中山大学学报（自然科学版）
第30卷 第4期 ACTA SCIENTIARUM NATURALIUM Vol.30 №.4
1991年 UNIVERSITATIS SUNYATSENI 1991

关于斜多项式的可分性及$\tilde{\rho}$-可分性

楼 小 龙
（数学系）

摘 要

给出斜多项式$\tilde{\rho}$-可分的一个等价条件，建立了可分与$\tilde{\rho}$-可分之间的一个关系，随后给出应用例子。

关键词 斜多项式环，环上的Galois扩张，可分扩张，$\tilde{\rho}$-可分，Galois集，可分集

1 符号和定义

总设R是一个带单位元1的环（不一定交换），ρ表示R上的一个环自同构，$R[X;\rho]$表示R上含一个变量的关于ρ的斜多项式环。作为自由R-模，$R[X;\rho]$的元素集合可表示为$R\oplus RX\oplus RX^2\oplus\cdots\oplus RX^n\oplus\cdots$，它的乘法结构由$aX=X\rho(a)$，$(\forall a\in R)$给出。用$R[X;\rho]_{(0)}$和$R^{\rho}[X]$分别表示$R[X;\rho]$中满足$gR[X;\rho]=R[X;\rho]g$的首项系数为1的斜多项式$g$和系数在$\rho$作用下不变的斜多项式的集合，$f\in R[X;\rho]_{(0)}$称为可分的，如果$R[X;\rho]/fR[X;\rho]$是$R$上的可分扩张；$f\in R[X;\rho]_{(0)}$称为是Galois的，如果$R[X;\rho]/fR[X;\rho]$是$R$上的Galois扩张；$f\in R[X;\rho]_{(0)}\cap R^{\rho}[X]$称为是$\tilde{\rho}$-可分的，如果$f$的导函数（形式上的）在$R[X;\rho]/fR[X;\rho]$中可逆。

设 $f=X^n+a_{n-1}X^{n-1}+a_{n-2}X^{n-2}+\cdots+a_1X+a_0\in R[X;\rho]_{(0)}$，则

$$S=R[X;\rho]/fR[X;\rho]=\left\{\sum_{i=0}^{n-1}r_ix^i\,\middle|\,r_i\in R,x=X+R[X;\rho]f\right\}$$

先定义左R-模投射π_i：$S\to R$，$\pi_i\left(\sum_{j=0}^{n-1}r_jx^j\right)=r_i$，$i=0,1\cdots n-1$。再定义$t:S\to R$，$t(u)=\sum_{i=0}^{n-1}\pi_i(ux^i)$，$\forall u\in S$，易验证$t$是$R$-$R$-模同态。用$t$定义一个（关于$f$的）矩阵$T_f$，$T_f=(t_{i+1,j+1})$，其中$t_{i+1,j+1}=t(x^{i+j})$，$i,j=0,1,\cdots n-1$。易见$T_f$为$R$上对称的$n\times n$矩阵（即$T_f'=T_f$）

下面文中还将用B_k表示集合$\{s\in R\mid rs=s\rho^{-k}(r),\forall r\in R\}$，其中$k\in Z$；用$\rho^*$表示$R[X;\rho]\to R[X;\rho]$的由$\sum_{i=0}^{m}X^id_i\to\sum_{i=0}^{m}X^i\rho(d_i)$定义的环同态，易见它为环同构。

本文1989年11月25日收到

2　关于$\tilde{\rho}$-可分的一个等价条件

为简便起见，把R上的$m\times m$矩阵(c_{ij})，它满足$c_{ij}\in B_l$（对某个$l\in Z$），$i,j=1,\cdots,m$，称为R上$m\times m$的ρ-矩阵。另外约定：$\rho\{(c_{ij})\}=\{\rho(c_{ij})\}$，其中$(c_{ij})$为$R$上的矩阵。

