

VỀ MỘT GIẢ THUYẾT CỦA HERSTEIN

Nguyễn Văn Thìn, Bùi Xuân Hải
 Trường Đại học Khoa học Tự Nhiên, ĐHQG - HCM

TÓM TẮT: Cho D là vành chia tâm F . Ta nói N là nhóm con của D với qui ước rằng N thực ra là nhóm con của nhóm nhân D^* của vành chia D . Bài này xoay quanh giả thuyết sau đây được N. I. Herstein đưa ra năm 1978 [2, Conjecture 3]: Nếu N là nhóm con á chuẩn tắc (subnormal) căn trên F của D thì N nằm trong F . Trong bài báo nêu trên chính Herstein đã chứng minh giả thuyết này đúng nếu N là nhóm con á chuẩn tắc hữu hạn của D . Tuy nhiên trong trường hợp tổng quát giả thuyết này vẫn chưa được giải quyết. Trong bài này, chúng tôi trình bày một số tính chất của nhóm con á chuẩn tắc trong vành chia nhằm cung cấp những thông tin cần thiết có thể đưa tới việc giải quyết giả thuyết nói trên. Nói riêng, giả thuyết được chúng tôi chứng minh là đúng cho những vành chia hữu hạn chiều địa phương trên tâm.

Từ khóa: vành chia, căn, tâm, á chuẩn tắc.

1. MỞ ĐẦU

Cho D là vành chia tâm F . Ký hiệu $D^* = D \setminus \{0\}$ là nhóm nhân của D , $D' := [D, D]$ là nhóm con hoán tử của D^* . Với $S \subseteq D$ là tập con khác rỗng của D , ký hiệu $F[S]$ (tương ứng $F(S)$) là vành con (tương ứng vành chia con) nhỏ nhất của D chứa F và S . Phần tử $a \in D^*$ được gọi là căn trên S nếu tồn tại số nguyên dương k sao cho $a^k \in S$. Tập con $A \subseteq D$ được gọi là căn trên S nếu mọi phần tử của A đều căn trên S . Vành chia D được gọi là hữu hạn chiều địa phương trên tâm nếu $F(S)$ là hữu hạn chiều trên F đối với mọi tập con hữu hạn S . Ta ký hiệu $C_D(S) = \{x \in D : xs = sx, \forall s \in S\}$ và gọi nó là tâm hóa tử của tập S trong D .

Cho F và K là hai trường, nếu $F \subset K$ thì ta nói K là mở rộng của F và ký hiệu là K/F . Chuẩn của K trên F được ký hiệu là $N_{K/F}$. Cho G là một nhóm, ký hiệu $Z(G)$ là tâm của G . Nhóm con N của G được gọi là á chuẩn tắc nếu tồn tại dãy chuẩn tắc $N \triangleleft G_1 \triangleleft \dots \triangleleft G_r = G$.

Định lý 1. Cho D là vành chia hữu hạn chiều địa phương trên tâm F và G là nhóm con á chuẩn tắc của D^* . Khi đó, nếu G căn trên F thì nằm trong F .

Chứng minh. Nếu D là trường thì không có gì cần chứng minh. Vậy, có thể giả sử D không giao hoán và G là nhóm con á chuẩn tắc căn trên F . Xét hai phần tử bất kỳ a, b của G và đặt $K = F(a, b)$. Theo giả thiết K là không gian véc tơ hữu hạn chiều trên F , kéo theo K là vành chia hữu hạn tâm. Vì G á chuẩn tắc trong D^* nên $G \cap K^*$ á chuẩn tắc trong K^* . Hơn nữa, do $G \cap K^*$ căn trên F nên $G \cap K^*$ căn trên tâm $Z(K)$ của K . Theo [1, Th. 1], $G \cap K^* \subseteq Z(K)$, suy ra a và b giao hoán với nhau. Vậy G là nhóm aben. Áp dụng [4, 14.4.4, p. 440], suy ra $G \subseteq F$.

Định lý 2. Cho D là vành chia tâm F và giả sử N là nhóm con á chuẩn tắc của D^* căn trên F . Khi đó $\forall a \in N, Gal(F(a)/F) = 1$.

Chứng minh. Xét phần tử $a \in N$. Nếu $a \in F$ thì không có gì để chứng minh.

