一类有限阶可解完全群

翟起滨
(解放军工程技术学院，郑州)

文献〔1〕证明，有限素域 $F_p(p>3)$ 上一切形如

$$a=\begin{pmatrix}1 & b_{12} & b_{13}\cdots b_{1n}\\ & a_1 & b_{23}\cdots b_{2n}\\ & & \ddots\quad\vdots\\ & & a_{n-1}\end{pmatrix}\qquad (1)$$

的 n 阶可逆方阵，对方阵乘法所成的群的自同构群为有限阶可解完全解．本文用异于〔1〕的方法推广了这个结果．证明，若设 q 元有限域 $F_q(q=p^m, q>2, p$ 为素数）上形如（1）的 n 阶可逆方阵全体对方阵的乘法所成的群为G，则G的自同构群为有限阶可解完全群．

易见，G内对角线系数皆为1的全体方阵组成G的幺幂子群，记为T；G内全体对角方阵组成G的 Abel—子群，记为K．不难证明，T◁G，G=KT．

不失一般性，我们设 F_q 为由 F_p 上 m 次不可约多项式 $f(x)$ 所决定的分裂域。a 为 $f(x)$ 的根，则有

$$F_q=\{c_0+c_1a+\cdots+c_{m-1}a^{m-1}\mid c_i\in F_p,\ f(a)=0\}$$

我们有下面的

引理 1 T的生成元系由下列元素组成：

$$E_i(a^s)=\begin{pmatrix}1 & & & & \\ & \ddots & & & \\ & & 1 & a^s & \\ & & & 1 & \\ & & & & \ddots \\ & & & & & 1\end{pmatrix}$$

其中非零非对角线系数 a^s 位于第 i 行，第 $i+1$ 列 $s=0,1,2,\cdots,m-1$；$i=1,2,\cdots,n-1$．

证明从略．

引理 2 G的换位子群〔G，G〕=T；T的下中心列为

$$T=T_0\triangleright T_1\triangleright T_2\triangleright\cdots\triangleright T_{n-1}=\langle 1\rangle$$

其中，T_i 的元素具有形式

$$\begin{pmatrix}1 & \overbrace{0\ \cdots\ 0}^{i} & * & \cdots & *\\ & \ddots & & \ddots & \vdots\\ & & \ddots & & *\\ & & & \ddots & 0\\ & & & & \vdots\\ & & & & 0\\ & & & & 1\end{pmatrix}$$

* 1984年3月7日收到．

证明　（应分 $\mathrm{char}F_q=2$，$\mathrm{char}F_q>2$ 两种情形证明，证明过程从略）．

下文中，我们用 $\mathrm{Aut}\,G$ 表示由G的全体自同构组成的G的自同构群．σ_g 表示由G内元素 g 诱导出的G的内自同构．$I_{nn}G$ 表示G的全体内自同构组成的群．FieldG 表示由 F_q 的自同构诱导出的G的域自同构全体组成的域自同构群．X charG 表示X为G的特征子群．

引理 3　对于任意的 $\psi\in\mathrm{Aut}\,G$，一定存在 $\sigma_g\in I_{nn}G$，使得G的子群K在 $\psi\sigma_g$ 下不变．

证明：当 F_q 的特征数 $\mathrm{char}F_q=2$ 时：此时 $q=2^m>2$，由 $|K|=(2^m-1)^{n-1}$ 为奇数，而 $|T|=(2^m)^{\frac{(n-1)n}{2}}$ 为 2 的方幂，所以存在奇素数 v，使得 $v\mid|K|$，但是 $v\nmid|T|$．注意，$G=KT$．由此推断，K内的Sylow v-子群V也是G的Sylow-v子群．因为G内的 Sylow v-子群彼此共轭，所以一定存在 σ_g 使得 $V^{\psi\sigma_g}=V$．我们还容易证明 $K=C_G(V)$，所以有 $K^{\psi\sigma_g}=C_G(V^{\psi\sigma_g})=K$，亦即，$K^{\psi\sigma_g}=K$．

