S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 16, стр. 1069–1078 (2019) УДК 512.542.6
DOI 10.33048/semi.2019.16.074 MSC 20E99, 20G40

ON THE MAXIMAL TORI IN FINITE LINEAR AND UNITARY GROUPS

ANDREI V. ZAVARNITSINE

Abstract. To follow up on the results of [1], we propose a computationally efficient explicit cyclic decomposition of the maximal tori in the groups $\mathrm{SL}_n(q)$ and $\mathrm{SU}_n(q)$ and their projective images. We also derive some corollaries to simplify practical calculation of the maximal tori. The result is based on a generic cyclic decomposition of a finite abelian group which might also be of interest.

Keywords: maximal torus, cyclic decomposition.

1. Introduction

The maximal tori in finite groups of Lie type have been extensively studied. For $\mathrm{SL}_n(q)$ and $\mathrm{SU}_n(q)$ as well as their projective versions $\mathrm{PSL}_n(q)$ and $\mathrm{PSU}_n(q)$, the structure of maximal tori is clarified in [1]. The conjugacy classes of maximal tori in these groups are parameterized by unordered partitions of n. Given such a partition $n = n_1 + \ldots + n_s$, one can use the canonical formulas in [1, Theorems 2.1, 2.2] to find the orders of cyclic factors of the tori. However, these formulas have combinatorial computational growth as the number s of partition components increases, see Theorem 6 below. We propose another (noncanonical, in general) explicit cyclic decomposition for these tori which might be useful in practical computations, see Theorem 1. It is based on a generic cyclic decomposition of a finite abelian group stated in Proposition 5 which can also be used for finding efficiently the invariant divisors of the group.

In order to formulate the main result, we introduce some notation. For a nonzero integer n, we denote by $\mathbb{Z}_n$ a cyclic group of order $|n|$. Let q be a prime power.

Zavarnitsine, A.V., On the maximal tori in finite linear and unitary groups.

This research was supported by the Program of Fundamental Scientific Research of the SB RAS № I.1.1., project № 0314-2016-0001.

Received February, 27, 2019, published August, 7, 2019.

Denote $(\mathrm{P})\mathrm{SL}_n(-q) = (\mathrm{P})\mathrm{SU}_n(q)$ and let $\varepsilon = \pm 1$. Throughout, the ligature $\mathfrak{q}$ stands for the product εq. The gcd and lcm of nonzero integers $n_1, \dots, n_s$ are assumed to be positive and denoted by $(n_1, \dots, n_s)$ and $[n_1, \dots, n_s]$, respectively.

Theorem 1. *Let T be a maximal torus of $\mathrm{SL}_n(\mathfrak{q})$ parameterized by the partition $n = n_1 + \ldots + n_s$. Denote*

$$\begin{aligned} a_1 &= \mathfrak{q}^{(n_1,\dots,n_s)} - 1, \\ a_2 &= [\mathfrak{q}^{n_1} - 1, \mathfrak{q}^{(n_2,\dots,n_s)} - 1], \\ a_3 &= [\mathfrak{q}^{n_2} - 1, \mathfrak{q}^{(n_3,\dots,n_s)} - 1], \\ &\vdots \\ a_{s-1} &= [\mathfrak{q}^{n_{s-2}} - 1, \mathfrak{q}^{(n_{s-1},n_s)} - 1], \\ a_s &= [\mathfrak{q}^{n_{s-1}} - 1, \mathfrak{q}^{n_s} - 1]. \end{aligned} \tag{1}$$

Then

$$T \cong \mathbb{Z}_{a_1'} \times \mathbb{Z}_{a_2} \times \ldots \times \mathbb{Z}_{a_s}, \tag{2}$$

where $a_1' = a_1/(\mathfrak{q} - 1)$.

Let $\overline{T}$ be the image of T in $\mathrm{PSL}_n(\mathfrak{q})$. Set

$$d = (n, \mathfrak{q} - 1), \qquad d' = (n/(n_1, \dots, n_s), \mathfrak{q} - 1)\,.$$

For any relabeling of $a_2, \dots, a_s$, we have

$$\overline{T} \cong \mathbb{Z}_{b_1'} \times \mathbb{Z}_{b_2'} \times \mathbb{Z}_{b_3} \ldots \times \mathbb{Z}_{b_s}, \tag{3}$$

where $b_1' = d' a_1/d(\mathfrak{q} - 1)$, $b_2' = b_2/d'$, and

$$\begin{aligned} b_2 &= (a_2, \dots, a_s), \\ b_3 &= [a_2, (a_3, \dots, a_s)], \\ &\vdots \\ b_{s-1} &= [a_{s-2}, (a_{s-1}, a_s)], \\ b_s &= [a_{s-1}, a_s]. \end{aligned} \tag{4}$$

Theorem 1 allows us to give a simplified cyclic decomposition of the maximal tori of $\mathrm{SL}_n(\mathfrak{q})$ in many particular partition cases. For example, the following rather general fact holds.

Corollary 2. *Let T be a maximal torus of $\mathrm{SL}_n(\mathfrak{q})$ parameterized by the partition $n = n_1 + \ldots + n_s$. Denote $t = (n_1, \dots, n_s)$ and let $n_i = tn_i'$ for $i = 1, \dots, s$. If $(n_i', n_j') = 1$ for $i \neq j$ then we have*

$$T \cong \mathbb{Z}_{(\mathfrak{q}^t - 1)/(\mathfrak{q} - 1)} \times \mathbb{Z}_{(\mathfrak{q}^{n_i} - 1)(\mathfrak{q}^{n_j} - 1)/(\mathfrak{q}^t - 1)} \times \prod_{\substack{k=1,\dots,s \\ k \neq i,j}} \mathbb{Z}_{\mathfrak{q}^{n_k} - 1}. \tag{5}$$

In particular,

- *if $n_i' = 1$ for some i then*

$$T \cong \mathbb{Z}_{(\mathfrak{q}^t - 1)/(\mathfrak{q} - 1)} \times \prod_{\substack{k=1,\dots,s \\ k \neq i}} \mathbb{Z}_{\mathfrak{q}^{n_k} - 1}; \tag{6}$$

- *if* $(n_i, n_j) = 1$ *for* $i \neq j$ *then*

$$T \cong \mathbb{Z}_{(q^{n_i}-1)(q^{n_j}-1)/(q-1)} \times \prod_{\substack{k=1,\dots,s \\ k\neq i,j}} \mathbb{Z}_{q^{n_k}-1};$$

- *if* $n_1 = \ldots = n_s \ \ (= t)$ *then*

$$T \cong \mathbb{Z}_{(q^t-1)/(q-1)} \times \mathbb{Z}_{q^t-1}^{s-1}. \tag{7}$$

Decomposition (7) can also be readily deduced from [1], see Theorem 6 below.