Giả sử $a \notin F$, $Gal(F(a)/F) \neq 1$, và $1 \neq \sigma \in Gal(F(a)/F)$. Theo [3, Th.2, p.162], tồn tại $x \in D^*$ sao cho $\sigma(a) = x^{-1}ax$. Do a căn trên F nên $|Gal(F(a)/F)| < \infty$. Suy ra, tồn tại $t \in \mathbb{N}, t > 1$ sao cho $\sigma^t = 1$, dẫn đến $a = \sigma^t(a) = x^{-t}ax^t$. Do đó a giao hoán với x^t . Đặt $D_1 = C_D(x^t); Z_1 = [C_D(x^t)]$. Khi đó a và x đều nằm trong D_1 . Hơn nữa, từ $F(x^t) \subseteq Z_1$ ta có x và a đều căn trên Z_1 . Mặt khác, do $x^{-1}ax = \sigma(a) \in F(a)$, nên tồn tại $m \in \mathbb{N}, \alpha_0, \alpha_1, \dots, \alpha_m \in F$ sao cho $ax = x \sum_{i=0}^m \alpha_i a^i = \sum_{i=0}^m \alpha_i x a^i$. Do đó, vành chia $D_2 = Z_1(a, x)$ là hữu hạn chiều trên tâm $Z(D_2)$. Do N á chuẩn tắc trong D^* , nên tồn tại dãy chuẩn tắc $N_n = N \triangleleft N_{n-1} \triangleleft \dots \triangleleft N_1 = D^*$. Đặt $G_i = N_i \cap D_2 (i = \overline{1, n})$. Khi đó $G = G_n \triangleleft D_2$. Rõ ràng G căn trên $Z(D_2)$, nên theo Định lý 1, $G \subseteq Z(D_2)$. Nhưng $a \in N \cap D_2 = G$, nên $a \in Z(D_2)$, suy ra a giao hoán với x , dẫn tới $\sigma = 1$. Điều vô lý này kết thúc chứng minh.

Hệ quả 1. Cho D là vành chia tâm F và giả sử N là nhóm con á chuẩn tắc của D^* căn trên F . Nếu $a \in N, a^{n(a)} = 1 (n(a) \in \mathbb{N})$ thì $a \in F$.

Chứng minh. Giả sử $a \in N \setminus F$ và tồn tại số nguyên dương nhỏ nhất $k > 1$ sao cho $a^k = 1$. Khi đó $F(a)/F$ là mở rộng chuẩn tắc hữu hạn, do đó nhóm $Gal(F(a)/F) \neq 1$. Điều này mâu thuẫn với Định lý 2, dẫn tới $a \in F$.

Một chứng minh khác của Hệ quả 1 được trình bày trong [2].

Từ Hệ quả 1 ta suy ra ngay hệ quả sau:

Hệ quả 2. Cho D là vành chia tâm F, N là nhóm con á chuẩn tắc của D^* . Nếu N là nhóm xoắn thì N nằm trong F .

Hệ quả 3. Cho D là vành chia tâm F, N là nhóm con á chuẩn tắc của D^* . Nếu N là nhóm xoắn và F hữu hạn thì N là nhóm con cyclic nằm trong F .

Chứng minh. Xét phần tử $a \in N$. Khi đó tồn tại số nguyên dương k sao cho $a^k = \alpha \in F$. Mặt khác do F hữu hạn nên có số nguyên dương m mà $\alpha^m = 1$, suy ra $a^{km} = 1$. Từ Hệ quả 1 ta có $a \in F$, dẫn tới $N \subseteq F$. Do F hữu hạn nên N cũng hữu hạn. Hơn nữa, $char F = p > 0$, kéo theo N là nhóm cyclic.

Một kết quả cổ điển của Jacobson là: "Cho D là vành chia và F là một trường con hữu hạn của D . Nếu D đại số trên F thì D giao hoán". Hệ quả sau là tổng quát hóa của kết quả này.

Hệ quả 4. Cho D là vành chia, F là một trường con hữu hạn của D và N là nhóm con á chuẩn tắc của D^* . Nếu N đại số trên F thì N nằm trong tâm của D .