当 $\mathrm{Char}F_q>2$ 时：此时，$2\mid|K|$，所以K内存在Sylow2-子群V；然而 $2\nmid|T|$，$G=KT$，于是可断言K内的 Sylow2-子群也是G内的 Sylow2-子群．所以定存在 σ_g，使得 $V^{\psi\sigma_g}=V$，同理有 $K^{\psi\sigma}=K$．

由引理3 知 $K^{\psi\sigma_g}=K$，下文中我们令 $\varphi=\psi\sigma_g$，于是 $K^{\varphi}=K$．

引理 4　若取T的生成元系中的 $E_1(a^0)$，则 $E_1(a^0)$ 在 φ 下的象为

$$E_1(a^0)^{\varphi}=\begin{pmatrix}1 & & c_1(a^0) \\ & \ddots & \\ & & 1\end{pmatrix}$$

其中非零非对角线系数 $C_1(a^0)$ 不是位于第1 行、2 列，就是位于第 $n-1$ 行、n 列．

证明　首先算得

$$|C_K(E_1(a^0))|=(q-1)^{n-2} \tag{1}$$

于是可断定

$$|C_K(E_1(a^0)^{\varphi})|=(q-1)^{n-2} \tag{2}$$

若使（2）式成立，仅当

$$E_1(a^0)^{\varphi}=\begin{pmatrix}1 & & c_1(a^0) \\ & \ddots & \\ & & 1\end{pmatrix} \tag{3}$$

其中，非零非对角线系数 $C_1(a^0)$ 位于第 r 行，j 列．

再由
$$|C_T(E_1(a^0))|=|T|q^{-(n-2)} \tag{4}$$
$$|C_T(E_1(a^0)^{\varphi})|=q^{-(n-(j-r)-1)} \tag{5}$$

若使（4）、（5）两式相等，仅当 $j=r+1$．所以，（3）式中的 $c_1(a^0)$ 位于矩阵的第 r 行，$r+1$ 列．

再计算得

$$|C_{T_{n-2}}(E_1(a^0))|=|T_{n-2}|q^{-1}.$$

若使 $|C_{T_{n-2}}(E_1(a^0)^{\varphi})|=|T_{n-2}|q^{-1}$，仅当 $r=1$ 或者 $r=n-1$．

下面我们定义G到其自身的满单射 τ、对于G内的任意元素 β，

$$\beta^{\tau}=\rho(\beta)J\beta'^{-1}J$$

其中 $\rho(\beta)$ 表示 β 的第 n 行、n 列的系数.

$$J=\begin{pmatrix} & & & 1\\ & & 1 & \\ & \iddots & & \\ 1 & & & \end{pmatrix}$$

易验证，如此构造的 τ 是G的一个外自同构.

从 $E_1(a^0)$ 在 φ 下的象 $E_1(a^0)^{\varphi}$ 出发，定义G的自同构.

$$\mu_1=\begin{cases}\varphi & \text{如果 } E_1(a^0)^{\varphi} \text{ 的非零非对角线系数 } c_1(a^0) \text{ 位于第1行，2列.}\\ \varphi\tau & \text{如果 } E_1(a^0)^{\varphi} \text{ 内系数 } c_1(a^0) \text{ 位于第 } n-1 \text{ 行，} n \text{ 列.}\end{cases}$$

易见，此时有

$$E_1(a^0)^{\mu_1}=\begin{pmatrix}1 & c_1(a^0) & & \\ & 1 & & \\ & & \ddots & \\ & & & 1\end{pmatrix}.$$

再设

$$g_0=\operatorname{diag}(1,\ c_1(a^0)^{-1},\ c_1(a^0)^{-1},\cdots,c_1(a^0)^{-1})$$

易验证

$$g_0^{-1}E_1(a^0)^{\mu_1}g_0=\begin{pmatrix}1 & 1 & & \\ & 1 & & \\ & & \ddots & \\ & & & 1\end{pmatrix}$$

亦即，$E_1(a^0)^{\mu_1\sigma_{g_0}}=E_1(a^0)$. 同时，还可验证

$$K^{\mu_1\sigma_{g_0}}=K$$

我们设 $\mu=\mu_1\sigma_{g_0}$；用H表示 F_q 上由一切形如

$$\begin{pmatrix}1 & b_{12} & b_{13}\cdots b_{1n}\\ & 1 & 0\ \cdots\ 0\\ & & 1 & \\ & & & \ddots & \\ & & & & 1\end{pmatrix}$$

的方阵组成的G的子群. 我们有

引理 5 $H=\langle x^{-1}E_1(a^0)x \mid x\in G\rangle$

证明从略.

