均可逆的元素的左右逆元必相等，称为逆元,且逆元唯一.

含单位元的半群(结合)称为幺群

若幺群 $M$ 中存在 $g, s.t. \forall a \in M, a = g^m$,则称 $M$ 为循环幺群,$g$ 为 $M$ 的一个生成元. 显然循环幺群必可交换.

$(A, \cdot), (B, \star), f : A \to B. \forall a, b \in A, f(a \cdot b) = f(a) \star f(b)$. 称 $f$ 是 $A$ 到 $B$ 的同态.$f$ 为单射，满射，双射时,分别称作单同态,满同态,同构.

群:一个集合与一个二元运算,满足封闭,结合,单位元,逆元，记做 $(G, \cdot, e)$ 事实上可证,只需有左单位元和左逆元的半群就是群.

欲证 $H$ 是 $G$ 的子群,需证 $H$ 仍满足封闭，单位元，逆元.或合为一个条件:$\forall a, b \in H, ab^{-1} \in H$.

循环群 $G$ 由 $a$ 生成,记做 $G = \langle a \rangle$, 阶数 $O\langle a \rangle$. 若 $O\langle a \rangle = \infty, G$ 中生成元只有 $a, a^{-1}$. 若 $O\langle a \rangle = n, G$ 中有 $\varphi(n)$ 个生成元.

循环群的子群都是循环群,无限循环群的非平凡子群是无限群. 有限循环群 $G = \langle a \rangle, |G| = n, a^k$ 是 $H$ 中 $a$ 的最小正幂,则 $|H| = \frac{n}{k}$, 且对 $n$ 的每个正因子 $d, G$ 有且只有一个 $d$ 阶子群.

循环群要么和 $(Z, +)$ 同构,要么和 $(Z_n, +)(mod)$ 同构.

环:加法构成交换群,乘法构成半群,乘法对加法左右分配.记加法单位元为 0
若环中乘法交换,称为交换环.

若乘法存在单位元,称为有单位元环,记其为 1

环 $R$ 中 $\exists b \neq 0, s.t. ab = 0$,称 $a$ 为左零因子.若没有非平凡零因子,称为无零因子环.

有单位元的无零因子交换环称为整环.

$R_1$ 成为 $R$ 的充要条件是 $R_1$ 对 $R$ 的减法与乘法封闭.(减法才能得出加法逆元存在)

在有单位元环中,存在逆元的元素称为可逆元

域:加法与乘法均构成交换群

## 2 order

偏序: 反对称,传递,自反(eg. 整除关系). 也称半序.

拟序: 非自反,传递

全序: 反对称,传递,完全(任两者可比). 也称线序/简单序.

完全性蕴含自反性 $\Rightarrow$ 全序蕴涵偏序

良序: 任意非空子集都有最小元的偏序.

良序集一定是全序集,有限全序集一定是良序集.

定义一个非良序集合上的全序关系使之成为良序集,成为良序化.

(良序定理)任意集合可以良序化.是选择公理的等价形式之一.

偏序集 $\langle A, \leq \rangle$ 上的子集 $B$ 中任两元素可比,称 $B$ 是 $A$ 的一条链; 任两元素不可比,称为反链.

(Zorn)若一个偏序集的每条链都有上界,则此集中有极大元.

Theorem: 设 $A$ 中最长链长度为 $n$,则将 $A$ 中元素分为不交的反链,反链个数至少为 $n$.

**证**:归纳.设 $A$ 中最长链长为 $k+1$, 令 $M$ 为 $A$ 的极大元的集合,则 $M$ 为反链,且 $A - M$ 中最长链长为 $k$.归纳即得.

Erdos-Szekeres: $mn+1$ 个元素的 $A$ 中或存在长为 $n+1$ 的链,或存在长为 $m+1$ 的反链.

