COMPOSITIO MATHEMATICA

ALI NESIN

On split $B-N$ pairs of rank 1

Compositio Mathematica, tome 76, n° 3 (1990), p. 407-421
<http://www.numdam.org/item?id=CM_1990__76_3_407_0>

Compositio Mathematica **76**: 407–421, 1990.

On split B–N pairs of rank 1

ALI NESIN
University of California, Department of Mathematics U.C.I., Irvine CA 92717, U.S.A.

Received 3 December 1988; accepted in revised form 26 February 1990

1. Introduction

A split $B-N$ pair of rank 1 is a group G with 2 distinguished subgroups U and T and a distinguished element ω satisfying ($N = N(T)$ denotes the normalizer of T in G, B denotes the subgroup generated by U and T):

(1) $B = U \rtimes T$,
(2) $\omega \in N$ and $\omega^2 \in T$, $\omega \notin B$,
(3) $G = B \dot{\cup} U\omega B$ and each element g of $G-B$, can be written uniquely as $u\omega b$ for $u \in U$, $b \in B$.

Finite split $B-N$ pairs of rank 1 are classified by Shult [Sh] and by Hering, Kantor, Seitz [HKS]. The classification of infinite ones is still open.

In this paper we will assume a fourth axiom

(4) $\omega^2 = 1$.

The author does not know if condition (4) holds in all simple split $B-N$ pairs of rank 1.

Groups satisfying the above conditions are 2-transitive groups (when viewed as acting on the coset space G/B). Interesting examples of infinite, non-simple, 2-transitive groups can be found in [Ca], $G = \mathrm{PSL}_2(K)$ is a simple group satisfying conditions (1)–(4).

Let G be a group satisfying the above conditions (1)–(4). For $t \in T$, let $b(t) = t^\omega$. b is an involutive automorphism of T. For $x \in U^* = U \backslash \{1\}$, x^ω is not in B (because of (3)). Thus

$$x^\omega = \varphi(x)\omega\alpha(x)\beta(x)$$

for some unique $\varphi(x)$, $\alpha(x) \in U$, $\beta(x) \in T$. In fact it is easy to show that $\varphi(x)$, $\alpha(x) \in U^*$. From G we obtained four functions b, α, β, φ. The group multiplication can be written in terms of these four functions. Of course these functions will have to satisfy some functional relations to insure e.g. the associativity of the group product. These relations are given in Proposition 1. We learned from the referee that this was done by Thompson [Th] in 1972 and later we saw a similar statement in [Su] in a special case. As the referee pointed out the relations "are straightforward and technical and only justified by their use for proving theorems that do not need the bulk of alpha and beta in their statements." The sufficiency of these relations to get a split B–N pair of rank 1 is stated in Proposition 2.

The main results of the paper are about the simplicity of a split B–N pair of rank 1. Theorem 1, whose proof is quite easy, states that if G is simple then $C_T(U) = 1$ and $T = T_1$ where

$$T_1 = \{\beta(x_1)\cdots\beta(x_{2n+1}) \colon n \in \mathbb{N} \text{ and } x_i \in U^*\}.$$

The converse of this statement is false (take $G = K^+ \rtimes K^*$ for some field K, then $T = \{1\}$). In Theorem 2, whose proof is not at all conceptual, we show that if $\alpha(x) = x^{-1}$ (as is the case when $G = \mathrm{PSL}_2(K)$) then the converse of Theorem 1 also holds except for a finite number of finite groups. An open problem is the classification of all simple split B–N pairs of rank 1. We do not think that they are all of the form $\mathrm{PSL}_2(K)$ for some field K. [See [M] for a characterisation of $\mathrm{PSL}_2(K)$ as a permutation group).

Our notation is standard. If H is a group with 1 as identity, H^* stands for $H \backslash \{1\}$. x^y stands for $y^{-1}xy$ and x^{-y} for $y^{-1}x^{-1}y$.

2. Conditions on α, β, φ and b

PROPOSITION 1. *Let $G = B \veebar U\omega B$, $B = U \rtimes T$ be a split B–N pair of rank 1 (with $\omega^2 = 1$). Let*

$$b \in \operatorname{Aut} T,$$
$$\alpha, \varphi \colon U^* \to U^*,$$
$$\beta \colon U^* \to T$$

be functions defined by

$$b(t) = t^\omega \quad (t \in T),$$
$$\omega x \omega = \varphi(x)\omega\alpha(x)\beta(x) \quad (x \in U^*).$$

Then for all $x, y \in U^*$ for which $xy \neq 1$ and for all $t \in T$ we have

(a) $\varphi(x) = \alpha(x^{-1})^{-\beta(x^{-1})} = \alpha(\alpha(x)^{-1})^{\beta(x)}$,
(b) $b(t) = \beta(x)^{-1} t \beta(x^t)$,

(c) $b(\beta(x)) = \beta(x^{-1})^{-1} = \beta(\alpha(x))^{-1}$,
(d) $\alpha^2 = \varphi^2 = \mathrm{Id}_{U^*}$, $b^2 = \mathrm{Id}_T$,
(e) $\alpha(x^t) = \alpha(x)^t$,
(f) $\alpha(xy) = \alpha(z)\alpha(y)^{\beta(x^{-1})\beta(z)^{-1}}$,
(g) $\beta(xy) = \beta(z)b\beta(x)\beta(y)$

where $z = \alpha(x)\alpha(y^{-1})^{-\beta(y^{-1})\beta(x)^{-1}}$.

