The Mathematics Student ISSN: 0025-5742
Vol. 85, Nos. 1-2, January-June (2016), 79-96

MATRIX GROUPS OVER RINGS

B. SURY

Abstract. This write-up is in the nature of an exposition of some work dealing with matrix groups over rings and their various decomposition theorems. The topic of matrix groups over rings like the integers is too general and too vast to allow a reasonable survey; so, we give an overview of some topics related to factorization. We discuss two types of related questions on matrix groups over rings here: (i) generating certain matrix groups by abstract subgroups like cyclic groups and implications on the structure of the ambient group; and (ii) '*finite width*' factorization into unipotent subgroups over rings.

1. Introduction.

Groups of matrices are ubiquitous in mathematics via their various avataars: Lie groups - if we work over $\mathbb{R}$ or $\mathbb{C}$, arithmetic subgroups - over integers and other number rings, finite simple groups - over finite fields, representation theory - over any ring. The existence of decompositions/factorizations into special types of pieces (for instance, Iwasawa, Cartan, Bruhat, Langlands,...) have traditionally played key roles. For example, Bruhat decomposition which arose in the theory of linear algebraic groups has proved useful in diverse contexts like numerical stability, and coding theory. In the paper ([19]), it is shown that for certain classes of matrices that have an exponential growth factor when Gaussian elimination with partial pivoting is applied, Bruhat decomposition has at most linear growth. In the paper ([17]), the authors present a new Bruhat decomposition design for constructing full diversity unitary space-time constellations for any number of antennas. The so-called Langlands decomposition of a parabolic subgroup is behind the "philosophy of cusp forms" due to Harish-Chandra (a precursor to Langlands's program) where the discrete groups take the backstage and inducing representations via the Langlands decomposition take center stage. So, generating matrix groups via special kinds of elements is useful. These are trickier

* The (modified) text of the 26^{th} Hansraj Gupta Memorial Award Lecture delivered at the 81^{st} Annual Conference of the Indian Mathematical Society held at the Visvesvaraya National Institute of Technology, Nagpur - 440 010, Maharashtra, during December 27-30, 2015.

2010 Mathematics Subject Classification: 11D45.
Keywords and Phrases: Matrix groups, bounded generation, unitriangularization, finite width, Chevalley groups, rings of stable rank 1.

and more subtle over rings which are not fields. In the next section, we describe a few of the applications where matrix groups over rings play a key role. The examples are chosen for their diversity. Following that, in section 3, we describe the more recent factorization theorems and their proofs.

2. Matrix groups over rings - some old applications

In this section, we briefly describe some of our earlier results on matrix groups over rings which are related to number theoretic and combinatorial group-theoretic questions. These examples are selected purely to demonstrate the diversity of applications that matrix groups over various rings have on other topics.

2.1. **Salem numbers.** A question due to D. H. Lehmer (which is still open from 1933) asks if there is a positive constant $c > 1$ such that for any integer coefficient polynomial, the product of the absolute values of its roots is strictly $> c$ unless the polynomial has only roots of unity as roots. Lehmer's computations revealed that the "worst" polynomials in this respect correspond to reciprocal polynomials with one real root $\tau > 1$ and other roots being $\frac{1}{\tau}$, $\tau_2, \overline{\tau_2}, \cdots, \tau_d, \overline{\tau_d}$ for $|\tau_i| = 1$. Such algebraic integers τ are known as Salem numbers - named after Raphael Salem who studied some of their properties. We can reformulate this question (see [25]) for the above subclass of polynomials in terms of the subgroups of $SL(2, \mathbb{R})$; the question is equivalent to asking if there is a neighbourhood U of the identity matrix such that every arithmetic subgroup Γ with no elements of finite order other than the identity and such that the quotient $SL(2, \mathbb{R})/\Gamma$ is compact, satisfies $\Gamma \cap U = \{I\}$.

2.2. **Generating a family of subgroups.** Here is an example to show how combinatorial-type properties may have bearing on deeper properties of the group. We proved (see [31]) the following theorem.

Theorem 2.1. *For any fixed $n \geq 3$, there is a number $N(n)$ depending only on n so that every group of the form*

$$Ker(SL_n(\mathbb{Z}) \to SL_n(\mathbb{Z}/k\mathbb{Z}))$$

can be generated by $N(n)$ elements for every $k > 1$. One may also wrote out a description of generators for each k.

Recently, Detinko, Flannery and Hulpke used the generators to give an algorithm (see [7]) to decide whether a subgroup of $SL_n(\mathbb{Z})$ (for $n > 2$) has finite index - in general, such problems are undecidable. In the above-mentioned paper, we had also given an example to show that there is no bound like $N(n)$ if we allow all normal subgroups of finite index. Very recently, Mark Shusterman proved a result bounding rank of a group in terms of its index where he elaborates on our example to show that his result is close to optimal.

2.3. **Infinitely presented matrix groups.** The following matrix group over a ring is an example of certain phenomena dealing with factorization, generation and finite presentation (see [26]).

Theorem 2.2. *Let p be a prime. We consider the ring $\mathbb{Z}[1/p]$ of rational numbers whose denominators can only be divisible by powers of p. Let*

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & p^n & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}[1/p], n \in \mathbb{Z} \right\}$$

has the remarkable properties. Then,
(a) $G = C_1 C_2 \cdots C_{12}$ where C_i's are cyclic groups (not necessarily distinct (that is, G has bounded generatios of degree ≤ 12);
(b) the commutator subgroup $[G, G]$ is not finitely generated;
(c) G is not finitely presented.

Indeed, if $x = diag(1, p, 1), y_{12} = I + E_{12}, y_{23} = I + E_{23} \in G$, then

$$\begin{pmatrix} 1 & ap^k & bp^l \\ 0 & p^n & cp^m \\ 0 & 0 & 1 \end{pmatrix} = x^{n-k} y_{12}^a x^{m-n+k} y_{23}^c x^{n-m} x^B y_{12}^A x^{-B} y_{23} x^B y_{12}^{-A} x^{-B}$$

where A, B are defined by $bp^l - acp^{m-n+k} = Ap^{-B}$.

The commutator subgroup of G is the unipotent group $\left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \right\}$ is infinitely generated; indeed, even its abelianization is infinitely generated. The fact that G is not finitely presentable follows from a criterion due to Bieri and Strebel.