## 3 一元多项式环

K 为一数域,$K[x]$ 为主理想环,但 $Z[x]$ 不是

一个 $n$ 次多项式能被其导数整除 $\Leftrightarrow f(x) = a(cx+b)^n$

必要性:由 $\dfrac{f(x)}{(f(x), f'(x))} = \dfrac{f(x)}{\mathrm{LM}(f'(x))}$ 为一次且无重因式即得.

(Sturm)判断一元多项式实根个数: 设 $f_0(x) = f(x), f_1(x) = f'(x)$,做辗转相除:$f_{s-1}(x) = q_s(x) f_s(x) - f_{s+1}(x)$ 直至 $f_{s+1}(x) = 0$

于是得到序列 $f_0 = f, f_1 = f', f_2, \cdots, f_s$

记 $V_c$ 表示序列 $f_i(c), (i = 0, \cdots, s)$ 的变号数,则 $f(x)$ 在区间 $(a, b), (f(a)f(b) \neq 0)$ 内的相异实根个数为 $V_a - V_b$

于是可在此区间内求数值解

多项式环上不可约的定义:因式只有可逆元和相伴元.$Q[x]$ 上不可约也许在 $Z[x]$ 上可约

$\alpha$ 为某个首一整系数多项式的复根,令 $J_\alpha = \{f(x) \in Q[x] | f(\alpha) = 0\}$, $J_\alpha$ 中次数最低的首一多项式称为 $\alpha$ 在 $Q$ 上的极小多项式 $m_\alpha(x)$

# 4 根

实系数多项式在实数域内可唯一分解为一次因式与判别式小于零的二次因式乘积.

$$x^{2m} - 1 = (x-1)\prod_{k=1}^{m}(x^2 - 2x\cos\frac{2k\pi}{2m+1} + 1)$$

$$x^{2m+1} - 1 = (x-1)(x+1)\prod_{k=1}^{m}(x^2 - 2x\cos\frac{k\pi}{m} + 1)$$

$$x^{2m+1} + 1 = (x+1)\prod_{k=1}^{m}(x^2 - 2x\cos\frac{(2k-1)\pi}{2m+1} + 1)$$

$$x^{2m} + 1 = \prod_{k=1}^{m}(x^2 - 2x\cos\frac{(2k-1)\pi}{2m} + 1)$$

取一些特殊值,可得等式: $\prod_{k=1}^{m}\cos\frac{k\pi}{2m+1} = \frac{1}{2^m}$, $\prod_{k=1}^{m-1}\sin\frac{k\pi}{2m} = \frac{\sqrt{m}}{2^{m-1}}$

$\deg f(x) \geq 2, f(x)$ 非负 $\Rightarrow \exists g(x), h(x), f(x) = g^2(x) + h^2(x)$

**证**:$f(x)$ 的所有一次因式均有偶幂指数,且任意恒正的首一二次式可写为平方和.

首一多项式 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ 的根为 $c_1 \cdots c_n$,定义其判别式为

$$D(f) = \prod_{1\leq j<i\leq n}(c_i - c_j)^2 = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ c_1 & c_2 & \cdots & c_n \\ \vdots & \vdots & & \vdots \\ c_1^{n-1} & c_2^{n-1} & \cdots & c_n^{n-1} \end{vmatrix} \begin{vmatrix} 1 & c_1 & \cdots & c_1^{n-1} \\ 1 & c_2 & \cdots & c_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & c_n & \cdots & c_n^{n-1} \end{vmatrix}$$

$$= \begin{vmatrix} s_0 & s_1 & \cdots & s_{n-1} \\ s_1 & s_2 & \cdots & s_n \\ \vdots & \vdots & & \vdots \\ s_{n-1} & s_n & \cdots & s_{2n-2} \end{vmatrix}$$