The proof of the above result consists of writing down the group axioms for a group and translating them in terms of α, β, φ and b. Note that (a) gives a definition of φ in terms of α and β. Alternatively, the same equality gives the definition of α in terms of φ and β. In the sequel we will tend to use α rather than φ. Note also that (b) gives the definition of the involutive automorphism b. Equality (c) gives an alternative definition of b on $\langle\beta(x): x \in U^*\rangle$. We will show that if G is simple then $\langle\beta(x): x \in U^*\rangle$ is in fact T. Therefore if G is simple, (c) gives two more definitions of b. Condition (d) implies that α and φ are bijections of U^*. Conditions (f) and (g) are consequences of

$$(\omega x \omega)(\omega y \omega) = \omega(xy)\omega.$$

Note that we do not have a definition of β in terms of α and b. Thus fixing α and b does not necessarily pin down the group G (modulo the knowledge of B).

The converse of the proposition is also true:

PROPOSITION 2. *Let* $B = U \rtimes T$ *be a group. If there are* 4 *functions* α, β, b, φ *satisfying the hypothesis of Proposition* 1 *then there is a split B–N pair G of rank* 1 *with*

$$B < G,$$
$$\omega^2 = 1,$$
$$t^\omega = b(t),$$
$$\omega x \omega = \varphi(x)\omega\alpha(x)\beta(x)$$

for all $x \in U^*$, $t \in T$.

The proof if elementary, one needs to check the group axioms (take G to be the formal set $B \cup U\omega B$, the product is given in the statement).

For the rest of the article, G will stand for a split B–N pair of rank 1 with $\omega^2 = 1$. We retain the notation already introduced.

3. Consequences of simplicity

Let T_1 and T_2 be the following subsets of T:

$$T_1 = \{\beta(x_1)\cdots\beta(x_{2n+1}): n \in \mathbb{N},\ x_i \in U^*\},$$
$$T_2 = \{\beta(x_1)\cdots\beta(x_{2n}): n \in \mathbb{N},\ x_i \in U^*\}.$$

LEMMA. $T_1T_1 \subseteq T_2$, $T_1T_2 = T_2T_1 = T_1$, $T_2 < T$, $b(T_1) \subseteq T_1$, $b(T_2) \subseteq T_2$, $T_1^{-1} \subseteq T_1$.

Proof. The first two statements are trivial. T_2 is clearly closed under products. By (b) of Proposition 1 we have, for all $x \in U^*$, $b\beta(x) = \beta(x^{\beta(x)})$, proving the fourth and the fifth statements. By (c) and the above equality we get $\beta(x^{-1})^{-1} = \beta(x^{\beta(x)})$.

Thus $\beta(x)^{-1} = \beta(x^{-\beta(x^{-1})})$. This shows that $T_1^{-1} \subseteq T_1$ and $T_2^{-1} \subseteq T_2$. □

PROPOSITION 3. *$G_1 = UT_2 \cup U\omega UT_1$ is a normal subgroup of G.*

Proof. It follows almost immediately from the above lemma that G_1 is a subgroup. To show that G_1 is normal we need two claims.

Claim 1. $T_2 \lhd T$.

From (b) it follows that $\beta(x^t) = t^{-1}\beta(x)b(t)$. Since $b^2(t) = t$, we also have $\beta(y^{b(t)}) = b(t)^{-1}\beta(y)t$. Multiplying these two, we get $\beta(x^t)\beta(y^{b(t)}) = t^{-1}\beta(x)\beta(y)t$. This proves the claim.

Claim 2. For all $t \in T$, $b(t)^{-1}T_1t \subseteq T_1$.

Let $t \in T$, $s_1 \in T_1$. There are $s_2 \in T_2$, $x \in U^*$ for which $s_1 = s_2\beta(x)$. Now we compute:

$$b(t)^{-1}s_1t = b(t)^{-1}s_2\beta(x)t = s_2^{b(t)}b(t)^{-1}\beta(x)t.$$

But as we saw in the proof of the above lemma $\beta(x) = \beta(y)^{-1}$ for some $y \in U^*$, thus

$$b(t)^{-1}s_1t = s_2^{b(t)}b(t)^{-1}\beta(y)^{-1}t = s_2^{b(t)}\beta(y^t)^{-1} \in T_2T_1 \subseteq T_1.$$

The second claim is proved.

Now the proposition follows easily. G_1 is normalized by G_1, so also by $U \subseteq G_1$ and $\omega \in G_1$. It remains to show that it is normalized by T. UT_2 is normalized by T because of claim 1. Use claim 2 to show that $U\omega UT_1$ is normalized by T. □

PROPOSITION 4. $C_T(U) \lhd G$.

