第31卷 第3期 1992年

中山大学学报（自然科学版）
ACTA SCIENTIARUM NATURALIUM UNIVERSITATIS SUNYATSENI

Vol.31 №.3 1992

带内Galois群的Galois扩张

马麟浚
（中山大学数学系）

司徒子治
（美国伯莱里大学数学系）

摘 要 本文在Azumaya代数的条件下，对一般的带内Galois群的Galois扩张的结构进行了刻划。

关键词 Azumaya代数，Galois群，Galois扩张

1 引 言

F.R.DeMeyer证明：如果A是中心Galois扩张（即A在它的中心C上是Galois的），带内Galois群G，G的元素都是A的内自同构，则A是一个投射群代数$C\cdot G_f=\left\{\sum_{\alpha\in G} r_\alpha U_\alpha \mid r_\alpha\in C\right\}$，其中$\{U_\alpha\}\subset A$在$C$上是线性无关的，$rU_\alpha=U_\alpha r$，$\forall r\in C$，$U_\alpha U_\beta=U_{\alpha\beta}f(\alpha,\beta)$，这里的$f$：$G\times G\to U(C)$（$C$的全体可逆元）是一个因子组[1]。本文的目的就是要将上述的结构定理推广到带内Galois群（即每一个元素都是内自同构的群）G的Galois扩张A，结果是：如果$C\cdot G_f$是一个Azumaya C-代数，则$A\cong C\cdot G_f\otimes A^G$，使得$A^G$是$C$上的Azumaya代数，这样，当$A$是中心Galois扩张，特别当$A$是Galois代数时，$A^G=C$。改进了F.R.DeMeyer的结构定理。

2 定义与符号

本文中的环都是有单位元1的环，模都是么模，环T称为环S的扩张，如果S是T的子环且有相同的单位元1。可分扩张、可分代数、Azumaya代数、Galois扩张、Galois代数、Galois集等概念或定义均按照文〔2〕与〔3〕。

设T为S上的Galois扩张，带Galois群G。若S是T的中心，则此Galois扩张称为中心Galois扩张。若G中的每个元素都是T的内自同构，则称此Galais群G是内Galois群。

设K是交换环，$\bar{U}(K)$表示K中所有可逆元组成的乘法群，G是一个有限群，映射f：$G\times G\longrightarrow\bar{U}(K)$称为一个因子组，如果

$$f(\alpha\beta,\gamma)\cdot f(\alpha,\beta)=f(\alpha,\beta\gamma)\cdot f(\beta,\gamma)\quad\forall\alpha,\beta,\gamma\in G$$

本文1987年11月18日收到

一个投射群代数$K\cdot G_f$是指一个以$\{U_\alpha|\alpha\in G\}$为基的自由K-模$\sum\limits_{\alpha\in G}KU_\alpha$，以及由下列运算及分配律定义乘法：

$$kU_\alpha=U_\alpha k \quad \forall k\in K,\ \alpha\in G,$$
$$U_\alpha U_\beta=U_{\alpha\beta}f(\alpha,\beta),$$

这里，f：$G\times G\longrightarrow U(K)$是一个因子组。

3　Galois 扩张

引理 1 设A是B的Galois扩张，带内Galois群G，C为A的中心，则

(1)　$C^G=C$

(2)　A包含G在C上带因子集f：$G\times G\longrightarrow U(C)$的投射群代数$C\cdot G_f$。

证明　(1)　显然$C^G\subset C$，另一方面，$\forall c\in C$，$\alpha\in G$，由于α是A的内自同构，故存在$U_\alpha\in A$，使得

$$\alpha(x)=U_\alpha xU_\alpha^{-1} \quad \forall x\in A,$$

特别有
$$\alpha(c)=U_\alpha cU_\alpha^{-1}=cU_\alpha U_\alpha^{-1} \quad (\text{因}c\in C)$$
$$=c$$

