Записки научных
семинаров ПОМИ
Том 479, 2019 г.

N. Vavilov

COMMUTATORS OF CONGRUENCE SUBGROUPS IN THE ARITHMETIC CASE

Abstract. In our joint paper with Alexei Stepanov it was established that for any two comaximal ideals A and B of a commutative ring R, $A+B=R$, and any $n \geqslant 3$ one has $[E(n,R,A),E(n,R,B)]=E(n,R,AB)$. Alec Mason and Wilson Stothers constructed counterexamples that show that the above equality may fail when A and B are not comaximal, even for such nice rings as $\mathbb{Z}[i]$. In the present note, we establish a rather striking result that this equality, and thus also the stronger equality $[\mathrm{GL}(n,R,A),\mathrm{GL}(n,R,B)]=E(n,R,AB)$, do hold when R is a Dedekind ring of arithmetic type with *infinite* multiplicative group. The proof is a blend of elementary calculations in the spirit of the previous papers by Wilberd van der Kallen, Roozbeh Hazrat, Zuhong Zhang, Alexei Stepanov, and the author, and an explicit computation of multirelative SK_1 from my 1982 paper, which in turn relied on very deep arithmetical results by Jean-Pierre Serre, and Leonid Vaserstein (as corrected by Armin Leutbecher and Bernhard Liehl).

To my dear friend and colleague Alexander Generalov, with admiration and gratitude

§1. Introduction

Let R be a commutative ring with 1, $G=\mathrm{GL}(n,R)$ be the general linear group of degree $n \geqslant 3$ over R. For an ideal $I \trianglelefteq R$ denote by $E(n,I)$ the corresponding elementary subgroup, generated by the elementary transvections of level I:

$$E(n,I)=\big\langle t_{ij}(a), a \in I, 1 \leqslant i \neq j \leqslant n\big\rangle.$$

The corresponding relative elementary subgroup $E(n,R,I)$ is defined as the normal closure of $E(n,I)$ in the absolute elementary subgroup $E(n,R)$.

Further, consider the reduction homomorphism

$$\rho_I : \mathrm{GL}(n,R) \longrightarrow \mathrm{GL}(n,R/I)$$

Key words and phrases: general linear group, congruence subgroups, elementary subgroups, standard commutator formulae, Dedekind rings of arithmetic type.

This publication is supported by Russian Science Foundation grant 17-11-01261.

modulo I. By definition, the principal congruence subgroup $\mathrm{GL}(n,R,I)$ is the kernel of ρ_I. In other words, $\mathrm{GL}(n,R,I)$ consists of all matrices $g \in \mathrm{GL}(n,R)$ congruent to e modulo I. Further, the full congruence subgroup $C(n,R,I)$ is the full pre-image of the centre of $\mathrm{GL}(n,R/I)$ with respect to ρ_I. In other words, $C(n,R,I)$ consists of all matrices $g \in \mathrm{GL}(n,R)$ congruent to a scalar matrix modulo I.

A decade ago Alexei Stepanov and myself obtained the following results, the birelative standard commutator formula, Theorem 4 of [47], and precise computation of the birelative elementary commutator subgroup in the special case of comaximal ideals, Theorem 5 of [47].

Theorem A. *Let A and B be two ideals of a commutative ring R and $n \geqslant 3$. Then*

$$\big[E(n,R,A),C(n,R,B)\big] = \big[E(n,R,A),E(n,R,B)\big].$$

Theorem B. *Let A and B be two comaximal ideals of a commutative ring R, $A+B=R$, and $n \geqslant 3$. Then*

$$\big[E(n,R,A),C(n,R,B)\big] = E(n,R,AB).$$

These results, and the preceding result by Hong You [50][1] unified and generalised a great number of keynote results by Bass, Mason and Stothers, Suslin, Vaserstein, Borewicz and myself, and many others, see, in particular [2,4,24,25,37,41] and a complete bibliography of early papers in [8,12,48]. These results were then expanded in several directions by Stepanov and myself, Hazrat and Zuhong Zhang, see [9–11, 13–19, 31–34, 45–47, 49].

One of our starting points in that work was the following significant result by Mason and Stothers, [25], Theorem 3.6 and Corollary 3.9, or [24] Theorem 1.3, which established a *stronger* commutator formula, however not for all commutative rings, but *at the stable level*. One can find an easy modern proof in [17], Theorem 13.