Proof. $C_T(U)$ is clearly normalized by U (in fact centralized). Since T

normalizes U, T also normalizes $C_T(U)$. It remains to show that ω normalizes $C_T(U)$. Let $t \in C_T(U)$, $x \in U$. Then by the definition of b and by (*b*) $t^\omega = b(t) = \beta(x)^{-1} t \beta(x^t)$, so

$$x^{(t^\omega)} = x^{\beta(x)^{-1} t \beta(x^t)} = x^{\beta(x)^{-1}\beta(x^t)} = x^{\beta(x)^{-1}\beta(x)} = x. \qquad \square$$

Now as a consequence of last two propositions we have:

THEOREM 1. *Let G be a simple split B–N pair of rank* 1. *Then* $C_T(U) = 1$ *and* $T = T_1$.

We will show that if $\alpha(x) = x^{-1}$ (as in $PSL_2(K)$) then the converse of Theorem 1 also holds except for some finite number of finite groups.

4. Case $\alpha(x) = x^{-1}$

Our purpose is to prove Theorem 2 which will soon be stated. But the following results (except may be for Lemma 6) that we will use in its proof are interesting in their own right.

LEMMA 1. *If* $\alpha(x) = x^{-1}$ *then conditions* (*a*)–(*g*) *of theorem* 1 *are equivalent to* $b \in \mathrm{Aut}\, T$, $b^2 = \mathrm{Id}$ *and*

(A) $x^{\beta(x)} = x^{\beta(x^{-1})}$,
(B) $\beta(x^t) = t^{-1}\beta(x)b(t)$,
(C) $\beta(x^{-1}) = b\beta(x)^{-1}$,
(D) $y^{-1}x^{-1} = y^{\beta(y)\beta(x)^{-1}} x y^{-\beta(y)\beta(xy)^{-1}}$,
(E) $\beta(xy) = \beta(x)\beta(x^{-\beta(x)}y^{-\beta(y)})\beta(y)$

for all $x, y \in U^*$ *for which* $xy \neq 1$ *and for all* $t \in T$.

Proof. Clear. $\square$

From now on we will always assume that $\alpha(x) = x^{-1}$. Then $\varphi(x) = x^{-\beta(x)}$ by (a) of theorem 1 and by (A) of the above lemma. Thus

$$(*) \quad x^\omega = x^{-\beta(x)}\omega x^{-1}\beta(x).$$

LEMMA 2. *Let* $x, y \in U^*$. *If* $\beta(x) = \beta(y)$ *and* $xy = yx$ *then* $x = y$ *or* y^{-1}.

Proof. Suppose $x \neq y^{-1}$. Then we can apply (D) to get $y^t = x^2y^2$ where $t = \beta(x)\beta(yx)^{-1}$. By exchanging the roles of x and y we get $x^s = y^2x^2$ where $s = \beta(y)\beta(xy)^{-1}$. But clearly $s = t$ and $x^2y^2 = y^2x^2$. Thus $y^t = x^t$ i.e. $x = y$. $\square$

LEMMA 3. *Let* $x \in U^*$. *Let n be an integer* $< o(x)$. *Then x and* x^{n^2} *are conjugate by T. In fact* $x^{n^2} = x^{\beta(x)\beta(x^n)^{-1}}$.

Proof. By induction on n. If $n = 1$ we are done. For $n > 1$, take $x = y^{n-1}$ in (D) to get

$$y^{-n} = y^{-1}y^{-n+1} = y^{\beta(y)\beta(y^{n-1})^{-1}}y^{n-1}y^{-\beta(y)\beta(y^n)^{-1}}.$$

Apply the induction hypothesis to the above equality to finish the proof. □

COROLLARY 4. *Let $x \in U^*$. Then $o(x)$ is either a prime number or is infinite.*

Proof. Suppose $o(x) = ab$ with $a \neq 1$, $b \neq 1$. By Lemma 3, x and x^{a^2} have the same order which is a contradiction. □

COROLLARY 5. *For $x \in U^*$, $C_U(x)$ is either a group of prime exponent or is torsion-free.*

Proof. By Corollary 4 if two elements x and y commute and they have finite order then the orders must be the same prime. Thus we only need to show that if $o(x) = p$ (prime), $o(y) = \infty$ then $xy \neq yx$.

Suppose $xy = yx$. Then by Lemma 3

$$y^{\beta(y)\beta(y^p)^{-1}} = y^{p^2} = (xy)^{p^2} = (xy)^{\beta(xy)\beta((xy)^p)^{-1}} = (xy)^{\beta(xy)\beta(y^p)^{-1}}.$$

Thus

$$y^{\beta(y)} = (xy)^{\beta(xy)}. \qquad (**)$$

Applying β to both sides and using (*B*) we get $b\beta(y) = b\beta(xy)$. Since b is an automorphism, this implies $\beta(y) = \beta(xy)$. This and (**) give $x = 1$, a contradiction. □

LEMMA 6. *Assume $T^2 = 1$, $C_T(U) = 1$, $T = T_1$ and $\beta(x) = \beta(x^{-1})$ for all $x \in U^*$. Then $|G| \leqslant 60$.*

Proof. Notice first that $T^2 = 1$ implies T is Abelian. Secondly, (C) and the hypothesis yield $b(t) = t$ for all $t \in T$. Thus by (B), $\beta(x^t) = \beta(x)$ for all $x \in U^*$, $t \in T$.

SUBLEMMA 1. *Elements of U have order* 1, 2, 3 *or* 5.

