交叉积的中心与环的Galois扩张

马麟浚　　司徒子治
（中山大学数学系）　（美国伯莱里大学数学系）

摘　要

本文对交换环R与其自同构群G的交叉积$\Delta(R,G)$的中心的元素，给出一个具体的表示形式，然后在$\Delta(R,G)$是可分的R^G-代数的假设下(R^G是G的不动环)，给出Galois扩张的一个判别准则，还对R对G的中心的元素的幂等Galois扩张进行讨论，并取得了一些结果.

§1 准　备

自始至终，R是一个有单位元1的交换环，G是R的阶数为n的有限的自同构群，R^G是G的不动环. R-代数A称为中心的，如果A是忠实的R-模且$R\cdot 1$是A的中心；R-代数A称为可分的，如果存在$\{x_i,y_i\in A\mid i=1,2,\cdots,n\}$，使得

$$\sum_{i=1}^{N}x_iy_i=1,\quad \sum_{i=1}^{N}xx_i\otimes y_i=\sum_{i=1}^{N}x_i\otimes y_ix,\quad \forall x\in A$$

这里的$\otimes$是张量积$\otimes_R$，中心的可分代数叫做Azumaya代数.

设S是交换的忠实的R-代数，K是S的有限的自同构群. 我们称S是R上的Galois扩张，如果满足：

(i)　$S^K=R$，(S^K是K的不动环)；

(ii)　$\forall 1\neq\sigma\in K$，由$\{x-\sigma x\mid x\in S\}$生成的$S$的理想$I_\sigma$都等于$S$.

§2 正　文

先考察交叉积$\Delta(R,G)$的中心Z.

定义　设R是有单位元1的交换环，G是R的有限的自同构群，$|G|=n<\infty$，所谓R与G的带平凡因子组的交叉积，记为$\Delta(R,G)$，是指有自由基$\{U_\sigma\mid\sigma\in G\}$的$R$-自由模

$$\Delta(R,G)=\sum_{\sigma\in G}RU_\sigma$$

它还具有如下规定的乘法：

本文1984年7月收到

$$(\sum r_i U_{\sigma_i})\cdot(\sum r_i U_{\sigma_j})=\sum_{i,j} r_i\sigma_i(y_i)U_{\sigma_i\sigma_j}$$

不难验证，$\Delta(R,G)$是一个R-代数，单位元是U_1，我们以Z表示$\Delta(R,G)$的中心。

由于$|G|=n<\infty$，故G可表为有限个两两互不相交的共轭类之并，即

$G=C_1\cup C_2\cup\cdots\cup C_k$　　对某正整数k，其中C_i为共轭类$(i=1,2,\cdots,k)$，$C_s\cap C_t=\phi$，$\forall s\neq t$。对于每个共轭类C_i，我们选定一个代表 $g_i\in C_i(i=1,2,\cdots,k)$，这样一来，

$$C_i=\{\sigma\in G\mid \exists\tau\in G\text{使得}\sigma=\tau g_i\tau^{-1}\}$$

我们约定$C_1=\{1\}$，这里的1是G的恒等同构，因此$g_1=1$。我们还将使用下列符号，

I_σ表示由$\{r-\sigma(r)\mid r\in R\}$生成的$R$的理想，特别记$I_i=I_{g_i}$，

J_σ表示I_σ的零化子，特别记$J_i=J_{g_i}$，

J_σ^σ表示σ在J_σ中的不动子集，特别记

$$J_i^{g_i}=J_{g_i}^{g_i}$$

我们有下面的

定理 1　$x\in Z$ 当且仅当

$$x=\sum_{i=1}^{k}\sum_{\sigma\in C_i}\tau(r_i)U_\sigma$$

其中　(1) $\sigma=\tau g_i\tau^{-1}$，

(2) $r_i\in J_i^{g_i}$　$(i=1,2,\cdots,k)$。

证明　设$x\in Z$，$x=\sum r_\sigma U_\sigma$。$\forall r\in R$，由$rx=xr$ $\Rightarrow$ $\sum r r_\sigma U_\sigma=\sum r_\sigma U_\sigma r$

$\Rightarrow$ $r r_\sigma=r_\sigma\sigma(r)$　$\forall\sigma\in G$ $\Rightarrow$ $r_\sigma(r-\sigma(r))=0$　$\forall\sigma\in G$

$\therefore$　$r_\sigma\in J_\sigma$。

$\forall U_\tau$，由$x\in Z\Rightarrow U_\tau x=xU_\tau\Rightarrow$ $\sum\tau(r_\sigma)U_\tau U_\sigma=\sum r_\sigma U_\sigma U_\tau$