幂和式可与初等对称多项式互化:

$$s_k = \sum_{i=1}^{n} x_i^k = \begin{vmatrix} \sigma_1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 2\sigma_2 & \sigma_1 & 1 & 0 & \cdots & 0 & 0 \\ 3\sigma_3 & \sigma_2 & \sigma_1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ (k-1)\sigma_{k-1} & \sigma_{k-2} & \sigma_{k-3} & \sigma_{k-4} & \cdots & \sigma_1 & 1 \\ k\sigma_k & \sigma_{k-1} & \sigma_{k-2} & \sigma_{k-3} & \cdots & \sigma_2 & \sigma_1 \end{vmatrix}$$

$$\sigma_k = \sum_{1\le j_1<\cdots<j_k\le n}\prod_{t=1}^{k} x_{j_t} = \frac{1}{k!}\begin{vmatrix} s_1 & 1 & 0 & \cdots & 0 & 0 \\ s_2 & s_1 & 2 & \cdots & 0 & 0 \\ s_3 & s_2 & s_1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ s_{k-1} & s_{k-2} & s_{k-3} & \cdots & s_1 & k-1 \\ s_k & s_{k-1} & s_{k-2} & \cdots & s_2 & s_1 \end{vmatrix}$$

设 $f(x)$ 为首一多项式,$g(x) = (x-a)f(x) \Rightarrow D(g) = D(f)f(a)^2$

# 5 polynomial in field

(Zero Function) 若 $k$ 为无限域,则 $f : k^n \to k$ 是零函数(值域为 0) $\Leftrightarrow f = 0$(零多项式)

于是,两个多项式诱导同一个函数当且仅当它们相等

有限域上未必,如 $\mathbb{Z}_3[x]$ 中 $x^3 + 2x^2 + 2$ 与 $2x^2 + x + 2$ 是同一函数.

判断 $f(x) = 3x^5 + 11x^2 + 7$ 不可约:将其转化到 $\mathbb{Z}_2$ 域中,得

$\tilde{f}(x) = x^2(x^3 + \bar{1}) + \bar{1} = x^2(x + \bar{1})(x^2 + x + \bar{1}) + \bar{1}$

但 $\mathbb{Z}_2$ 上的一次多项式只有 $x, x + \bar{1}$,不可约二次多项式只有 $x^2 + x + \bar{1}$, 都不是 $\tilde{f}(x)$ 的因式

$\mathbb{Z}_p$ 上的函数都是 $\mathbb{Z}_p$ 上的一元多项式函数:

**证**:考虑所有次数小于 $p$ 的一元多项式集合 $\mathbb{W}$,其中任两个不同的多项式诱导不同的函数, 否则由 Lagrange 定理可得矛盾.

考虑每个系数的取法,$|\mathbb{W}| = p^p$,与 $\mathbb{Z}_p$ 上函数的总个数相等.得证.

$\eta^n = 1, \eta^l \neq 1 (1 \le l < n)$, 称 $\eta$ 为本原 $n$ 次单位根

且有 $\eta^k$ 为本原 $\dfrac{n}{(n,k)}$ 次单位根

设 $\eta_1 \cdots \eta_{\varphi(n)}$ 是全部本原 $n$ 次单位根

定义 $n$ 阶分圆多项式 $f_n(x) = \prod_{i=1}^{\varphi(n)} (x - \eta_i)$

有:$f_n(x)$ 是集合 $\{f(x) \in \mathbb{Q}[x] \mid f(\eta) = 0\}$ 中次数最低的首一多项式(极小多项式)

$f_n(x)$ 在 $\mathbb{Q}$ 上不可约.