2.4. **Matrix groups over finite rings and elementary number theory.** Elementary number-theoretic identities often fall out when one looks at natural actions of matrix groups over *finite rings* (note that finite rings have stable rank 1 - our factorization theorems in the next section deal with rings of stable rank 1). For instance, the identity

$$\sum_{t_1 \in (\mathbb{Z}_n)^*, t_2, \cdots, t_r \in \mathbb{Z}_n} GCD(n, t_1 - 1, t_2, \cdots, t_r) = \phi(n)\sigma_{r-1}(n)$$

can be derived (see [24]) by applying the so-called Cauchy-Frobenius-Burnside lemma to the group

$$G = \{ \begin{pmatrix} t_1 & t_2 & t_3 & \cdots & t_r \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} : t_1 \in (\mathbb{Z}_n)^*, t_i \in \mathbb{Z}_n \ \forall i > 1 \}$$

acting naturally on $(\mathbb{Z}_n)^r$. More generally, the action of the full upper triangular subgroup U_r of $GL(r, \mathbb{Z}_n)$ yields:

$$\sum_{A \in U_r} \prod_{k=1}^{r} d_k = n^{\binom{r}{2}} \phi(n)^r d_r(n)$$

where $A = (a_{ij})$,

$$d_k = GCD\Bigg(n, \frac{na_{1,k}}{(n, a_{1,1} - 1, a_{1,2}, \cdots, a_{1,k-1})}, \\ \frac{na_{2,k}}{(n, a_{22} - 1, a_{23}, \cdots, a_{2,k-1})}, \cdots, \frac{na_{k-1,k}}{(n, a_{k-1,k-1} - 1)}\Bigg)$$

and $d_1(n) = \sum_{d|n} d$, $d_k = \sum_{d|n} d_{k-1}(d)$.

2.5. **Finite matrix groups as capable groups.** Matrix groups over finite fields provide natural and easy examples of certain phenomena which occur in finite groups. For instance we have the following theorem (see [23]).

Theorem 2.3. *If A is a finite abelian capable group (that is, $A \cong G/Z(G)$ for some group G) where the center $Z(G)$ of G is cyclic, then $A \cong B \times B$ for an abelian group B; in particular, the order of A is a perfect square. Further, this property of A is not necessarily true if $Z(G)$ is not cyclic.*

Thus, it is of interest to find simple examples where $Z(G)$ is not cyclic where $G/Z(G)$ has non-square order. In loc. cit., we constructed the following example.

Example. Let F be a finite field and $E \subset F$ be a proper subfield. Consider the group

$$G = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : b, c \in F; a \in E \right\}.$$

If we denote a typical element of G by $g(a, b, c)$, then

$$g(a, b, c)g(a', b', c') = g(a + a', b + b', ab' + c + c').$$

Further, $g(a, b, c)^{-1} = g(-a, -b, ab - c)$. Now, note that $g(a, b, c) \in Z(G)$ if and only if $ab' = a'b$ for all $a' \in E, b' \in F$. Thus, some $g(a, 0, c) \in Z(G)$ if and only if $ab' = 0$ for all $b' \in F$; that is, if and only if $a = 0$. On the other hand, if some $g(a, b, c) \in Z(G)$ with $b \neq 0$, then $g(a, b, c)g(1, 0, 0) = g(1, 0, 0)g(a, b, c)$ gives $0 = b$, a contradiction. Thus

$$Z(G) = \{g(0, 0, c) : c \in F\} \quad \text{and} \quad G/Z(G) \cong E \oplus F.$$

Note that the finite, abelian, capable group $G/Z(G)$ can have non-square order - for instance, if E has p elements and F has p^2 elements then $Z(G)$ is not cyclic.

2.6. **Matrix groups as monodromy groups of polynomials.** The problem of finiteness of number of solutions of Diophantine equations of the form $f(x) = g(y)$ where f, g are integer polynomials leads to questions on their monodromy groups which can be fruitfully answered by analyzing certain matrix groups which are isomorphic to finite dihedral groups. Work of Yuri Bilu showed (see [4]) that one may reduce the problem to determining the possible quadratic factors of the polynomial $f(X) - g(Y)$. Over an algebraically closed field K of any characteristic, the latter question is answered in the following manner.

Let x be transcendental over K, and set $t = f(x)$. If $f(X)-g(Y)$ has an irreducible factor of degree 2, then $K(x)$ has a quadratic extension L, the function field of this quadratic factor. Then $L/K(t)$ is Galois. The Galois group is generated by two involutions, hence it is dihedral. The intermediate field $K(x)$ is the fixed field of one of the involutions. By Lüroth's Theorem, KL is a rational field $K(z)$. So $Gal(K(z)/K(t))$ is a subgroup of $Gal(L/K(t))$. Also, the index is at most 2. The group of K-automorphisms of $K(z)$ is $PGL_2(K)$ acting as linear fractional transformations of z. Thus, to determine factors of degree at most 2 of $f(X)-g(Y)$, we have to determine the cyclic and dihedral subgroups of $PGL_2(K)$, and analyze the cases which give pairs f, g such that $f(X) - g(Y)$ has a quadratic factor over K. We may show (see [11]):

Proposition. Let K be an algebraically closed field of characteristic p, and $\rho \in PGL_2(K)$ be an element of finite order n. Then one of the following holds:

(a) p does not divide n, and ρ is conjugate to $\begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix}$, where ζ is a primitive n-th root of unity.

(b) $n = p$, and ρ is conjugate to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Using this, we may deduce the following (loc. cit.). First, we introduce two notations. For $u, v \in K[X]$, write $u \sim v$ if and only if there are linear polynomials $L, R \in K[X]$ with $u(X) = L(v(R(X)))$. Also, for $a \in K$, the Dickson polynomial $D_n(X, a)$ is defined by $D_n(z + a/z, a) = z^n + (a/z)^n$. It turns out that we have the following theorem.

Theorem 2.4. *Let $f, g \in K[X]$ be non-constant polynomials over a field K, such that $f(X) - g(Y) \in K[X, Y]$ has a quadratic irreducible factor $q(X, Y)$. If the characteristic p of K is positive, then assume that at least one of the polynomials f, g cannot be written as a polynomial in X^p. Let deg $f = n$. Then there are $f_1, g_1, \Phi \in K[X]$ with $f = \Phi \circ f_1$, $g = \Phi \circ g_1$ such that $q(X, Y)$ divides $f_1(X)-g_1(Y)$, and one of the following holds*

(a) $\max(\deg f_1, \deg g_1) = 2$ *and* $q(X, Y) = f_1(X) - g_1(Y)$.