引理1　设$B=(b_{ij})_{m\times m}$为R上的矩阵，满足

1）　$\rho(b_{ij})=b_{ij}$，　$b_{ij}=b_{ji}$，　$i,j=1,2\cdots,m$；

2）　B为ρ-矩阵；

3）　B有一个左逆（或右逆）ρ-矩阵$A=(a_{ij})_{m\times m}$。则B可定义行列式，且$|B|$为R中的可逆元。

证明　由于A为ρ-矩阵，故对a_{ij}，存在$k\in Z$，使得$a_{ij}\in B_k$，所以

$$b_{st}\cdot a_{ij}=a_{ij}\rho^{-k}(b_{st})=a_{ij}b_{st},\quad i,j,s,t=1,\cdots,m.$$

因为$AB=E\Leftrightarrow$　$\sum_{i=1}^{m}a_{ki}b_{il}=\delta_{kl}$，　$k,l=1,\cdots m$.

$\Leftrightarrow$　$\sum_{i=1}^{m}b_{il}a_{ki}=\delta_{kl}$，　$k,l=1,\cdots m$.

$\Leftrightarrow$　$B'A'=E$　　（E为单位矩阵）

又$B'=B$，故$AB=E\Leftrightarrow BA'=E$。由上式易见$A=A'$为$B$的逆矩阵。又因为$\rho(BA)=B\rho(A)=E$，因而$\rho(A)=A$，现得知$B$，$A$为满足$\rho(B)=B$，$\rho(A)=A$的$\rho$-矩阵，由此可推得$B$，$A$为$C(R^\rho)$的矩阵，其中$R^\rho=\{b\mid b\in R,\ \rho(b)=b\}$，$C(R^\rho)$为$R^\rho$的中心，所以可定义$B$，$A$的行列式，且由$BA=E$得$|B||A|=1$，从而$|B|$为$R$中可逆元。（证毕）

设$f\in R[X;\rho]_{(0)}\cap R^\rho[X]$，则由[1]知，$T_f$是$C(R^\rho)$上的矩阵。

引理2[2]　设$f\in R[X;\rho]_{(0)}\cap R^\rho[X]$，则$f$为$\tilde{\rho}$-可分$\Leftrightarrow|T_f|=\delta(f)$在$R$中可逆。

定理1　设$f\in R[X;\rho]_{(0)}\cap R^\rho[X]$，则下列条件等价。

1）　f为$\tilde{\rho}$-可分；

2）　$|T_f|=\delta(f)$为R中的可逆元；

3）　T_f有左逆ρ-矩阵。

证明　只要证明2）与3）等价即可。

3）$\Rightarrow$2）　由引理1，只要说明T_f是ρ-矩阵即可，$\forall a\in R$，

$at_{i+1,j+1}=at(x^{i+j})=t(ax^{i+j})=t(x^{i+j})\rho^{i+j}(a)=t_{i+1,j+1}\rho^{i+j}(a)$，从而

$t_{i+1,j+1}\in B_{-i-j}$，所以T_f为ρ-矩阵。

2）$\Rightarrow$3）　设$T_f^*=(A_{i+1,j+1})$为T_f的伴随矩阵，$T_f^*\cdot T_f=\delta(f)E$，其中$A_{i+1,j+1}$为$T_{i+1,i+1}$的代数余子式。$\forall a\in R$，

$$a\cdot t_{1,j_1}\cdot t_{2,j_2}\cdots t_{i,j_i}\cdot t_{i+2,j_{i+2}}\cdots t_{n,j_n}=t_{1,j_1}\cdot t_{2,j_2}\cdots t_{i,j_i}\cdot t_{i+2,j_{i+2}}\cdots t_{n,j_n}\rho^{n(n-1)-i-j}(a)$$

其中　j_1，$j_2\cdots j_i$，j_{i+2}，$\cdots j_n$为1，2，$\cdots$，i，$i+2$，$\cdots$，n的任一个排列。所以

$$a\,A_{i+1,j+1}=A_{i+1,j+1}\,\rho^{n(n-1)-i-j}(a),\quad i,j=0,1,2\cdots n-1.$$

由文[1]，　$a\,\delta(f)=\delta(f)\rho^{n(n-1)}(a)$，所以$\delta^{-1}(f)\cdot a=\rho^{n(n-1)}(a)\delta^{-1}(f)$，

