Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 401–412

On the structure of special rank one groups

Franz Georg Timmesfeld

§1. Introduction

A group X generated by two different nilpotent subgroups A and B satisfying:

$(*)$ For each $a \in A^\#$ there exists a $b \in B^\#$ satisfying $A^b = B^a$ and vice versa

is called a rank one group. The conjugates of A (and B) are called the *unipotent subgroup* of the rank one group X and the conjugates of $H = N_X(A) \cap N_X(B)$ will be called the *diagonal subgroups.* If A is abelian X is called a rank one group with *abelian unipotent* subgroups, abbreviated AUS. Moreover, if for each $a \in A^\#$ and $b \in B^\#$ which satisfy $(*)$ above, also

$$(**) \qquad a^b = b^{-a} (= (b^{-1})^a)$$

holds, X is called a *special rank one group.*

Rank one groups with abelian unipotent subgroups played a fundamental role in the theory of "abstract root subgroups" [Ti1]. Indeed by (3.18)(3) and (4.15) of [Ti1] all rank one Σ-subgroups occurring in a group generated by a class Σ of abstract root subgroups of "higher rank" are special. A theory of arbitrary rank one groups was developed in §2 of [Ti2]. In both papers one is not able to say very much about the structure of rank one groups, but one has to live with properties of such groups.

By Proposition (2.1) of [Ti2] the following are equivalent:

(i) $X = \langle A, B \rangle$ is a rank one group.

Received March 15, 1999.

(ii) The group Y is doubly transitive on a set Ω with $|\Omega| \geq 3$, such that for some $\alpha \in \Omega$, Y_α contains a nilpotent normal subgroup $A = A_\alpha$ which is regular on $\Omega \backslash \{\alpha\}$ and $X = \langle A^g \mid g \in Y \rangle$.

Namely if $X = \langle A, B \rangle$ is a rank one group one may set $\Omega = A^X$ and $Y = X$. Then it is easy to see that Y satisfies (ii). The reverse direction is also immediate. This shows that the notion of rank one groups and groups with a split BN-pair of rank one are equivalent. (Since $N_X(A) = AH$, $A \cap H = 1$, X has a split BN-pair of rank one!)

Moreover, if $X = \langle A, B \rangle$ is a rank one group, for given $a \in A^\#$ the element $b \in B^\#$ satisfying $A^b = B^a$ is by (2.2) of [Ti2] uniquely determined and so will be called $b(a)$. Further, if for given $b \in B^\#$ we call $a(b)$ the unique element of $A^\#$ satisfying $B^{a(b)} = A^b$, then the maps

$$a \to b(a),\ b \to a(b)$$

are bijections of $A^\#$ onto $B^\#$ resp. $B^\# \to A^\#$. If we denote by χ both maps, then χ is a bijection of $A^\#$ onto $B^\#$, $B^\#$ onto $A^\#$ satisfying $\chi^2 = \mathrm{id}$ and

$$A^{\chi(a)} = B^a,\ A^b = b^{\chi(b)} \text{ for all } a \in A^\#, b \in B^\#.$$

With this notation we can formulate the main results of this note:

Theorem 1. *Let $X = \langle A, B \rangle$ be a special rank one group with AUS. Then the following hold:*

(a) *Either*
  (i) *A is an elementary abelian p-group for some prime p.*
  or (ii) *A is torsionfree and divisible.*

(b) *For all $a \in A^\#$ and $b \in B^\#$ we have*

$$a^{1/n} = \chi(\chi(a)^n),\ b^{1/n} = \chi(\chi(b)^n)$$

where in case (i) *$n \in \mathbb{N}$ with $(p, n) = 1$, while in* (ii) *$n \in \mathbb{N}$ is arbitrary.*

(*Here $a^{1/n}$ denotes the unique $\overline{a} \in A$ with $\overline{a}^n = a$!*)

Theorem 2. *Let $X = \langle A, B \rangle$ be a special rank with AUS. Then one of the following holds:*

(a) *If A is an elementary abelian p-group, then $\langle a, b(a) \rangle \simeq (P)SL_2(p)$ for each $a \in A^\#$ (and of course also $\langle b, a(b) \rangle \simeq (P)SL_2(p), b \in B^\#$!)*

(b) *If A is torsionfree and divisible, $a \in A^\#$ and $b = \chi(a) \in B^\#$ set*

$$\begin{aligned} A(a) &= \{a^{m/n} \mid m, n \in \mathbb{Z}, n \neq 0, a^0 = 1\} \\ B(b) &= \{b^{m/n} \mid m, n \in \mathbb{Z}, n \neq 0, b^0 = 1\} \end{aligned}$$

($a^{m/n}$ is well-defined by $a^{m/n} = (a^{1/n})^m$ and Theorem 1). Then $A(a) \simeq (\mathbb{Q}, +) \simeq B(b)$ and $X(a) = \langle A(a), B(b) \rangle$ is a factor group of the universal perfect central extension of $SL_2(\mathbb{Q})$.

