中山大学学报（自然科学版）
第32卷 第2期 ACTA SCIENTIARUM NATURALIUM Vol.32 №.2
1993年 UNIVERSITATIS SUNYATSENI 1993

关于一类具有特殊Galois群的斜多项式的刻划

楼小龙 马麟浚
（中山大学数学系）

摘 要 在斜多项式环 $B[X;\rho]$ 含有一个特别的本原根的情况下，给出了 $f=X^n-u\in B[X;\rho]_{(0)}$ 为 Galois斜多项式的刻划。

关键词 Galois 扩张，斜多项式环，$\tilde{\rho}$-可分

1 符号和定义

全文总设B是一个含单位元 1 的环，ρ是B上的一个自同构，$B[X;\rho]=\Sigma_{i=0}\oplus X^iB$ 是关于B及ρ的斜多项式环，它的乘法由$aX=X\rho(a)$ $(\forall a\in B)$给出，我们分别用 $B[X;\rho]_{(0)}$ 及$B^\rho[X]$表示集合$\{f\in B[X;\rho]\mid fB[X;\rho]=B[X;\rho]f$，且 f的首项系数为1$\}$及具有 ρ不变系数的斜多项式集合。$f\in B[X;\rho]_{(0)}$称为是可分的(或带群G的Galois)斜多项式，如果$B[X;\rho]/fB[X;\rho]$是B上的可分扩张(或带群G的 Galois 扩张)；$f\in B^\rho[X]\cap B[X;\rho]_{(0)}$称为是 $\tilde{\rho}$-可分的斜多项式，如果 f的导 数f'(形式上的)模 $fB[X;\rho]$后在 $B[X;\rho]/fB[X;\rho]$中可逆。

全文中还使用下列约定记号

$C=\{a\in B\mid ab=ba,\forall b\in B\}$，$B^\rho=\{b\in B\mid\rho(b)=b\}$，$C^\rho=C\cap B^\rho$，$U(C^\rho)=\{a\in C^\rho\mid a$ 在 B 中可逆$\}$。对$f=X^n-a_{n-1}X^{n-1}-\cdots-a_0\in B[X;\rho]_{(0)}$，$S=B[X;\rho]/fB[X;\rho]=\{\Sigma_{i=0}^{n-1}r_ix^i\mid r_i\in B$，$x=X+B[X;\rho]f\}$，定义映射$\pi_i:S\to B$，$\pi_i(\Sigma_{j=0}^{n-1}r_jx^j)=r_i(\forall\Sigma_{j=0}^{n-1}r_jx^j\in S,i=0,1,2,\cdots n-1)$，$t:S\to B$，$t(u)=\Sigma_{i=0}^{n-1}\pi_i(ux^i)$，$(\forall\ u\in S)$，易验证$t$是$B$-$B$-模同态，记$T_f=(t_{i+1,j+1})$，其中$t_{i+1,j+1}=t(x^{i+j})$，$i,j=0,1,2,\cdots n-1$，易见$T_f$为$B$上的 $n\times n$ 对称矩阵，最后定义$\rho^*:B[X;\rho]\to B[X;\rho]$，$\rho^*(\Sigma_{i=0}^{k}X^id_i)=\Sigma_{i=0}^{k}X^i\rho(d_i)$，$\forall\Sigma_{i=0}^{k}X^id_i\in B[X;\rho]$。

2 正 文

设ω是B中的一个n次本原根，满 足$\omega\in U(C^\rho)$，$(1-\omega)(1-\omega^2)\cdots(1-\omega^{n-1})$ 为非零因

本文1991年10月21日收到

子，则对 $f=X^n-u\in B[X;\rho]_{(0)}$，$S=B[X;\rho]/fB[X;\rho]$，不难验证 $\alpha:\alpha(\Sigma_{i=0}^{n-1}r_ix^i)=\Sigma_{i=0}^{n-1}r_i\omega^ix^i$ 定义出 S 的一个自同构，且 α 的阶为 n，即 $\alpha^n=1$。

定理 1 ω 的假设如上，则 $f=X^n-u\in B[X;\rho]_{(0)}$ 为带群 $G=\langle\alpha\rangle$ 的 Galois 斜多项式 $\Leftrightarrow n$，u 在 B 中可逆。