$a(A_{i+1,j+1}\cdot\delta^{-1}(f))=A_{i+1,j+1}\rho^{n(n-1)-i-j}(a)\delta^{-1}(f)=A_{i+1,i+1}\delta^{-1}(f)\rho^{-i-j}(a)$, $i,j=0,1,\cdots,n-1$。所以 $A_{i+1,i+1}\delta^{-1}(f)\in B_{i+j}$, 从而 $T_f^{-1}=T_f^*\cdot\delta^{-1}(f)$ 为 ρ-矩阵(证毕)。

3 关于斜多项式的可分与 $\tilde{\rho}$-可分之间的关系

若f为$\tilde{\rho}$-可分, 则f为可分[2], 反之不一定成立[2], 本文的一个例子也能说明这一点。下面定理2给出了$\tilde{\rho}$-可分与可分之间的一个关系, 从某种意义上来说, 它刻划了这两种可分性之间存在的差距。

定理2 设$f\in R[X;\rho]_{(0)}\cap R^{\rho}[X]$, 则下列条件等价

1) f为$\tilde{\rho}$-可分;

2) f可分且存在一个可分集$\{x_i;y_i\}$, 满足$\sum_i x_i t(y_i)=1$。

证明 $2\Rightarrow 1)$。设$\{x_i;y_i\}$为满足2)可分集。$x_i=\sum_{k=0}^{n-1}x^k p_{ik}$, $y_i=\sum_{k=0}^{n-1}q_{ik}x^k$ ($n=\deg f$), 则$\sum_i x_i\otimes y_i=\sum_{k=0}^{n-1}x^k\otimes(\sum_i\sum_{s=0}^{n-1}p_{ik}q_{is}x^s)$, 记$d_{ks}=\sum_i p_{ik}q_{is}$, $z_k=\sum_{s=0}^{n-1}d_{ks}x_s$, $K=0,1,\cdots n-1$, 易证$\{x^k;z_k\}$仍为可分集, 且$\sum_{k=0}^{n-1}x^k t(z_k)=\sum_i x_i t(y_i)=1$。$\forall a\in R$, 因为 $\sum_{k=0}^{n-1}x^k\otimes z_k a=a\sum_{k=0}^{n-1}x^k\otimes z_k=\sum_{k=0}^{n-1}x^k\rho^k(a)\otimes z_k$ $=\sum_{k=0}^{n-1}x^k\otimes\rho^k(a)z_k$, 所以$\rho^k(a)d_{ks}=d_{ks}\rho^{-s}(a)$, 因而$d_{ks}\in B_{k+s}$。

下面证明 $\forall u\in S=R[X;\rho]/fR[X;\rho]$, 有$u=\sum_{k=0}^{n-1}x^k t(z_k u)$成立。作$1\otimes t$: $S\otimes_R S\to S$, $(1\otimes t)(s_1\otimes s_2)=s_1 t(s_2)$, 从当量积定义出发可验证上述映射的合理性, 故由$(1\otimes t)(u\sum_{k=0}^{n-1}x^k\otimes z_k)=(1\otimes t)(\sum_{k=0}^{n-1}x^k\otimes z_k u)$得:

$$u=u\sum_{k=0}^{n-1}x^k t(z_k)=\sum_{k=0}^{n-1}x^k t(z_k u)。$$

从而$x^j=\sum_{k=0}^{n-1}x^k t(z_k x^j)=\sum_{s=0}^{n-1}\sum_{k=0}^{n-1}x^k d_{ks}t(x^{s+j})$, 所以

$\sum_{s=0}^{n-1}d_{ks}t(x^{s+j})=\delta_{kj}$, $k,j=0,1,\cdots,n-1$。上式即为

$\sum_{s=0}^{n-1}d_{ks}t_{s+1,j+1}=\delta_{kj}$, $k,j=0,1,\cdots,n-1$。

令$A=(d_{k+1,s+1})$, 则$AT_f=E$, 且由$d_{ks}\in B_{k+s}$知A为ρ-矩阵, 所以由定理1知f为$\tilde{\rho}$-可分。