Example 1. Let the decomposition be $n = 1+2+3+4+5+6$. Applying directly the result of [1] gives the following structure of the corresponding torus of $\mathrm{SL}_{21}(q)$:

$$T \cong \mathbb{Z}_{q-1}^2 \times \mathbb{Z}_{q^2-1} \times \mathbb{Z}_{(q^3-1)(q+1)} \times \mathbb{Z}_{(q^6-1)(q^4+q^3+q^2+q+1)(q^2+1)},$$

whereas (6) yields

$$T \cong \mathbb{Z}_{q^2-1} \times \mathbb{Z}_{q^3-1} \times \mathbb{Z}_{q^4-1} \times \mathbb{Z}_{q^5-1} \times \mathbb{Z}_{q^6-1}.$$

Example 2. Let $\varepsilon = -1$ and let $n = 3+6+6+9$. Then $t = 3$ and (6) implies that the corresponding torus of $\mathrm{SU}_{24}(q)$ has the structure

$$T \cong \mathbb{Z}_{q^2-q+1} \times \mathbb{Z}_{q^6-1} \times \mathbb{Z}_{q^6-1} \times \mathbb{Z}_{q^9+1}.$$

Expression (5) alone allows us to explicitly write down by hand decompositions of all maximal tori of $\mathrm{SL}_n(q)$ for $n \leqslant 30$. For example, the tori of $\mathrm{SL}_{10}(q)$ are listed in Table 1. The following case, however, is not covered by (5).

Example 3. Let $n = 6+10+15$. Then, depending on the ordering of n_1, n_2, n_3, the corresponding torus of $\mathrm{SL}_{31}(q)$ can be decomposed by Theorem 1 in three ways

$$\begin{aligned} T &\cong \mathbb{Z}_{(q^{15}-1)(q+1)} \times \mathbb{Z}_{(q^{10}-1)(q^4+q^2+1)} \\ &\cong \mathbb{Z}_{(q^{10}-1)(q^2+q+1)} \times \mathbb{Z}_{(q^{15}-1)(q^3+1)} \\ &\cong \mathbb{Z}_{(q^6-1)(q^4+q^3+q^2+q+1)} \times \mathbb{Z}_{(q^{15}-1)(q^5+1)}, \end{aligned}$$

whereas [1] gives a fourth decomposition

$$T \cong \mathbb{Z}_{(q^{15}-1)(q^5+1)(q^2-q+1)} \times \mathbb{Z}_{(q^5-1)(q^2+q+1)(q+1)}.$$

Nevertheless, we can generalize (5) to include this case as follows.

Corollary 3. *In the notation of Corollary 2, if* $(n_i', n_j', n_k') = 1$ *for pairwise distinct* i, j, k *then*

$$T \cong \mathbb{Z}_{(q^t-1)/(q-1)} \times \mathbb{Z}_{[q^{n_i}-1, q^{(n_j,n_k)}-1]} \times \mathbb{Z}_{[q^{n_j}-1, q^{n_k}-1]} \times \prod_{\substack{l=1,\dots,s \\ l\neq i,j,k}} \mathbb{Z}_{q^{n_l}-1}.$$

A similar generalization can be inferred from Theorem 1 for arbitrarily many coprime numbers n_i'.

The projective case is somewhat more complicated. The following particular partitions of n yield a simplified decomposition of $\overline{T}$.

Corollary 4. *Let* $\overline{T}$ *be the image in* $\mathrm{PSL}_n(q)$ *of a maximal torus of* $\mathrm{SL}_n(q)$ *parameterized by the partition* $n = n_1 + \ldots + n_s$. *Denote* $t = (n_1, \ldots, n_s)$, $d = (n, q-1)$, *and* $d' = (n/t, q-1)$.
(*i*) *If* $s = 1$ *then* $\overline{T} \cong \mathbb{Z}_{(q^n-1)/d(q-1)}$.

(*ii*) *If* $s = 2$ *then*

$$\overline{T} \cong \mathbb{Z}_{d'(q^t-1)/d(q-1)} \times \mathbb{Z}_{(q^{n_1}-1)(q^{n_2}-1)/d'(q^t-1)}. \tag{8}$$

(*iii*) *If* $n_i = n_j = 1$ *for* $i \neq j$ *then*

$$\overline{T} \cong \mathbb{Z}_{(q-1)/d} \times \prod_{\substack{r=1,\dots,s \\ r\neq i,j}} \mathbb{Z}_{q^{n_r}-1};$$

(*iv*) *If* $n_i = 1$ *and* $(n_j, n_k) = 1$ *for pairwise distinct* i, j, k, *then*

$$\overline{T} \cong \mathbb{Z}_{(q-1)/d} \times \mathbb{Z}_{(q^{n_j}-1)(q^{n_k}-1)/(q-1)} \times \prod_{\substack{r=1,\dots,s \\ r\neq i,j,k}} \mathbb{Z}_{q^{n_r}-1}.$$

(*v*) *If* $(n_i, n_j) = 1$ *and* $(n_k, n_l) = 1$ *for pairwise distinct* i, j, k, l, *then*

$$\overline{T} \cong \mathbb{Z}_{(q-1)/d} \times \mathbb{Z}_{(q^{n_i}-1)(q^{n_j}-1)/(q-1)} \times \mathbb{Z}_{(q^{n_k}-1)(q^{n_l}-1)/(q-1)} \times \prod_{\substack{r=1,\dots,s \\ r\neq i,j,k,l}} \mathbb{Z}_{q^{n_r}-1}.$$

(*vi*) *Assume that* $n_i = t$ *for some* i. *Set* $r = \mathsf{gcd}\{n_l \mid l \neq i\}$.