注 1 很显然上述结论说明了[1]中定理4.2及定理4.4中 n 为可逆元的假设不但是必要的，而且还是充分的。

证明 "$\Rightarrow$" 因为 $(1-\omega)(1-\omega^2)\cdots(1-\omega^{n-1})$ 为非零因子，即 $(1-\omega)$、$(1-\omega^2)$、$\cdots(1-\omega^{n-1})$ 皆非零因子，所以由 $0=1-\omega^{kn}=(1-\omega^k)(1+\omega^k+\cdots+\omega^{(n-1)k})$，$k=1,2,\cdots n-1$，知 $1+\omega^k+\cdots+\omega^{(n-1)k}=0$，$k=1,2,\cdots n-1$。记 $t_G=\Sigma_{\sigma\in G}\sigma$，则 $t_G(\Sigma_{i=0}^{n-1}a_ix^n)=\Sigma_{i=0}^{n-1}a_i(1+\omega^i+\cdots+\omega^{(n-1)i})x^i=na_0$，由此易见 $\rho^*t_G=t_G\rho^*$，从而由[2]知，f 为 $\tilde{\rho}$-可分，因而 $\delta(f)=|Tf|$ 可逆。通过计算不难得到 $\delta(f)=n^nu^{n-1}$，因而 n、u 在 B 中可逆。

"$\Leftarrow$" 由 $\alpha(\Sigma_{i=0}^{n-1}a_ix^i)=\Sigma_{i=0}^{n-1}a_ix^i$ 得 $a_0=a_0,a_1(1-\omega)=0,a_2(1-\omega^2)=0,\cdots a_{n-1}(1-\omega^{(n-1)})=0$，由 ω 的所设知：$a_1=a_2=\cdots=a_{n-1}=0$，所以 $S^G=\{s\in S\mid\sigma(s)=s,\ \forall\sigma\in G\}=B$。由于 $x^n=u$，因而 x 在 S 中可逆，取 $C_i=\frac{x^{n-i-1}}{nx^{n-1}}$，$d_i=x^i$，$i=0,1,2\cdots n-1$，则 $\Sigma_{i=0}^{n-1}c_id_i=\frac{1}{nx^{n-1}}\cdot(nx^{n-1})=1$，$\Sigma_{i=0}^{n-1}c_i\alpha^x(d_i)=\frac{1}{nx^{n-1}}(1+\omega^k+\omega^{2k}+\cdots+\omega^{(n-1)k})x^{n-1}=0$，$k=1,2,\cdots n-1$，因而 $S\supset B$ 为带群 $G=\langle\alpha\rangle$ 的Galois扩张。

注意到在定理 1 的条件下，$t_G(x^i)=\begin{cases}0 & 0<i<n\\ n & i=0\end{cases}$。下面反过来考虑，若一个斜多项式 $f=X^m-a_{m-1}X^{m-1}-\cdots-a_0\in B[X;\rho]_{(0)}\cap B^\rho[X]$ 是 Galois 的，且所带的群 G 满足 $t_G(x_i)=\begin{cases}0 & 0<i<m\\ m & i=0\end{cases}$，那么 f 应该满足什么样的刻划条件？

定理 2 设 $f=X^m-a_{m-1}X^{m-1}-\cdots-a_0\in B[X;\rho]\cap B^\rho[X]$ 为带群 G 的 Galois斜多项式，且 $t_G(x^i)=\begin{cases}0 & 0<i<m\\ m & i=0\end{cases}$，则 m,a_0 在 B 中可逆，且 $ia_{m-i}=0$，$i=1,2,\cdots m-1$。

证明 由 t_G 所设，易见 $t_G\rho^*=\rho^*t_G$，因而由[2]知，$\delta(f)=|Tf|$ 可逆，且 $t(x^k)=t_G(x^k)$，$k=0,1,2,\cdots m-1$，从 $t(x^{i+j})=t_G(x^{i+j})=\begin{cases}m & i=j=0\\ 0 & 0<i+j<m\\ ma_0 & i+j=m\end{cases}$ 出发，不难计算出 $\delta(f)=m^m\cdot a_0^{m-1}$，因而 ma_0 在 B 中可逆。