所以　$c\in C^G$，$C\subset C^G$，因此$C^G=C$。

(2)　由(1)我们有$\{U_\alpha|\alpha\in G\}$，使得

$$\alpha(x)=U_\alpha xU_\alpha^{-1} \quad \forall x\in A,\ \alpha\in G.$$

于是有一个C-子代数$\sum\limits_{\alpha\in G}CU_\alpha$，它由$\{U_\alpha|\alpha\in G\}$在$C$上生成，使得

$$U_\alpha U_\beta=U_{\alpha\beta}f(\alpha,\beta),$$

其中　$f(\alpha,\beta)=U_\alpha U_\beta U_{\alpha\beta}^{-1}$，事实上，一方面$\alpha\beta(U_\alpha U_\beta)=U_{\alpha\beta}U_\alpha U_\beta U_{\alpha\beta}^{-1}$，另一方面，

$$\alpha\beta(U_\alpha U_\beta)=\alpha(U_\beta U_\alpha U_\beta U_\beta^{-1})=\alpha(U_\beta U_\alpha)=U_\alpha U_\beta U_\alpha U_\alpha^{-1}=U_\alpha U_\beta$$

所以，$U_\alpha U_\beta=U_{\alpha\beta}U_\alpha U_\beta U_{\alpha\beta}^{-1}=U_{\alpha\beta}f(\alpha,\beta)$，易见，$f(\alpha,\beta)\in U(C)$，

且
$$f:\ G\times G\longrightarrow U(C)$$

是一个因子集。

兹往证$\{U_\alpha|\alpha\in G\}$在C上是线性无关的。

由于A在B上是Galois的，带内Galois群G，所以存在A的Galois集$\{a_i,b_i\in A\mid i=1,2,\cdots,k\}$，$k$为某自然数。

设　$\sum\limits_\alpha r_\alpha U_\alpha=0$，$r_\alpha\in C$，则

$$\sum_{i,\alpha}r_\alpha a_iU_\alpha\beta^{-1}(b_i)=0 \quad \forall\beta\in G$$

从而
$$\sum_{i,\alpha}r_\alpha a_i\alpha\beta^{-1}(b_i)U_\alpha=0 \quad \forall\beta\in G$$

由于 $\sum_i a_i(\alpha\beta^{-1})(b_i)=\begin{cases}1 & \beta=\alpha\\ 0 & \beta\neq\alpha\end{cases}$

从而有 $r_\alpha U_\alpha=0 \quad \forall\alpha$

于是由U_α是可逆的，有

$$r_\alpha=0 \quad \forall\alpha$$

即得证$\{U_\alpha|\alpha\in G\}$在C上是线性无关的。

综合上述，可见$\sum_{\alpha\in G}CU_\alpha$是投射群代数$C\cdot G_f$，含于$A$

定理1 设A是Azumaya C-代数，又是B上的Galois扩张，带内Galois群G。如果$C\cdot G_f$（引理1所给）是Azumaya$C$-代数，则

(1) $A\cong C\cdot G_f\otimes_C A^G$是Azumaya C-代数。

(2) $(C\cdot G_f)^G=C$。

证明 (1) 由假设，A与$C\cdot G_f$都是Azumaya C-代数，$C\cdot G_f$是A的C-子代数，$C\cdot G_f\supset C$，则

$$A\cong C\cdot G_f\otimes_C E$$

其中E是$C\cdot G_f$在A中的换位子，也是Azumaya C-代数[4]。下面往证$E=A^G$：

一方面，$\forall x\in E$，$xU_\alpha=U_\alpha x \quad \forall\alpha\in G$，从而

$$\alpha(x)=U_\alpha xU_\alpha^{-1}=xU_\alpha U_\alpha^{-1}=x \quad \forall\alpha\in G.$$

$$\therefore \quad x\in A^G,\ E\subset A^G.$$

另一方面，$\forall a\in A^G$。

$$aU_\alpha=U_\alpha\alpha^{-1}(a)=U_\alpha a \quad \forall\alpha\in G.$$

从而 $ad=da \quad \forall d\in C\cdot G_f$。

$$\therefore \quad a\in E \quad A^G\subset E,$$

于是得证$E=A^G$，因此得证

$$A\cong C\cdot G_f\otimes_C A^G,\ A^G\text{是Azumaya } C\text{-代数。}$$

(2) 令$D=C\cdot G_f=\sum_{\alpha\in G}CU_\alpha$，由于$D\supset C$，$C^G=C$

故显然有 $D^G\supset C$。

反之，若$x\in D^G$，则$\alpha(x)=x \quad \forall\alpha\in G$，从而

$$U_\alpha x=\alpha(x)U_\alpha=xU_\alpha \quad \forall\alpha\in G$$

从而 $xd=dx \quad \forall d\in D$ (i)