这样一来，当$\tau g_i=\sigma\tau$对某σ时，我们有

$\sigma=\tau g_i\tau^{-1}$ 与 $U_\tau U_{g_i}=U_\sigma U_\tau$

$\Rightarrow$ $\tau(r_{g_i})=r_\sigma$，$\sigma\in C_i$

特别，　$g_i(r_{g_i})=r_{g_i}$，即$r_{g_i}\in J_i^{g_i}$，记$r_i=r_{g_i}$

于是

$$x=\sum_{i=1}^{k}\sum_{\sigma\in C_i}\tau(r_i)U_\sigma$$

其中　$\sigma=\tau g_i\tau^{-1}$；　$r_i\in J_i^{g_i}$。

反之，设

$$x=\sum_{i=1}^{k}\sum_{\sigma\in C_i}\tau(r_i)U_\sigma$$

其中

(1) $\sigma=\tau g_i\tau^{-1}$

(2) $r_i\in J_i^{g_i}$ $(i=1,2,\cdots,k)$

先证 $rx=xr$ $\quad\forall r\in R$

为此，注意：由 $r_i\in J_i^{g_i}\subset J_i$及$J_i$是$I_i$的零化子可推得$Rr_i\subseteq J_i^{g_i}$。

$$rx=\sum_{i=1}^{k}\sum_{\sigma\in C_i}r\tau(r_i)U_\sigma$$

$$xr=\sum_{i=1}^{k}\sum_{\sigma\in C_i}\tau(r_i)U_\sigma r=\sum_{i=1}^{k}\sum_{\sigma\in C_i}\tau(r_i)\sigma(r)U_\sigma$$

$$\begin{aligned}\tau(r_i)\sigma(r)&=\tau(r_i)\tau g_i\tau^{-1}(r)=\tau(r_i(g_i(\tau^{-1}(r))))\\&=\tau(g_i(r_i)(g_i(\tau^{-1}(r))))=\tau(g_i(r_i\tau^{-1}(r)))\\&=\tau(\tau^{-1}(r)r_i)=\tau\tau^{-1}(r)\tau(r_i)=r\tau(r_i)\end{aligned}$$

$\therefore rx=xr$

再证 $U_\phi x=xU_\phi$ $\quad\forall\phi\in G$

$$U_\phi x=\sum_{i=1}^{k}\sum_{\sigma\in C_i}U_\phi\tau(r_i)U_\sigma=\sum_{i=1}^{k}\sum_{\sigma\in C_i}\phi(\tau(r_i))U_\phi U_\sigma$$

$$xU_\phi=\sum_{i=1}^{k}\sum_{\sigma\in C_i}\tau(r_i)U_\sigma U_\phi$$

对于给定的σ，必存在ϕ 使得

$\phi\sigma=\phi\phi$ 从而 $\phi=\phi\sigma\phi^{-1}\Rightarrow\phi$与$\sigma$同属一个共轭类，以及 $U_\phi U_\sigma=U_\phi U_\phi$

当$\sigma\in C_i$时，$\phi\in C_i$

$U_\phi x$中$U_\phi U_\sigma$的系数为$\phi(\tau(r_i))$，其中有

$\sigma=\tau g_i\tau^{-1}$

由于$\phi=\phi\sigma\phi^{-1}=\phi\tau g_i\tau^{-1}\phi^{-1}=(\phi\tau)g_i(\phi\tau)^{-1}$，故$xU_\phi$中$U_tU_\phi$的系数是$(\phi\tau)(r_i)=\phi(\tau(r_i))$，恰好等于$U_\phi x$中$U_\phi U_\sigma$的系数。

$\therefore U_\phi x=xU_\phi$

综合起来得

$$(\sum_{\sigma\in G}RU_\sigma)x=x(\sum_{\sigma\in G}RU_\sigma)$$

$\therefore x\in Z$。

引理 2 如果$\Delta(R,G)$是AzumayaR^G-代数，则R是R^G上的Galois扩张。

证明见[4]的定理2。

推论 3 设$\Delta(R,G)$是R^G上可分代数。如果 $\forall i=2,3,\cdots,k$，I_i有非零因子的元素，则R是R^G上的Galois扩张。