Chứng minh. Lấy $a \in N$, do a đại số trên F nên $[F(a) : F] = n < \infty$ với một số nguyên dương n nào đó. Do F hữu hạn nên $F(a)$ cũng là trường hữu hạn. Đặc biệt $F(a)^*$ là nhóm cyclic, do đó a là phần tử xoắn, kéo theo N là nhóm xoắn. Áp dụng Hệ quả 2, suy ra N nằm trong tâm của D .

Hệ quả 5. Cho D là vành chia tâm F và N là nhóm con á chuẩn tắc của D^* căn trên F . Nếu $a, b^{-1}ab$ nằm trong N và a giao hoán với $b^{-1}ab$ thì a giao hoán với b .

Chứng minh. Giả sử a không giao hoán với b . Khi đó $1 \neq \alpha = a^{-1}b^{-1}ab \in N$. Vì N căn trên F nên tồn tại số nguyên dương $k > 1$ sao cho $a^k \in F$, suy ra $\alpha^k = (a^{-1}b^{-1}ab)^k = a^{-k}b^{-1}a^k b = 1$. Do $\alpha \in N$, nên theo Hệ quả 1 ta có $\alpha \in F$, suy ra $a \neq b^{-1}ab = \alpha a \in F(a)$. Do đó đẳng cấu $\psi(x) = b^{-1}xb$ trên $F(a)$ là không tầm thường, dẫn đến $Gal(F(a)/F) \neq 1$, mâu thuẫn với Định lý 2. Vậy a giao hoán với b .

Hệ quả dưới đây được suy ra trực tiếp từ Hệ quả 5:

Hệ quả 6. Cho D là vành chia tâm F . Giả sử N là nhóm con chuẩn tắc của D^* căn trên F và $a \in N$. Nếu a giao hoán với $b^{-1}ab$ thì a giao hoán với b .

Định lý 3. Cho D là vành chia tâm F và giả sử N là nhóm con chuẩn tắc của D^* căn trên F . Nếu $a \in N, a^2 \in F$ thì $a \in F$.

Chứng minh. Giả sử $a \notin Z(N)$. Khi đó tồn tại $b \in N$ sao cho $x = a^{-1}b^{-1}ab \neq 1$. Từ $a^2 \in F$ ta có $a^2 = b^{-1}a^2b = (b^{-1}ab)^2 = (ax)^2 = axax \Rightarrow a = xax \Rightarrow x^{-1} = axa^{-1}$. Nếu $x = x^{-1}$ thì $x^2 = 1$, dẫn đến $x = \pm 1$. Do $x \neq 1$ nên $x = -1$, suy ra $b^{-1}ab = -a$. Do đó tự đẳng cấu θ trên D cho bởi $\theta(d) = b^{-1}db (\forall d \in D)$ hạn chế xuống $F(a)$ là tự đẳng cấu không tầm thường, dẫn đến $Gal(F(a)/F) \neq 1$. Điều này mâu thuẫn với Định lý 2, suy ra $x \neq x^{-1} = axa^{-1} \in N$. Lý luận tương tự như trên ta có $Gal(F(x)/F) \neq \{1\}$, hơn nữa $x \in N$ suy ra cũng mâu thuẫn. Do đó $a \in Z(N)$. Mặt khác $Z(N) \triangleleft D^*$, nên theo [4, Th. 14.4.4 p.440], $Z(N) \subseteq F$, dẫn đến $a \in F$.

Để bắt đầu với định lý tiếp theo, trước tiên ta xét bổ đề sau:

Bổ đề 1. Cho D là vành chia tâm F đặc trưng $p > 0$. Nếu $a \in D \setminus F$ và có số nguyên dương $n > 0$ sao cho $a^{p^n} \in F$ thì tồn tại $b \in D$ sao cho $aba^{-1} = 1 + b$.