Theorem C. *Let A and B be two ideals of a commutative ring R and $n \geqslant \max(\mathrm{sr}(R)+1,3)$. Then*

$$\big[\,\mathrm{GL}(n,R,A),\mathrm{GL}(n,R,B)\big] = \big[E(n,R,A),E(n,R,B)\big].$$

In the special case of *comaximal* ideals in a Dedekind ring of arithmetic type, this result can be made even more precise, see [25], Theorem 5.1

[1] Of which we were not aware at the time of writing [18, 46, 47], see the discussion in [14].

Theorem D. *Let A and B be two comaximal ideals of a Dedekind ring of arithmetic type $R = \mathcal{O}_S$, $A + B = R$ and $n \geqslant 3$. Then*

$$\big[\mathrm{GL}(n, R, A), \mathrm{GL}(n, R, B)\big] = E(n, R, AB).$$

The proof of this last result relied on the full force of the work by Bass, Milnor and Serre [3] on the congruence subgroup problem. Also, Mason and Stothers gave examples which show that the equality in this theorem — and even the weaker equality in our Theorem 2 — may fail when A and B are not comaximal.

The simplest such counter-example is $A = B = (1 + i)^3 R$, where $R = \mathbb{Z}[i]$ in the ring of Gaussian integers. In this case the relative elementary subgroup $E(n, R, A^2)$ in the right hand side has index 2 in $[E(n, R, A), E(n, R, A)]$, see [24, 25] and [9, 17]. A similar counter-example $A = B = 2(1 + 2\omega)R$ can be constructed also in the ring $R = \mathbb{Z}[\omega]$ of Eisensteinian integers.

Quite amazingly, in the arithmetic case these are essentially the only such counter-examples! Namely, in the case of Dedekind rings of arithmetic type $R = \mathcal{O}_S$ with *infinite* multiplicative group (or, what is the same, $|S| \geqslant 2$) the claim of Theorem 2 remains valid for *all* pairs of ideals.

Theorem 1. *Let A and B be two ideals of a Dedekind ring of arithmetic type $R = \mathcal{O}_S$. Assume that the multiplicative group R^* is infinite and that $n \geqslant 3$. Then*

$$\big[\mathrm{GL}(n, R, A), \mathrm{GL}(n, R, B)\big] = E(n, R, AB).$$

Here, again the main difficulty was not to write up the proof, but simply to convince oneself that such a theorem could hold as stated. The proof proceeds as follows. First of all, we invoke the above Theorem C and the following recent unrelativisation result, [45], Theorem 2 (or more general [49], Theorem 1).

Theorem E. *Let A and B be two ideals of a commutative ring R, $n \geqslant 3$. Then*

$$\big[E(n, A), E(n, B)\big] = \big[E(n, R, A), E(n, R, B)\big].$$

In view of these two results, it only remains to to prove the following.

Theorem 2. *Let A and B be two ideals of a Dedekind ring of arithmetic type $R = \mathcal{O}_S$. Assume that the multiplicative group R^* is infinite and that $n \geqslant 3$. Then*

$$\big[E(n, A), E(n, B)\big] = E(n, R, AB).$$

Let us mention the following important special case, where the proof is quite a bit easier, which I noticed first, looking at the papers [27, 28].

Corollary. *Let I be an ideal of a Dedekind ring of arithmetic type $R = \mathcal{O}_S$. Assume that the multiplicative group R^* is infinite and that $n \geqslant 3$. Then*

$$\big[E(n, I), E(n, I)\big] = E(n, R, I^2).$$

Then, trying to reconcile it with Theorem B, I inevitably arrived the above results.

The rest of this paper is dedicated to the proof of Theorem 2. It consists of two parts. First, we relate the left hand side with another elementary subgroup defined in terms of ideals A and B, namely with

$$\mathrm{EE}(n, A, B) = \big\langle U(n, A), U^-(n, B)\big\rangle,$$

where $U(n, A)$ and $U^-(n, B)$ are the upper and lower unitriangular subgroups, with parameters in A and B, respectively. See §§2, 3 for notation and precise definitions of these and further relative and birelative subgroups. (Observe that $\mathrm{EE}(n, I, I) = E(n, I)$.)