$x^n - 1 = \prod_{d|n} f_d(x)$

# 6 结式

设 $f(x) = \sum_{i=0}^{n} a_i x^{n-i}, g(x) = \sum_{i=0}^{m} b_i x^{m-i}$ 为 $K[x]$ 中两个多项式,$m, n > 0$,则 $Res(f, g) = 0 \Leftrightarrow a_0 = b_0 = 0$ 或 $f(x), g(x)$ 有公共复根

**分析**:$a_0, b_0$ 不全为 0 时,$f, g$ 有公共复根

$\Leftrightarrow \exists f_1(x), g_1(x), \deg f_1(x) < n, \deg g_1(x) < m, f(x)g_1(x) = g(x)f_1(x)$

则可设 $f_1(x) = \sum_{i=0}^{n-1} u_i x^{n-1-i}, g_1(x) = \sum_{i=0}^{m-1} v_i x^{m-1-i}$.,代入上式,有

$$\begin{cases} a_0v_0 & & & = & b_0u_0 & & \\ a_1v_0+a_0v_1 & & & = & b_1u_0+b_0u_1 & & \\ \cdots\cdots & & \cdots & = & \cdots\cdots & & \cdots \\ & a_nv_{m-2}+a_{n-1}v_{m-1} & = & & & b_mu_{n-2}+b_{m-1}u_{n-1} \\ & a_nv_{m-1} & = & & & b_mu_{n-1} \end{cases}$$

此 $m+n$ 元齐次线性方程组有非零解 $\Leftrightarrow$

$$Res(f,g)=\begin{vmatrix} a_0 & a_1 & \cdots & \cdots & \cdots & \cdots & a_n & & & \\ & a_0 & a_1 & \cdots & \cdots & \cdots & \cdots & a_n & & \\ & & \cdots & \cdots & \cdots & \cdots & \cdots & & & \\ & & & a_0 & a_1 & \cdots & \cdots & \cdots & & a_n \\ b_0 & b_1 & \cdots & b_m & & & & & & \\ & b_0 & b_1 & \cdots & b_m & & & & & \\ & & \cdots & \cdots & \cdots & \cdots & \cdots & & & \\ & & & & & & b_0 & b_1 & \cdots & b_m \end{vmatrix}=0$$

也即 Sylvester's Matrix $S_{f,g}$ 的行列式为 0.
事实上有 $\deg(\gcd(f,g))=m+n-\operatorname{rank}S_{f,g}$

在多项式方程组求解的应用:
仅以 $\begin{cases} f(x,y)=0 \\ g(x,y)=0 \end{cases}$ 为例,以 $x$ 为主元,求得结式 $R_x(f,g)$,是 $y$ 的多项式
则对 $R_x(f,g)$ 的每个零点 $y_0, f(x,y_0), g(x,y_0)$ 有公共复根,求出即可

设 $f(x)$ 的复根为 $c_1,\cdots c_n$,$g(x)$ 的复根为 $d_1,\cdots d_m$,则
$Res(f,g)=a_0^m\prod_{i=1}^{n}g(c_i)=(-1)^{mn}b_0^n\prod_{i=1}^{m}f(d_j)=a_0^mb_0^n\prod_{i=1}^{n}\prod_{j=1}^{m}(c_i-d_j)$
设判别式 $D(f)=a_0^{2n-2}\prod_{1\le j<i\le n}(c_i-c_j)^2$, 有 $Res(f,f')=a_0(-1)^{\frac{n(n-1)}{2}}D(f)$
$D(fg)=D(f)D(g)(Res(f,g))^2$
$Res(f,g_1g_2)=Res(f,g_1)Res(f,g_2)$

用于化参数方程为坐标方程:$\begin{cases} x=\dfrac{-t^2+2t}{t^2+1} \\ y=\dfrac{2t^2+2t}{t^2+1} \end{cases}$
**解**:任取点 $P(x,y), \exists t_0\in\mathbb{R}, s.t.\begin{cases} f(t)=(t^2+1)x+t^2-2t \\ g(t)=(t^2+1)y-2t^2-2t \end{cases}$ 有公共根 $t_0$
排除掉 $x+1=y-2=0$ 的情形,只能 $Res(f,g)=0\Leftrightarrow 8x^2-4xy+5y^2+12x-12y=0, (x,y)\neq(-1,2)$ 为最终结果