Chứng minh. Xét D như là không gian vectơ trên F . Định nghĩa toán tử tuyến tính ψ trên D cho bởi $\psi(x) = ax - xa (\forall x \in D)$. Khi đó $\psi^{p^n}(x) = a^{p^n}x - xa^{p^n} = 0$. Suy ra $\psi^{p^n} = 0$. Lấy số nguyên dương t lớn nhất thỏa $\psi^t \neq 0$, và chọn $x \in D$ sao cho $\psi^t(x) \neq 0$. Khi đó với $b = \psi^{t-1}(x)\psi^t(x)^{-1}a$ ta có:

$$\begin{aligned} \psi(b) &= \left[(a\psi^{t-1}(x) - \psi^{t-1}(x)a)\psi^t(x)^{-1} - \psi^{t-1}(x)\psi^t(x)^{-1}(a\psi^t(x) - \psi^t(x)a)\psi^t(x)^{-1} \right] a \\ &= \left(1 - \psi^{t-1}(x)\psi^t(x)^{-1}\psi^{t+1}(x)\psi^t(x)^{-1} \right) a = a \end{aligned}$$

$$\Rightarrow ab - ba = a \Rightarrow aba^{-1} = 1 + b.$$

Định lý 4. Cho D là vành chia tâm F đặc trưng $p > 0$, và giả sử N là nhóm con chuẩn tắc của D^* căn trên F . Nếu $a \in N$ và có số nguyên dương $t > 0$ sao cho $a^{p^t} \in F$ thì $a \in F$.

Chứng minh. Nhận xét rằng ta chỉ cần chứng minh điều khẳng định cho trường hợp $t=1$ là đủ. Vậy, giả sử $a^p \in F$ và $a \notin F$. Theo Bổ đề 1, tồn tại $b \in D^*$ sao cho $aba^{-1} = 1 + b$. Chú ý rằng với mọi số nguyên dương k ta có $a^k b a^{-k} = b + k$. Đặt

$c = \prod_{k=0}^{p-1} (k+b)$; $D_1 = C_D(c)$; $F_1 = Z(D_1)$. Khi đó cả a và b đều nằm trong D_1 . Mặt khác

$a^p \in F \subseteq F_1$, b là nghiệm của phương trình $\prod_{k=0}^{p-1} (k+x) - c \in F_1[X]$ nên a, b cùng đại số trên

F_1 . Từ mối quan hệ $aba^{-1} = 1 + b$ ta có $F_1(a, b)$ là vành chia hữu hạn chiều trên tâm. Đặt $N_1 = N \cap F_1(a, b)$, khi đó N_1 á chuẩn tắc trong $F_1(a, b)^*$ và $a \in N$. Áp dụng Định lý 2 ta có $a \in Z(F_1(a, b))$, đặc biệt a giao hoán với b dẫn tới mâu thuẫn với quan hệ $aba^{-1} = 1 + b$. Suy ra $a \in F$.

Hệ quả 7. Cho D là vành chia tâm F có đặc trưng $p > 0$ và N là nhóm con á chuẩn tắc của D^* căn trên F . Nếu $a \in N$ và k là số nguyên dương nhỏ nhất sao cho $a^k \in F$ thì p không là ước của k .

Chứng minh. Nếu $a \in F$ thì kết quả là hiển nhiên. Giả sử $a \notin F$ và p là ước số của k . Khi đó $k = p^r s$; $(s, p) = 1$; $s < k$. Suy ra $a^k = (a^s)^{p^r} \in F$. Theo Định lý 4 ta có $a^s \in F$, nhưng điều này mâu thuẫn với tính nhỏ nhất của k . Vậy p không là ước của k .

Hệ quả 8. Cho D là vành chia tâm F và N là nhóm con á chuẩn tắc của D^* căn trên F . Khi đó mọi phần tử $a \in N$ đều tách được trên F .

Chứng minh. Lấy $a \in F$. Nếu $\text{char} F = 0$ thì rõ ràng a tách được trên F . Bây giờ, giả sử $\text{char} F = p > 0$ và k là số nguyên dương nhỏ nhất thỏa $a^k \in F$. Theo Hệ quả 7, k không là ước của p , suy ra a tách được trên F .

Định lý 5. Cho D là vành chia tâm F và N là nhóm con chuẩn tắc của D^* căn trên F . Khi đó, $\forall a \in N$, đa thức tối thiểu của a trên F có dạng $x^t - N_{F(a)/F}(a)$. Hơn nữa t là một số lẻ.