This is done by elementary but somewhat bizarre calculations expressing all elementary generators of $[E(n, A), E(n, B)]$ in terms of some of them, *à la* Wilberd van der Kallen [20], Lemma 2.2, or its extension to all Chevalley groups in the work of Alexei Stepanov [31], Theorem 3.4, etc. However, since now we are interested in the case of *two* ideals, we have a further type of generators to deal with, so that our calculations are even fancier than that, see §4. In particular, there I prove the following result, which is the main new step towards the proof of Theorem 2.

Theorem 3. *Let A and B be two ideals of a commutative ring R and $n \geqslant 3$. Then*

$$\big[E(n, A), E(n, B)\big] \leqslant \mathrm{EE}(n, A, B).$$

So far, all results were general, and apply to all commutative rings. In § 5 the fun starts. Namely, let $R = \mathcal{O}_S$ be a Dedekind ring of arithmetic type and let $\mathrm{SF}(n, A, B)$ be the minimal congruence subgroup in $\mathrm{SL}(n, R)$ containing $\mathrm{EE}(n, A, B)$. It can be described as follows. First, let $G(n, A, B)$ be the subgroup defined by congruences $g_{ij} \in A$ for $i < j$ and $g_{ij} \in B$ for $i > j$. Inside $G(n, A, B)$ the subgroup $F(n, A, B)$ is defined by the congruences $g_{ii} \equiv 1 \,(\mathrm{mod}\ AB)$ and $\mathrm{SF}(n, A, B)$ is its intersection with $\mathrm{SL}(n, R)$, see § 3 for details. Then one of the main results of my ancient paper [44], Theorem 2, gives in particular the following computation of the

birelative SK_1 which, combined with the above results, implies Theorem 2.

Theorem F. *Let A and B be two ideals of a Dedekind ring of arithmetic type $R = \mathcal{O}_S$. Assume that the multiplicative group R^* is infinite and that $n \geqslant 3$. Then*

$$\mathrm{SF}(n, A, B)/\,\mathrm{EE}(n, A, B) \cong \mathrm{SK}_1(R, AB).$$

The proof of this result in [43, 44] depended on deep arithmetic results pertaining to the case of $\mathrm{SL}(2, R)$, due to Serre, Vaserstein, Leutbecher and Liehl [22,23,30,40]. In fact, the main results of [44], were much more general than that. They applied to the elementary subgroup $E(\sigma)$ corresponding to any net $\sigma = (\sigma_{ij})$, $1 \leqslant i, j \leqslant n$, of non-zero ideals $\sigma_{ij} \trianglelefteq R$.

Finally, in § 6 we collect some further related observations, and state some unsolved problems.

§2. Notation

For two subgroups $F, H \leqslant G$, we denote by $[F, H]$ their mutual commutator subgroup spanned by all commutators $[f, h]$, where $f \in F$, $h \in H$. Observe that our commutators are always left-normed, $[x, y] = xyx^{-1}y^{-1}$. The double commutator $[[x, y], z]$ will be denoted simply by $[x, y, z]$. Further, ${}^x y = xyx^{-1}$ denotes the left conjugate of y by x. In the sequel we repeatedly use obvious commutator identities such as $[y, x] = [x, y]^{-1}$, or $[xy, z] = {}^x[y, z]\cdot[x, z]$ and $[x, yz] = [x, y]\cdot{}^y[x, z]$, mostly without any specific reference.

Let, as in the introduction, R be any commutative ring with 1 and $\mathrm{GL}(n, R)$ be the corresponding general linear group of degree $n \geqslant 2$. As usual, e denotes the identity matrix and e_{ij} is a standard matrix unit. For $c \in R$ and $1 \leqslant i \neq j \leqslant n$, we denote by $t_{ij}(c) = e + ce_{ij}$, the corresponding [elementary] transvection. A matrix $g \in \mathrm{GL}(n, R)$ is written as $g = (g_{ij})$, $1 \leqslant i, j \leqslant n$, where g_{ij} is its entry in the position (i, j). Entries of the inverse matrix $g^{-1} = (g'_{ij})$, $1 \leqslant i, j \leqslant n$, are denoted by g'_{ij}.