Let $x \in U^*$ have order > 2. Then by Lemma 3, $x = x^{t^2} = x^{16}$, for some $t \in T$, i.e. $x^{15} = 1$. By corollary 4, $x^3 = 1$ or $x^5 = 1$.

SUBLEMMA 2. *If $x, y \in U^*$ are such that $\beta(x) = \beta(y)$ then $x = y$ or y^{-1}.*

Assume this is not the case. By (E), (B) and (C):

$$\beta(xy) = \beta(x^{-\beta(x)}y^{-\beta(x)}) = \beta((x^{-1}y^{-1})^{\beta(x)})$$
$$= \beta(x)^{-1}\beta(x^{-1}y^{-1})b\beta(x) = \beta(x)^{-1}\beta(x^{-1}y^{-1})\beta(x^{-1})^{-1}.$$

So, with the assumption $\beta(x) = \beta(x^{-1})$, we get

$$\beta(xy) = \beta(yx).$$

Let $t = \beta(x)\beta(yx)^{-1} = \beta(y)\beta(xy)^{-1}$. Then by (D)

$$(+) \quad y^t = xy^2x \quad \text{and} \quad x^t = yx^2y.$$

Therefore $y^{txyt^{-1}} = x$ and x and y have the same order. Since $t^2 = 1$, $(+)$ yields:

$$(++) \quad y^2xyx^2y^2x^2yxy^2x = x^2yxy^2x^2y^2xyx^2y = 1.$$

These can be written as

$$(++)' \quad (x^2y^2x^2)(yxy)^3 = (y^2x^2y^2)(xyx)^3 = 1.$$

$(+)$ shows that $x^2 \neq 1$. Suppose $x^3 = 1$. Then by $(+)$ $(xy^2x)^3 = 1$, i.e. $(x^2y^2)^3 = 1$, i.e. $x^2y^2x^2 = yxy$. Putting this in $(++)'$ we get $(y^2x)^4 = 1$. By Corollary 4, $(y^2x)^2 = 1$. This shows that xy^2 has order 2.

On the other hand $\beta(x) = \beta(y^{-1})$. So as for x and y

$$\beta(xy^{-1}) = \beta(y^{-1}x).$$

But $xy^{-1} = xy^2$ has order 2. Thus, for what we have proved for elements of order 2, $xy^{-1} = y^{-1}x$ or $xy^{-1} = x^{-1}y$. The first equality shows that x and y commute which gives a contradiction in view of Lemma 2. The second one shows that $x = y$, which is also a contradiction.

Suppose now $x^5 = 1$. Then $y^5 = 1$ also. I claim that yxy has order 5. It does not have order 1 (Lemma 2). If it has order 3 then by $(++)'$, $x = y^2$, a contradiction (Lemma 2). If it has order 2, then $y^{-2} = xy^2x = y^t$ so $y = y^{t^2} = y^4$, again a contradiction. By sublemma 1, yxy has order 5. Similarly xyx has order 5. Thus by $(++)'$

$$(++)'' \quad x^2y^2x^2 = (yxy)^2 \quad \text{and} \quad y^2x^2y^2 = (xyx)^2.$$

Clearly $\beta(x) = \beta(x^t) = \beta(yx^2y)$. If $yx^2y = x$ then $(++)$ gives $y^2x^4y^2x = 1$, i.e. $y^2x = xy^3$. But then $y^2x = xy^3 = yx^2yy^3$, $yx = x^2y^4$, $yxy = x^2$. and with $(++)''$, this implies $y^2 = 1$, a contradiction. Now if $yx^2y = x^{-1}$ then from $(++)$ we get $x = y$, again a contradiction. Thus $\beta(yx^2y) = \beta(x)$ and $yx^2y \neq x, x^{-1}$. Thus yx^2y has order 5. Hence we may apply $(++)''$ to x and yx^2y (instead of to x and y) to get

$$(yx^2y)^2x^2(yx^2y)^2 = (x(yx^2y)x)^2.$$

Let us calculate left and right sides of this equality:

$$(yx^2y)^2x^2(yx^2y)^2 = yx^2y^2x^2yx^2yx^2y^2x^2y = yx^2y^2(x^2y)^3yx^2y$$
$$= yx^2y^2(x^2y)^{-2}yx^2y = yx^2yx^3y^4x^3yx^2y,$$
$$(x(yx^2y)x)^2 = xyx^2yx^2yx^2yx = xy(x^2y)^3x = xy(x^2y)^{-2}x = x^4y^4x^4.$$

Equating these we get

$$xyxyx^2yx^3y^4x^3yx^2y = 1,$$

now using $(++)''$:

$$1 = xy(xyx)^2x^2y^4x^3yx^2y = xy^3x^2y^2x^2y^4x^3yx^2y.$$

Using $(++)''$ once more

$$1 = y^3x^2y^2x^2y^4x^3yx^2yx = y^3x^2y^2x^2y^4x^2y^4x^2(xyx)^2$$
$$= y^3x^2y^2x^2y^4x^2y^2x^2y^2,$$

i.e. $x^4y^2x^2y^4x^2y^2 = 1$, $x = (y^2x^2y^2)^2 = (yxy)^4 = y^{-1}x^{-1}y^{-1}$, so $xyx = y^{-1}$, by $(++)''$ this gives $y^2x^2y^2 = y^2$, i.e. $x^2 = y^{-1}$. Thus x and y commute, this contradicts lemma 2.