$1)\Rightarrow 2)$ 由定理1知, T_f有一个逆ρ-矩阵。设$T_f^{-1}=(d_{i+1,j+1})$, $y_{i+1}=\sum_{k=0}^{n-1}d_{i+1,k+1}x^k$, $i=0,1,\cdots,n-1$, 则由[3]知$\{y_{i+1};x^i\}$是一组可分集。由

于$T_f^{-1}\cdot T_f=E$，所以，$\sum_{i=0}^{n-1} d_{i+1,k+1}\,t(x^i)=\delta_{k0}$，$k=0,1,\cdots,n-1$，从而

$$\sum_{i=0}^{n-1} y_{i+1}\,t(x^i)=\sum_{i=0}^{n-1}\sum_{k=0}^{n-1} d_{i+1,k+1}\,x^k\,t(x^i)=\sum_{k=0}^{n-1}\sum_{i=0}^{n-1} x^k\,d_{i+1,k+1}\,t(x_i)=1,$$

所以$\{y_{i+1};x^i\}$为所需的可分集。（证毕）

由上述定理的2)⇒1)知，在不假定$f\in R^{\rho}[X]$时，我们仍可知T_f有一个左逆ρ-矩阵，因而有

定理3　设$f\in R[X;\rho]_{(0)}$。若f可分，且存在一个可分集$\{x_i;y_i\}$使得$\sum_i x_i\,t(y_i)=1$，则T_f有一个左逆ρ-矩阵。

注：当R为交换环时，f如果满足定理3，则$|T_f|$有意义，且为R中的可逆元。

4　应用及举例

设f为带有限自同构群G的Galois斜多项式，记$t_G=\sum_{\sigma\in G}\sigma$，易见$t_G$为$S\to R$的$R$-$R$-模同态。

引理3　设$S\supset R$为带有限自同构群G的Galois扩张，$\{x_i;y_i\}$为它的一组Galois集，则$\forall u\in S$，有$u=\sum_i x_i\,t_G(y_i\,u)$。

证明　由于$\{x_i;y_i\}$为Galois集，故它为可分集[4]，且$\sum_i x_i\,t_G(y_i)=1$。用定理2的2)⇒1)证明中的类似方法可证得　$u=\sum_i x_i\,t_G(y_i\,u)$。（证毕）

引理4　设f为带有限自同构群G的Galois斜多项式，且$t_G\,\rho^*=\rho^*\,t_G$。则$t=t_G$。

证明　因为$S=R[X;\rho]/fR[X;\rho]\supset R$为Galois扩张，故存在Galois集$\{x_i;z_i\}$，设$x_i=\sum_{k=0}^{n-1}x^k\,p_{ik}$，$z_i=\sum_{k=0}^{n-1}q_{ik}\,x^k$，则$\sum_i x_i\otimes z_i=\sum_{k=0}^{n-1}[x^k\otimes(\sum_i\sum_{s=0}^{n-1}p_{ik}\,q_{is}x^s)]$，记$d_{ks}=\sum_i p_{ik}q_{is}$，$y_k=\sum_{s=0}^{n-1}d_{ks}x^s$，$k=0,1,\cdots,n-1$，易证$\{x^k;y_k\}$仍为Galois集。

