第33卷 第3期
1994年 7月

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

Vol. 33 No. 3
Jul. 1994

交换环上的Galois扩张的G－同态*

邓信德 (中山大学数学系,广州 510275)

司徒子治 (美国伯莱里大学数学系)

摘 要 定义了交换环R的关于自同构群G的G－自同态,给出有关G－自同态的一些基本性质,证明了Galois扩张的G－自同态象仍为Galois扩张,并且还得到它的逆命题.

关键词 Galois扩张,G－同态,G－理想

分类号 O153.4

对环上的Galois理论已作过很多的研究[1~3],证明了交换环R是由它的有限自同构群G的固定元素构成的子环R^G上的Galois扩张的充要条件是$I_a = R, \forall\ 1 \neq a \in G$,其中$I_a$是$R$的由$\{r - a(r) \mid r \in R\}$生成的理想.本文证明交换环的Galois扩张的$G$－自同态象仍为Galois扩张带由$G$导出的Galois群$G'$.反之,设$\varnothing$是环$R$的$G$－自同态,如果$\varnothing(R)$是Galois扩张带Galois群$G'$,其中$G'$是由$G$导出且同构于$G$,则$R$亦是Galois扩张带Galois群$G$.而且$\varnothing(R) \subseteq R/\ker\varnothing$是$G'$－同构,$G' \subseteq \overline{G}$,其中$\overline{G}$是$R/ker\varnothing$的Galois群且$\overline{G}$是由$G$导出并同构于$G$.一般地,本文将上述结果推广到带自同构群$G$的交换环$R$到带自同构群$G^*$的交换环$T$的$G$－同态,证明了Galois扩张的$G$－同态象仍为Galois扩张带Galois群$G'$,其中$G'$是由$G$导出的.最后,利用$R$的$G$－同态与$G$－理想的关系,由$G$的子群或正规子群导出若干类$G$－理想.

1 符号与定义

在本文中,环都是有单位元的交换环,环同态把单位元映为单位元.R表示环,G是R的一个自同构群.

R的理想I称为G－理想,如果$a(I) = I, \forall\ a \in G$.

如果G和G'分别是环R和环R'的自同构群,$\theta : G \to G', a \mapsto a'$是群同态,环同态$\varnothing : R \to R'$称为$G$－同态,如果$\varnothing(a(r)) = a'(\varnothing(r)), \forall\ r \in R, a \in G$.特别地,当$R = R', G = G', \theta = 1_G$时,$\varnothing$称为$R$的$G$－自同态.

收稿日期:1990-12-14. 修改完成日期:1994-4-28

* 中山大学高等学术研究中心资助课题

如果 $\alpha \in G$，R 的由 $\{r - \alpha(r) | r \in R\}$ 生成的理想记为 I_α.

如果 H 是 G 的子群(记为 $H < G$)，R 的由 $\{r - \alpha(r) | r \in R, \alpha \in H\}$ 生成的理想记为 I_H.

如果 $\alpha \in G$，$[\alpha] = \{\beta\alpha\beta^{-1} | \beta \in G\}$ 表示 α 在 G 中的共轭类. R 的由 $\{r - \beta(r) | r \in R, \beta \in [\alpha]\}$ 生成的理想记为 $I_{[\alpha]}$.

环 R 是环 S 上的 Galois 扩张带 Galois 群 G 的定义见文[4].

2 G — 同态

在本节，设 R 和 T 是分别带自同构群 G 和 G^* 的交换环，$\theta : G \to G^*$ 是群同态. $\varnothing$ 是 R 到 T 的 G — 同态，I 是 $\varnothing$ 的核(记为 $\ker\varnothing$). 将证明：

(i) I 是 R 的 G — 理想；

(ii) $R/I \cong \varnothing(R)$ 是 $\overline{G}$ — 同构；

(iii) $\overline{G} \cong G'$.

其中 $\overline{G}$ 是由 G 导出的 R/I 的自同构群和 G' 是由 G 导出的 $\varnothing(R)$ 的自同构群.

当 G 是 R 的有限自同构群时，还得出 R/I 是带 Galois 群 $\overline{G}$ 的 Galois 扩张当且仅当 $\varnothing(R)$ 是带 Galois 群 G' 的 Galois 扩张.