证明 $I_i(i=2,\cdots,k)$有非零因子的元素

$$\Rightarrow\quad J_i=\{0\}\quad i=2,3,\cdots,k,$$

$$\Rightarrow\quad J_i^{g_i}=\{0\}\quad i=2,3,\cdots,k,$$

$$\Rightarrow \quad \tau(J_i^{g_i}) = \{0\} \quad \forall \tau \in G \quad i = 2, \cdots, k,$$

$$\Rightarrow \quad Z = R^G U_1 \cong R^G.$$

所以$\Delta(R,G)$是Azumaya R^G-代数，从而由引理 2 即得本推论。

推论 4　设$\Delta(R,G)$是R^G上可分代数．如果R是整环，则R是R^G上的Galois扩张。

证明　因整环的非零理想必有非零因子的元素。

现在，我们来讨论一些关于G的中心$C(G)$的元素的问题。

引理 5　如果$g_i \in C(G)$，则I_i是G-不变理想(即$\forall \sigma \in G$，均有$\sigma(I_i) = I_i$)。

证明　$\forall \sigma \in G$

$$\sigma[s(r - g_i(r)] = \sigma(s)[\sigma(r) - g_i(\sigma(r))] \in I_i \quad \forall s, r \in R$$

$$\Rightarrow \quad \sigma(I_i) \subseteq I_i \Rightarrow \quad \sigma^{-1}(I_i) \subseteq I_i \Rightarrow I_i \subseteq \sigma(I_i).$$

$$\therefore \quad \sigma(I_i) = I_i \quad \forall \sigma \in G$$

定理 6　如果$g_i \in C(G)$，则$I_i[\Delta(R,G)]$是$\Delta(R,G)$的理想。

证明　由引理 5，$\sigma(I_i) = I_i$

$$\Rightarrow \quad U_\sigma I_i = \sigma(I_i) U_\sigma = I_i U_\sigma \quad \forall U_\sigma \quad \Rightarrow \quad [\Delta(R,G)] I_i = I_i [\Delta(R,G)].$$

定理 7　如果$\Delta(R,G)$是可分的R^G-代数，$g_i \in C(G)$，则

(1) $\dfrac{\Delta(R,G)}{I_i[\Delta(R,G)]}$是Azumaya $\dfrac{Z + I_i[\Delta(R,G)]}{I_i[\Delta(R,G)]}$ - 代数

(2) $J_i = \mathrm{Re}, I_i = R(1-e)$对某幂等元素$e \in J_i^{g_i}$使得$R = J_i \oplus I_i$且$R^{g_i} = \mathrm{Re} + R^{g_i}(1-e) = R_e + (R(1-e))^{g_i}$

(3) $J_i \subseteq R^{g_i}$

证明　(1)是文[3]的第二章命题1.11与定理3.8的直接推论。

(2)　由于

$$\overline{r - g_i(r)} = \overline{0} \quad \text{在} \frac{\Delta(R,G)}{I_i[\Delta(R,G)]} \quad \Rightarrow \quad \bar{r} = \overline{g_i(r)} \quad \forall r \in R,$$

又由　$U_{g_i} r = g_i(r) U_{g_i} \Rightarrow U_{g_i} \bar{r} = \overline{g_i(r)} U_{g_i}$

从而有

$$U_{g_i} \bar{r} = \bar{r} U_{g_i} \quad \forall r \in R$$

还有，由$g_i \in C(G) \Rightarrow U_{g_i} U_\sigma = U_\sigma U_{g_i} \quad \forall U_\sigma$

由此可得

$$U_{g_i} \in \frac{Z + I_i[\Delta(R,G)]}{I_i[\Delta(R,G)]}$$

注意到在Z中 U_{g_i} 的系数属于 $J_i^{g_i} \subseteq J_i$，我们得到

$$1 = e + a \quad \text{对某} e \in J_i^{g_i} \subseteq J_i, \ a \in I_i$$

由于J_i是I_i的零化子，$ea = 0 \Rightarrow e^2 = e, \ a^2 = a$，

再由$e \in J_i^{g_i}$，$a = 1 - e \Rightarrow a \in I_i^{g_i}$．

往证$J_i = \mathrm{Re}$

一方面$e\in J_i\Rightarrow Re I_i=\{0\}\Rightarrow \mathrm{Re}\subseteq J_i$，

另一方面，$\forall r\in J_i$，由$1=e+a\Rightarrow r=re\Rightarrow r\in Re\Rightarrow J_i\subseteq \mathrm{Re}$

$\therefore J_i=\mathrm{Re}$。

类似可得 $I_i=R(1-e)$

$R=J_i\oplus I_i$是显然的。

现往证 $R^{g_i}=Re+R^{g_i}(1-e)=Re+(R(1-e))^{g_i}$

由于显然有

$$R^{g_i}\subseteq Re+R^{g_i}(1-e),\ R^{g_i}(1-e)\subseteq R^{g_i},$$
$$R^{g_i}(1-e)\subseteq(R(1-e))^{g_i},$$