注意、由引理5 的事实，易见 $H^{\mu}=H$.

定理 1 G的自同构群

$$\operatorname{Aut}G=\langle \tau, f, \sigma_g \mid \tau\text{如前文定义，} f\in\operatorname{Field}G,\ \sigma_g\in I_{nn}G\rangle.$$

证明：对于T的生成元系内的任意元素 $E_i(a^s)$，计算 $|C_K(E_i(a^s))|$ 得

$$|C_K(E_i(a^s))| = (q-1)^{n-2} \qquad (1)$$

于是可断定
$$|C_K(E_i(a^s)^\mu)| = (q-1)^{n-2} \qquad (2)$$

若使（2）式成立，仅当

$$E_i(a^s)^\mu = \begin{pmatrix} 1 & & c_i(a^s) \\ & \ddots & \\ & & 1 \end{pmatrix}$$

其中，$c_i(a^s)$ 位于第 r 行，j 列.

再由

$$|C_T(E_i(a^s))| = |T| q^{-(n-2)} \qquad (3)$$

$$|C_T(E_i(a^s)^\mu)| = |T| q^{-[n-(j-r)-1]} \qquad (4)$$

若使（3），（4）两式相等，仅当 $j=r+1$. 所以，$E_i(a^s)^\mu$ 表示式内的系数 $c_i(a^s)$ 位于矩阵的第 r 行，$r+1$ 列. 我们再注意 $H^\mu=H$，及 T 的下中心列中的 T_j，T_j char G. 利用这些，我们可推断 $r=i$. 否则，如果 $r>i$，取 T_{i-1} 做算式

$$|C_{T_{i-1}}(E_i(a^s)) \cap H| = |T_{i-1} \cap H| = q^{n-i} \qquad (5)$$

$$|C_{T_{i-1}}(E_i(a^s)^\mu) \cap H| = |T_{i-1} \cap H| q^{-1} = q^{n-i-1} \qquad (6)$$

（5），（6）两式不等，矛盾. 所以 r 不大于 i.

如果 $r<i$，取 T_{r-1}，同样有

$$|C_{T_{r-1}}(E_i(a^s)) \cap H| \neq |C_{T_{r-1}}(E_i(a^s)^\mu) \cap H|,$$

矛盾. 所以 r 不小于 i.

综上知，必有 $r=i$. 即 $c_i(a^s)$ 位于第 i 行，$i+1$ 列.

下面我们设

$$l = \mathrm{diag}(1, c_1(a^0)^{-1}, c_1(a^0)^{-1}c_2(a^0)^{-1}, \cdots\cdots, \prod_{i=1}^{n-1} c_i(a^0)^{-1}).$$

易验证，$K^{\mu\sigma_l}=K$；$E_i(a^0)^{\mu\sigma_l}=E_i(a^0)$. 并且，$E_i(a^s)^{\mu\sigma_l}$ 矩阵表示式的非零非对角线系数的位置仍然与 $E_i(a^s)^\mu$ 的情形相同. 不失一般性，仍然将此系数记为 $c_i(a^s)$，将 $\mu\sigma_l$ 记为 μ. 注意，$K^\mu=K$，$E_i(a_0)^\mu=E_i(a_0)$.