首先，我们给出一个环的 G — 理想与它的 G — 同态象的 G — 理想之间的对应关系.

定理1 设 G 和 G' 分别是环 R 和环 R' 的自同构群，$f : G \to G'$，$\alpha \mapsto \alpha'$ 是群同态，如果 $\varnothing$ 是 R 到 R' 的 G — 满同态，则

(i) $\varnothing$ 的核 K 是 R 的 G — 理想；

(ii) $I \mapsto \varnothing(I)$ 给出 R 的包含 K 的所有 G — 理想所构成的集合到 R' 的所有 G' — 理想所构成的集合之间的一一对应.

证明 (i) 由 $\varnothing$ 是 G — 同态，容易验证 K 是 G — 理想.

(ii) 首先，如果 I 是 R 的 G — 理想，由 $\varnothing$ 是 G — 同态，即得 $\alpha'(\varnothing(I)) = \varnothing(I)$，$\forall\ \alpha' \in G'$. 其次，如果 I' 是 R' 的 G' — 理想，那末，$\forall\ r \in \varnothing^{-1}(I') = \{r \in R | \varnothing(r) \in (I')$，有 $\varnothing(\alpha(r)) = \alpha'(\varnothing(r)) \in I'$，$\forall\ \alpha \in G$，显然 $K \subseteq \varnothing^{-1}(I')$.

推论1 如果 I 是 R 的一个 G — 理想，$\overline{R} = R/I = \{\bar{r} = r + I | r \in R\}$，$\overline{G} = \{\bar{\alpha} | \bar{\alpha}(\bar{r}) = \overline{\alpha(r)}, \forall\ r \in R, \alpha \in G\}$. 则

(i) $\overline{G}$ 是 $\overline{R}$ 的自同构群，$\eta = G \to \overline{G}$，$\alpha \mapsto \bar{\alpha}$ 是群的满同态，且 $\ker\eta = \{\alpha \in G | \alpha(r) \in r + I, \forall\ r \in R\}$；

(ii) $\pi : R \to R/I$，$r \mapsto \bar{r}$ 是 G — 满同态；

(iii) 存在 R 的包含 I 的所有 G — 理想所构成的集合与 R/I 的所有 $\overline{G}$ — 理想所构成的集合之间的一一对应.

证明 (i) 由 I 是 G — 理想，易见 $\bar{\alpha}$ 的定义是合理的. 显然，$\bar{\alpha}$ 是 $\overline{R}$ 的满自同态，如果 $\bar{\alpha}(\bar{r}) = \bar{0}$，即 $\alpha(r) \in I$，从而 $r \in I$. 因而 $\bar{r} = \bar{0}$. 所以 $\bar{\alpha}$ 是 $\overline{R}$ 的自同构，显然，$\overline{\alpha\beta} = \bar{\alpha}\,\bar{\beta}$，$\forall\ \alpha, \beta \in G$. 从而 η 是满同态且 $\overline{G}$ 是 $\overline{R}$ 的自同构群. $\ker\eta = \{\alpha \in G | \bar{\alpha} = \bar{1}\} = \{\alpha \in G | \alpha(r)$

$-r\in I\}$.

(ii)　$\pi(\alpha(r))=\overline{\alpha(r)}=\bar{\alpha}(\bar{r})=\bar{\alpha}(\pi(r)),\forall\ \alpha\in G$.

(iii)　由(ii)及定理 1 即得.

由定理 1 及推论 1 即有

定理 2　设 G 和 G^* 分别是环 R 和环 T 的自同构群，$\theta:G\to G^*,\alpha\mapsto\alpha^*$ 是群同态. 如果环同态 $\varnothing:R\to T$ 是 G － 同态，$I=\ker\varnothing$. 则

(i) I 是 R 的 G － 理想；

(ii) $\overline{R}(=R/I)$ 有自同构群 $\overline{G}=\{\bar{\alpha}\mid\bar{\alpha}(\bar{r})=\overline{\alpha(r)},\forall\ r\in R,\alpha\in G\}$ 并且 $\eta:G\to\overline{G}$，$\alpha\mapsto\bar{\alpha}$ 是群的满同态，$\ker\eta=\{\alpha\in G\mid\alpha(r)\in r+I,\forall\ r\in R\}$；

(iii) $\pi:R\to R/I,r\mapsto\bar{r}$ 是 G － 满同态.