Here $(P)SL_2$ denotes any center factor group of SL_2. It will be shown in §2 that the universal perfect central extension of $SL_2(k)$, k a field with $|k| > 4$ and $|k| \neq 9$, is a special rank one group with AUS. So in some sense, theorem 2 is the best possible. On the other hand, as the large list of examples in §2 shows, it seems unlikely that one can determine the exact structure (isomorphism type) of arbitrary special rank one groups with AUS, also there are some results in this direction under additional hypotheses. (i.e. A acts quadratically on some $\mathbb{Z}X$-module, see Theorem 1 of [Ti3]). Since arbitrary rank one groups occur in many situations in group theory, for example as classical groups of Witt-index 1, see [Ti2, (2.15)], or as a subgroup generated by two opposite root-subgroups on a Moufang building, see [Ti2, (2.12)], and since there is a connection between arbitrary rank one groups and special rank one groups with AUS (i.e. conditions under which $\langle Z(A), Z(B) \rangle$ is special [Ti2, (2.9)]), I believe that any result on the structure of special rank one groups is of interest.

§2. Examples and known properties of rank one groups

In this section we discuss certain examples of special rank one groups and state, for the convenience of the reader, basic properties which will be needed for the proof of theorem 1 and 2. These results are, with exception of (2.3), contained in §2 of [Ti1] and [Ti2].

(2.1) **Example** ([Ti1, (2.2)]). Let R be a ring with one element 1 and $L \subseteq R$ satisfying:

(1) $1 \in L$ and L is an additive subgroup of R.
(2) All elements of L^* are units of R and L^* is closed under inverses.
(3) If $t, c \in L$, then $tct \in L$.

Let $A = \{\left(\begin{smallmatrix} 1 & \\ c & 1 \end{smallmatrix}\right) \mid c \in L\}, B = \{\left(\begin{smallmatrix} 1 & c \\ & 1 \end{smallmatrix}\right) \mid c \in L\}$ and $X = \langle A, B \rangle$ (considered as subgroup of $GL_2(R)$!). Then X is a special rank one group with AUS. Further, if $|L| > 3$, then X is quasisimple. Abusing notation we call this group $SL_2(L)$.

A concrete example is given by: R a division ring, σ an antiautomorphism and $L = \{c \in R \mid c = c^\sigma\}$.

(2.2) **Example** ([Ti3]). Let K be a division ring or a Cayley division algebra, $V = K^2$ and $X = SL_2(K)$ be the subgroup of $\mathrm{Aut}(V)$ generated by the maps $a(t), b(t), t \in K$ that act on V as follows:

$$(c,d)^{a(t)} = (c + dt, d) \quad ; \quad (c,d)^{b(t)} = (c, ct + d).$$

Then X is a special rank one group with AUS with unipotent subgroups $A = \{a(t) \mid t \in K\}$ and $B = \{b(t) \mid t \in K\}$. Further, if $|K| > 3$, then X is quasisimple.
(If $L \subseteq K$ satisfying (1) - (3) of (2.1) one obtains similar examples as in (2.1). These will be contained in a forthcoming book of the author on "Abstract root subgroups".)

(2.3) **Example.** Let k be a field with $|k| > 4$ and $|k| \neq 9$ and let X be the universal perfect central extension of $SL_2(k)$ in the sense of [St]. Then, by theorem 10 of [St], X is the group generated by symbols

$$a(t), b(t); t \in k$$

subject to the relations:

(A) $a(t)a(\tau) = a(t + \tau), b(t)b(\tau) = b(t + \tau); t, \tau \in k.$
(B) $a(u)^{n(t)} = b(-t^{-2}u); u \in k$ and $t \in k^*$
where $n(t) = a(-t)b(t^{-1})a(-t)$.