(b) *There are $\alpha, \beta, \gamma, \delta \in K$ with $g_1(X) = f_1(\alpha X+\beta)$, and $f_1(X) = h(\gamma X+\delta)$, where $h(X)$ is one of the following polynomials.*

(i) *p does not divide n, and $h(X) = D_n(X, a)$ for some $a \in K$. If $a \neq 0$, then $\zeta + 1/\zeta \in K$ where ζ is a primitive n-th root of unity.*

(ii) *$p \geq 3$, and $h(X) = X^p - aX$ for some $a \in K$.*

(iii) *$p \geq 3$, and $h(X) = (X^p + aX + b)^2$ for some $a, b \in K$.*

(iv) *$p \geq 3$, and $h(X) = X^p - 2aX^{\frac{p+1}{2}} + a^2X$ for some $a \in K$.*

(v) *$p = 2$, and $h(X) = X^4 + (1 + a)X^2 + aX$ for some $a \in K$.*

(c) *n is even, p does not divide n, and there are $\alpha, \beta, \gamma, a \in K$ such that $f_1(X) = D_n(X+\beta, a)$, $g_1(X) = -D_n((\alpha X+\gamma)(\xi+1/\xi), a)$. Here ξ denotes a primitive $2n$-th root of unity. Furthermore, if $a \neq 0$, then $\xi^2+1/\xi^2 \in K$.*

(d) *$p \geq 3$, and there are quadratic polynomials $u(X), v(X) \in K[X]$, such that $f_1(X) = h(u(X))$ and $g_1(X) = h(v(X))$ with $h(X) = X^p - 2aX^{\frac{p+1}{2}} + a^2X$ for some $a \in K$.*

The theorem excludes the case that f and g are both polynomials in X^p. The following theorem handles this case; a repeated application of it reduces to the situation of the Theorems

Theorem 2.5. *Let $f, g \in K[X]$ be non-constant polynomials over a field K, such that $f(X) - g(Y) \in K[X, Y]$ has an irreducible factor $q(X, Y)$ of degree at most 2. Suppose that $f(X) = f_0(X^p)$ and $g(X) = g_0(X^p)$, where $p > 0$ is the characteristic of K. Then one of the following holds:*

(a) *$q(X, Y)$ divides $f_0(X) - g_0(Y)$, or*

(b) *$p = 2$, $f(X) = f_0(X^2)$, $g(X) = f_0(aX^2 + b)$ for some $a, b \in K$, and $q(X, Y) = X^2 - aY^2 - b$.*

2.7. **Bounded generation and finite width.** The matrix groups over integers like $SL_n(\mathbb{Z})$ are finitely generated and even have finite presentations. However, a remarkable refinement of the first property came to the fore in the work of A.S.Rapinchuk. This is known as bounded generation. An abstract group G is said to be boundedly generated of degree $\leq n$ if there exists a sequence of (not necessarily distinct) elements $g_1, \cdots, g_n$ such that

$$G = < g_1 > < g_2 > \cdots < g_n >$$

that is,

$$G = \{g_1^{a_1} g_2^{a_2} \cdots g_n^{a_n} : a_i \in \mathbb{Z}\}.$$

A free, non-abelian group (and therefore, $SL_2(\mathbb{Z})$ also) is not boundedly generated. On the other hand, a group like $SL_n(\mathbb{Z})$ for $n \geq 3$, is boundedly generated by elementary matrices (an elementary proof of this can be given using Dirichlet's theorem on primes in arithmetic progressions). It turns out that this difference is an indicator of a deeper attribute called the congruence subgroup property; viz., every subgroup of finite index in $SL_n(\mathbb{Z})$ for $n \geq 3$ contains a subgroup of the form

$$Ker(SL_n(\mathbb{Z}) \to SL_n(\mathbb{Z}/k\mathbb{Z}))$$

This was revealed in the work of V.P.Platonov & A.S.Rapinchuk ([21]) and also in the work of A.Lubotzky ([16]).

Matrix groups which are finitely generated have an abundance of subgroups of finite index. More precisely, they are residually finite - that is, the intersection of all subgroups of finite index is the trivial group. In this case, it is beneficial to define a topology using as a basis the subgroups of finite index - residual finiteness

guarantees this is Hausdorff. The completion with respect to this topology is known as the profinite completion; this is a compact group in which the original group embeds.

A finitely generated group for which the normal subgroups which have indices powers of a (fixed) prime p intersect in the identity, is said to be residually-p. The corresponding profinite completion is called the pro-p completion. In general, a profinite group is formed by putting together a tower of finite groups by a limiting process; a classical example is that of Galois group of the algebraic closure. Notions involved in the theory of finite groups and many properties find resonance in the theory of profinite groups and the topology available in the latter theory makes it possible to deduce properties of abstract, discrete groups.

A profinite group G is said to be boundedly generated as a profinite group if there exists a sequence of (not necessarily distinct) elements $g_1, \cdots, g_n$ such that

$$G = \overline{< g_1 >< g_2 >} \cdots \overline{< g_n >}$$

where the 'bar' denotes closure.

It follows from Lazard's deep work on p-adic Lie groups (see [12]) and the solution to the restricted Burnside problem that a pro-p group has bounded generation (as a profinite group) if and only if it is a p-adic compact Lie group; this can be thought of as an analogue of Hilbert's 5th problem for the p-adic case.

If an abstract group has bounded generation, then so do its pro-p completions for each prime p (as does the full profinite completion). Therefore, we have a nice sufficient criterion for an abstract group to have a faithful linear representation - viz., if it has bounded generation and is virtually residually-p. We can use this idea to show that the automorphism group of a free group does not have bounded generation (see [26]).

The question of existence of bounded generation for matrix groups over number-theoretic rings has rather deep connections with other properties. The profinite completion of an arithmetic group is boundedly generated if, and only if, it has the congruence subgroup property - this was proved independently by V. P. Platonov & A. S. Rapinchuk and by A. Lubotzky (see [21]) and [16]). Lubotzky also conjectured that the congruence subgroup property holds for an S-arithmetic group if, and only if, it can be embedded as a closed subgroup of $SL_n(\mathbf{A})$ - a so-called adelic group. This was proved in [22], where we also conjectured that finitely generated closed subgroups of adelic groups have bounded generation. Then M.Liebeck & L.Pyber proved ([15]) that if G is a subgroup of $GL_n(K)$ where K is of characteristic p which is large compared to n, and if G is generated by elements of orders powers of p, then G is a product of 25 Sylow p-subgroups. They used it to prove our conjecture mentioned above.

It is still an intriguing open question as to whether the property of bounded generation for an S-arithmetic group Γ equivalent to bounded generation for its

profinite completion (which is, as mentioned earlier, equivalent to the congruence subgroup property holding good for Γ). The answer is perhaps in the negative and certain arithmetic subgroups of $Sp(n,1)$ could provide counter-examples. Moreover, this is a subtle question specific to arithmetic groups and not for more general profinite groups because the group $\prod_{r\geq 1} PSL_n(\mathbf{F}_{2^r})$ is boundedly generated group as a profinite group but none of its discrete subgroups is boundedly generated.

O.Tavgen proved bounded generation of arithmetic groups in rank > 1 groups (see [33]). However, bounded generation for co-compact arithmetic lattices is still an open question in general excepting the case of quadratic forms (see [8]); note here that there are no unipotent elements.

A notion related to but weaker than bounded generation is that of finite width wirh respect to a subset defined as follows.

A group G has finite width with respect to a subset E if there exists a positive integer n such that each element of G can be expressed as $g = e_1 e_2 \cdots e_r$ with $r \leq n$ and $e_i \in E$.

If we look at rings R that are finitely generated as abelian groups, then $SL(n,R)$ has bounded generation if it has finite width with respect to the set of all elementary matrices $X_{ij}(t)$ with $t \in R$ and $i \neq j$.