类似地有$ad=da \quad \forall a\in A^G$，$\forall d\in D$

从而 $ax=xa \quad \forall a\in A^G$ (ii)

由(1)知 $A\cong C\cdot G_f\otimes_C A^G$

同构映射为[4] $C\cdot G_f\otimes_C A^G\longrightarrow A$

$$d\otimes a\longmapsto da$$

由此可得 $A=(C\cdot G_f)\cdot A^G=D\cdot A^G$

从而由(i)、(ii)得$x\in C$，$D^G\subset C$。

于是得证$(C\cdot G_f)^G=C$。

推论 1　设A是Azumaya C-代数，又是B上的Galois扩张，带内Galois群G。$C\cdot G_f$（引理1）是Azumaya C-代数，则A是中心Galois B-代数，当且仅当A在C上的秩可定义且等于G的阶$|G|$，其中A在C上的秩的定义按[4]。

证明（$\Longrightarrow$）。设A是B上的中心Galois代数，则$A^G=B=C, A\cong C\cdot G_f\otimes_C C\cong C\cdot G_f$。（定理1），因此$A$在$C$上的秩$rank_C(A)=|G|$。

（$\Longleftarrow$）。如果$rank_C(A)=|G|$，由定理1，$A\cong C\cdot G_f\otimes_C A^G$。所以$rank_C A^G$可定义，使得　$rank_C(A)=|G|\cdot rank_C(A^G)$。从而得　$rank_C(A^G)=1$。

由于A^G是Azumaya C-代数，所以C是A^G的直和项[4]，于是由$rank_C(A^G)=1$，就得出$A^G=C$。因此，$A\cong C\cdot G_f$是C上的中心Galois代数，带内Galois群G，或者说A是B上的中心Galois代数，（因$B=A^G=C$）带内Galois群G

注意，在中心Galois扩张的情形，$C\cdot G_f$自然是Azumaya C-代数[5]。所以，上述定理中$C\cdot G_f$是Azumaya的条件是多余的。

下面是对定理1中Azumaya代数CG_f的特征的一个刻划。

定理 2　设A是Azumaya C-代数，又是B上的Galois扩张，带内Galois群G，G的阶为某正整数n，则$C\cdot G_f$是Azumaya C-代数，当且仅当n在C中是可逆的且$C\cdot G_f\cap B=C$。

证明（$\Longrightarrow$）。设$C\cdot G_f$是Azumaya C-代数，则n在C中是可逆的[6]。又显然$C\subset C\cdot G_f\cap B$。反之，设$x\in C\cdot G_f\cap B$，则$U_\alpha x=\alpha(x)U_\alpha=xU_\alpha$　$\forall\alpha\in G$。因此$x\in Z(C\cdot G_f)$（$C\cdot G_f$的中心），从而$x\in C$。所以$C=C\cdot G_f\cap B$。

（$\Longleftarrow$）。设n在C中是可逆的，所以$C\cdot G_f$是可分C-代数[6]。又易见$C\cdot G_f\cap B$是$C\cdot G_f$的中心，事实上，若$x\in C\cdot G_f\cap B$，则$U_\alpha x=\alpha(x)U_\alpha=xU_\alpha$　$\forall\alpha\in G$。因此$x\in Z(C\cdot G_f)$。反之，若$y\in Z(C\cdot G_f)$。则$\sigma(y)=U_\sigma yU_\sigma^{-1}=yU_\sigma U_\sigma^{-1}=y$。故$y\in C\cdot G_f\cap B$。所以$Z(C\cdot G_f)=C\cdot G_f\cap B$，从而由$C\cdot G_f\cap B=C$知$Z(C\cdot G_f)=C$。因此$C\cdot G_f$在$C$上是Azumaya的。

现在我们应用定理1与2来改进带内Galois群的中心Galois代数的DeMeyer的结构定理。

推论 2　如果A是B上的Galois代数，带内Galois群G，G的阶n在B中是可逆的。则
$A=B\cdot G_f$。

其中，$f(\alpha,\beta)=U_\alpha U_\beta U_{\alpha\beta}^{-1}$，$\alpha(x)=U_\alpha xU_\alpha^{-1}$　$\forall\alpha\in G$，某$U_\alpha\in A$与$\forall x\in A$。