Let $U(n, R)$ and $U^-(n, R)$ be the groups of upper unitriangular and lower unitriangular matrices, respectively. These are unipotent radicals of the standard Borel subgroup, and its opposite Borel subgroup. They can be defined either by equations

$$U(n, R) = \big\{g = (g_{ij}) \in \mathrm{GL}(n, R) \mid g_{ij} = 0, i > j,\ g_{ii} = 1\big\},$$

$$U^-(n, R) = \big\{g = (g_{ij}) \in \mathrm{GL}(n, R) \mid g_{ij} = 0, i < j,\ g_{ii} = 1\big\},$$

or by generators

$$U(n,R) = \big\langle t_{ij}(c),\ 1 \leqslant i < j \leqslant n,\ c \in R \big\rangle,$$

$$U^-(n,R) = \big\langle t_{ij}(c),\ 1 \leqslant j < i \leqslant n,\ c \in R \big\rangle.$$

Clearly, $E(n,R) = \langle U(n,R), U^-(n,R) \rangle$.

Let $I \trianglelefteq R$ be an ideal of R. Some of the relative subgroups of level I were already defined in the introduction. In particular, the unrelative elementary group $E(n,I)$ and the relative elementary group $E(n,R,I)$ of level I. One denotes $z_{ij}(a,c) = {}^{t_{ji}(c)}t_{ij}(a)$. The following result on generation of $E(n,R,I)$ as a subgroup was first stated in [39, 41, 42].

Lemma 1. *Let $I \trianglelefteq R$ be an ideal of a commutative ring, $n \geqslant 3$. Then*

$$E(n,R,I) = \big\langle z_{ij}(a,c),\ 1 \leqslant i \neq j \leqslant n,\ a \in I,\ c \in R \big\rangle.$$

In terms of reduction modulo I we defined there the principal and the full congruence subgroups of level I:

$$\begin{aligned} \mathrm{GL}(n,R,I) = \big\{ g = (g_{ij}) \in \mathrm{GL}(n,R) \mid {} & g_{ij} \equiv 0 \,(\mathrm{mod}\ I)\,, \\ & i \neq j,\ g_{ii} \equiv 1 \,(\mathrm{mod}\ I) \big\}, \\ C(n,R,I) = \big\{ g = (g_{ij}) \in \mathrm{GL}(n,R) \mid {} & g_{ij} \equiv 0 \,(\mathrm{mod}\ I)\,, \\ & g_{ii} \equiv g_{jj} \,(\mathrm{mod}\ I)\,,\ i \neq j, \big\}. \end{aligned}$$

Further, let $\mathrm{SL}(n,R)$ be the special linear group of degree n over R, consisting of all matrices $g \in \mathrm{GL}(n,R)$ with $\det(g) = 1$. We denote by $\mathrm{SL}(n,R,I)$ and $\mathrm{SC}(n,R,I)$ the corresponding principal and full congruence subgroups,

$$\mathrm{SL}(n,R,I) = \mathrm{GL}(n,R,I) \cap \mathrm{SL}(n,R), \quad \mathrm{SC}(n,R,I) = C(n,R,I) \cap \mathrm{SL}(n,R).$$

Suslin's normality theorem (the special case of Theorem A where $B = R$) asserts that for $E(n,R,I) \trianglelefteq \mathrm{GL}(n,R)$, whenever $n \geqslant 3$. In particular, we can define the quotients

$$K_1(n,R,I) = \mathrm{GL}(n,R,I)/E(n,R,I),$$
$$\mathrm{SK}_1(n,R,I) = \mathrm{SL}(n,R,I)/E(n,R,I).$$

The same notation will be used for $n = 2$, but in this case these are not groups, in general, just pointed sets.

§3. Groups $\mathrm{EE}(n,A,B)$ and $F(n,A,B)$

Let $A,B \trianglelefteq R$ be two ideals of a commutative ring R. We define the two following congruence subgroups modulo (A,B). Both of them consist of matrices, whose entries above the principal diagonal belong to A, whereas the entries below the principal diagonal belong to B. The difference is that for the first one of them the diagonal entries are congruent to 1 modulo the product AB, whereas for the second one no conditions are imposed on the diagonal entries:

$$\begin{aligned} F(n,A,B) = \big\{g=(g_{ij}) \in \mathrm{GL}(n,R) \mid g_{ij} \equiv 0 \,(\mathrm{mod}\ A)\,,\ i<j,\\ g_{ij} \equiv 0 \,(\mathrm{mod}\ B)\,,\ i>j,\ g_{ii} \equiv 1 \,(\mathrm{mod}\ AB)\big\},\\ G(n,A,B) = \big\{g=(g_{ij}) \in \mathrm{GL}(n,R) \mid g_{ij} \equiv 0 \,(\mathrm{mod}\ A)\,,\ i<j,\\ g_{ij} \equiv 0 \,(\mathrm{mod}\ B)\,,\ i>j\big\}. \end{aligned}$$