More generally, for any commutative ring R, one could look at the question of finite width for elementary group $E_n(R)$ which may be a proper subgroup of $SL(n,R)$. It is not difficult to check that $E_n(R)$ has this property if and only if $K_1(n,R^{\mathbb{N}}) \to K_1(n,R)^{\mathbb{N}}$ is injective, where the K-group K_1 is the quotient of GL by E.

3. Finite unipotent width over stable rank 1 rings

We describe some results on finite width obtained in collaboration with Vavilov and Smolensky. The following problem arises in several independent contexts. It addresses Chevalley groups which we will describe shortly.

Problem. *For a commutative ring R, find the shortest factorization $G = UU^-UU^- \ldots U^{\pm}$ of an elementary Chevalley group $E(\Phi,R)$, in terms of the unipotent radical $U = U(\Phi,R)$ of the standard Borel subgroup $B = B(\Phi,R)$, and the unipotent radical $U^- = U^-(\Phi,R)$ of the opposite Borel subgroup $B^- = B^-(\Phi,R)$.*

There are following two problems here.

- first, to establish the *existence* of such factorizations, and
- second, to estimate their *length*.

We can prove the following theorem for rings of stable rank 1 ([28]).

Theorem 3.1. *Let Φ be a reduced irreducible root system and R be a commutative ring such that the stable rank of R is 1. Then the elementary Chevalley group $E(\Phi,R)$ admits a uni-triangular factorisation*

$$E(\Phi,R) = U(\Phi,R)U^-(\Phi,R)U(\Phi,R)U^-(\Phi,R)$$

of length 4. *Further,* 4 *is the minimum possible for such a result to hold good if* R *has a nontrivial unit.*

Here, a commutative ring has **stable rank** 1, if for all $x, y \in R$, which generate R as an ideal, there exists a $z \in R$ such that $x + yz$ is invertible. In this case we write $\mathrm{sr}(R) = 1$. Examples of ring of stable rank 1 are semilocal rings, and the ring of ALL algebraic integers.

The same method allows us to prove (see [29]) the following theorem.

Theorem 3.2. *With* R *as above, the elementary Chevalley group* $E(\Phi, R)$ *admits a Gauss decomposition*

$$E(\Phi, R) = (T(\Phi, R) \cap E(\Phi, R))U(\Phi, R)U^-(\Phi, R)U(\Phi, R).$$

Conversely, if Gauss decomposition holds for some elementary Chevalley group, then $\mathrm{sr}(R) = 1$.

Actually, a corollary of this last theorem is the following statement which also shows theorem 3.1 holds at least in the weaker form with length 5.

Corollary 3.3. *Let* Φ *be a reduced irreducible root system and* R *be a commutative ring such that* $\mathrm{sr}(R) = 1$. *Then any element* g *of the elementary Chevalley group* $E(\Phi, R)$ *is conjugate to an element of*

$$U(\Phi, R)H(\Phi, R)U^-(\Phi, R).$$

In the 1960's, N. Iwahori & H. Matsumoto, E. Abe & K. Suzuki, and M. Stein discovered (see [1], [2], [10], [30]) that Chevalley groups $G = G(\Phi, R)$ over a semilocal ring admit the remarkable Gauss decomposition $G = TUU^-U$, where $T = T(\Phi, R)$ is a split maximal torus, whereas $U = U(\Phi, R)$ and $U^- = U^-(\Phi, R)$ are unipotent radicals of two opposite Borel subgroups $B = B(\Phi, R)$ and $B^- = B^-(\Phi, R)$ containing T. It follows from the classical work of Hyman Bass and Michael Stein that for classical groups Gauss decomposition holds under weaker assumptions such as $\mathrm{sr}(R) = 1$ or $\mathrm{asr}(R) = 1$. Later N. Vavilov noticed that condition $\mathrm{sr}(R) = 1$ is necessary for Gauss decomposition to be valid. In our theorems, we show that for the elementary group $E(\Phi, R)$, the condition $\mathrm{sr}(R) = 1$ is also sufficient for Gauss decomposition to hold good. In other words, $E = HUU^-U$, where $H = H(\Phi, R) = T \cap E$. This surprising result pinpoints the fact that stronger conditions on the ground ring, such as being semi-local, $\mathrm{asr}(R) = 1$, $\mathrm{sr}(R, \Lambda) = 1$, etc., were only needed to guarantee that for simply connected groups $G = E$, rather than to verify the Gauss decomposition itself. Our method of proof is an elaboration of a beautiful idea of O. Tavgen ([32]).

Results equivalent to writing matrices in terms of upper and lower triangular matrices have been proved piece-meal in various situations by programmers working on computational linear algebra and others ([20],[13], [5], [3], [9], [27], [34]). So, results such as the above unitriangular factorization admit potential applications in computational linear algebra, wavelet theory, computer graphics and Control

theory. For instance, the one-dimensional shears correspond to transvections that are standard in the study of matrix groups over rings.

3.1. **Number rings-finite width.** Number-theoretic rings are usually more complicated. Over the ring $\mathbb{Z}[1/p]$, we prove (see [28]):

Theorem 3.4. *Let p be a prime. The elementary Chevalley group $E\left(\Phi, \mathbb{Z}\left[\frac{1}{p}\right]\right)$ admits unitriangular factorisation*

$$E\left(\Phi, \mathbb{Z}\left[\frac{1}{p}\right]\right) = \left(U\left(\Phi, \mathbb{Z}\left[\frac{1}{p}\right]\right)U^-\left(\Phi, \mathbb{Z}\left[\frac{1}{p}\right]\right)\right)^3$$

of length 6.

The theorem is deduced from the one below for SL_2 which we can prove in the following slightly stronger form.

Lemma 3.5.

$$SL_2\left(\mathbf{Z}\left[\frac{1}{p}\right]\right) = UU^-UU^-U = U^-UU^-UU^-.$$

From this factorization, we deduce explicitly that $SL_2(\mathbb{Z}[\frac{1}{p}])$ has bounded generation. This is known earlier (see [14]), but the bounded generation was deduced either using generalized Riemann Hypothesis or deep analytic results like Vinogradov's three primes theorem or an indirect model-theoretic proof is given where there was no information on the degree of bounded generation.

Such factorizations can be treated by relating them to division chains (see [6]) in the ring $\mathbb{Z}[\frac{1}{p}]$. Note that expressing a matrix in the group $SL(2, R)$ over a Euclidean ring R as a product of elementary matrices is equivalent to studying continued fractions. Existence of arbitrary long division chains in $\mathbf{Z}$ shows that the group $SL(2, \mathbf{Z})$ cannot have bounded width in elementary generators. If $\begin{pmatrix} A & C \\ B & D \end{pmatrix}$ is in $SL_2(\mathbb{Z}[\frac{1}{p}])$, then we have the following lemma.