(*vi*.1) *If* $n_j = r$ *for* $j \neq i$ *then*

$$\overline{T} \cong \mathbb{Z}_{d'(q^t-1)/d(q-1)} \times \mathbb{Z}_{(q^r-1)/d'} \times \prod_{\substack{l=1,\dots,s \\ l\neq i,j}} \mathbb{Z}_{q^{n_l}-1}.$$

In particular, if $n_1 = \ldots = n_s \ \ (= t)$ *then*

$$\overline{T} \cong \mathbb{Z}_{d'(q^t-1)/d(q-1)} \times \mathbb{Z}_{(q^t-1)/d'} \times \mathbb{Z}_{q^t-1}^{s-2}. \tag{9}$$

(*vi*.2) *If* $(n_j, n_k) = r$ *for pairwise distinct* i, j, k *then*

$$\overline{T} \cong \mathbb{Z}_{d'(q^t-1)/d(q-1)} \times \mathbb{Z}_{(q^r-1)/d'} \times \mathbb{Z}_{(q^{n_j}-1)(q^{n_k}-1)/(q^r-1)} \times \prod_{\substack{l=1,\dots,s \\ l\neq i,j,k}} \mathbb{Z}_{q^{n_l}-1}. \tag{10}$$

Observe that decompositions (8) and (9) can also be readily deduced from [1].

Example 4. Let $n = 3 + 6 + 9 + 12$. Then $t = 3$ and $r = 3$. We may set $n_j = 6$, $n_k = 9$. By (10), the image of T in $\mathrm{PSL}_{30}(q)$ is

$$\overline{T} \cong \mathbb{Z}_{(q^2+q+1)/d_3} \times \mathbb{Z}_{(q^3-1)/d_{10}} \times \mathbb{Z}_{(q^9-1)(q^3+1)} \times \mathbb{Z}_{q^{12}-1},$$

where $d_3 = (3, q-1)$ and $d_{10} = (10, q-1)$.

In Table 1, we give decompositions for all images $\overline{T}$ in $\mathrm{PSL}_{10}(q)$. Most of them are consequences of Corollary 4.

2. A cyclic decomposition of finite abelian groups

Let $m_1, \dots, m_s \in \mathbb{N}$. The direct product of cyclic groups

$$A = \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_s}$$

has a cyclic direct factor of order $d_1 = (m_1, \dots, m_s)$. In other words, $A \cong \mathbb{Z}_{d_1} \times A'$ for an abelian group A'. We are interested in an explicit cyclic decomposition of A'. By "explicit" we mean a decomposition in which the orders of cyclic factors are expressed by finite formulas in the original parameters $m_1, \dots, m_s$. One such decomposition can be obtained canonically. We have

$$A = \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_s}, \tag{11}$$

where $d_k = \delta_k/\delta_{k-1}$, $k = 1, \ldots, s$, and

$$\delta_k = \mathsf{gcd}\{m_{i_1} \cdot \ldots \cdot m_{i_k} \mid 1 \leqslant i_1 < \ldots < i_k \leqslant s\}, \tag{12}$$

$k = 0, \ldots, s$, is the *k-th determinant divisor* of the matrix $\mathrm{diag}(m_1, \ldots, m_s)$, i. e. the gcd of all its $k \times k$ minors. Clearly, (11) provides a decomposition for A':

$$A' = \mathbb{Z}_{d_2} \times \ldots \times \mathbb{Z}_{d_s}.$$

There are two alternative descriptions of the invariants $d_1, \ldots, d_s$. The first one uses prime factorization. Given[1] a prime p, let $p^{\mu_{p,i}} \parallel m_i$ for suitable $\mu_{p,i} \geqslant 0$, $i = 1, \ldots, s$. Also, let $\nu_{p,1} \leqslant \ldots \leqslant \nu_{p,s}$ be such that

$$\{\!\{ \nu_{p,1}, \ldots, \nu_{p,s} \}\!\} = \{\!\{ \mu_{p,1}, \ldots, \mu_{p,s} \}\!\}$$

is the equality of multisets (i. e. sets with repetitions). Then

$$\delta_k = \prod_p p^{\nu_{p,1}+\ldots+\nu_{p,k}}, \qquad d_k = \prod_p p^{\nu_{p,k}}, \tag{13}$$

$k = 1, \ldots, s$, the products being taken over all primes. This readily follows from (12) and the fact that

$$\mathsf{min}\{\mu_{p,i_1} + \ldots + \mu_{p,i_k} \mid 1 \leqslant i_1 < \ldots < i_k \leqslant s\} = \nu_{p,1} + \ldots + \nu_{p,k}$$

for every p. The second description is that

$$d_k = \mathsf{lcm}\{(m_{i_1}, \ldots, m_{i_{s-k+1}}) \mid 1 \leqslant i_1 < \ldots < i_{s-k+1} \leqslant s\}, \tag{14}$$

$k = 1, \ldots, s$, which follows from (13) and the fact that

$$\mathsf{max}\{\mathsf{min}\{\mu_{p,i_1}, \ldots, \mu_{p,i_{s-k+1}}\} \mid 1 \leqslant i_1 < \ldots < i_{s-k+1} \leqslant s\} = \nu_{p,k}.$$

for every p.