由于t，t_G皆为R-R-模同态，故只须证明$t(x^l)=t_G(x^l)$，$l=0,1,\cdots,n-1$，即知结论成立。由定义：

$$\begin{aligned}t(x^l)&=\sum_{i=0}^{n-1}\pi_i(x^l\cdot x^i)=\sum_{i=0}^{n-1}\pi_i\Big(x^l\cdot\sum_{j=0}^{n-1}x^j\,t_G(y_i\,x^i)\Big)\\&=\sum_{j=0}^{n-1}\sum_{i=0}^{n-1}\pi_i(x^{l+i})\rho^{-i}(t_G(y_ix^i))=\sum_{j=0}^{n-1}\sum_{i=0}^{n-1}\pi_i(x^{l+i})(\rho^*)^{-i}\,t_G(y_i\,x^i)\\&=\sum_{j=0}^{n-1}\sum_{i=0}^{n-1}\pi_i(x^{l+i})t_G(\rho^*)^{-i}(y_ix^i)=\sum_{j=0}^{n-1}\sum_{i=0}^{n-1}\pi_i(x^{l+i})t_G(x^iy_i)\\&=\sum_{j=0}^{n-1}t_G\Big(\sum_{i=0}^{n-1}\pi_i(x^{l+i})x^iy_i\Big)=\sum_{j=0}^{n-1}t_G(x^{l+i}\,y_i)=t_G\Big(x^l\sum_{j=0}^{n-1}x^j\,y_i\Big)\\&=t_G(x^l)。\text{（证毕）}\end{aligned}$$

由于Galois集必为可分集，故f为Galois的，则f为可分的。由定理2即得。

定理4　设$f\in R[X;\rho]_{(0)}$。若f为带有限自同构群G的Galois斜多项式，且$t_G\,\rho^*=\rho^*t_G$，则T_f有一个左逆ρ-矩阵。特别当R为交换环时，$|T_f|$有意义且为R中的可逆元。

举例（1）　说明条件$t_G\,\rho^*=\rho^*\,t_G$是合理的。

由〔5〕，当$f=x^2-xa-b\in R[X;\rho]_{(0)}$为Galois斜多项式时，它的自同构群为$\{1,\sigma\}$，这里$\sigma$的定义为：$\forall xb_1+b_0\in S=R[X;\rho]/fR[X;\rho]$，$\sigma(xb_1+b_0)=(a-x)b_1+b_0$，则$\rho^* t_G(xb_1+b_0)=\rho(a)\rho(b_1)+2\rho(b_0)$，$t_G\rho^*(xb_1+b_0)=a\rho(b_1)+2\rho(b_0)$。因为$f$为Galois的，从而也为可分的，由〔6〕知$\rho(a)=a$。所以$t_G\rho^*=\rho^* t_G$。

（2）说明可分不一定能推出$\tilde{\rho}$-可分。

取$R=\mathbf{Z}/(4)\oplus\mathbf{Z}/(4)$（环的直和），易见，$R$为交换环。作$\rho$：$R\to R$，$\rho(x_1,x_2)=(x_2,x_1)$。易验证$\rho$为环自同构，且$\rho^2=1$。作斜多项式环$R[X;\rho]$，取$f=X^2-1$，易见$f\in R[X;\rho]_{(0)}\cap R^{\rho}[X]$。令$d=(\bar{1},\bar{0})$，则$d+\rho(d)=\bar{1}$，因而$f$为可分[5]。但$|T_f|=\delta(f)=b^2-4ac=4\cdot\bar{1}=\bar{0}$非可逆元。故$f$非$\tilde{\rho}$-可分。

参 考 文 献

1 Ikehata S. Math J Okayama Univ,1983;25:23～28
2 Ikehata S. Math J Okayama Univ,1980;22:115～129
3 Szeto G. J Austal Math Soc (series A),1985;38:275～280
4 Miyashita Y. J Fac Sci Hokkaido Univ Ser I,1966;19:114～134
5 Nagahara T. Math J Okayama Univ,1976;19:65～95
6 Nagahara T. Math J Okayama Univ,1983;25:43～48

On $\tilde{\rho}$-Separability and Separability in Skew Polynomial Rings

*Lou Xiaolong**

Abstract

A characterization of the $\tilde{\rho}$-separable polynomial is given and a relation between $\tilde{\rho}$-separbility and separability is also obtained.

Keywords skew polynomial ring, Galois extensions of rings, separable extension, $\tilde{\rho}$-separable, Galois set, separable set

* Department of Mathemetics