证明　由于A是B上的Galois代数，所以A是可分的B-代数[5]。因此A在它中心上是Azumaya代数[4]，现在，由于$B\subset C$（A是B-代数）所以$B=C$（因由引理1，$C=C^G\subset A^G=B$）。因此，$C\cdot G_f\cap B=C$，又，n在C中可逆，所以$C\cdot G_f$是Azumaya C-代数（根据定理2），$A\cong C\cdot G_f\otimes_C A^G\cong C\cdot G_f=B\cdot G_f$（根据定理1，及$A^G=B=C$）。

注意，对任何带内Galois群的中心Galois代数，该群的阶数n自然是可逆的[2]。

最后，以定理1的逆定理来结束本文。

定理 3　设A是交换环K上的Azumaya代数，带有限的内K-自同构群G。如果$\sum_{\alpha\in G}KU_\alpha$

是K的Azumaya投射群代数。则A是$Z_A(\sum\limits_{\alpha\in G}KU_\alpha)$（$\sum\limits_{\alpha\in G}KU_\alpha$在$A$中的换位子子代数）上的Galois扩张，带Galois群G。

证明 设$B=Z_A(\sum\limits_{\alpha\in G}KU_\alpha)$，由于$A$与$\sum\limits_{\alpha\in G}KU_\alpha$都是Azumaya K-代数。所以根据Azumaya代数的换位子定理[4]有

$$A\cong(\sum_{\alpha\in G}KU_\alpha)\otimes_K B$$

使得B在K上是Azumaya的。$\forall b\in B$，由于$bU_\alpha=U_\alpha b=\alpha(b)U_\alpha$，$\forall\alpha\in G$，从而$\alpha(b)=b$ $\forall\alpha\in G$，因此$b\in A^G$，$B\subset A^G$，类似地，$\forall a\in A^G$，$aU_\alpha=U_\alpha a$ $\forall\alpha\in G$，从而$ad=da$ $\forall d\in\sum\limits_{\alpha\in G}KU_\alpha$，因此$A^G\subset B$。故有$B=A^G$。

再有，由于$\sum\limits_{\alpha\in G}KU_\alpha$是$K$上Azumaya投射群代数，所以它是Galois K-代数，带内Galois群$G|_{\sum\limits_{\alpha\in G}KU_\alpha}$（〔6〕定理3）。

注意到[4]（$\sum\limits_{\alpha\in G}KU_\alpha)B=A$，带自同构群$G$使得$B=A^G$，我们就可得到$A$是$A^G(=B)$上Galois扩张，因为$\sum\limits_{\alpha\in G}KU_\alpha$的Galois集可用作$A$的Galois集。

参 考 文 献

1 F R DeMeyer. Osaka J Math, 1965(2): 117～127
2 马麟浚，司徒子治. 中山大学学报（自然科学版）,1986,3: 46～49
3 马麟浚，司徒子治. 中山大学学报论丛（自然科学）,〔10〕: 62～65
4 DeMeyer F R, Ingraham E. Lecture Notes Math, [Berlin-Heidelberg-NewYork Springer-Verlag, 1971, 181
5 Y Miyashita. Finte Outer Galois Theory of Non-Commutative Rings. J Fac Sei Hokkaido Univ, Ser.I, 1966,19: 114～134
6 F R DeMeyer. IL Math, 1966,10: 287～295

Galois Extensions with Inner Galois Groups

Ma Linjun   George Szeto*

Abstract Suppose that ring A is a Galois extension over its subring B, with finite inner Galois group G.

The main result of this paper is as follows:

If (1) A is an AzumayaC - Algebra,

and (2) $C\cdot G_f$ is an Azumaya C-Algebra(or eguivalently, $n\in U(C)$ and $C\cdot G_f\cap B=C$)

then $A\cong C\cdot G_f\otimes_C A^G$ such that A^G is an Azumaya C-Algebra, where C is the center of A, U(C)the units of C, $C\cdot G_f$ the projective group algebra of G over C, with factor set $f: G\times G\to U(C)$.

Moreover, the corresponding converse theorem is also given.

Keyword Azumaya algebras, Galois group, Galois extension

* Department of Mathemetics, Zhongshan University