Chứng minh. Không mất tính tổng quát ta có thể coi $F^* \subset N$. Lấy $a \in N$ và gọi $f(x) = \sum_{i=0}^t \alpha_i x^i$ (1) là đa thức tối thiểu của a trên F . Theo định lý phân tích nhân tử Wedderburn, tồn tại $g_1, g_2, \dots, g_t \in D^*$ sao cho: $f(x) = (x - a^{g_1})(x - a^{g_2}) \dots (x - a^{g_t})$ (2). Ở đây $a^{g_j} = g_j^{-1} a g_j$. Cân bằng hệ số của (1) và (2) ta nhận được $N_{F(a)/F}(a) = a^{g_1} a^{g_2} \dots a^{g_t}$. Mặt khác, ta có:

$$\begin{aligned} a^{g_1} a^{g_2} \dots a^{g_t} &= g_1^{-1} a g_1 g_2^{-1} a g_2 \dots g_t^{-1} a g_t \\ &= a' a^{-t+1} a^{-1} g_1^{-1} a g_1 a^{t-1} a^{-t+2} a^{-1} g_2^{-1} a g_2 a^{-t+2} \dots a^{-1} g_t^{-1} a g_t \\ &= a' \{ a^{-t+1} [a, g_1] a^{t-1} \} \{ a^{-t+2} [a, g_2] a^{t-2} \} \dots \{ a^{-1} [a, g_{t-1}] a \} [a, g_t] \\ &= a' [a, g_1]^{a^{t-1}} [a, g_2]^{a^{t-2}} \dots [a, g_{t-1}]^a [a, g_t]. \end{aligned}$$

Đặt $d_a = [a, g_1]^{a^{t-1}} \dots [a, g_t]$. Khi đó $N_{F(a)/F}(a) = a' d_a (*)$. Suy ra $d_a = N_{F(a)/F}(a) a^{-t} \in N \cap F(a)$. Tác dụng $N_{F(a)/F}$ lên hai vế của (*), ta nhận được:

$$N_{F(a)/F} [N_{F(a)/F}(a)] = N_{F(a)/F} [a' d_a] \Rightarrow [N_{F(a)/F}(a)]^t = N_{F(a)/F}(a') N_{F(a)/F}(d_a) \Rightarrow N_{F(a)/F}(d_a) = 1.$$

Gọi k là số nguyên dương nhỏ nhất sao cho $a^k \in F$. Khi đó $N_{F(a)/F}(a)^k = a^{tk} d_a^k$, suy ra $d_a^k \in F$. Từ $N_{F(a)/F}(d) = 1$, ta có $1 = N_{F(a)/F}(d_a)^k = N_{F(a)/F}(d_a^k) = d_a^{tk}$. Theo Hệ quả 1, $d_a \in F$. Do (*) nên đa thức $x^t - N_{F(a)/F}(a)d_a^{-1}$ nhận a làm nghiệm. Nếu t là số chẵn thì $a^t = (a^r)^{2^l}$; $(2, r) = 1$; $r < t$. Theo Định lý 3 $a^r \in F$, điều này mâu thuẫn với $\deg(\min(a, F)) = t$, suy ra t là số lẻ. Từ tính duy nhất của đa thức tối thiểu ta có $d_a = 1$ suy ra $f(x) = x^t - N_{F(a)/F}(a)$.

Hệ quả 9. Cho D là vành chia tâm F và N là nhóm con chuẩn tắc của D^* căn trên F . Khi đó, nếu $a \in N \setminus F$ thì với mọi $\alpha \in F^*$ ta có $a + \alpha \notin N$.

Chứng minh. Giả sử tồn tại $a \in N \setminus F$ và $\alpha \in F^*$ sao cho $a + \alpha \in N$. Khi đó, $F(a) = F(a + \alpha)$, suy ra $k := \deg \min(a, F) = \deg \min(a + \alpha, F)$. Từ Định lý 5, ta có:

$$\min(a, F) = x^k - N_{F(a)/F}(a) \text{ và } \min(a + \alpha, F) = x^k - N_{F(a)/F}(a + \alpha). \text{ Suy ra}$$

$$(a + \alpha)^k - N_{F(a)/F}(a + \alpha) - a^k + N_{F(a)/F}(a) = k\alpha a^{k-1} + \beta_{k-2}a^{k-2} + \dots + \beta_0 = 0 (\beta_i \in F, i = \overline{0, k-2}).$$

Do đó đa thức $k\alpha x^{k-1} + \beta_{k-2}x^{k-2} + \dots + \beta_1x + \beta_0$ nhận a làm nghiệm và có bậc là $k-1$. Điều này chỉ có thể xảy ra khi $\text{char}F = p > 0$ và $p | k$. Nhưng theo Hệ quả 7 thì p không là ước của k điều này dẫn tới mâu thuẫn. Vậy $a + \alpha \notin N$.