In this context, we use the prefix "S" in the same meaning as above, to denote intersetcions with the corresponding special linear groups:

$$\begin{aligned} \mathrm{SF}(n,A,B) &= F(n,A,B) \cap \mathrm{SL}(n,R),\\ \mathrm{SG}(n,A,B) &= G(n,A,B) \cap \mathrm{SL}(n,R). \end{aligned}$$

In the special case, where $A=B=I$ the above congruence subgroups boil down to the *true congruence subgroup* $F(n,I)$ of level I and the *brimming congruence subgroup* $G(n,I)$ of level I

$$\begin{aligned} F(n,I) &= \big\{g=(g_{ij}) \in \mathrm{GL}(n,R) \mid g_{ij} \equiv 0 \,(\mathrm{mod}\ I)\,,\ i\neq j,\ g_{ii} \equiv 1 \,(\mathrm{mod}\ I^2)\big\},\\ G(n,I) &= \big\{g=(g_{ij}) \in \mathrm{GL}(n,R) \mid g_{ij} \equiv 0 \,(\mathrm{mod}\ I)\,,\ i\neq j\big\}. \end{aligned}$$

Observe that $F(n,I)$ is sometimes called the *unrelativised* congruence subgroup and denoted by $\mathrm{GL}(n,I)$. On the other hand (following Tits [39]) Nica [28] uses the notation $F(n,R,I)$ to denote $E(n,I)$.

Further, set

$$U(n,I) = U(n,R) \cap \mathrm{GL}(n,R,I), \quad U^-(n,I) = U^-(n,R) \cap \mathrm{GL}(n,R,I).$$

Clearly,

$$\begin{aligned} U(n,I) &= \big\langle t_{ij}(a),\ 1 \leqslant i < j \leqslant n,\ a \in I \big\rangle,\\ U^-(n,I) &= \big\langle t_{ij}(a),\ 1 \leqslant j < i \leqslant n,\ a \in I \big\rangle. \end{aligned}$$

Now, let A and B be two ideals of R. We introduce the main protagonist of all subsequent calculations:

$$\mathrm{EE}(n,A,B)=\big\langle U(n,A),U^-(n,B)\big\rangle.$$

This is a straightforward generalisation of the unrelativised elementary subgroup $E(n,I)$. Indeed, when $A=B=I$ one gets $\mathrm{EE}(n,I,I)=E(n,I)$.

In the proof of Theorem 1 we need the following lemma. Actually, when R is a Dedekind ring and $n\geqslant 3$ it immediately follows from the characterisation of $F(n,A,B)$ as the smallest congruence subgroup containing $\mathrm{EE}(n,A,B)$. But since it is so easy also in the general case, we reproduce the proof.

Lemma 2. *Let A and B be two ideals of a commutative ring R, $n\geqslant 2$. Then*

$$F(n,A,B)=\mathrm{EE}(n,A,B)\cdot\mathrm{GL}(n,R,AB).$$

Proof. Let $g=(g_{ij})\in F(n,A,B)$. First, we clear its entries above the principal diagonal by elementary transformations from $\mathrm{EE}(n,A,B)$. With this end form the matrix $u=(u_{ij})$ by setting $u_{ij}=g_{ij}$ for $i<j$, and $u_{ij}=\delta_{ij}$ otherwise. Clearly, by the very definition of $F(n,A,B)$ one has $u\in U(n,A)\leqslant\mathrm{EE}(n,A,B)$ and $g\equiv u\,(\mathrm{mod}\ B)$.

Thus, $gu^{-1}\in F(n,A,B)\cap\mathrm{GL}(n,R,B)$ and now we can do the same with the entries below the principal diagonal. Form the matrix $v=(v_{ij})$ by setting $v_{ij}=(gu^{-1})_{ij}$ for $i>j$, and $v_{ij}=\delta_{ij}$ otherwise. Clearly, by the very definition of $F(n,A,B)$ one has $v\in U^-(n,B)\leqslant\mathrm{EE}(n,A,B)$ and $gu^{-1}\equiv v\,(\mathrm{mod}\ A)$. Since already $gu^{-1}\equiv v\equiv e\,(\mathrm{mod}\ B)$, one has $gu^{-1}v^{-1}\in\mathrm{GL}(n,R,AB)$, as claimed. □

§4. Proof of Theorem 3

Now, we are starting to compare the groups $[E(n,A),E(n,B)]$ and $\mathrm{EE}(n,A,B)$. Mostly, the corresponding calculations are already contained in the previous papers by Wilberd van der Kallen, Roozbeh Hazrat, Alexei Stepanov, Zuhong Zhang, and myself.