($n(t)$ is defined slightly different as in §6 of [St]. This is necessary since we conjugate in the usual group-theoretic fashion, i.e. $x^y = y^{-1}xy$.)

Now it is easy to see that the relations (A) + (B) are equivalent to (A) +(B'), where

(B') $a(u)^{b(t^{-1})} = b(-t^{-2}u)^{a(t)}; u \in k, t \in k^*$.
If now $t \in k^*$ is fixed, then $k = \{-t^{-2}u \mid u \in k\}$, whence

$$A^{b(t^{-1})} = B^{a(t)} \text{ for } A = \{a(u)\},\ B = \{b(u)\}.$$

Further

$$a(t)^{b(t^{-1})} = b(-t^{-1})^{a(t)} = (b(t^{-1}))^{-a(t)}.$$

Hence, setting $b(a(t)) := b(t^{-1})$, it follows that X is a special rank one group with AUS.

Notice that if $|k| = \infty$ usually X is different from $SL_2(k)$, see §7 of [St].

For the rest of this section we assume that $X = \langle A, B\rangle$ is a special rank one group with AUS. We state some properties of such an X, which will be needed for the proof of theorem 1 and 2.

(2.4) Let $\Omega = A^X$. Then $X = \langle C, D\rangle = \langle C, d\rangle$ for all $C \neq D \in \Omega$ and $d \in D^\#$. Further $N_C(D) = 1$.

(2.5) For $a \in A^\#$ and $b \in B^\#$ one has

$$\chi(a^{-1}) = \chi(a)^{-1},\ \chi(b^{-1}) = \chi(b)^{-1}.$$

(2.6) Let $N \trianglelefteq X$. Then either $N \leq Z(X)$ or $X = NA$. Especially X is quasisimple if $X = X'$. Moreover, X is not nilpotent.

These results are contained in §2 of [Ti1]. Notice that, together with theorem 2, (2.6) implies that X is quasisimple, except when $p \leq 3$ in case (a)(i) of theorem 1. Now by (2.10) and (2.12) of [Ti1] we have

(2.7) One of the following holds:

(a) $X \simeq SL_2(2)$ or $X \simeq (P)SL_2(3)$.
(b) $X = X'A$, X' quasisimple and $|[A, H]| > 3$.

Actually I believe that either case (a) of (2.7) holds or X is quasisimple. A proof of this would simplify the known simplicity proofs for classical and Lie-type groups, which are not defined over $GF(2)$ or $GF(3)$. (See Theorem (3.17) of [Ti1]!)

§3. Proof of theorem 1

Assume in this section that $X = \langle A, B\rangle$ is a special rank one group with AUS with unipotent subgroups A and B. For each $n \in \mathbb{N}$ let $A_n = \{a \in A \mid a^n = 1\}$ and $A^n = \{a^n \mid a \in A\}$ and similarly B_n, B^n. If for some $a \in A^\#$ there exists a unique $\widetilde{a} \in A^\#$ with $\widetilde{a}^n = a$ we write $\widetilde{a} = a^{1/n}$ and similarly for $b \in B^\#$. We first show:

(3.1) Suppose there exists an $a \in A$ with $a^2 \neq 1$. Then the following hold:

(a) $A_2 = 1$ and $A = A^2$.

(b) For each $a \in A^\#$ and $b \in B^\#$ we have

$$a^{1/2} = \chi(\chi(a)^2),\ b^{1/2} = \chi(\chi(b)^2).$$

(χ as defined in the introduction. Notice that A and B are conjugate in X, so (a) also holds for B!)

Proof. It suffices to prove (b) only for $a \in A^\#$, since then it holds by symmetry also for $b \in B^\#$.

Pick $a \in A^\#$ with $a^2 \neq 1$ and set $b = \chi(a)$. Then, as $a^b = b^{-a}$ we have $o(b) = o(b^{-1}) = o(a) \neq 2$. Hence there exists a unique $\bar{a} \in A$ with $A^{b^2} = B^{\bar{a}}$. This implies $b^2 = \chi(\bar{a})$ and, since X is special,

$$\bar{a}^{b^2} = (b^2)^{-\bar{a}}.$$

Further by (2.5)