SUBLEMMA 3. $x^t = x^{-1}$ *for all* $x \in U$, $t \in T - \{1\}$.

In the beginning of the proof we noticed that $\beta(x^t) = \beta(x)$. Thus by sublemma 2, $x^t = x$ or x^{-1} for all $x \in U$. Now fix $t \neq 1$. Let $A = C_U(t)$, $B = U - C_U(t)$. If $A = U$ then $t \in C_T(U) = 1$, a contradiction. Thus $B \neq \varnothing$. Let $y \in B$. So $y^t = y^{-1}$. Let $x \in A^*$. Since $xy \notin A$ we have

$$xy^{-1} = x^ty^t = (xy)^t = (xy)^{-1} = y^{-1}x^{-1},$$

i.e. $x^y = x^{-1}$ for all $x \in A$, $y \in B$. In particular A is Abelian.

If for some $z, y \in B$, $zy \in B$ then for all $x \in A^*$: $x^{-1} = x^{zy} = (x^z)^y = x$, $x^2 = 1$. Since $zy \in C_U(x)$ and $x^2 = 1$, zy has order 2 also; but then clearly $zy \notin B$. Thus $B^2 \subseteq A$. So for $y \in B$, $y^{-2} = (y^t)^2 = (y^2)^t = y^2$, $y^4 = 1$, and $y^2 = 1$. Then $y \in A$, a contradiction. So $A^* = \varnothing$, and the sublemma is proved.

End of the proof of Lemma 6: Since $C_T(U) = 1$, Sublemma 3 shows that $|T| \leqslant 2$. By Sublemma 2, this implies $|U| \leqslant 5$. Thus $|G| \leqslant 60$.

THEOREM 2. *Let* G *be an infinite split* B–N *pair of rank* 1 (*with* $\omega^2 = 1$). *Suppose* $\alpha(x) = x^{-1}$. *Then* G *is simple if and only if* $C_T(U) = 1$ *and* $T_1 = T$.

REMARK. It is possible to refine the condition 'G infinite' of the theorem by $|G| > N$ for some natural number N. But finite simple groups are known, so we will not worry about it.

The rest of the article will be devoted to the proof of Theorem 2.

Proof. Theorem 1 is half of the statement. So assume $C_T(U) = 1$ and $T_1 = T$ (thus $T_2 = T$ also). Let $H \lhd G$, $H \neq G$. We want to show that $H = 1$. We will show (in that order) that $U \cap H = 1$, $T \cap H = 1$, $B \cap H = 1$, $\omega B \cap H = \varnothing$, $U\omega B \cap H = \varnothing$. The third and last equalities imply $H = 1$.

In the sequel the symbol '$\equiv$' will mean 'modulo H'.

Claim 1. $U \cap H = 1$.

Let $x \in U \cap H - \{1\}$. Then for all $y \in U^*$ for which $xy \neq 1$, we have (by (D)):

$$1 \equiv yx^{-1}y^{-1} = yx^{\beta(x)\beta(y)^{-1}}yx^{-\beta(x)\beta(yx)^{-1}} \equiv y^2.$$

Thus for all $y \in U$, $y^2 \in H$.

Also by $(*)$

$$1 \equiv x^{\omega} = x^{-\beta(x)}\omega x^{-1}\beta(x) \equiv \omega\beta(x).$$

Thus $\omega t \in H$ for some $t \in T$. Fix this t till the end of this claim. Now for all $s \in T$

$$1 \equiv (\omega t)^s = \omega b(s)^{-1}ts;$$

also $t^{-1}\omega \in H$. Thus $t^{-1}b(s)^{-1}ts \in H$, i.e.

$$ts \equiv b(s)t \quad (\text{all } s \in T). \tag{1.1}$$

Since $t^2 = t\omega\omega t = (\omega t)^{t^{-1}}\omega t$, $t^2 \in H$:

$$t^2 \in H. \tag{1.2}$$

Notice that if we set $t = s$ in (1.1) we get $t \equiv b(t)$.

Now we will use the fact that $y^2 \in H$ for all $y \in U$:

$$\begin{aligned} 1 \equiv (\omega t)^y(\omega t) &\equiv y\omega ty\omega t = yb(t)\omega y\omega t \\ &\underset{(*)}{\equiv} yb(t)y^{\beta(y)}\omega y\beta(y)t \\ &\equiv yty^{\beta(y)}t^{-1}y\beta(y)t \end{aligned}$$

where the last congruence follows from (1.1) and the fact that $\omega \equiv t^{-1}$. Set

$$z = yy^{\beta(y)t^{-1}}y, \qquad s = \beta(y)t.$$

Thus $zs \in H$. So $sz^2s \in H$ also. Since $z^2 \in H$, this shows that $s^2 \in H$; replacing s by its definition we get

$$1 \equiv \beta(y)t\beta(y)t \underset{1.1}{\equiv} \beta(y)b\beta(y)t^2 \underset{1.2}{\equiv} \beta(y)b\beta(y)$$

i.e.