Lemma 3.6. $A = Q_1B + R_1, \qquad B = Q_2R_1 + R_2 \qquad R_1 = Q_3R_2 + 1.$

Thus

$$\begin{pmatrix} 1 & 0 \\ -R_2 & 1 \end{pmatrix}\begin{pmatrix} 1 & -Q_3 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -Q_2 & 1 \end{pmatrix}\begin{pmatrix} 1 & -Q_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} A & C \\ B & D \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

3.2. **Number rings - explicit bounded generation.** Using the above theorem, for the matrices $T = \begin{pmatrix} p^{-1} & 0 \\ 0 & p \end{pmatrix}$, $U_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $V_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, we can deduce unconditionally the following theorem.

Theorem 3.7. *Let p be a prime number. Then $SL_2(\mathbb{Z}[\frac{1}{p}])$ has bounded generation of degree at the most* 11. *In fact, we have*

$$SL_2(\mathbb{Z}[1/p]) = \{T^{a_1}U_1^{b_1}T^{a_2}V_1^{c_1}T^{a_3}U_1^{b_2}T^{a_4}V_1^{c_2}T^{a_5}U_1^{b_3}T^{a_6} : a_i, b_i, c_i \in \mathbb{Z}\}.$$

One should note that this is not completely straightforward from the above unitriangular factorization theorem because one can show that the group $SL_2(\mathbb{Z}[1/p])$ *cannot* have bounded generation with respect to only unipotent matrices!

Let us mention in passing that some matrix groups over rings of polynomials are finitely generated but are not boundedly generated. For instance, the group of 2×2 matrices $\begin{pmatrix} t^m & t^n f(t) \\ 0 & 1 \end{pmatrix}$ where f is any polynomial with integer coefficients and m, n are any integers, is an infinite group (it can be identified with the wreath product of $\mathbb{Z}$ by $\mathbb{Z}$) and it has an infinitely generated abelian subgroup, but is itself generated by just two matrices $\begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. One can prove by combinatorial methods that the above matrix group does not have bounded generation. In fact, we have (see [18]) the following result.

If A and B are groups then $A \wr B$ has bounded generation if and only if A has bounded generation and B is finite.

4. Elementary Chevalley groups over rings

We now proceed to introduce the Chevalley groups and the elementary subgroups occurring in the statements of our theorems 1 and 2.

Let Φ be a reduced irreducible root system of rank l, $W = W(\Phi)$ be its Weyl group and $\mathcal{P}$ be a lattice intermediate between the root lattice $\mathcal{Q}(\Phi)$ and the weight lattice $\mathcal{P}(\Phi)$. Further, we fix an order on Φ and denote by $\Pi = \{\alpha_1, \dots, \alpha_l\}$, Φ^+ and Φ^- the corresponding sets of fundamental, positive and negative roots, respectively.

It is classically known that with these data one can associate the Chevalley group $G = G_{\mathcal{P}}(\Phi, R)$ for any ring R; this is the group of R-points of an affine groups scheme $G_{\mathcal{P}}(\Phi, -)$ - the Chevalley-Demazure group scheme. The group is said to be simply connected (res. adjoint) if $\mathcal{P}$ is the weight lattice (resp. root lattice). Since our results do not depend on the choice of the lattice $\mathcal{P}$, we will usually assume that $\mathcal{P} = \mathcal{P}(\Phi)$ and omit any reference to $\mathcal{P}$ in the notation. Thus, $G(\Phi, R)$ will denote the simply connected Chevalley group of type Φ over R.

Fix a split maximal torus $T(\Phi, -)$ of the group scheme $G(\Phi, -)$ and set $T = T(\Phi, R)$. Fix isomorphisms $x_\alpha : R \mapsto X_\alpha$. Here, the elements $x_\alpha(\xi)$; $\xi \in R$, $\alpha \in \Phi$ are called root unipotents and, the root groups X_α comprised of these elements when ξ varies in R, are interrelated by the Chevalley commutator formulae. The root subgroups X_α, $\alpha \in \Phi$ generate the elementary subgroup $E(\Phi, R)$ of $G(\Phi, R)$.

Let $\alpha \in \Phi$ and $\varepsilon \in R^*$. Set $h_\alpha(\varepsilon) = w_\alpha(\varepsilon) w_\alpha(1)^{-1}$, where $w_\alpha(\varepsilon) = x_\alpha(\varepsilon) x_{-\alpha}(-\varepsilon^{-1}) x_\alpha(\varepsilon)$. The elements $h_\alpha(\varepsilon)$ are called semisimple root elements. For a simply connected group one has

$$T = T(\Phi, R) = \langle h_\alpha(\varepsilon),\ \alpha \in \Phi,\ \varepsilon \in R^* \rangle.$$

One also defines $H(\Phi, R) = T(\Phi, R) \cap E(\Phi, R)$. Let $N = N(\Phi, R)$ be the algebraic

normalizer of the torus $T = T(\Phi, R)$, i. e. the subgroup, generated by $T = T(\Phi, R)$ and all elements $w_\alpha(1)$, $\alpha \in \Phi$. The factor-group N/T is canonically isomorphic to the Weyl group W, and for each $w \in W$ we fix its preimage n_w in N.
The theorems 1 and 2 stated above generalize and strengthen results which were proved piecemeal over finite fields by several authors with a much simpler, uniform proof. Recall the statements again in the following form.

Theorem 4.1. *$E(\Phi, R)$ admits a Gauss decomposition*

$$E(\Phi, R) = H(\Phi, R)U(\Phi, R)U^-(\Phi, R)U(\Phi, R).$$

Conversely, if Gauss decomposition holds for some elementary Chevalley group, then $\mathrm{sr}(R) = 1$.

Corollary 4.2. *(to Theorem 1). We have a unitriangular factorisation*

$$E(\Phi, R) = U(\Phi, R)U^-(\Phi, R)U(\Phi, R)U^-(\Phi, R)$$

of length 4. *Further,* 4 *is the minimum possible for such a result to hold good if R has a nontrivial unit.*

The proofs rely on a beautiful idea of Oleg Tavgen on rank reduction (see [32]); we use the fact that for systems of rank ≥ 2 every fundamental root falls into the subsystem of smaller rank obtained by dropping either the first or the last fundamental root. One needs to study elementary parabolic subgroups then. We just discuss a toy case first.

4.1. **Toy case of theorem 3.1.** The following lemma is this Toy case.

Lemma 4.3. *Let R be a commutative ring of stable rank* 1. *Then*

$$\mathrm{SL}(2, R) = U(2, R)U^-(2, R)U(2, R)U^-(2, R).$$

In particular, $\mathrm{SL}(2, R) = E(2, R)$.

The toy case is the only place where the stability condition on R is invoked. To deduce the general theorem, we use only the theory of linear algebraic groups. Let us prove the toy case above.

proof. Let us trace how many elementary transformations one needs to bring an arbitrary matrix $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, R)$ to the identity. We will not introduce new notation at each step, but rather replace the matrix g by its current value, as is common in computer science. Obviously, its entries a, b, c, d should be also reset to their current values at each step.

Step 1. Multiplication by a single *lower* elementary matrix on the right allows to make the element in the South-West corner invertible.