$$b^{-2} = (b^2)^{-1} = \chi(\bar{a})^{-1} = \chi(\bar{a}^{-1})$$

so that $B^{\bar{a}^{-1}} = A^{b^{-2}}$. Now

$$\begin{aligned} B^{\bar{a}} &= (A^b)^b = B^{ab} = B^{a^b} = B^{(b^{-1})^a} = B^{a^{-1}b^{-1}a} \\ &= A^{b^{-1}b^{-1}a} = A^{b^{-2}a} = B^{\bar{a}^{-1}a}, \end{aligned}$$

since by (2.5) $b^{-1} = \chi(a^{-1})$. We obtain $B^{\bar{a}^2 a^{-1}} = B$. Hence $\bar{a}^2 a^{-1} \in N_A(B)$ and thus $\bar{a}^2 = a$ by (2.4). Since $\bar{a} = \chi(b^2)$ (as $\chi^2 = \mathrm{id}$!) we obtain the equation:

$$(*) \qquad a = \chi(\chi(a)^2)^2 \text{ for each } a \in A^\# \text{ with } a^2 \neq 1.$$

Now $(*)$ shows that each element of A with $a^2 \neq 1$ is a square in A. This implies $A = A_2 \cup A^2$. Since no group is the union of two proper subgroups this implies $A = A^2$.

Suppose $\tilde{a} \in A^\#$ has even order. If $o(\tilde{a}) \neq 2$, then there exists by $(*)$ an $\bar{a} \in A$ with $\bar{a}^2 = \tilde{a}$ and $\bar{a} = \chi(\chi(\tilde{a}^2))$. Since the elements a and $\chi(a)^{-1}$ are conjugate in X by definition of χ, this implies

$$o(\bar{a}) = o(\chi(\tilde{a}^2)) = o(\tilde{a})^2,$$

which obviously contradicts $\bar{a}^2 = \tilde{a}$.

This shows that each element of even order in $A^{\#}$ has order 2. But as $A^2 = A$, this implies that there exists no element of order 2 in A, whence $A_2 = 1$ which proves (a).

Now (a) and (*) imply that $\widehat{a} = \chi(\chi(a)^2)$ is the unique element of A with $\widehat{a}^2 = a$. Hence by definition $\widehat{a} = a^{1/2} = \chi(\chi(a)^2)$, which proves (3.1). Q.E.D.

Next we show

(3.2) Suppose A is an elementary abelian q-group for some prime q. Then we have for all $m \in \mathbb{N}$ with $(m, q) = 1$ and for all $a \in A^{\#}, b \in B^{\#}$:

$$a^{1/m} = \chi(\chi(a)^m),\ b^{1/m} = \chi(\chi(b)^m).$$

Proof. We first show, that it suffices to prove (3.2) for $m \leq q-1$. Namely let $m = n \cdot q + r, r \leq q-1$. Then, since A and B are elementary abelian q-groups, we have $\chi(a)^m = \chi(a)^r$ and if $\chi(\chi(a)^r)^r = a$, then also $\chi(\chi(a)^m)^m = a$. Hence (3.2) holds for m if it holds for r.

We now prove (3.2) for $m \leq q-1$ by induction on m, the induction assumption $m = 2$ being (3.1). So suppose that (3.2) holds for $n < m$. Pick $a \in A^{\#}$ and let $\overline{a} = \chi(\chi(a)^m)$. Then we have with $b = \chi(a)$:

$$B^{\overline{a}} = A^{b^m} = A^{b^{m-1}b} = B^{\chi(b^{m-1})b} = B^{a^{1/m-1}b} = B^{(a^{1/m-1})^b}$$

since (3.2) holds for $m-1$.

Now, as $a^{ba^{-1}} = b^{-1}$, we have $(a^{1/m-1})^{ba^{-1}} = (b^{-1})^{1/m-1}$, whence $(a^{1/m-1})^b = ((b^{-1})^{1/m-1})^a$. This implies

$$\begin{aligned} B^{\overline{a}} &= B^{(a^{1/m-1})^b} = B^{((b^{-1})^{1/m-1})^a} = B^{a^{-1}(b^{-1})^{1/m-1}a} \\ &= A^{b^{-1}(b^{-1})^{1/m-1}a} = A^{(b^{-m})^{1/m-1}a} \end{aligned}$$

by (2.5) and since

$$b^{-1}(b^{-1})^{1/m-1} = (b^{-1})^{1+1/m-1} = (b^{-1})^{m/m-1} = (b^{-m})^{1/m-1}.$$