下面用归纳法证明 $ia_{m-i}=0$，$i=1,2,\cdots m-1$。设当 $n<i$ 时，都有 $na_{m-n}=0$ 成立。因为 $t(x^i)=\Sigma_{j=0}^{m-1}\pi_j(x^{i+j})=\Sigma_{j=m-i}^{m-1}\pi_j(x^{i+j})=\Sigma_{l=0}^{i-1}\pi_{m-i+l}(x^{m+l})$，记 $d_l=\pi_{m-i+l}(x^{m+l})$，$b_l=\pi_{m-1}(x^{m+l})$，$l=0,1,2\cdots i-1$，则 $d_{l+1}=\pi_{m-i+l+1}(x^{m+l+1})=d_l+b_la_{m-i+l+1}$，$l=0,1,2\cdots l-2$。由上面的递推公式得：$d_{l+1}=d_0+b_0a_{m-i+1}+b_1a_{m-i+2}+\cdots+b_la_{m-i+l+1}$，$l=0,1,2\cdots i-2$。因而 $t(x^i)=d_0+d_1+\cdots+d_{i-1}=id_0+(i-1)b_0a_{m-i+1}+\cdots+b_{i-2}a_{m-1}$，再由归

纳假设及$d_0=\pi_{m-i}(x^m)=a_{m-i}$ 知，$0=t_G(x^i)=t(x^i)=ia_{m-i}$，因而$ia_{m-i}=0$，$i=0,1,2\cdots m-1$。

由定理2，我们就定理1的情况如下部分地回答了前面提出的问题。

定理3　设B中含有定理1中所叙的n次本原根，且Z在B中非零因子，则$f=X^n-a_{n-1}X^{n-1}-\cdots-a_0\in B[X;\rho]\cap B^\rho[X]$为带群$G$的 Galois斜多项式，且$t_G(x^i)=\begin{cases}0 & a<i<n\\ n & i=0\end{cases}$ $\Leftrightarrow f=X^n-a_0$，且$n,a_0$在$B$中可逆。

注2　从上述结果知道，对许多情况来说t_G 满足$t_G(x^i)=\begin{cases}0 & 0<i<n\\ n & i=0\end{cases}$是形式为 X^n-u的斜多项式为带群G的Galois扩张的特征。

作为定理2的部分逆有

定理4　设$f=X^m-a_{m-1}X^{m-1}-\cdots-a_0\in B[X;\rho]_{(0)}\cap B^\rho[X]$，若$m_1a_0$在$B$中可逆，且$ia_{m-i}=0$，$i=1,2,\cdots m-1$，则$f$为$\tilde{\rho}$-可分

证明　由定理2的归纳法证明，部分可以看出 $t(x^i)=\begin{cases}0 & 0<i<m\\ m & i=0\end{cases}$ 因而 $t(x^{i+j})=\begin{cases}m & i=j=0\\ 0 & 0<i+j<m\\ ma_0 & i+j=m\end{cases}$，由此不难算出，$\delta_{(f)}=|Tf|=m^ma_0^{m-1}$，由所设知$\delta(f)$可逆，由[2]知$f$为$\tilde{\rho}$-可分。

定理3的应用，举例说明如下

设B是复域R上的n维空间组成的环，即$B=R^n$。如下作B上的自同构 ρ：$\rho(x_1,x_2\cdots x_n)=(x_2,x_3\cdots x_n,x_1)$，$\forall(x_1,x_2\cdots x_n)\in B$。易见$\rho$为环同构。由于$R$为复域，所以$B$上可以就任何正整数找到满足定理3的$m$次本原根，且$Z$在 B中为非零因子，因此对于环 B 而言，$f=X^m-a_{m-1}X^{m-1}-\cdots-a_0\in B[X;\rho]\cap B^\rho[X]$ 为带群G的 Galois 斜多项式，且 $t_G(x^i)=\begin{cases}0 & 0<i<m\\ m & i=0\end{cases}\Leftrightarrow f=X^m-a_0$，其中$a_0$在$B$中可逆。

参考文献

1　Ma L J, Szeto G, Sea Bull Math, 1991, 15(1): 43～48

2　楼小龙. 中山大学学报(自然科学版), 1991, 30(4): 24～28

Characterization of Skew Polynomials with a Special Galois Group

*Lou Xiaolong**　　*Ma Linjun*

Abstract　Under the condition that a special prime root is ineluded in the skew polynomial ring $B[X;\rho]$, a characterization of skew polynomials with a given Galois group is obtained.

Keywords　Galois extension, skew polynomial ring, $\tilde{\rho}$-separable

*Department of Mathematics, Zhongshan University