The explicit formulas (12) and (14) are not computationally efficient for calculating the canonical decomposition (11), because the number of their arguments grows combinatorially. Neither are relations (13) due to their dependence on prime factorization. Although there are efficient algorithms for determining the invariant divisors $d_1, \ldots, d_s$ (see, e. g., [2]), they cannot be readily used to obtain generic expressions for the d_i's in terms of the original parameters $m_1, \ldots, m_s$.

An alternative explicit (noncanonical, in general) cyclic decomposition for A' provided by the following proposition will be used in the proof of Theorem 1 and can also be used iteratively to determine the invariants $d_1, \ldots, d_s$ of A as we will explain below.

Proposition 5. *For $m_1, \ldots, m_s \in \mathbb{N}$, we have*

$$\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_s} \cong \mathbb{Z}_{a_1} \times \ldots \times \mathbb{Z}_{a_s}, \tag{15}$$

[1]The notation $p^\mu \parallel m$ stands for the fact that p^μ *exactly divides* m, i. e. $p^\mu \mid m$ and $p^{\mu+1} \nmid m$.

where

$$\begin{aligned} a_1 &= (m_1, \ldots, m_s),\\ a_2 &= [m_1, (m_2, \ldots, m_s)],\\ a_3 &= [m_2, (m_3, \ldots, m_s)],\\ &\vdots\\ a_{s-1} &= [m_{s-2}, (m_{s-1}, m_s)],\\ a_s &= [m_{s-1}, m_s]. \end{aligned} \tag{16}$$

Proof. We give two proofs. First, induct on s. The claim holds for $s = 1$. Assuming the validity for a given s, we have by induction

$$\mathbb{Z}_{m_0} \times \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_s} \cong \mathbb{Z}_{m_0} \times \mathbb{Z}_{a_1} \times \ldots \times \mathbb{Z}_{a_s},$$

where $a_1, \ldots, a_s$ are as in (16). It remains to note that

$$\mathbb{Z}_{m_0} \times \mathbb{Z}_{a_1} \cong \mathbb{Z}_{(m_0, m_1, \ldots, m_s)} \times \mathbb{Z}_{[m_0, (m_1, \ldots, m_s)]},$$

because $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{(m,n)} \times \mathbb{Z}_{[m,n]}$ for arbitrary $m, n \in \mathbb{N}$, see [1, Lemma 1.6].

The second proof is independent, albeit more technical. Fix a prime p. Let $p^{\mu_i} \parallel m_i$ and let $p^{\alpha_i} \parallel a_i$, $i = 1, \ldots, s$. Set $\mu_0 = 0$. By (16), we have

$$\alpha_i = \mathsf{max}\{\mu_{i-1}, \mathsf{min}\{\mu_i, \ldots, \mu_s\}\} \tag{17}$$

for $i = 1, \ldots, s$. It suffices to show that the equality of multisets $\{\{\mu_1, \ldots, \mu_s\}\} = \{\{\alpha_1, \ldots, \alpha_s\}\}$ holds. Define $i_0, i_1, \ldots$ by the rule $i_0 = 0$ and i_k is such that

$$\mu_{i_k} = \mathsf{min}\{\mu_{i_{k-1}+1}, \mu_{i_{k-1}+2}, \ldots, \mu_s\} \tag{18}$$

for $k = 1, \ldots, l$, where l is the smallest index with $\mu_{i_l} = \mu_s$. An explicit bijection between $\mu_1, \ldots, \mu_s$ and $\alpha_1, \ldots, \alpha_s$ is then given as follows. For every $k = 0, \ldots, l-1$, we have by (17) and (18)

$$\alpha_{i_k+1} = \mathsf{max}\{\mu_{i_k}, \mathsf{min}\{\mu_{i_k+1}, \ldots, \mu_s\}\} = \mathsf{max}\{\mu_{i_k}, \mu_{i_{k+1}}\} = \mu_{i_{k+1}}$$

and

$$\alpha_i = \mathsf{max}\{\mu_{i-1}, \mathsf{min}\{\mu_i, \ldots, \mu_s\}\} = \mathsf{max}\{\mu_{i-1}, \mu_{i_{k+1}}\} = \mu_{i-1},$$

where $i_k + 2 \leqslant i \leqslant i_{k+1}$. The claim follows. □

We emphasize that the decomposition on the right-hand side of (15) may essentially depend on the ordering of $m_1, \ldots, m_s$.

A repeated application of Proposition 5 can efficiently yield the canonical decomposition (11) for $A = \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_s}$ as follows. On first run, A is decomposed by (15) as the direct product of $\mathbb{Z}_{a_1}$ and $\mathbb{Z}_{a_2} \times \ldots \times \mathbb{Z}_{a_s}$, so we obtain the first invariant $d_1 = a_1$. On second run, we similarly decompose the factor $\mathbb{Z}_{a_2} \times \ldots \times \mathbb{Z}_{a_s}$ whose first invariant equals $(a_2, \ldots, a_s) = d_2$, so we obtain the second invariant of A. Continuing in this manner, we determine all d_i's. This can be performed in polynomial time due to the recursive form of equations (16) which justifies the efficiency of this algorithm.

3. Auxiliary facts

We state explicitly the necessary facts from [1] slightly modifying the original notation.