Now, since $\overline{a} = \chi(b^m)$, (2.5) implies

$$\overline{a}^{-1} = \chi(b^m)^{-1} = \chi(b^{-m})$$

and thus applying χ to this equation $b^{-m} = \chi(\overline{a}^{-1})$. We obtain:

$$(b^{-m})^{1/m-1} = \chi(\overline{a}^{-1})^{1/m-1} = \chi((\overline{a}^{-1})^{m-1})$$

by induction assumption and since $\chi^2 = \mathrm{id}$. Substituting this in the above equation, we obtain

$$B^{\overline{a}a^{-1}} = A^{(b^{-m})^{1/m-1}} = A^{\chi((\overline{a}^{-1})^{m-1})} = B^{(\overline{a}^{-1})^{m-1}}$$

and thus $B^{\overline{a}^m a^{-1}} = B$. Hence $\overline{a}^m a^{-1} \in N_A(B) = \{1\}$ by (2.4) and $\overline{a}^m = a$. This implies $\overline{a} = a^{1/m}$, which proves (3.2) by definition of $\overline{a}$. Q.E.D.

(3.2) shows that Theorem 1 holds if A is an elementary abelian q-group for some prime q. So we assume from now on that this is not the case. We show next:

(3.3) Let p be a prime and $a \in A$ with $a^p \neq 1$. Then the following holds:

(i) $A_p = 1$ and $A = A^p, B_p = 1$ and $B = B^p$.
(ii) For each $a \in A^\#$ and $b \in B^\#$ we have:

$$a^{1/p} = \chi(\chi(a)^p),\ b^{1/p} = \chi(\chi(b)^p).$$

Proof. If $p = 2$ (3.3) is (3.1). Proceeding by induction assume that p is the smallest prime for which (3.3) is false. Then it holds for all primes $q < p$. In particular, we obtain:

(1) If $q < p$ is a prime, then $q \nmid o(a)$ for all $a \in A$.

Indeed if $q \mid o(a)$ for some $a \in A$ then some power of a has order q. But then $A = A_q$, since we assume (3.3) holds for q. This contradicts the assumption we made for the rest of section 3.

From (1) we obtain

(2) If $n \leq p - 1$ then the following hold:
  (i) $A_n = 1$ and $A = A^n$.
  (ii) $a^{1/n} = \chi(\chi(a)^n), b^{1/n} = \chi(\chi(b)^n)$ for all $a \in A^\#$ and $b \in B^\#$.

Indeed (2) holds for each prime $q \mid n$. Hence immediately $A = A^n$ and $A_n = 1$. To prove (ii) let $n = q \cdot r, (q, r) = 1$ and $q > 1, r > 1$ and, proceeding by induction, we may assume that (ii) holds for q and r. Pick $a \in A^\#$ and let $a_1 = a^{1/r}, a_2 = a_1^{1/q}$. Then

$$a_2^n = a_2^{qr} = a_1^r = a.$$

Further, by induction assumption:

$$a_1 = \chi(\chi(a)^r) \text{ and } a_2 = a_1^{1/q} = \chi(\chi(a_1)^q).$$

This implies

$$\begin{aligned} a^{1/n} &= a_1^{1/q} = \chi(\chi(a_1)^q) = \chi(\chi(a^{1/r})^q) \\ &= \chi((\chi(a)^r)^q) = \chi(\chi(a)^{rq}) = \chi(\chi(a)^n) \end{aligned}$$

since $\chi^2 = \mathrm{id}$.

We now lead the existence of p to a contradiction. Let $a \in A$ with $a^p \neq 1$. Then by (2)(ii) $a^{p-1} \neq 1$ and $a^{1/p-1} = \chi(\chi(a)^{p-1})$. Now we argue as in the proof of (3.2). Let $\overline{a} = \chi(\chi(a)^p)$. (Since a and $\chi(a)^{-1}$ are conjugate, also $\chi(a)^p \neq 1$!) Then we have for $b = \chi(a)$:

$$\begin{aligned} B^{\overline{a}} &= A^{b^p} = A^{b^{p-1}b} = B^{a^{1/p-1}b} = B^{(a^{1/p-1})^b} \\ &= B^{(b^{-1/p-1})^a} = B^{a^{-1}b^{-1/p-1}a} = A^{b^{-1}b^{-1/p-1}a} \\ &= A^{(b^{-1})^{p/p-1}a} = A^{(b^{-p})^{1/p-1}a} \end{aligned}$$