定理 3　设 $R,T,G,G^*,\theta:G\to G^*,\varnothing:R\to T$ 等均如定理 2 中所示，又设 $T'=\varnothing(R)$. 对任意 $\alpha\in G$，令 $\alpha':T'\to T',\varnothing(r)\mapsto\varnothing(\alpha(r))$. 则

(i) α' 是环 T' 的自同构，且 $\alpha'=(\alpha^*\mid T')$，$G'=\{\alpha'\mid\alpha\in G\}$ 是 T' 的自同构群；

(ii) $f:G\to G',\alpha\mapsto\alpha'$ 是群的满同态，$\ker f=\{\alpha\in G\mid(\alpha^*\mid T')=1_{T'}\}$.

证明　(i) 由 $\varnothing$ 是 G － 同态，易见 α' 的定义是合理的. 显然，α' 是 T' 的满自同态，如果 $\alpha'(\varnothing(r))=0$，即 $\varnothing(\alpha(r))=0$. 因而 $\alpha^*(\varnothing(r))=0$，从而 $\varnothing(r)=0$. 所以 α' 是 T' 的自同构. 因为 $\alpha'(\varnothing(r))=\varnothing(\alpha(r))=\alpha^*(\varnothing(r)),\forall\ r\in R$，所以，$\alpha'=(\alpha^*\mid T')$. 容易验证 $\alpha'\beta'=(\alpha\beta)',\forall\ \alpha,\beta\in G$. 从而易见 G' 是 T' 的自同构群.

(ii)　由于 $\alpha'\beta'=(\alpha\beta)',\forall\ \alpha,\beta\in G$，显然，$f$ 是群的满同态. 最后，$\alpha\in kerf\Leftrightarrow\alpha'=1\Leftrightarrow(\alpha^*\mid T')=1_{T'}$.

定理 4　设 $R,T,G,G^*,\varnothing:R\to T,\theta:G\to G^*,I=\ker\varnothing,\overline{R}=R/I,T'=\varnothing(R),G'=\{\alpha'\mid\alpha\in G\},\overline{G}=\{\bar{\alpha}\mid\alpha\in G\}$ 等均如定理 2 和定理 3 中所示，则

(i)　$\theta':\overline{G}\to G',\bar{\alpha}\mapsto\alpha'$ 是群同构；

(ii)　$\psi:\overline{R}\to T',\bar{r}\mapsto\varnothing(r)$ 是 $\overline{G}$ － 同构.

证明　(i)　由 $I=\ker\varnothing$ 及 $\varnothing$ 是 G － 同态，易见 θ' 的定义是合理的. 由 $(\alpha\beta)'=\alpha'\beta',\forall\ \alpha,\beta\in G$，易见 θ' 是满同态. 如果 $\theta'(\bar{\alpha})=1'$. 那末，$\forall\ r\in R,\alpha'(\varnothing(r))=\varnothing(r)$，即 $\varnothing(\alpha(r))=\varnothing(r)$，因而 $\alpha(r)-r\in I$，从而 $\overline{\alpha(r)}=\bar{r}$，于是 $\bar{\alpha}(\bar{r})=\bar{r}$，所以 $\bar{\alpha}=\bar{1}$.

(ii)　由 $I=\ker\varnothing$，易见 ψ 的定义是合理的，显然，ψ 是满同态，如果 $\psi(\bar{r})=0,r\in R$，即有 $\varnothing(r)=0$，从而 $r\in I$，因而 $\bar{r}=\bar{0}$. 最后，$\psi(\bar{\alpha}(\bar{r}))=\psi(\overline{\alpha(r)})=\varnothing(\alpha(r))=\alpha'(\varnothing(r))=\alpha'(\psi(\bar{r})),\forall\ r\in R,\alpha\in G$. 所以，$\psi$ 是 G － 同构.