Indeed, since the rows of the matrix are unimodular, one has $cR + dR = R$ and since $\mathrm{sr}(R) = 1$, there exists such an $z \in R$, that $c + dz \in R^*$. Thus,

$$gt_{21}(z) = \begin{pmatrix} a + bz & b \\ c + dz & d \end{pmatrix}.$$

Step 2. We (can) assume that $c \in R^*$; then, multiplication by a single *upper* elementary matrix on the right allows to make the element in the South-East corner equal to 1. Indeed,

$$gt_{12}(c^{-1}(1-d)) = \begin{pmatrix} a & b + ac^{-1}(1-d) \\ c & 1 \end{pmatrix}.$$

Step 3. We (can) assume that $d = 1$; so, multiplication by a single *lower* elementary matrix on the right allows to make the element in the South-West corner equal to 0. Indeed,

$$gt_{21}(-c) = \begin{pmatrix} a - bc & b \\ 0 & 1 \end{pmatrix}.$$

Since $\det(g) = 1$, the matrix on the right hand side is equal to $t_{12}(b)$. Bringing all elementary factors to the right hand side, we see that any matrix g with determinant 1 can be expressed as a product of the form $t_{12}(*)t_{21}(*)t_{12}(*)t_{21}(*)$, as claimed in the lemma.

4.2. **A concrete case of theorem 3.2.** We discuss a special concrete case. If $N(n, R)$ is the group of monomial matrices over any commutative ring R, then we have the following result.

Proposition 4.4. *Let R be an arbitrary commutative ring. Then one has the following inclusion* $N(n, R) \subseteq U(n, R)U^-(n, R)U(n, R)U^-(n, R)$.

Proof. Let $g = (g_{ij}) \in N(n, R)$. Let us argue by induction on $n \geq 2$.

Case 1. First, let $g_{nn} = 0$. Then, there exists a unique $1 \leq r \leq n-1$ such that $a = g_{rn} \neq 0$ and a unique $1 \leq s \leq n-1$ such that $b = g_{ns} \neq 0$, all other entries in the s-th and the n-th columns are equal to 0. Since g is invertible, automatically $a, b \in R^*$. The matrix $gt_{sn}(b^{-1})$ differs from g only in the position (n, n), where now we have 1 instead of 0. Consecutively multiplying the resulting matrix on the right by $t_{ns}(-b)$ and then by $t_{sn}(b^{-1})$, we get the matrix h, which differs from g only at the intersection of the r-th and the n-the rows with the s-th and the n-th columns, where now instead of $\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}$ one has $\begin{pmatrix} -ab & 0 \\ 0 & 1 \end{pmatrix}$.

Observe, that the determinant of the leading submatrix of order $n-1$ of the matrix h equals 1, and thus we can apply induction hypothesis and obtain for that last matrix the desired factorisation in the group $\mathrm{SL}(n-1, R)$. This factorisation does not affect the last row and the last column. We have shown

$$gt_{sn}(b^{-1})t_{ns}(-b)t_{sn}(b^{-1}) = u_1u_1^-u_2u_2^-,$$

where these matrices have no role in the n-th row and column. As they normalize the t_{sn}'s and the t_{ns}'s, the proof can be completed in this case; this is where the general root system requires a carefully proved normalization result stated below as key lemma.

Case 2. Let $b = g_{nn} \neq 0$. Take arbitrary $1 \leq r, s \leq n-1$ for which $a = g_{rs} \neq 0$. Again, automatically $a, b \in R^*$. As in the previous case, let us concentrate on the

r-th and the n-th rows and the s-th and the n-th columns. Since there are no further non-zero entries in these rows and columns, any additions between them do not change other entries of the matrix, and only affect the submatrix at the intersection of the r-th and the n-th rows with the s-th and the n-th columns. Now, multiplying g by $t_{ns}(b^{-1})t_{sn}(1-b)t_{ns}(-1)t_{ns}(-b^{-1}(1-b))$ on the right, we obtain the matrix h, where this submatrix, which was initially equal to $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, will be replaced by $\begin{pmatrix} ab & 0 \\ 0 & 1 \end{pmatrix}$. At this point the proof can be finished in exactly the same way as in the previous case.

4.3. **Towards the proof - elementary parabolics.** The main role in the proofs in general is played by Levi decomposition for elementary parabolic subgroups. Denote by $m_k(\alpha)$ the coefficient of α_k in the expansion of α with respect to the fundamental roots

$$\alpha = \sum m_k(\alpha)\alpha_k, \quad 1 \leq k \leq l.$$

Fix any $r = 1, \ldots, l$ - in fact, in the reduction to smaller rank it suffices to employ only terminal parabolic subgroups, even only the ones corresponding to the first and the last fundamental roots, $r = 1, r = l$.

Denote by

$$S = S_r = \big\{\alpha \in \Phi,\ m_r(\alpha) \geq 0\big\}$$

the r-th standard parabolic subset in Φ. As usual, the reductive part $\Delta = \Delta_r$ and the special part $\Sigma = \Sigma_r$ of the set $S = S_r$ are defined as

$$\Delta = \big\{\alpha \in \Phi,\ m_r(\alpha) = 0\big\}, \quad \Sigma = \big\{\alpha \in \Phi,\ m_r(\alpha) > 0\big\}.$$

The opposite parabolic subset and its special part are defined similarly as

$$S^- = S_r^- = \big\{\alpha \in \Phi,\ m_r(\alpha) \leq 0\big\}, \quad \Sigma^- = \big\{\alpha \in \Phi,\ m_r(\alpha) < 0\big\}.$$

Obviously, the reductive part of S_r^- equals Δ.

Denote by P_r the *elementary* maximal parabolic subgroup of the elementary group $E(\Phi, R)$. By definition

$$P_r = E(S_r, R) = \big\langle x_\alpha(\xi),\ \alpha \in S_r,\ \xi \in R\big\rangle.$$

By the Levi decomposition

$$P_r = L_r \leftthreetimes U_r = E(\Delta, R) \leftthreetimes E(\Sigma, R).$$

Recall that

$$L_r = E(\Delta, R) = \big\langle x_\alpha(\xi), \quad \alpha \in \Delta, \quad \xi \in R\big\rangle,$$

whereas

$$U_r = E(\Sigma, R) = \big\langle x_\alpha(\xi),\ \alpha \in \Sigma,\ \xi \in R\big\rangle.$$

A similar decomposition holds for the opposite parabolic subgroup P_r^-, whereby the Levi subgroup is the same as for P_r, but the unipotent radical U_r is replaced by the opposite unipotent radical $U_r^- = E(-\Sigma, R)$. As a matter of fact, we use Levi decomposition in the following form. It will be convenient to slightly change

the notation and write $U(\Sigma, R) = E(\Sigma, R)$ and $U^-(\Sigma, R) = E(-\Sigma, R)$.