按下述方式递归地定义 $\rho_{i,i+k}(a^s)$：

$$\rho_{ii}(a^s) = E_i(a^s)$$

$$\rho_{i,i+k}(a^s) = \rho_{i,i+k-1}(a^s) E_{i+k}(a^0) \rho^{-1}_{i,i+k-1}(a^s) E^{-1}_{i+k}(a^0) \qquad (7)$$

从 $k=1$ 时的式（7）开始，每次用 μ 作用等式（7）的两边，易得到 $\rho_{i,i+k}(a^s)$ 在 μ 下的象为

$$\begin{pmatrix} 1 & & c_i(a^s) \\ & \ddots & \\ & & 1 \end{pmatrix}$$

其中 $c_i(a^s)$ 位于第 i 行，$i+k+1$ 列. 注意，系数 $c_i(a^s)$ 不依赖于 k 的变化. 下面我们设

$$c_i(a^s) = (a^s)^{\sigma_i}, \quad \sigma_i \text{ 为 } F_q \text{ 到自身的单一映射.}$$

再把等式

$$E_i(a^0)^{-1}E_{i+1}(a^s)^{-1}E_i(a^0)E_{i+1}(a^s)=\rho_{i,i+1}(a^s) \tag{8}$$

两边用 μ 作用，则有

$$c_{i+1}(a^s)=c_i(a^s)\ \text{，即}\ (a^s)^{\sigma_{i-1}}=(a^s)^{\sigma_i}\ ,$$

所以有 $\sigma_1=\sigma_2=\cdots=\sigma_{n-1}$. 于是可令 $\sigma=\sigma_i\,(i=1,2,\cdots,n-1)$.

下面我们定义

$$E_{ij}(x)=\begin{pmatrix}1 & & & \\ & \ddots & x & \\ & & \ddots & \\ & & & 1\end{pmatrix}$$

其中系数 x 为 F_q 的任意元素，位于第 i 行，j 列. 不难验证 $E_{ij}(x)^\mu=E_{ij}(x^\sigma)$，特别 $E_{ij}(1)^\mu=E_{ij}(1)$.

对于任意的 $k=\mathrm{diag}(1,a_1,\cdots,a_{n-1})\in K$，由于 $k^\mu\in K$，所以可设 $k^\mu=\mathrm{diag}(1,a_1',\cdots,a_{n-1}')$. 可算得

$$k^{-1}E_{1i}(1)k=\begin{pmatrix}1 & 0\cdots 0 & a_{i-1} & 0\cdots 0\\ & \ddots & 0 & \\ & & \vdots & \\ & & 0 & \\ & & 1 & \\ & & & \ddots \\ & & & & 1\end{pmatrix}=E_{1i}(a_{i-1})$$

等式两边用 μ 作用，有

$$k^{-1\mu}E_{1i}(1)^\mu k^\mu=(E_1(a_{i-1}))^\mu=E_{1i}(a_{i-1}^\sigma).$$

所以有 $a_{i-1}'=a_{i-1}^\sigma$，$i=2,3,\cdots,n$. 再把等式

$E_{1,2}(x)E_{1,2}(y)=E_{1,2}(x+y)$ 两边用 μ 作用，易见有 $x^\sigma+y^\sigma=(x+y)^\sigma$ $(x,y\in F_q)$. 再设

$$k_1=\mathrm{ding}(1,x,1,\cdots,1),\quad k_2=\mathrm{diag}(1,y,1,\cdots,1),$$

则有，$k_1k_2=\mathrm{diag}(1,xy,1,\cdots,1)$，它的两边用 μ 作用，易见 $x^\sigma y^\sigma=(xy)^\sigma$. 综上知 σ 为 F_q 的自同构. 不难看出这个 σ 诱导出G的一个域自同构，把此域自同构记为 f. 易见，μf^{-1} 是G的单位自同构. 这就证明了定理的结论.

定理 2 群G的自同构群 Aut G 为有限阶可解完全群.

证明： 为方便计，我们将 Aut G 简记为 $\widetilde{G}$. 对于G中的任意子群X，我们用 $\overline{X}$ 表示由X中的元素所诱导的内自同构所组成的 $\widetilde{G}$ 的子群.