Hence $B^{\overline{a}a^{-1}} = A^{(b^{-p})^{1/p-1}}$. Now arguing as in (3.2) $\overline{a} = \chi(b^p)$ implies by (2.4)

$$\overline{a}^{-1} = \chi(b^p)^{-1} = \chi(b^{-p})$$

and so, since $\chi^2 = \mathrm{id}$

$$\chi(\overline{a}^{-1}) = b^{-p}.$$

Now by (2) (ii) applied to $\chi(\overline{a}^{-1})$ we obtain:

$$(b^{-p})^{1/p-1} = \chi(\overline{a}^{-1})^{1/p-1} = \chi((\overline{a}^{-1})^{p-1}).$$

Substituting this in the above equation we get

$$B^{\overline{a}a^{-1}} = A^{\chi((\overline{a}^{-1})^{p-1})} = B^{(\overline{a}^{-1})^{p-1}}.$$

Hence $B^{\overline{a}^p a^{-1}} = B$ and $\overline{a}^p = a$ by (2.4). This shows that we have:

$$(*) \qquad \chi(\chi(a)^p)^p = a \text{ for all } a \in A^{\#} \text{ with } a^p \neq 1.$$

Next we show, as in the proof of (3.1), that if $p \mid o(a)$ for some $a \in A^{\#}$, then $o(a) = p$. Namely if $o(a) \neq p$ then $(*)$ holds for a. But since a and $\chi(a)^{-1}$ are conjugate we have $o(a) = o(\chi(a))$ and thus by the same argument

$$o(\chi(\chi(a)^p) = o(\chi(a)^p) = \frac{o(a)}{p},$$

which obviously contradicts $(*)$. This shows that each $a \in A^\#$ with $o(a) \neq p$ satisfies $(o(a), p) = 1$ and thus is a p-power. Hence $A = A_p \cup A^p$ and so as in (3.1) $A = A^p$. If now $\widetilde{a} \in A$ has order p, then because of $A = A^p$ we know that $\widetilde{a}$ is a p-th power. But this is impossible since each element whose order is divisible by p has order p. Thus $A_p = 1$ and (3.3)(i) holds. But then $a^{1/p}$ exists for each $a \in A^\#$ and $(*)$ implies $a^{1/p} = \chi(\chi(a)^p)$ which proves (3.3). Q.E.D.

Now (3.3) implies that $A_p = 1$ and $A = A^p$ for each prime p. Namely if $A_p \neq 1$, then $A = A_p$ by (3.3) contradicting our assumption. This shows that A is torsionfree and divisible by each prime p, whence it is divisible. Now it follows from (3.3)(ii) with the same argument as in the proof of (2)(ii) that

$$a^{1/n} = \chi(\chi(a)^n) \text{ for each } a \in A^\# \text{ and } n \in \mathbb{N}.$$

Hence Theorem 1 holds. Q.E.D.

§4. Proof of theorem 2.

Pick $a \in A^\#$ and set $b = \chi(a)$. If A is an elementary abelian p-group, set

$$A_0 = \{a^m \mid m \leq p\} \text{ and } B_0 = \{b^m \mid m \leq p\}$$

while in case A is torsionfree and divisible set $A_0 = \{a^{m/n} \mid m, n \in \mathbb{Z}, n \neq 0\}$ with the convention $a^0 = 1$ and similarly B_0. We treat both cases (a) and (b) of theorem 2 together, with the convention that, if A is an elementary abelian p-group, all exponents m, n, ℓ, k occurring in the proof are elements of $\mathbb{Z}_p$. Then by definition of $(\overline{a})^{1/n}, \overline{a} \in A^\#$ we have

$$(a^m)^{1/n} = a^{m/n} = (a^{1/n})^m, \; n \neq 0.$$

Hence

$$(a^{\ell/m} \cdot a^{k/n})^{mn} = a^{\ell n} \cdot a^{km} = a^{\ell n + kn}$$

for $m \neq 0 \neq n$ and thus:

$$a^{\ell/m} \cdot a^{k/n} = (a^{\ell n + kn})^{1/mn} = a^{\frac{\ell n + kn}{mn}} = a^{\ell/m + k/n}.$$