$$\beta(y)b\beta(y) \in H \quad (\text{all } y \in U^*). \tag{1.3}$$

We compute once more:

$$1 \equiv zs = yty^{\beta(y)}t^{-1}y\beta(y)t \underset{1.2}{\equiv} yt\beta(y)^{-1}y\beta(y)ty\beta(y)t$$

$$\underset{1.3}{\equiv} ytb\beta(y)(y\beta(y)t)^2 \underset{1.1}{\equiv} (y\beta(y)t)^3.$$

So $(ys)^3 \in H$. Since we know that $s^2 \in H$, this shows

$$1 \equiv (ys)^3 = yy^{s^{-1}}y^{s^{-2}}s^3 \equiv yy^sys.$$

Also $1 \equiv (yy^sys)^2 \equiv (yy^s)^3$. Therefore for any $y \in U$, $(yy^s)^3 \in H$. But also $(yy^s)^2 \in H$. Thus for any $y \in U$,

$$yy^s \in H. \tag{1.4}$$

Computing again and using the definition of $s = \beta(y)t$, we get

$$\beta(y^s)\beta(y)^{-1} \underset{(B)}{=} s^{-1}\beta(y)b(s)\beta(y)^{-1} \underset{1.1}{\equiv} s^{-1}\beta(y)tst^{-1}\beta(y)^{-1}$$
$$= s^{-1}\beta(y)t(\beta(y)t)t^{-1}\beta(y)^{-1} = s^{-1}\beta(y)t = 1.$$

Now we use the above result:

$$1 \underset{1.4}{\equiv} y^{-s}y^{-1} \underset{(D)}{=} y^{s\beta(y^s)\beta(y)^{-1}}yy^{-s\beta(y^s)\beta(yy^s)^{-1}} \equiv y^syy^{-s\beta(y^s)\beta(yy^s)^{-1}}$$

$$\underset{1.4}{\equiv} y^{-s\beta(y^s)\beta(yy^s)^{-1}}.$$

Thus $y \in H$. So we showed that $U \subseteq H$.

As for x, $\omega\beta(y) \in H$ for all $y \in U^*$. This easily shows that $T_2 \subseteq H$. Thus $T \subseteq H$.

It remains to show that $\omega \in H$. But this is clear because $\omega\beta(x) \in H$ and $T \subseteq H$. So $H = G$, a contradiction. Claim 1 is now proved.

Claim 2. $H \cap T = \{1\}$.

Suppose $t \in H \cap T$. Then for all $x \in U$, $t^x t^{-1} \in H \cap U = 1$. Thus, $x^t = x$, i.e. $t \in C_T(U) = 1$.

Claim 3. $H \cap B = 1$.

This will take some time. By Claims 1 and 2 we may assume that $xt \in H \cap B$, $x \in U^*$, $t \in T^*$. We will get a contradiction.

We first show that x and t commute. This is easy: $xt \in H$, so $tx = (xt)^{t^{-1}} \in H$, so $x^{-1}t^{-1} = (tx)^{-1} \in H$. Thus $(xt)(x^{-1}t^{-1}) \in H \cap U = 1$. Let us record this:

$$xt \in H \cap B \Rightarrow xt = tx. \tag{3.1}$$

By (B) and (3.1) we get $\beta(x) = \beta(x^t) = t^{-1}\beta(x)b(t)$, i.e. $b(t) = t^{\beta(x)}$:

$$xt \in H \cap B \Rightarrow b(t) = t^{\beta(x)}. \tag{3.2}$$

Using (3.2) we compute $(xt)^\omega$ modulo H:

$$1 \equiv (xt)^\omega = \omega x \omega b(t) \underset{(*)}{=} x^{-\beta(x)}\omega x^{-1}\beta(x)b(t) \underset{(3.2)}{=} x^{-\beta(x)}\omega x^{-1}t\beta(x).$$

Thus, replacing x^{-1} by t we get

$$xt \in H \cap B \Rightarrow \omega t^3\beta(x) = \omega s \in H \tag{3.3}$$

where $s = t^3\beta(x)$. Since $s\omega \in H$ also, we have $s^2 \in H \cap T = 1$:

$$xt \in H \cap B \Rightarrow s^2 = (t^3\beta(x)^2 = 1. \tag{3.4}$$

Also for all $u \in T$, $(\omega s)^u \in H$. Thus

$$1 \equiv s\omega(\omega s)^u = s\omega u^{-1}\omega s u = sb(u)^{-1}su,$$

i.e. $sb(u)^{-1}su \in H \cap T = 1$, since $s^2 = 1$ this gives

$$b(u) = u^s \quad \text{for all } u \in T. \tag{3.5}$$

We will now show that $t^2 = 1$ or $t^3 = 1$.

Since $xt \in H$, by (3.1), $(xt)^n = x^n t^n \in H$. In view of Claims 1 and 2, this shows that $o(x) = o(t)$. Now if $n < o(x)$ then applying (3.3) to $x^n t^n$ we have $\omega t^{3n}\beta(x^n) \in H$.