Theorem 6 ([1, Theorems 2.1, 2.2])**.** *Let $n \geqslant 2$ and let T be a maximal torus of $\mathrm{SL}_n(\mathfrak{q})$ parameterized by the partition $n = n_1 + \ldots + n_s$. For $k = 1, \ldots, s$, denote*

$$d_k = \mathsf{lcm}\{(\mathfrak{q}^{n_{i_1}} - 1, \ldots, \mathfrak{q}^{n_{i_{s-k+1}}} - 1) \mid 1 \leqslant i_1 < \ldots < i_{s-k+1} \leqslant s\}. \tag{19}$$

Then d_k divides $d_{k'}$ for $k \leqslant k'$ and

$$T \cong \mathbb{Z}_{d_1'} \times \mathbb{Z}_{d_2} \times \ldots \times \mathbb{Z}_{d_s},$$

where $d_1' = d_1/(\mathfrak{q} - 1)$. Let $\overline{T}$ be the image of T in $\mathrm{PSL}_n(\mathfrak{q})$. Denote

$$d = (n, \mathfrak{q} - 1), \qquad d' = (n/(n_1, \ldots, n_s), \mathfrak{q} - 1)\,.$$

If $s = 1$ then $\overline{T} \cong \mathbb{Z}_{d_1'}$, where $d_1' = d_1/d(\mathfrak{q} - 1)$. If $s > 1$ then

$$\overline{T} \cong \mathbb{Z}_{d_1'} \times \mathbb{Z}_{d_2'} \times \mathbb{Z}_{d_3} \times \ldots \times \mathbb{Z}_{d_s},$$

where $d_1' = d'd_1/d(\mathfrak{q} - 1)$ and $d_2' = d_2/d'$.

The following number-theoretic result will also be used.

Lemma 7. *Let $a, b, q \in \mathbb{N}$, let $\varepsilon = \pm 1$, and let $\mathfrak{q} = \varepsilon q$. Then up to sign we have*

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

Proof. We use [3, Lemma 6(iii)]. If either $\varepsilon = 1$ or both a, b even, we have

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

If $\varepsilon = -1$, a even, b odd, we have

$$(q^a - 1, q^b + 1) = q^{(a,b)} + 1.$$

If $\varepsilon = -1$, a odd, b even, we have

$$(q^a + 1, q^b - 1) = q^{(a,b)} + 1.$$

If $\varepsilon = -1$, a odd, b odd, we have

$$(q^a + 1, q^b + 1) = q^{(a,b)} + 1.$$

The claim follows. □

4. Proof of main results

We first prove Theorem 1.

Proof. We may assume $n \geqslant 2$. Denote $m_i = \mathfrak{q}^{n_i} - 1$, $i = 1, \ldots, s$, and $d_1 = (m_1, \ldots, m_s)$. Let

$$A = \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_s}.$$

and $A_1 = \mathbb{Z}_{d_1}$. By (11), we have $A \cong A_1 \times A'$, where

$$A' = \mathbb{Z}_{d_2} \times \ldots \times \mathbb{Z}_{d_s}$$

and the d_k's are given by equations (14) which are clearly the same as (19). In particular, Theorem 6 implies $T \cong A_1/A_1' \times A'$, where $A_1' \cong \mathbb{Z}_{\mathfrak{q}-1}$ is a cyclic subgroup of A_1. On the other hand, Proposition 5 yields

$$A' \cong \mathbb{Z}_{a_2} \times \ldots \times \mathbb{Z}_{a_s} \tag{20}$$

and the a_k's are given by (16). Lemma 7 implies that the a_k's are the same as defined in (1). Hence the required decomposition (2) holds.

We now consider the image $\overline{T}$ of T in $\mathrm{PSL}_n(q)$. We may assume $s > 1$. The argument is similar except that we now consider A' in place of A. We have

$$A \cong A_1 \times A_2 \times A'',$$

where $A_2 = \mathbb{Z}_{d_2}$. Theorem 6 implies $\overline{T} \cong A/(A_1'' \times A_2'')$, where $A_1'' \cong \mathbb{Z}_{d(q-1)/d'}$ and $A_2'' \cong \mathbb{Z}_{d'}$ are cyclic subgroups of A_1 and A_2, respectively. Since $A_2 \times A'' \cong A'$, decomposition (20) implies $d_2 = (a_2, \ldots, a_s)$. Moreover, Proposition 5 with $a_2, \ldots, a_s$ playing the role of $m_1, \ldots, m_s$ and ordered arbitrarily yields

$$A'' \cong \mathbb{Z}_{b_3} \times \ldots \times \mathbb{Z}_{b_s},$$

where the b_i's are the same as defined in (4). Therefore, we have the required decomposition (3) for $\overline{T}$. □

We now prove Corollary 2.

Proof. First, let us make no assumptions on the components n_i's. In the notation of Theorem 1, define

$$A_{n_1,\ldots,n_s}(q) = \mathbb{Z}_{a_2} \times \ldots \times \mathbb{Z}_{a_s}. \tag{21}$$

Then (2) implies

$$T \cong \mathbb{Z}_{a_1'} \times A_{n_1,\ldots,n_s}(q). \tag{22}$$

Setting $t = (n_1, \ldots, n_s)$ we can rewrite (22) as

$$T \cong \mathbb{Z}_{(q^t-1)/(q-1)} \times A_{n_1',\ldots,n_s'}(q^t), \tag{23}$$

where $n_i = tn_i'$ for $i = 1, \ldots, s$.

Now let $(n_i, n_j) = 1$ for distinct i, j. Since the ordering of n_i's is not fixed, we may assume that $\{i, j\} = \{s-1, s\}$ (although we could proceed without this assumption). Then (1) implies that $a_1 = q-1$, $a_2 = q^{n_1} - 1$, $\ldots$, $a_{s-1} = q^{n_{s-2}} - 1$, and $a_s = [q^{n_{s-1}} - 1, q^{n_s}] = (q^{n_i} - 1)(q^{n_j} - 1)/(q-1)$. Therefore, Theorem 1 and expression (21) imply

$$A_{n_1,\ldots,n_s}(q) \cong \mathbb{Z}_{(q^{n_i}-1)(q^{n_j}-1)/(q-1)} \times \prod_{\substack{k=1,\ldots,s \\ k \neq i,j}} \mathbb{Z}_{q^{n_k}-1}. \tag{24}$$

Finally, if $(n_i', n_j') = 1$ for distinct i, j then both (23) and (24) yield the required decomposition (5). □

Corollary 3 can be proved similarly. We also outline a proof of Corollary 4.