若能证明 $\overline{G}$ char $\widetilde{G}$ 则由文献〔3〕,即得出 Aut G 为完全的. 下面证明 $\overline{G}$ char $\widetilde{G}$. 因为〔G, G〕= T, 所以 $\overline{T}\leq[\widetilde{G},\widetilde{G}]$. 我们取 F_q 的本原元 ζ，则有 $F_q^*=\langle\zeta\rangle$. 取G的子群K内的元素

$$z_i=\mathrm{diag}(1,\cdots,1,\zeta,1,\cdots,1),\ i=2,3,\cdots,n\ .$$

再取 FieldG 内的元素 f_1（f_1 将G内任意元素中的系数 x 映成对应的系数 x^p），则有

$$[\sigma_{z_i},f_1]=\sigma_{z_i^{-1}}f_1^{-1}\sigma_{z_i}f_1=\sigma_{z_i^{p-1}}\ .$$

注意，$z_i^{p-1} = \mathrm{diag}(1, \cdots, 1, \zeta^{p-1}, 1, \cdots, 1)$．

再取$\tilde{G}$内的元素τ，则有

$$[\tau, \sigma_{z_i}] = \tau^{-1}\sigma_{z_i}^{-1}\tau\sigma_{z_i} = \sigma_{z_i^{-1}\tau z_i}$$

这里

$$z_i^{-1}\tau z_i = \begin{cases} z_i \cdot z_{n-i+1}, & i = 2, 3, \cdots, n-1 \\ \mathrm{diag}(1, \zeta^{-1}, \cdots, \zeta^{-1}, 1), & i = n \end{cases}$$

定义G的子群

$K_1 = \langle z_i^{p-1}, z_i^{-1}\tau z_i \mid z_i$的定义如上，$i = 2, 3, \cdots, n\rangle$，易见$\overline{K_1}\,\overline{T} \leq [\tilde{G}, \tilde{G}]$．又从定理1可验证$\tau f = f\tau$．对于任意的$g \in G$，由$G = KT$，可知存在$l \in K$，$t \in T$使得$g = lt$．于是

$$f^{-1}\sigma_g^{-1}f\sigma_g \equiv f^{-1}\sigma_l^{-1}f\sigma_l \equiv 1 \quad (\mathrm{mod}\,\overline{K_1}\,\overline{T})$$

$$\tau^{-1}\sigma_g^{-1}\tau\sigma_g \equiv \tau^{-1}\sigma_l^{-1}f\sigma_l \equiv 1 \quad (\mathrm{mod}\,\overline{K_1}\,\overline{T})$$

所以$\tilde{G}/\overline{K_1}\,\overline{T}$为Abel一群．于是，$\overline{K_1}\,\overline{T}$为$\tilde{G}$的换位子群．

我们注意K_1的子群

$$A = \langle z_i^{p-1} \mid i = 2, 3, \cdots, n\rangle$$

易见$|\overline{A}| = \left(\dfrac{p^m-1}{p-1}\right)^n \Big| \, |\overline{K_1}|$．

当$p = 2$时：由于此时$m \neq 1$，于是存在奇素数$d \Big| \left(\dfrac{p^m-1}{p-1}\right)^n$，即$d \mid (2^m-1)^n$．而此时$|\overline{T}|$为2的方幂，所以$\overline{K_1}$内存在Sylow$d$－子群$\overline{D}$，并且由于$(d, |\overline{T}|) = 1$，则$\overline{D}$也为$[\tilde{G}, \tilde{G}]$的Sylow$d$—子群．于是对于任意的$\eta \in \mathrm{Aut}\tilde{G}$，存在$\sigma_\eta \in I_{nn}\tilde{G}$，使得有$\overline{D}^{\eta\sigma_\eta^{-1}} = \overline{D}$．而又由于$C_{\tilde{G}}(\overline{D}) = C_{\overline{G}}(\overline{D}) = \overline{K}$，则得到，$\overline{K}^{\eta\sigma_\eta^{-1}} = C_{\overline{G}}(\overline{D}^{\eta\sigma_\eta^{-1}}) = \overline{K}$．再注意，$[\tilde{G}, \tilde{G}]$与$\overline{K}$可生成群$\overline{G}$，易见$\overline{G}^{\eta\sigma_\eta^{-1}} = \overline{G}$．进一步有，$\overline{G}^{\eta} = \overline{G}^{\sigma_\eta} = \overline{G}$．而因为$\eta$为$\mathrm{Aut}\tilde{G}$的任意自同构，所以$\overline{G}\,\mathrm{char}\,\tilde{G}$