Lemma 4.5. *(Key Lemma) The group* $\langle U^\sigma(\Delta, R), U^\rho(\Sigma, R)\rangle$*, where* $\sigma, \rho = \pm 1$*, is the semidirect product of its normal subgroup* $U^\rho(\Sigma, R)$ *and the complementary subgroup* $U^\sigma(\Delta, R)$*.*

In other words, the subgroup $U^\pm(\Delta, R)$ normalizes each of the groups $U^\pm(\Sigma, R)$ so that, in particular, one has the following four equalities for products

$$U^\pm(\Delta, R)U^\pm(\Sigma, R) = U^\pm(\Sigma, R)U^\pm(\Delta, R).$$

Furthermore, the following four obvious equalities for intersections hold

$$U^\pm(\Delta, R) \cap U^\pm(\Sigma, R) = 1.$$

In particular, one has the following decompositions

$$U(\Phi, R) = U(\Delta, R) \leftthreetimes U(\Sigma, R), \quad U^-(\Phi, R) = U^-(\Delta, R) \leftthreetimes U^-(\Sigma, R).$$

5. Idea of proofs of theorems 1 and 2

Start with the following result which is easy, well known, and very useful.

Lemma 5.1. *The elementary Chevalley group* $E(\Phi, R)$ *is generated by unipotent root elements* $x_\alpha(\xi)$*,* $\alpha \in \pm\Pi$*,* $\xi \in R$*, corresponding to the fundamental and negative fundamental roots.*

Proof. Indeed, every root is conjugate to a fundamental root by an element of the Weyl group, while the Weyl group itself is generated by the fundamental reflections w_α, $\alpha \in \Pi$. Thus, the elementary group $E(\Phi, R)$ is generated by the root unipotents $x_\alpha(\xi)$, $\alpha \in \Pi$, $\xi \in R$, and the elements $w_\alpha(1)$, $\alpha \in \Pi$. It remains only to observe that $w_\alpha(1) = x_\alpha(1)x_{-\alpha}(-1)x_\alpha(1)$.

Further, let $B = B(\Phi, R)$ and $B^- = B^-(\Phi, R)$ be a pair of opposite Borel subgroups containing $T = T(\Phi, R)$, standard with respect to the given order. Recall that B and B^- are semidirect products $B = T \leftthreetimes U$ and $B^- = T \leftthreetimes U^-$, of the torus T and their unipotent radicals

$$U = U(\Phi, R) = \langle x_\alpha(\xi),\ \alpha \in \Phi^+,\ \xi \in R\rangle,$$

$$U^- = U^-(\Phi, R) = \langle x_\alpha(\xi),\ \alpha \in \Phi^-,\ \xi \in R\rangle.$$

Recall that a subset S in Φ is *closed*, if for any two roots $\alpha, \beta \in S$ whenever $\alpha + \beta \in \Phi$, already $\alpha + \beta \in S$. For closed S, define $E(S) = E(S, R)$ to be the subgroup generated by all elementary root unipotent subgroups X_α, $\alpha \in S$:

$$E(S, R) = \langle x_\alpha(\xi), \quad \alpha \in S, \quad \xi \in R\rangle.$$

In this notation, U and U^- coincide with $E(\Phi^+, R)$ and $E(\Phi^-, R)$, respectively. The groups $E(S, R)$ are particularly important in the case where $S \cap (-S) = \varnothing$. In this case $E(S, R)$ coincides with the *product* of root subgroups X_α, $\alpha \in S$, in some/any fixed order.

Again, let $S \subseteq \Phi$ be a closed set of roots; then S can be decomposed into a disjoint union of its *reductive = symmetric* part S^r, consisting of those $\alpha \in S$, for

which $-\alpha \in S$, and its *unipotent* part S^u, consisting of those $\alpha \in S$, for which $-\alpha \notin S$. The set S^r is a closed root subsystem, whereas the set S^u is special. Moreover, S^u is an *ideal* of S (i.e., if $\alpha \in S$, $\beta \in S^u$ and $\alpha + \beta \in \Phi$, then $\alpha + \beta \in S^u$).

Levi decomposition shows that the group $E(S, R)$ decomposes into the semidirect product $E(S, R) = E(S^r, R) \leftthreetimes E(S^u, R)$ of its Levi subgroup $E(S^r, R)$ and its unipotent radical $E(S^u, R)$.

5.1. **Reduction to smaller rank.** As mentioned earlier, the proofs depend on the reduction of rank as in the following theorem.

Theorem 5.2. *Let Φ be a reduced irreducible root system of rank $l \geq 2$, and R be a commutative ring.*

(a) Suppose that for subsystems $\Delta = \Delta_1, \Delta_l$ the elementary Chevalley group $E(\Delta, R)$ admits unitriangular factorisation

$$E(\Delta, R) = (U(\Delta, R)U^-(\Delta, R))^L.$$

Then the elementary Chevalley group $E(\Phi, R)$ admits unitriangular factorisation

$$E(\Phi, R) = (U(\Phi, R)U^-(\Phi, R))^L.$$

of the same length $2L$.

(b) Suppose that for subsystems $\Delta = \Delta_1, \Delta_l$ the elementary Chevalley group $E(\Delta, R)$ admits the Gauss decomposition

$$E(\Delta, R) = H(\Delta, R)U(\Delta, R)U^-(\Delta, R)) \cdots U^{\pm}(\Delta, R)$$

of length L. Then, the elementary Chevalley group $E(\Phi, R)$ admits the Gauss decomposition

$$E(\Phi, R) = H(\Phi, R)U(\Phi, R)U^-(\Phi, R)) \cdots U^{\pm}(\Phi, R)$$

of the same length L.

Clearly, Theorem 2 immediately follows from Theorem 5.2 and the rank 1 case; so, it only remains to prove Theorem 5.2.

Observation. If Y is a subset in $E(\Phi, R)$ and if X is a symmetric generating set satisfying $XY \subseteq Y$, then clearly $Y = G$.

Therefore, to prove (a), we will prove $XY \subseteq Y$ with $X = \{x_\alpha(\xi) \mid \alpha \in \pm\Pi,\ \xi \in R\}$ and $Y = (U(\Phi, R)U^-(\Phi, R))^L$. The proof of (b) is similar with the same X and $Y = H(\Phi, R)U(\Phi, R)U^-(\Phi, R) \cdots U^{\pm}(\Phi, R)$.

Proof of Theorem 5.2. As we noted, the group G is generated by the fundamental root elements $X = \{x_\alpha(\xi) \mid \alpha \in \pm\Pi,\ \xi \in R\}$. Thus, to prove (a), it suffices to prove that $XY \subseteq Y$ where $Y = (U(\Phi, R)U^-(\Phi, R))^L$.