Proof. Items (i) and (ii) are straightforward. They also readily follow from Theorem 6. We show (v). The proof of (iii) and (iv) is similar and simpler. As above we may assume that $\{i, j\} = \{s-1, s\}$ to obtain $a_1 = q-1$, $a_2 = q^{n_1} - 1$, $\ldots$, $a_{s-1} = q^{n_{s-2}} - 1$, and $a_s = [q^{n_{s-1}} - 1, q^{n_s}] = (q^{n_i} - 1)(q^{n_j} - 1)/(q-1)$. Now, we may also assume $\{k, l\} = \{s-3, s-2\}$ and relabel the last three a_i's so that $a_{s-2} = (q^{n_i} - 1)(q^{n_j} - 1)/(q-1)$, $a_{s-1} = q^{n_{s-3}} - 1$, $a_s = q^{n_{s-2}} - 1$. This does not affect the validity of isomorphism (3), since we did not assume that the ordering of $a_2, \ldots, a_s$ is fixed when proving Theorem 1. Thus, (4) implies $b_2 = q-1$, $b_3 = a_2 = q^{n_1} - 1$, $\ldots$, $b_{s-2} = a_{s-3} = q^{n_{s-4}} - 1$, $b_{s-1} = a_{s-2} = (q^{n_i} - 1)(q^{n_j} - 1)/(q-1)$,

$b_s = [a_{s-1}, a_s] = [\mathfrak{q}^{n_{s-3}} - 1, \mathfrak{q}^{n_{s-2}} - 1] = (\mathfrak{q}^{n_k} - 1)(\mathfrak{q}^{n_l} - 1)/(\mathfrak{q} - 1)$. The claim now follows by (3) because $d = d'$ in this case.

We now prove $(vi.2)$. The proof of $(vi.1)$ is similar. We may assume that $i = s$. Then $a_1 = \mathfrak{q}^t - 1$, $a_l = \mathfrak{q}^{n_{l-1}} - 1$, $l = 2, \dots, s$. Also, assume that $\{j, k\} = \{s-2, s-1\}$. Then $b_2 = \mathfrak{q}^r - 1$, $b_3 = a_2$, $\dots$, $b_{s-1} = a_{s-2}$, $b_s = (\mathfrak{q}^{n_i} - 1)(\mathfrak{q}^{n_j} - 1)/(\mathfrak{q}^r - 1)$. The claim now follows by (3). □

TABLE 1. The maximal tori of $\mathrm{SL}_{10}(\mathfrak{q})$ and their images in $\mathrm{PSL}_{10}(\mathfrak{q})$. Notation: $\mathfrak{q} = \pm q$, $d_2 = (2, \mathfrak{q} - 1)$, $d_5 = (5, \mathfrak{q} - 1)$, $d = d_2 d_5 = (10, \mathfrak{q} - 1)$.