当$p \neq 2$，$m \neq 1$时：注意$|\overline{A}| = \left(\dfrac{p^m-1}{p-1}\right)^n \Big| \, |\overline{K_1}|$．由于$\left(\dfrac{p^m-1}{p-1}\right)^n = (1 + p + \cdots + p^{m-1})^n \neq (p-1)^n$，于是存在素数$d$及正整数$\lambda$，使得$d^\lambda \nmid |\overline{T}|$，$d^\lambda \mid |\overline{K_1}|$，但是$d^\lambda \nmid (p-1)^n$．所以，$\overline{K_1}$内存在的Sylow$d$—子群$\overline{D}$含有这样的元素$\sigma_\omega$，$\omega$内的系数不完全属于基域$F_p$．然而又由$(|\overline{T}|, d) = 1$，所以$\overline{K_1}$内的Sylow$d$—子群$\overline{D}$也是$[\tilde{G}, \tilde{G}]$的Sylow—子群．仿照$p = 2$情形的证法，同样有$\overline{G}\,\mathrm{char}\,\tilde{G}$的结论．

当$p \neq 2$，$m = 1$时：此时$\tilde{G} = \langle \tau, \sigma_g \mid g \in G\rangle$．在此情形下有

$K_1 = \{\mathrm{diag}(1, a_1, \cdots, a_r, a_{r+1}, a_r, \cdots, a_1, 1) \mid a_i \in F_p^*$，若$2 \mid n$，$a_{r+1}$不存在$\}$

不难看出$2 \mid |\overline{K_1}|$；但是$2 \nmid |\overline{T}|$，所以$\overline{K_1}$内存在Sylow 2一子群$\overline{D}$．$\overline{D}$也为$[\tilde{G}, \tilde{G}]$的Sylow 2一子子群．仿照$p = 2$时的情形，同样证得$\overline{G}\,\mathrm{char}\,\tilde{G}$．

综上，对于任意情形的有$\overline{G}\,\mathrm{char}\,\tilde{G}$．参见文献〔3〕，即知$\tilde{G}$是完全的．易见$\tilde{G}$有限，可解，中心为单位，所以$\tilde{G}$是有限可解完全群．

参 考 文 献

〔1〕郑燕生、柳政、杨德荣，一类有限阶可解完全群，数学研究与评论，1981年第2期，7--20.

〔2〕L. Dickson, Linear Groups with an Exposition the Galois Field Theory, Dover Publications Inc., New York, 1958.

〔3〕Derek J. S Robinson, A Course in the Theory of Groups, p399, Springor-Verlag, New York Heidelberg Berlin, 1980.

On a Class of Complete Solvable Groups of Finite Order

Zhai Qibin

Abstract

It has been shown in the present paper that the automorphism group of the group of upper triangular matrices (a_{ij}) with entries in the finite field F_q $(q=p^m, q>2, p$ is prime) and with $a_{11}=1$ is solvable and complete.

《应用数学》创刊

为了开展应用数学研究，及时报导应用数学理论与实践的成果．华中工学院创办了《应用数学》季刊。本刊为综合性应用数学学术刊物。于1988年1月起，通过邮局在全国公开发行，并对国外进行交流。

《应用数学》主要刊登应用数学方面的创造性论文，特别是新方法，新应用方面的论文。开辟研究简报，研究通讯，专题讲座，综合评述等栏目。介绍国内外数学名流科研工作经验及指导青年数学工作者从事科研的文章。

读者对象为数学工作者，应用科学工作者，大专院校理、工、管诸方面的教师，研究生，科技工作者以及其他应用数学爱好者。

欢迎订阅，邮发代号为38—61，欢迎投稿，来稿请一式二份，五千字左右，挂号寄武汉华中工学院《应用数学》编辑部。