Fix a fundamental root unipotent $x_\alpha(\xi)$. Since $\mathrm{rk}(\Phi) \geq 2$, the root α belongs to at least one of the subsystems $\Delta = \Delta_r$, where $r = 1$ or $r = l$, generated by all fundamental roots, except for the first or the last one, respectively. Set $\Sigma = \Sigma_r$ and express $U^{\pm}(\Phi, R)$ in the form

$$U(\Phi, R) = U(\Delta, R)U(\Sigma, R), \quad U^-(\Phi, R) = U^-(\Delta, R)U^-(\Sigma, R).$$

We see that

$$Y = (U(\Delta, R)U^-(\Delta, R))^L (U(\Sigma, R)U^-(\Sigma, R))^L.$$

Since $\alpha \in \Delta$, one has $x_\alpha(\xi) \in E(\Delta, R)$, so that the inclusion $x_\alpha(\xi)Y \subseteq Y$ immediately follows from the assumption. This completes the proof of theorem 5.2 (a). The proof of (b) is entirely similar with

$$Y = H(\Phi, R)U(\Phi, R)U^-(\Phi, R)\dots U^{\pm}(\Phi, R).$$

Remarks. To prove theorems 1 and 2, in theorem 5 above, one needs the decomposition of $E(\Delta, R)$ only for subsystems Δ whose union contains all the fundamental roots. These subsystems do not have to be terminal as in theorem 5.

References

[1] Abe, E., *Chevalley groups over local rings.* — Tôhoku Math. J. **21**, no. 3, (1969), 474–494.

[2] Abe, E. and Suzuki, K., *On normal subgroups of Chevalley groups over commutative rings.* — Tôhoku Math. J. **28**, no. 1, (1976), 185–198.

[3] Baoquan, Chen and Kaufman, A., 3D *volume rotation using shear transformations.* — Graph. Models **62** (2000), 308–322.

[4] Bilu, Y., *Quadratic factors of f(x)-g(y)*, Acta Arith. **90**, no. 4, (1999), 341–355.

[5] Huanyin, Chen and Miaosen, Chen, *On products of three triangular matrices over associative rings.* — Linear Algebra Applic. **387** (2004), 297–311.

[6] Cooke, G. and Weinberger, P. J., *On the construction of division chains in algebraic number rings, with applications to* SL_2, Commun. Algebra, **3** (1975), 481–524.

[7] Detinko, A. S., Flannery, D. L. and Hulpke, A., *Algorithms for arithmetic groups with the congruence subgroup property*, J. Algebra **421** (2015), 234–259.

[8] Erovenko, I. V. and Rapinchuk, A. S., *Bounded generation of some S-arithmetic orthogonal groups.* — C. R. Acad. Sci. **333**, no. 5, (2001), 395–398.

[9] Pengwei, Hao, *Customizable triangular factorizations of matrices*, Linear Algebra Applic., **382** (2004), 135–154.

[10] Iwahori, N. and Matsumoto, H., On some Bruhat decomposition and structure of the Hecke rings of p-adic Chevalley groups, Publ. Math. Inst. Haut. Etudes Sci. **25** (1965), 5–48.

[11] Kulkarni, M., Muller, P. & Sury, B., *Quadratic factors of f(x)-g(y)*, Indagationes Math., **18** (2007), 233–243.

[12] Lazard, M., *Groupes analytiques p-adiques* (French), Inst. Hautes tudes Sci. Publ. Math. **26** (1965), 389–603.

[13] Yang, Lei, Hao, Pengwei and Wu, Dapeng, *Stabilization and optimization of PLUS factorization and its application to image coding.* — J. Visual Communication & Image Representation **22**, no. 1, (2011), 9–22.

[14] Liehl, B., *Beschränkte Wortlänge in* SL_2. — Math. Z. **186** (1984), 509–524.

[15] Liebeck, M. and Pyber, L., *Finite linear groups and bounded generation.* — Duke Math. J. **107** (2001), 159–171.

[16] Lubotzky, A., *Subgroup growth and congruence subgroups*, Invent. Math. **119**, no. 2, (1995), 267–295.

[17] Niyomsataya, T., Miri, A. and Nevins, M., *An Application of the Bruhat Decomposition to the Design of Full Diversity Unitary SpaceTime Codes*, IEEE Transactions on Information Theory, **55**, (2009), 232–244.

[18] Nikolov N. and Sury, B., *Bounded generation of wreath products,* Journal of Group Theory, **18**, no. 6, (2015), 951–959.

[19] Odeh, O. H., Olesky, D. D. and Driessche, P. Van den, *Bruhat decomposition and numerical stability*, SIAM J. Matrix Anal. Appl. **19** (1998), 89–98.

[20] Paeth, A., *A fast algorithm for general raster rotation.* — In: Graphics Gems, Acad. Press (1990), 179–195.

[21] Platonov, V. P and Rapinchuk, A. S., *Abstract characterizations of arithmetic groups with the congruence property*, Soviet Math. Dokl. **44**, no. 1, (1992), 342–347.

[22] Platonov V. P. and Sury, B., *Adelic profinite groups* - Jour. of Algebra, **193** (1997), 757–763.

[23] Sury, B., *An interesting consequence of the Heisenberg construction*, Elemente der Mathematik, **63** (2008), 184–188.

[24] Sury, B., Some number-theoretic identities from group actions, Rendiconti del circolo matematico di Palermo, **58** (2009), 99–108.

[25] Sury, B., *Arithmetic groups and Salem numbers* - Manuscripta Math., **75** (1992), 97–102.

[26] Sury, B., *Bounded generation does not imply finite presentation* – Comm. Alg., **25** (1997), 1673–1683.

[27] Yiyuan, She and Pengwei, Hao, *On the necessity and sufficiency of PLUS factorizations*, Linear Algebra Applic., **400** (2005), 193–202.

[28] Smolensky, A. V., Sury, B. and Vavilov, N. A., Unitriangular factorizations of Chevalley groups, Zapiski Nauchnyh Seminarov POMI, **388** (2011), 17– 47(in Russian).
English translation: J. Math. Sci. (N. Y.) **183**, no. 5, (2012), 584–599. **Read G as E in the main theorems!**

[29] Smolensky, A. V., Sury, B. and Vavilov, N. A., *Gauss decomposition for Chevalley groups - Revisited,* International Journal of Group Theory, **1**, no. 1, (2012), 3–16.

[30] Stein, M. R., *Surjective stability in dimension* 0 *for* K_2 *and related functors*, Trans. Amer. Math. Soc., **178** (1973), 176–191.

[31] Sury, B. and Venkataramana, T. N., *Generators for all principal congruence subgroups of SL(n,Z) with* $n \geq 3$ - Proc. Amer Math. Soc., **122** (1994), 355–358.

[32] Tavgen, O. I., *Finite width of arithmetic subgroups of Chevalley groups of rank* ≥ 2, Soviet Math. Doklady, **41**, no. 1, (1990), 136–140.

[33] Tavgen, O. I., *Bounded generation of normal and twisted Chevalley groups over the rings of S-integers*, Contemp. Math., **131**, no. 1, (1992), 409–421.

[34] Toffoli, T., and Quick, J., *Three dimensional rotations by three shears.* — Graphical Models & Image Processing **59** (1997), 89–96.

B. Sury
Statistics & Mathematics Unit, Indian Statistical Institute
8th Mile Mysore Road, Bangalore-560 059, India
E-mail: *sury@ms.isibang.ac.in*