$[n_1, ..., n_s]$	$\mathrm{SL}_{10}(\mathfrak{q})$	$\mathrm{PSL}_{10}(\mathfrak{q})$
$[1^{10}]$	$\mathbb{Z}_{\mathfrak{q}-1}^9$	$\mathbb{Z}_{\mathfrak{q}-1}^8 \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[2, 1^8]$	$\mathbb{Z}_{\mathfrak{q}^2-1} \times \mathbb{Z}_{\mathfrak{q}-1}^7$	$\mathbb{Z}_{\mathfrak{q}^2-1} \times \mathbb{Z}_{\mathfrak{q}-1}^6 \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[2^2, 1^6]$	$\mathbb{Z}_{\mathfrak{q}^2-1}^2 \times \mathbb{Z}_{\mathfrak{q}-1}^5$	$\mathbb{Z}_{\mathfrak{q}^2-1}^2 \times \mathbb{Z}_{\mathfrak{q}-1}^4 \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[2^3, 1^4]$	$\mathbb{Z}_{\mathfrak{q}^2-1}^3 \times \mathbb{Z}_{\mathfrak{q}-1}^3$	$\mathbb{Z}_{\mathfrak{q}^2-1}^3 \times \mathbb{Z}_{\mathfrak{q}-1}^2 \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[2^4, 1^2]$	$\mathbb{Z}_{\mathfrak{q}^2-1}^4 \times \mathbb{Z}_{\mathfrak{q}-1}$	$\mathbb{Z}_{\mathfrak{q}^2-1}^4 \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[2^5]$	$\mathbb{Z}_{\mathfrak{q}^2-1}^4 \times \mathbb{Z}_{\mathfrak{q}+1}$	$\mathbb{Z}_{\mathfrak{q}^2-1}^3 \times \mathbb{Z}_{(\mathfrak{q}^2-1)/d_5} \times \mathbb{Z}_{(\mathfrak{q}+1)/d_2}$
$[3, 1^7]$	$\mathbb{Z}_{\mathfrak{q}^3-1} \times \mathbb{Z}_{\mathfrak{q}-1}^6$	$\mathbb{Z}_{\mathfrak{q}^3-1} \times \mathbb{Z}_{\mathfrak{q}-1}^5 \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[3, 2, 1^5]$	$\mathbb{Z}_{\mathfrak{q}^3-1} \times \mathbb{Z}_{\mathfrak{q}^2-1} \times \mathbb{Z}_{\mathfrak{q}-1}^4$	$\mathbb{Z}_{\mathfrak{q}^3-1} \times \mathbb{Z}_{\mathfrak{q}^2-1} \times \mathbb{Z}_{\mathfrak{q}-1}^3 \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[3, 2^2, 1^3]$	$\mathbb{Z}_{\mathfrak{q}^3-1} \times \mathbb{Z}_{\mathfrak{q}^2-1}^2 \times \mathbb{Z}_{\mathfrak{q}-1}^2$	$\mathbb{Z}_{\mathfrak{q}^3-1} \times \mathbb{Z}_{\mathfrak{q}^2-1}^2 \times \mathbb{Z}_{\mathfrak{q}-1} \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[3, 2^3, 1]$	$\mathbb{Z}_{\mathfrak{q}^3-1} \times \mathbb{Z}_{\mathfrak{q}^2-1}^3$	$\mathbb{Z}_{(\mathfrak{q}^3-1)(\mathfrak{q}+1)} \times \mathbb{Z}_{\mathfrak{q}^2-1}^2 \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[3^2, 1^4]$	$\mathbb{Z}_{\mathfrak{q}^3-1}^2 \times \mathbb{Z}_{\mathfrak{q}-1}^3$	$\mathbb{Z}_{\mathfrak{q}^3-1}^2 \times \mathbb{Z}_{\mathfrak{q}-1}^2 \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[3^2, 2, 1^2]$	$\mathbb{Z}_{\mathfrak{q}^3-1}^2 \times \mathbb{Z}_{\mathfrak{q}^2-1} \times \mathbb{Z}_{\mathfrak{q}-1}$	$\mathbb{Z}_{\mathfrak{q}^3-1}^2 \times \mathbb{Z}_{\mathfrak{q}^2-1} \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[3^2, 2^2]$	$\mathbb{Z}_{(\mathfrak{q}^3-1)(\mathfrak{q}+1)} \times \mathbb{Z}_{\mathfrak{q}^3-1} \times \mathbb{Z}_{\mathfrak{q}^2-1}$	$\mathbb{Z}_{(\mathfrak{q}^3-1)(\mathfrak{q}+1)}^2 \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[3^3, 1]$	$\mathbb{Z}_{\mathfrak{q}^3-1}^3$	$\mathbb{Z}_{\mathfrak{q}^3-1}^2 \times \mathbb{Z}_{(\mathfrak{q}^3-1)/d}$
$[4, 1^6]$	$\mathbb{Z}_{\mathfrak{q}^4-1} \times \mathbb{Z}_{\mathfrak{q}-1}^5$	$\mathbb{Z}_{\mathfrak{q}^4-1} \times \mathbb{Z}_{\mathfrak{q}-1}^4 \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[4, 2, 1^4]$	$\mathbb{Z}_{\mathfrak{q}^4-1} \times \mathbb{Z}_{\mathfrak{q}^2-1} \times \mathbb{Z}_{\mathfrak{q}-1}^3$	$\mathbb{Z}_{\mathfrak{q}^4-1} \times \mathbb{Z}_{\mathfrak{q}^2-1} \times \mathbb{Z}_{\mathfrak{q}-1}^2 \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[4, 2^2, 1^2]$	$\mathbb{Z}_{\mathfrak{q}^4-1} \times \mathbb{Z}_{\mathfrak{q}^2-1}^2 \times \mathbb{Z}_{\mathfrak{q}-1}$	$\mathbb{Z}_{\mathfrak{q}^4-1} \times \mathbb{Z}_{\mathfrak{q}^2-1}^2 \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[4, 2^3]$	$\mathbb{Z}_{\mathfrak{q}^4-1} \times \mathbb{Z}_{\mathfrak{q}^2-1}^2 \times \mathbb{Z}_{\mathfrak{q}+1}$	$\mathbb{Z}_{\mathfrak{q}^4-1} \times \mathbb{Z}_{\mathfrak{q}^2-1} \times \mathbb{Z}_{(\mathfrak{q}^2-1)/d_5} \times \mathbb{Z}_{(\mathfrak{q}+1)/d_2}$
$[4, 3, 1^3]$	$\mathbb{Z}_{\mathfrak{q}^4-1} \times \mathbb{Z}_{\mathfrak{q}^3-1} \times \mathbb{Z}_{\mathfrak{q}-1}^2$	$\mathbb{Z}_{\mathfrak{q}^4-1} \times \mathbb{Z}_{\mathfrak{q}^3-1} \times \mathbb{Z}_{\mathfrak{q}-1} \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[4, 3, 2, 1]$	$\mathbb{Z}_{\mathfrak{q}^4-1} \times \mathbb{Z}_{\mathfrak{q}^3-1} \times \mathbb{Z}_{\mathfrak{q}^2-1}$	$\mathbb{Z}_{(\mathfrak{q}^3-1)(\mathfrak{q}+1)} \times \mathbb{Z}_{\mathfrak{q}^4-1} \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[4, 3^2]$	$\mathbb{Z}_{(\mathfrak{q}^4-1)(\mathfrak{q}^2+\mathfrak{q}+1)} \times \mathbb{Z}_{\mathfrak{q}^3-1}$	$\mathbb{Z}_{(\mathfrak{q}^4-1)(\mathfrak{q}^2+\mathfrak{q}+1)} \times \mathbb{Z}_{(\mathfrak{q}^3-1)/d}$
$[4^2, 1^2]$	$\mathbb{Z}_{\mathfrak{q}^4-1}^2 \times \mathbb{Z}_{\mathfrak{q}-1}$	$\mathbb{Z}_{\mathfrak{q}^4-1}^2 \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[4^2, 2]$	$\mathbb{Z}_{\mathfrak{q}^4-1}^2 \times \mathbb{Z}_{\mathfrak{q}+1}$	$\mathbb{Z}_{\mathfrak{q}^4-1} \times \mathbb{Z}_{(\mathfrak{q}^4-1)/d_5} \times \mathbb{Z}_{(\mathfrak{q}+1)/d_2}$
$[5, 1^5]$	$\mathbb{Z}_{\mathfrak{q}^5-1} \times \mathbb{Z}_{\mathfrak{q}-1}^4$	$\mathbb{Z}_{\mathfrak{q}^5-1} \times \mathbb{Z}_{\mathfrak{q}-1}^3 \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[5, 2, 1^3]$	$\mathbb{Z}_{\mathfrak{q}^5-1} \times \mathbb{Z}_{\mathfrak{q}^2-1} \times \mathbb{Z}_{\mathfrak{q}-1}^2$	$\mathbb{Z}_{\mathfrak{q}^5-1} \times \mathbb{Z}_{\mathfrak{q}^2-1} \times \mathbb{Z}_{\mathfrak{q}-1} \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[5, 2^2, 1]$	$\mathbb{Z}_{\mathfrak{q}^5-1} \times \mathbb{Z}_{\mathfrak{q}^2-1}^2$	$\mathbb{Z}_{(\mathfrak{q}^5-1)(\mathfrak{q}+1)} \times \mathbb{Z}_{\mathfrak{q}^2-1} \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[5, 3, 1^2]$	$\mathbb{Z}_{\mathfrak{q}^5-1} \times \mathbb{Z}_{\mathfrak{q}^3-1} \times \mathbb{Z}_{\mathfrak{q}-1}$	$\mathbb{Z}_{\mathfrak{q}^5-1} \times \mathbb{Z}_{\mathfrak{q}^3-1} \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[5, 3, 2]$	$\mathbb{Z}_{\mathfrak{q}^5-1} \times \mathbb{Z}_{(\mathfrak{q}+1)(\mathfrak{q}^3-1)}$	$\mathbb{Z}_{(\mathfrak{q}^5-1)(\mathfrak{q}^2+\mathfrak{q}+1)(\mathfrak{q}+1)} \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[5, 4, 1]$	$\mathbb{Z}_{\mathfrak{q}^5-1} \times \mathbb{Z}_{\mathfrak{q}^4-1}$	$\mathbb{Z}_{(\mathfrak{q}^5-1)(\mathfrak{q}^3+\mathfrak{q}^2+\mathfrak{q}+1)} \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$
$[5^2]$	$\mathbb{Z}_{\mathfrak{q}^5-1} \times \mathbb{Z}_{\mathfrak{q}^4+\mathfrak{q}^3+\mathfrak{q}^2+\mathfrak{q}+1}$	$\mathbb{Z}_{(\mathfrak{q}^5-1)/d_2} \times \mathbb{Z}_{(\mathfrak{q}^4+\mathfrak{q}^3+\mathfrak{q}^2+\mathfrak{q}+1)/d_5}$
$[6, 1^4]$	$\mathbb{Z}_{\mathfrak{q}^6-1} \times \mathbb{Z}_{\mathfrak{q}-1}^3$	$\mathbb{Z}_{\mathfrak{q}^6-1} \times \mathbb{Z}_{\mathfrak{q}-1}^2 \times \mathbb{Z}_{(\mathfrak{q}-1)/d}$