定理 5　设 $R,T,G,G^*,\varnothing,\theta,I,\overline{R},T',G',\overline{G},\theta'$ 等均如定理 4 中所示，并且 G 是有限群，则 T' 是 $T'^{G'}$ 上的 Galois 扩张带 Galois 群 G'，当且仅当 $\overline{R}$ 是 $\overline{R}^{\overline{G}}$ 上的 Galois 扩张带 Galois 群 $\overline{G}$.

证明　由定理 4，$\psi:\overline{R}\to T',\bar{r}\mapsto\varnothing(r)$ 是 $\overline{G}$ － 同构且 $\theta':\overline{G}\to G',\alpha\mapsto\alpha'$ 是群同构，因而如果 $a_i,b_i\in R,i=1,\cdots,n$，那末.

$$\sum_{i=1}^{n}\bar{a}_i\bar{\alpha}(\bar{b}_i)=\delta_{1,\bar{\alpha}}\Leftrightarrow\sum_{i=1}^{n}\varnothing(a_i)\alpha'(\varnothing(b_i))=\delta_{1',\alpha'}.$$

3 G — 理想和 Galois 扩张

在本节，G 仍表示环 R 的自同构群，首先由 G 的子群或正规子群可构造出若干类 G — 理想，然后，设 G 是有限群，仍设 G^* 是环 T 的自同构群，$\theta: G \to G^*$ 是群同态，$\varnothing: R \to T$ 是 G — 同态. $I = \ker\varnothing$. 我们将证明，如果 R 是 Galois 扩张带 Galois 群 G，则 $\varnothing(R)$ 亦是 Galois 扩张带 Galois 群 G'. 其中 G' 是由 G 导出的. 从而 R/I 亦是 Galois 扩张带 Galois 群 $\overline{G} = \{\bar{\alpha} | \bar{\alpha}(\bar{r}) = \overline{\alpha(r)}, \forall\, r \in R, \alpha \in G\}$. 当 $T = R$ 时，逆定理亦成立.

命题 1 设 G 是环 R 的自同构群，$\alpha \in G$，$H < G$，$[\alpha]$ 表示 α 在 G 中的共轭类. I_α 是 R 的由 $\{r - \alpha(r) | r \in R\}$ 生成的理想，I_H 是 R 的由 $\{r - \alpha(r) | r \in R, \alpha \in H\}$ 生成的理想，$I_{[\alpha]}$ 是由 $\{r - \beta(r) | r \in R, \beta \in [\alpha]\}$ 生成的理想. 则

(i) $I_\alpha = I_{\alpha^{-1}}$;

(ii) $I_H = \sum_{\alpha \in H} I_\alpha$;

(iii) $I_{[\alpha]} = \sum_{\beta \in [\alpha]} I_\beta$;

(iv) $\beta(I_\alpha) \subseteq I_{\beta\alpha\beta^{-1}}, \forall\, \beta \in G$;

(v) 如果 G 是交换群，则 I_α 是 G — 理想;

(vi) 如果 I_α 是 G — 理想，则 $\alpha^{-1}(I_\alpha) = I_{\alpha^{-1}}$;

(vii) I_α 是 G — 理想 $\Leftrightarrow I_{\beta\alpha\beta^{-1}} = I_\alpha, \forall\, \beta \in G$;

(viii) 如果 I_α 是 G — 理想，则 $\beta(I_\alpha) = I_{\beta\alpha\beta^{-1}}, \forall\, \beta \in G$;

(ix) $I_{[\alpha]}$ 是 G — 理想;

(x) 如果 H 是 G 的正规子群，则 I_H 是 G — 理想.