Hệ quả 10. Cho D là vành chia tâm F và N là nhóm con chuẩn tắc của D^* căn trên F . Khi đó, nếu a, b là hai phần tử nằm trong N mà $a + b \in N$ thì tồn tại $\alpha \in F$ sao cho $a = \alpha b$.

Chứng minh. Nếu $a \in F$ thì theo Hệ quả 9 ta có $b \in F$. Khi đó $\alpha = ab^{-1} \in F$ và $a = \alpha b$. Vậy, giả sử $a \in N \setminus F$. Từ $a + b = (ab^{-1} + 1)b \in N$ ta có $(ab^{-1} + 1) \in N$. Áp dụng Hệ quả 9, suy ra $\alpha := ab^{-1} \in F^*$ hay $a = \alpha b$.

Định lý 6. Cho D là vành chia tâm F và N là nhóm con chuẩn tắc của D^* căn trên F . Nếu $a \in N, a^3 \in F$ thì $a \in F$.

Chứng minh. Nếu N là nhóm con chuẩn tắc căn trên F thì F^*N cũng là nhóm con chuẩn tắc căn trên F . Do đó, không mất tính tổng quát ta có thể xem $F^* \subset N$. Nếu $a \in F$ hoặc $a^2 \in F$ thì theo Định lý 3 ta có $a \in F$. Bây giờ, giả sử rằng $a \notin F$ và $a^2 \notin F$. Áp dụng Định lý 5 ta có $\min(a, F) = x^3 - \alpha$ ($\alpha \in F$). Theo Định lý phân tích nhân tử Wedderburn, tồn tại $d_1, d_2 \in D^*$ sao cho

$$x^3 - \alpha = (x - a^{d_1})(x - a^{d_2})(x - a).$$

Từ đó suy ra $a^{d_1} + a^{d_2} + a = 0$, dẫn đến $a^{d_2} + a = -a^{d_1} \in N$. Theo Hệ quả 10, tồn tại $\beta \in F$ sao cho $a = \beta a^{d_2}$, suy ra a giao hoán với $d_2^{-1}ad_2$, dẫn tới a giao hoán với d_2 bởi Hệ quả 6. Tương tự ta có a giao hoán với d_1 , kéo theo $3a = 0$. Do đó $\text{char}F = 3$. Áp dụng Định lý 4 ta nhận được $a \in F$, đây là điều mâu thuẫn. Vậy $a \in F$.

ON ONE OF HERSTEIN'S CONJECTURES

Nguyen Van Thin, Bui Xuan Hai
University of Sciences, VNU-HCM

ABSTRACT: Let D be a division ring with the center F . We say that N is a subgroup of D with understanding that N is in fact a subgroup of the multiplicative group D^* of D . In this note we discuss the conjecture which was posed by Herstein in 1978 [2, Conjecture 3]: If N is a subnormal subgroup of D which is radical over F , then N is contained in F . In his paper, Herstein himself showed that the conjecture is true if N is a finite subnormal subgroup of D . However, it is not proven for the general cases. In this note, we establish some properties of subnormal subgroups in division rings which could give some information in the direction of verifying this longstanding conjecture. In particular, it is shown that the conjecture is true for locally centrally finite division rings.

Keywords: division ring, radical, central, subnormal.

TÀI LIỆU THAM KHẢO

- [1]. Bui Xuan Hai and Le Khac Huynh, *On subnormal subgroups of the multiplicative group of a division ring*, Vietnam J. Math. 32 (2004), no. 1, 21-24, MR2052718.
- [2]. I.N.Herstein, *Multiplicative commutators in division rings*, Israel J. Math. 31 (1978) 180-188.
- [3]. Jacobson, *Structure of Rings*, American Mathematical Society Volum XXXVI..
- [4]. W.R.Scott, *Group Theory*, Dover Publication INC 1987.