$[6,2,1^2]$	$\mathbb{Z}_{q^6-1} \times \mathbb{Z}_{q^2-1} \times \mathbb{Z}_{q-1}$	$\mathbb{Z}_{q^6-1} \times \mathbb{Z}_{q^2-1} \times \mathbb{Z}_{(q-1)/d}$
$[6,2^2]$	$\mathbb{Z}_{q^6-1} \times \mathbb{Z}_{q^2-1} \times \mathbb{Z}_{q+1}$	$\mathbb{Z}_{q^6-1} \times \mathbb{Z}_{(q^2-1)/d_5} \times \mathbb{Z}_{(q+1)/d_2}$
$[6,3,1]$	$\mathbb{Z}_{q^6-1} \times \mathbb{Z}_{q^3-1}$	$\mathbb{Z}_{q^6-1} \times \mathbb{Z}_{(q^3-1)/d}$
$[6,4]$	$\mathbb{Z}_{(q^6-1)(q^2+1)} \times \mathbb{Z}_{q+1}$	$\mathbb{Z}_{(q^6-1)(q^2+1)/d_5} \times \mathbb{Z}_{(q+1)/d_2}$
$[7,1^3]$	$\mathbb{Z}_{q^7-1} \times \mathbb{Z}^2_{q-1}$	$\mathbb{Z}_{q^7-1} \times \mathbb{Z}_{q-1} \times \mathbb{Z}_{(q-1)/d}$
$[7,2,1]$	$\mathbb{Z}_{q^7-1} \times \mathbb{Z}_{q^2-1}$	$\mathbb{Z}_{(q^7-1)(q+1)} \times \mathbb{Z}_{(q-1)/d}$
$[7,3]$	$\mathbb{Z}_{(q^7-1)(q^2+q+1)}$	$\mathbb{Z}_{(q^7-1)(q^2+q+1)/d}$
$[8,1^2]$	$\mathbb{Z}_{q^8-1} \times \mathbb{Z}_{q-1}$	$\mathbb{Z}_{q^8-1} \times \mathbb{Z}_{(q-1)/d}$
$[8,2]$	$\mathbb{Z}_{q^8-1} \times \mathbb{Z}_{q+1}$	$\mathbb{Z}_{(q^8-1)/d_5} \times \mathbb{Z}_{(q+1)/d_2}$
$[9,1]$	$\mathbb{Z}_{q^9-1}$	$\mathbb{Z}_{(q^9-1)/d}$
$[10]$	$\mathbb{Z}_{q^9+q^8+\ldots+q+1}$	$\mathbb{Z}_{(q^9+q^8+\ldots+q+1)/d}$

Acknowledgement. The author is thankful to the anonymous referee for suggesting a number of improvements to the original text.

References

[1] A. A. Buturlakin and M. A. Grechkoseeva, *The cyclic structure of maximal tori of the finite classical groups*, Algebra and Logic, **46**:2 (2007), 73–89. Zbl 1155.20047

[2] A. Storjohann, *Near optimal algorithms for computing Smith normal forms of integer matrices*, Proceedings of the 1996 international symposium on symbolic and algebraic computation, ISSAC '96, Zürich, Switzerland, July 24–26, 1996, New York, NY: ACM Press, 1996, 267–274. Zbl 0914.65043

[3] A. V. Zavarnitsine, *Recognition of the simple groups $L_3(q)$ by element orders*, J. Group Theory, **7**:1 (2004), 81–97. Zbl 1042.20006

Andrei V. Zavarnitsine
Sobolev Institute of Mathematics,
4, Koptyug ave.,
Novosibirsk, 630090, Russia
E-mail address: zav@math.nsc.ru