故仅需证明$\mathrm{Re}\subseteq R^{g_i}$与$(R(1-e))^{g_i}\subseteq R^{g_i}(1-e)$

首先$\forall r\in R$，由于$e\in J_i^{g_i}\subseteq J$，$r-g_i(r)\in I_i$

$\Rightarrow re-g_i(re)=re-g_i(r)g_i(e)=re-g_i(r)e=(r-g_i(r))e=0$

$\Rightarrow re\in R^{g_i}\ \ \therefore \mathrm{Re}\subseteq R^{g_i}$

其次，$\forall r\in(R(1-e))^{g_i}\Rightarrow r=r_1(1-e)$，$r_1\in R\quad g_i(r)=r$

$\Rightarrow r=g_i(r_1)(1-e)$即$r_1(1-e)=g_i(r_1)(1-e)$

$\Rightarrow r_1-g_i(r_1)=(r_1-g_i(r_1))e=0\Rightarrow r_1\in R^{g_i}\Rightarrow r\in R^{g_i}(1-e)$

$\therefore (R(1-e))^{g_i}\subseteq R^{g_i}(1-e)$

至于(3)的结论，在上面已经得到。

推论 8 如果$\Delta(R,G)$是可分的R^G—代数，G是交换群，R仅有幂等元素0与1，则R是R^G上的Galois扩张。

证明 $\forall 1\neq g_i\in G$，由定理7，有

$$I_i=R(1-e)\quad e\text{为幂等元素}$$

因为$I_i\neq\{0\}$，$\therefore e\neq 1\Rightarrow e=0\Rightarrow I_i=R$，所以$R$是$R^G$上的Galois扩张。

从前面的讨论中可见，当$\Delta(R,G)$为可分的R^G-代数时，对于每一个$g\in C(G)$，都导出一个子环$R(1-e)$(这里的e为R的幂等元素，$g(e)=e$)，单位元是$1-e$，因为$g(R(1-e))=R(1-e)$，所以$\langle g\rangle$是$R(1-e)$上的一个自同构群。下面讨论这方面的Galois扩张问题。

引理 9 设$g\in G$，g的阶数m为素数，以I表示由$\{r-g(r)\mid r\in R\}$生成的R的理想，$I^{(k)}$表示由$\{r-g^k(r)\mid r\in R\}$生成的R的理想，则

$$I^{(k)}=I\quad \forall k=1,2,\cdots,m-1$$

证明 由于$\langle g\rangle=\langle g^k\rangle$，$(k=1,2,\cdots,m-1)$

$\Rightarrow\exists$整数l使得

$$g=(g^k)^l$$

$$\Rightarrow r-g(r)=r-(g^k)^l(r)=(1-(g^k)^l)(r)$$
$$=(1-g^k)(1+g^k+\cdots+(g^k)^{l-1})(r)$$
$$=(1-g^k)(t),\ (t=(1+g^k+\cdots+(g^k)^{l-1})(r))$$
$$=t-g^k(t)\in I^{(k)}\quad \forall r\in R$$

$\therefore I\subseteq I^{(k)}$

类似有$I^{(k)}\subseteq I$。所以$I^{(k)}=I$，$(k=1,2,\cdots,m-1)$。

定理10 设$\Delta(R,G)$为可分的R^G-代数，$g_i\in C(G)$，g_i的阶数为素数，则$R(1-e)$是$(R(1-e))^{g_i}$上带Galois群$\langle g_i\rangle$的Galois扩张(这里的$R(1-e)$是定理7中的)。

证明 由引理9　$\forall 1\neq\sigma\in\langle g_i\rangle$，都有

$$I_\sigma=R(1-e)$$

故剩下来要证明的是

$$I_\sigma=I'_\sigma$$

这里的I'_σ是由$\{r-\sigma(r)\mid r\in R(1-e)\}$生成的$R(1-e)$理想。

一方面，显然有

$$\{r-\sigma(r)\mid r\in R(1-e)\}\subseteq\{r-\sigma(r)\mid r\in R\}$$

$$\therefore\quad I'_\sigma\subseteq I_\sigma$$

另一方面，$\forall r\in R$，由于$R=J_i\oplus I_i, J_i\subseteq R^{g_i}\Rightarrow\exists r_1\in J_i, r_2\in I_i$使得$r=r_1+r_2$，$g_i(r_1)=r_1$从而$\forall\sigma\in\langle g_i\rangle$，有$\sigma(r_1)=r_1$　$\Rightarrow$　$r-\sigma(r)=r_1+r_2-(\sigma(r_1)+\sigma(r_2))=r_2-\sigma(r_2)\in I'_\sigma$

$\Rightarrow$　$I_\sigma\subseteq I'_\sigma$

所以$I_{\sigma'}=I_\sigma=R(1-e)$　$\forall 1\neq\sigma\in\langle g_i\rangle$，证完。

参考文献

[1] S. Chase, D. Harrison and A. Rosenbeerg, Galois theory and Galois Cohomology of Commutative Rings, Mem. Amer. Math. Soc., 152(1965).