Thus $st^{3n}\beta(x^n) = (s\omega)(\omega t^{3n}\beta(x^n)) \in H \cap T = 1$. Hence $\beta(x^n) = t^{-3n}s$. We apply this to Lemma 3

$$x^{n^2} = x^{\beta(x)\beta(x^n)^{-1}} = x^{t^{-3}sst^{3n}} = x^{t^{3n-3}} \underset{(3.1)}{=} x.$$

So $x^{n^2-1} = 1$ for all $n < o(x)$. If $o(x) > 3$, take $n = 3$ to get $x^8 = 1$. By Corollary 4, $x^2 = 1$, a contradiction. Thus $o(x) = 2$ or 3; by 3.1 the same holds for t:

$$xt \in H \Rightarrow (x^2 = 1 \text{ and } t^2 = 1) \text{ or } (x^3 = 1 \text{ and } t^3 = 1). \tag{3.6}$$

We will now show that for any $u \in T$, either $u^2 = 1$ or $u^3 = 1$.

Let $y \in U^*$. Since $\omega s \in H \lhd G$, we have:

$$1 \equiv (\omega s)^{y\omega} = \omega y^{-1}\omega sy\omega = y^{\beta(y^{-1})}\omega y\beta(y^{-1})sy\omega$$

$$\underset{(3.3)}{=} y^{\beta(y^{-1})}sy\beta(y^{-1})sys \underset{(3.5)}{=} y^{\beta(y^{-1})}y^s b\beta(y^{-1})ys$$

$$\underset{(C)}{=} y^{\beta(y^{-1})}y^s\beta(y)^{-1}ys \underset{(A)}{=} y^{\beta(y)}y^s y^{\beta(y)}\beta(y)^{-1}s.$$

Let us record this for future use:

$$\text{For all } y \in U^*,\ y^{\beta(y)}y^s y^{\beta(y)}\beta(y)^{-1}s \in H. \tag{3.7}$$

In particular, all properties stated above for x and t are also valid for $y^{\beta(y)}y^s y^{\beta(y)}$ and $\beta(y)^{-1}s$ unless they are 1. (3.7) shows that for any $y \in U^*$ there is a $z \in U$ for which $z\beta(y)^{-1}s \in H$. Since $T_2 = T$ and $s^2 = 1$, this easily implies that for any $u \in T$, there is a $z \in U$ for which $zu \in H$. So as in (3.6) $u^2 = 1$ or $u^3 = 1$; thus we showed:

$$\text{For any } u \in T, \text{ either } u^2 = 1 \text{ or } u^3 = 1. \tag{3.8}$$

(3.7) and (3.1) give $(y^{\beta(y)}y^s y^{\beta(y)})^{\beta(y)^{-1}s} = y^{\beta(y)}y^s y^{\beta(y)}$ for all $y \in U^*$, i.e. $y^s y^{s\beta(y)^{-1}s} y^s = y^{\beta(y)}y^s y^{\beta(y)}$. By (3.5) this means $y^s y^{b\beta(y)^{-1}} y^s = y^{\beta(y)}y^s y^{\beta(y)}$, which is by (A) and (C) equivalent to

$$y^s y^{\beta(y)} y^s = y^{\beta(y)}y^s y^{\beta(y)}. \tag{3.9}$$

On the other hand $(y^s y^{\beta(y)} y^s)^6 = 1$ by (3.6) and (3.7). This and the equality (3.9) give $(y^{\beta(y)}y^s)^9 = 1$. By Corollary 4, $(y^{\beta(y)}y^s)^3 = 1$. Using (3.9) once more this gives $(y^{\beta(y)}y^s y^{\beta(y)})^2 = 1$. But now by (3.6) and (3.7) $(\beta(y)^{-1}s)^2 = 1$, i.e. $\beta(y)^{-1} = \beta(y)^s$. By (3.5) $\beta(y)^{-1} = b\beta(y)$ and by (C) $\beta(y) = \beta(y^{-1})$:

For any $y \in U^*$, $b\beta(y) = \beta(y)^{-1} = \beta(y)^s = \beta(y^{-1})^{-1}$. (3.10)

Assume now $\beta(x) = \beta(y)$ and $xy \neq 1$, $xy^{-1} \neq 1$. We will show that $x^2 \neq 1$, $x^3 \neq 1$. By (E)

$$\beta(xy) = \beta(x)\beta((yx)^{-\beta(x)})\beta(x),$$

by (B)

$$\beta(xy) = \beta(x)\beta(x)^{-1}\beta((yx)^{-1})b\beta(x)\beta(x),$$

by (3.10)

$$\beta(xy) = \beta((yx)^{-1}) = \beta(yx).$$

Now as in Sublemma 2 of Lemma 6 we have

$$\begin{aligned} &x^t = yx^2y, \\ &y^t = xy^2x, \qquad\qquad (3.11)\\ &y \text{ and } x \text{ are conjugate.} \end{aligned}$$

This shows that $x^2 \neq 1$. So assume $x^3 = 1$. Thus $y^3 = 1$ also. In particular yx^2y, $x^2y^2 = (yx)^{-1}$ and xy have order 3. Similarly xy^2x has order 3. If $t^2 = 1$, as in Sublemma 2 we get a contradiction. So $t^3 = 1$ (by (3.8)). Then

$$\begin{aligned} x = x^{t^3} &\underset{(3.11)}{=} (yx^2y)^{t^2} \underset{(3.11)}{=} (xy^2x(yx^2y)^2xy^2x)^t = (xy^2x(yx^2y)^{-1}xy^2x)^t \\ &\times ((xy^2)^4x)^t \underset{(3.11)}{=} (yx^2y(xy^2x)^2)^4yx^2y = (yx^2y(xy^2x)^{-1})^4yx^2y \\ &= (yx^2)^{12}yx^2y = (yx^2)^{13}y. \end{aligned}$$