证明 (i)，(ii)，(iii) 是显然的. (iv) $\beta(r - \alpha(r)) = \beta(r) - \beta\alpha\beta^{-1}\beta(r) \in I_{\beta\alpha\beta^{-1}}$. (v) 由 (iv) 即得. (vi) 由 (iv) 及 (i) 即得. (vii) 如果 I_α 是 G — 理想，那末，$\forall\, \beta \in G, r - \beta\alpha\beta^{-1}(r) = \beta(\beta^{-1}(r) - \alpha\beta^{-1}(r)) \in I_\alpha$，故有 $I_{\beta\alpha\beta^{-1}} \subseteq I_\alpha$. 由 (iv) 又有 $I_{\beta\alpha\beta^{-1}} \supseteq \beta(I_\alpha) = I_\alpha$. 反之，如果 $I_{\beta\alpha\beta^{-1}} = I_\alpha, \forall\, \beta \in G$，由 (iv) $\beta(I_\alpha) \subseteq I_{\beta\alpha\beta^{-1}} = I_\alpha$，所以，$I_\alpha$ 是 G — 理想. (viii) 由 (vii) 即得. (ix) 是显然的. (x) $\forall\, \beta \in G$，由 (iv)，$\beta(I_\alpha) \subseteq I_{\beta\alpha\beta^{-1}} \subseteq I_H, \forall\, \alpha \in H$.

命题 2 设 $H_{[\alpha]} = \{\beta \in G | I_\beta \subseteq I_{[\alpha]}\}$，其中 $\alpha \in G$，则

(i) $H_{[\alpha]}$ 是 G 的正规子群;

(ii) $R/I_{[\alpha]}$ 有自同构群 $G/H_{[\alpha]}$.

证明 (i) $\forall\, \beta, \gamma \in H_{[\alpha]}$，即 $I_\beta, I_\gamma \subseteq I_{[\alpha]}$. 由此易见 $I_{\beta\gamma} \subseteq I_{[\alpha]}$，即有 $\beta\gamma \in H_{[\alpha]}$. 又因 $I_{\beta^{-1}} = I_\beta \subseteq I_{[\alpha]}$，所以，$\beta^{-1} \in H_{[\alpha]}$. 因 $I_{[\alpha]}$ 是 G — 理想，所以，$\forall\, g \in G, \beta \in H_{[\alpha]}, r \in R$，$r - g\beta g^{-1}(r) = g(g^{-1}(r) - \beta g^{-1}(r)) \in g(I_\beta) \subseteq I_{[\alpha]}$，所以，$I_{g\beta g^{-1}} \subseteq I_{[\alpha]}$，即 $g\beta g^{-1} \in H_{[\alpha]}$.

(ii) 对于任意 $\bar{g} \in G/H_{[\alpha]}$，$\bar{r} \in R/I_{[\alpha]}$，定义 $\bar{g} \cdot \bar{r} = \overline{g(r)}$，由 $I_{[\alpha]}$ 是 G — 理想，易见这定义是合理的. 显然，$\bar{g}$ 是 $R/I_{[\alpha]}$ 的满自同态. 最后，如果 $\bar{g}(\bar{r}) = \bar{O}$，即有 $g(r) \in I_{[\alpha]}$，从而 $r \in I_{[\alpha]}$，即有 $\bar{r} = \bar{O}$.

由 [5] 的第三章命题 1.2，有

定理 6　R 是 R^G 上 Galois 扩张带 Galois 群 G 的充要条件是 $I_\alpha = R, \forall\ 1 \neq \alpha \in G$.

由命题 1 的(v)和定理 6 即有

推论 2　如果 G 是交换群，且 R 没有非平凡 G － 理想，则 R 是 R^G 上 Galois 扩张带 Galois 群 G.

定理 7　设 R 是 R^G 上的 Galois 扩张带 Galois 群 G，如果 I 是 R 的一个 G － 理想，则 $\overline{R}(=R/I)$ 是 $\overline{R}^{\overline{G}}$ 上 Galois 扩张带 Galois 群 $\overline{G}$，其中 $\overline{G} = \{\bar{\alpha} \mid \alpha \in G, \bar{\alpha}(\bar{r}) = \overline{\alpha(r)}, \forall\ r \in R\}$ 是 $\overline{R}$ 的由 G 导出的自同构群.

证明　因 R 是 R^G 上 Galois 扩张带 Galois 群 G，由定理 6，$\forall\ 1 \neq \alpha \in G$，$R$ 是由 $\{r - \alpha(r) \mid r \in R\}$ 生成，从而，$\forall\ \bar{1} \neq \bar{\alpha} \in \overline{G}$，$\overline{R}$ 是由 $\{\bar{r} - \bar{\alpha}(\bar{r}) \mid \bar{r} \in \overline{R}\}$ 生成. 再由定理 6，$\overline{R}$ 是 $\overline{R}^{\overline{G}}$ 上的 Galois 扩张.