[2] F. DeMeyer, *Osaka J. Math.*, 2(1965), 117-127.

[3] F. DeMeyer and E. Ingraham, Separable algebras over Commutative Rings, *Lecture Note, Math.*, 181(1971), Berlin-Heidelberg-New York, Springer.

[4] S. Ikehata, *Math. J. OKayama Univ.*, 23(1981), 17-18.

[5] S. Ikeheta, Azumaya Algebras and skew Polynomial Rings, *Math J. Okayama Univ.*, 23(1981).

[6] G. Szeto, *J. Pure and Appl Algebra*, 16(1980), 315-322.

[7] G. Szeto and Y. F. Wong, *J. Austral. Math. Soc.* (Series A), 32(1982),165-170.

[8] G. Szeto. On Separable Abelian extension of Rings, *Internat. J. Math. and Math. Sci.*, 4(1982).

[9] G. Szeto and Y. F. Wong, *J. Austral Math. Soc.* (Series A), 34(1983),394-398.

The Center of Crossed Product and Galois Extension of Rings

Ma Linjun
(Department of Mathematics
Zhong Shan University
The People's Republic of China)

George Seeto
(Department of Mathematics
Bradley University
U.S.A.)

Abstract

Let R be a Commutative ring with identity 1, G be a finite group of automorphism of R, It's order is n, $C(G)$ be the center of G, $R^G=\{r\in R\mid\sigma(r)=r\ \forall\sigma\in G\}$, $C_i=\{\sigma\in G\mid\sigma=\tau g_i\tau^{-1}$ for some $\tau\in G\}$, where $g_i\in G$, $i=1,2,\cdots,k$, $g_1=1$ such that

$$G=C_1\cup C_2\cup\cdots\cup C_k,\ C_s\cap C_t=\phi\ (s\neq t)$$

I_i be the ideal of R generated by $\{r-g_i(r)\mid r\in R\}$, J_i be the annihilator of I_i, $R^{g_i}=\{r\in R\mid g_i(r)=r\}$, $\Delta(R,G)$ be the Crossed product of R and G with trivial factor set. That is

$$\Delta(R,G)=\sum_{\sigma\in G}RU_\sigma \text{ such that}$$

$$(\Sigma r_\sigma U_\sigma)(\Sigma r_\tau U_\tau)=\sum_{\sigma,\tau}r_\tau\sigma(r_\tau)U_{\sigma\tau}$$

The main results of this paper as follows.

Firet,

Theorem 1. $x\in Z$ if and only if

$$x=\sum_{i=1}^{k}\sum_{\sigma\in C_i}\tau(r_i)U_\sigma$$

where (1) $\sigma=\tau g_i\tau^{-1}$

(2) $r_i\in J_i^{g_i}$ $(i=1,2,\cdots,k)$

In next, Under the hypothes: The $\Delta(R,G)$ is a separable R^G-algebra.

We have

Corollary 3. If I_i has non-zero-divisors $\forall i=2,3,\cdots,k$. Then R is a Galois Extension over R^G.

Theorem 7. If $g_i\in C(G)$, Then

(1) $\frac{\Delta(R,G)}{I_i[\Delta(R,G)]}$ is an Azumaya $\frac{Z+I_i[\Delta(R,G)]}{I_i[\Delta(R,G)]}$-Algebra.

(2) $J_i=Re$, $I_i=R(1-e)$ for some idempotent e in $J_i^{g_i}$, such that

$R=J_i\oplus I_i$ and $R^{g_i}=Re+R^{g_i}(1-e)=R_e+(R(1-e))^{g_i}$

(3) $J_i\subseteq R^{g_i}$

Theorem10. If $g_i\in C(G)$ and the order of g_i is prime. Then $R(1-e)$ is a Galois Extension over $(R(1-e))^{g_i}$ with Galois group $\langle g_i\rangle$ (where the $R(1-e)$ as theorem 7)