This implies that the map $\sigma : \ell/m \to a^{\ell/m}$ is an isomorphism of $(\mathbb{Q}, +)$ (resp. $(\mathbb{Z}_p, +)$) onto A_0. We next show that:

$$(*) \qquad \chi(a^{m/n}) = b^{n/m} \text{ for all } n \neq 0 \neq m.$$

Now to prove $(*)$ it suffices to show that:

$$(+) \qquad \begin{matrix} \chi(\bar{a}^m) = \chi(\bar{a})^{1/m} \\ \chi(\bar{a}^{1/m}) = \chi(\bar{a})^m \end{matrix} \quad \text{for all } \bar{a} \in A^\# \text{ and } m \neq 0.$$

Indeed if these equations hold, then

$$\begin{aligned} \chi(a^{m/n}) &= \chi((a^{1/n})^m) = \chi(a^{1/n})^{1/m} = (\chi(a)^n)^{1/m} \\ &= \chi(a)^{n/m} = b^{n/m}. \end{aligned}$$

Now, as $\chi^2 = \mathrm{id}$, the second equation in $(+)$ is a consequence of part (b) of theorem 1. Let $\bar{b} = \chi(\bar{a})$. Then also by theorem 1

$$\chi(\bar{a})^{1/m} = \bar{b}^{1/m} = \chi(\chi(\bar{b})^m) = \chi(\bar{a}^m).$$

Hence $(*)$ holds, which shows that χ induces a bijection of $A_0^\#$ onto $B_0^\#$ (and also $B_0^\#$ onto $A_0^\#$). Now for $\lambda = m/n, n \neq 0$ set $a(\lambda) = a^{m/n}$ and $b(\lambda) = b^{m/n}$. Then the group $X_0 = \langle A_0, B_0 \rangle$ is generated by elements $a(\lambda), b(\lambda)$ where $\lambda \in \mathbb{Q}$ (resp. $\lambda \in \mathbb{Z}_p$). Further, since σ is an isomorphism, the relations (A) of (2.3) are satisfied. Hence to prove theorem 2, it suffices to show that also the relations (B') are satisfied. (We may assume $p > 3$, since otherwise $A_0^\# = \{a, a^{-1}\}$, $B_0^\# = \{b, b^{-1}\}$, whence $\{A_0\} \cup B_0^{A_0}$ is X_0-invariant.)

Now $(*)$ can be expressed as:

$$(**) \qquad \chi(a(\lambda)) = b(\lambda^{-1}),\ \lambda \in \mathbb{Q}^* \text{ resp. } \mathbb{Z}_p^*.$$

Hence we have

$$a(\lambda)^{b(\lambda^{-1})} = a(\lambda)^{\chi(a(\lambda))} = b(\lambda^{-1})^{-a(\lambda)} \text{ for all } \lambda \neq 0.$$

Now let $\lambda = n/m$ and $\mu = r/s$ with $n \neq 0 \neq m$ and $r \neq 0 \neq s$. Then $a(\lambda) = a(\mu)^{sn/rm}$. Hence we obtain:

$$\begin{aligned} a(\lambda)^{b(\mu^{-1})} &= (a(\mu)^{sn/rm})^{b(\mu^{-1})} = (b(\mu^{-1})^{-a(\mu)})^{sn/rm} \\ &= (b(-\mu^{-1})^{sn/rm})^{a(\mu)} = ((b^{-1})^{s^2n/r^2m})^{a(\mu)} \\ &= b(-\frac{\lambda}{\mu^2})^{a(\mu)}, \end{aligned}$$

Since as shown in the proof of (3.2) we have for all $\bar{a} \in A^\#$:

$$(\bar{a}^{m/n})^{b(\bar{a})} = (\bar{a}^{b(\bar{a})})^{m/n},\ m \neq 0 \neq n.$$

This shows that the relations (B') are also satisfied which proves theorem 2. Q.E.D.

References

[St] R. Steinberg: Lectures on Chevalley Groups.

[Ti1] F. G. Timmesfeld: Abstract Root Subgroups and Quadratic Action. Advances in Math., **142** (1999), 1–150.

[Ti2] F. G. Timmesfeld: Structure and Presentations of Lie-type Groups. Proc. London Math. Soc., (3) (2000), 428–484.

[Ti3] F. G. Timmesfeld: Moufang planes and the groups E_6^K and $SL_2(K)$, K a Cayley division algebra. Forum Math., **6** (1994), 209–231.

Mathematisches Institut
Arndtstrasse 2
35392 Giessen
Germany