定理 8　设 $R, T, G, G^*, \varnothing, \theta, I, \overline{R}, T', G', \overline{G}, \theta'$ 等均如定理 4 中所示. 如果 R 是 R^G 上的 Galois 扩张带 Galois 群 G，则

(i) $\overline{R}$ 是 $\overline{R}^{\overline{G}}$ 上的 Galois 扩张带 Galois 群 $\overline{G}$；

(ii) T' 是 $T'^{G'}$ 上的 Galois 扩张带 Galois 群 G'.

证明 (i)　由定理 2，$I(=\ker \varnothing)$ 是 R 的 G － 理想，由定理 7，$\overline{R}$ 是 $\overline{R}^{\overline{G}}$ 上 Galois 扩张带 Galois 群 $\overline{G}$.

(ii) 由(i)及定理 5 即得.

在定理 8 中，取 $T = R, G^* = G, \theta = 1_G$，即有

推论 3　设 $\varnothing$ 是 R 的 G － 自同态，$I = \ker\varnothing$，$\overline{R} = R/I$，$R' = \varnothing(R)$，又设 $\overline{G}$ 和 G' 分别是 $\overline{R}$ 和 R' 的由 G 导出的自同构群(见定理 2 和定理 3)，如果 R 是 R^G 上 Galois 扩张带 Galois 群 G，则

(i) $\overline{R}$ 是 $\overline{R}^{\overline{G}}$ 上 Galois 扩张带 Galois 群 $\overline{G}$；

(ii) R' 是 $R'^{G'}$ 上 Galois 扩张带 Galois 群 G'.

下面我们还得出推论 3 的逆定理.

定理 9　设 $\varnothing$ 是 R 的 G － 同态，$I = \ker\varnothing$，$\overline{R}, R', \overline{G}, G'$ 如推论 3 中所示. 如果 R' 是 $R'^{G'}$ 上的 Galois 扩张带 Galois 群 G' 且 $G \cong G'$(或者 $\overline{R}$ 是 $\overline{R}^{\overline{G}}$ 上的 Galois 扩张带 Galois 群 $\overline{G}$ 且 $G \cong \overline{G}$)，则 R 是 R^G 上的 Galois 扩张带 Galois 群 G.

证明　由于 R' 有 Galois 集 $\{a_i, b_i \in R' \mid i = 1, \cdots, n\}$ 使得 $\sum_{i=1}^{n} a_i \cdot \alpha'(b_i) = \delta_{1',\alpha'}, \forall\ \alpha' \in G'$. 因 $\alpha' = (\alpha \mid R')$ 且 $G \cong G'$，故有，$\alpha = 1_R \Leftrightarrow \alpha' = 1_{R'}$. 所以，有 $\sum_{i=1}^{n} a_i \cdot \alpha(b_i) = \delta_{1,\alpha}, \forall\ \alpha \in G$.

参 考 文 献

1 Auslander M.Goldman O. Tran Amer Math soc. 1960.97：367 ～ 409
2 Chase S U. Harrison D K. Rosenberg A. Mem Amer Math Soc. 1965.52:15 ～ 33
3 Harrison D K. Mem Amer Math Soc. 1965.52:1 ～ 14
4 邓信德.司徒子治. Azumaya 代数与中心Galois 代数. 中山大学学报论丛(自然科学)〔10〕1987. 66 ～ 71
5 Demeyer F R. Ingraham E. Lecture Notes in Mathematics .181.Berlin — Heidelberg — New York. Springer — Verlag. 1971

The G — Homomorphisms of Galois Extensions of a Commutative Ring

Deng Xinde * *George Szeto*

Abstract A G — endomorphism $\varnothing$ of a commutative ring R with an endomorphism group G is defined. and it is shown that R is a Galois extension with Galois group G if and only if $\varnothing$(R) is a Galois extension with Galois group induced by G. More basic properties about a G — endomorphism $\varnothing$ are also given.

Keywords Galois extension. G — homomorphism. G — ideal

* Department of Mathematics.Zhongshan University. Guangzhou