So $(yx^2)^{14} = 1$. By Corollary 4, $(yx^2)^2 = 1$ or $(yx^2)^7 = 1$. If $(yx^2)^2 = 1$ we get a contradiction by replacing x by x^{-1} in the above argument: as above $\beta(yx^2) = \beta(x^2y)$, since yx^2 has order 2, we must have $yx^2 = x^2y$ or $yx^2 = (x^2y)^{-1} = y^2x$; the first case contradicts Lemma 2, the second case gives $x = y$. Thus $(yx^2)^7 = 1$. Similarly $(y^2x^2)^7 = 1$. But we have showed (after (3.11) that $(y^2x^2)^3 = 1$. This shows that $y^2x^2 = 1$, i.e. $x = y^{-1}$, a contradiction. Hence

$$\beta(x) = \beta(y),\ x^2 = 1 \quad \text{or } x^3 = 1 \Rightarrow x = y \quad \text{or } y^{-1}. \qquad (3.12)$$

Now suppose $u \in T$ and $u^3 = 1$. We showed just before (3.8) that $yu \in H$ for some $y \in U$. By (3.3) $\omega u^3\beta(y) \in H$. Thus $su^3\beta(y) \in H \cap T = 1$ thus $\beta(y) = s$ and so by (3.12) and (3.1) the set

$$\{y \in U : \exists u \in T u^3 = 1 \text{ and } yu \in H\}$$

has cardinality $\leqslant 3$. Since for each such u there is a unique such y, T has at most 2 elements of order 3, the rest of its elements having order 2. Thus if T has an element of order 3, say u, then $2 = |u^T| = |T/C_T(u)|$. But $C_T(u)$ contains only elements of order 3 (if not T would have elements of order 6). Thus $|C_T(u)| = 3$. Thus $|T| = 6$, i.e. $T = S_3$. (3.1) shows that U has finitely many elements of order 2 and 3. As for T, U must be finite (use Corollary 5). Thus G is finite. (In fact (3.12) shows that U has at most 12 elements of order 2 and 3).

If T has no elements of order 3 then $T^2 = 1$ and since (3.10) holds we can apply Lemma 6 that shows that $|G| \leqslant 60$.

Claim 4. $H \cap \omega B = \varnothing$.
Let $\omega xt \in H$ for $x \in U$, $t \in T$. We have $xtxt = (\omega xt)^{\omega}(\omega xt) \in H \cap B$.
So by Claim 3, $xtxt = 1$, hence $t^2 = 1$.
Now for any $y \in U^*$:

$$1 \equiv (\omega xt)^{y\omega} = \omega y^{-1}\omega xty\omega = y^{\beta(y)}\omega y\beta(y^{-1})xty\omega$$
$$\equiv y^{\beta(y)}t^{-1}x^{-1}y\beta(y^{-1})xtyt^{-1}x^{-1} = zt^{-1}\beta(y^{-1})$$

for some $z \in U$. Thus $\beta(y^{-1}) = t$, so for all $y \in U^*$, $\beta(y) = t$. Hence $T = \{1, t\}$, $T^2 = 1$ and $b = \mathrm{Id}$. So by (C) $\beta(y) = \beta(y^{-1})$. Lemma 6 again implies that G is finite; $|G| \leqslant 60$.

Claim 5. $H = 1$.
By claim 3, $H \cap B = 1$. If $x\omega b \in H (x \in U, b \in B)$, then $\omega bx \in H \cap \omega B = \varnothing$.
This finishes the proof of Theorem 2. □

Acknowledgement

Research partially supported by NSF Grant DMS-8801021. The article was written while the author was visiting Notre Dame University. He would like to thank the Department of Mathematics for their kind hospitality. However the main result was obtained in the military jail of Isparta (Turkey). The author is in debt to his superiors (in particular to Gen. Yusuf Haznedaroglu) for giving him this once in a lifetime opportunity.

References

[Ca] P. J. Cameron: Normal subgroups of infinite multiply transitive permutation groups, *Combinatorica* 1(4) (1981), 343–347.

[HKS] C. Herring, W. Kantor and G. Seitz: Finite groups with a split BN-pair of rank 1, *J. of Algebra* 20 (1972), 435–475.

[M] H. Mäurer: Eine Charakterisierung der zwischen PS-L (2, K) und PGL(2, *K*) liegenden Permutationsgruppen, *Arch. Math.*, 40 (1983), 405–411.

[Sh] E. Shult, On a class of doubly permutation groups, *Illinois J. Math.* 16 (1972), 434–455.

[Su] M. Suzuki, On a class of doubly permutation groups, *Annals of Math.* 75, No. 1, (1962), 105–145.

[Th] J. G. Thompson, Toward a characterisation of $E_2^*(q)$, II, *Journal of Algebra* 20 (1972), 610–621.