The following result is [17], Lemma 1A. However, what we need for the sequel, is not this statement, but the first paragraph of its proof.

Lemma 3. *Let A and B be two ideals of a commutative ring R, $n\geqslant 3$. Then*

$$E(n,R,AB)\leqslant\big[E(n,A),E(n,B)\big].$$

The next result can be extracted from the proof of [45], Theorem 1, but was first stated in this form as the Main Lemma of [49], in the context of Chevalley groups.

Lemma 4. *Let A and B be two ideals of a commutative ring R, $n \geqslant 3$. Then as a group $[E(n,A),E(n,B)]$ is generated by $E(n,R,AB)$ and the elementary commutators $[t_{ij}(a),t_{ji}(b)]$, where $1 \leqslant i \neq j \leqslant n$, $a \in A$, $b \in B$.*

Let us state a result by Wilberd van der Kallen, [20], Lemma 2.2. Morally, it is a trickier and mightier version of Lemma 1, with a smaller set of generators.

Lemma 5. *Let $I \trianglelefteq R$ be an ideal of a commutative ring, $n \geqslant 3$. Then as a subgroup $E(n,R,I)$ is generated by $E(n,I)$ and $z_{ih}(a,c)$, for a fixed $1 \leqslant h \leqslant n$, and all $i \neq h$, $a \in I$, $c \in R$.*

Alternatively, one could take as extra generators $z_{hj}(a,c)$, for a fixed $1 \leqslant h \leqslant n$, and all $j \neq h$. This lemma served as an inspiration for Stepanov's much more general results, see for instance [33], Theorem 2.2. Of course, Stepanov proves such similar results for all Chevalley groups, and not just for U and U^-, as we need, or for U_1 and U_1^-, as van der Kallen does, but rather for the unipotent radicals U_P and U_P^- of an arbitrary parabolic subgroup P and its opposite. Besides, when 2 is not invertible in R, symplectic groups require some additional care, and some of the statements have to be modified in this case.

The following lemma is a typical result of Stepanov's "elementary calculus", developed with this end, see [31], Lemma 2.1.

Lemma 6. *Let A and B be two ideals of a commutative ring R, $n \geqslant 3$. Then*

$$E(n,AB) \leqslant \mathrm{EE}(n,A,B).$$

For actual calculations it is usually more expedite to use it in the following slightly more precise form [33], Lemma 2.1.

Lemma 7. *Let A and B be two ideals of a commutative ring R, $n \geqslant 3$. Then*

$$E(n,AB) \leqslant \big[U(n,A),U^-(n,B)\big] \cdot U(n,AB) \cdot U^-(n,AB).$$

Now, we can summarise Lemmas 3, 5 and 6.

Lemma 8. *Let A and B be two ideals of a commutative ring R, $n \geqslant 3$. Then*

$$E(n, R, AB) \leqslant \mathrm{EE}(n, A, B).$$

Proof. From Lemma 6 we already know that $E(n, AB) \leqslant \mathrm{EE}(n, A, B)$. Next, we wish to show that $z_{ij}(ab, c)$, where $1 \leqslant i \neq j \leqslant n$, $a \in A$, $b \in B$, $c \in R$, also belong to $\mathrm{EE}(n, A, B)$.

Assume that $(i, j) \neq (1, n), (n, 1)$. Then there exists either $h > i, j$ or $h < i, j$. In the first case express $t_{ij}(ab)$ as

$$t_{ij}(ab) = \big[t_{ih}(a), t_{hj}(b)\big] \in \big[U(n, A), U^-(n, B)\big].$$

Similarly, in the second case express one has

$$t_{ij}(ab) = \big[t_{ih}(b), t_{hj}(a)\big] \in \big[U^-(n, B), U(n, A)\big].$$

Up to switching the ideals A and B, we can assume, we are in the first case. Then, clearly,

$$z_{ij}(ab, c) = {}^{t_{ji}(c)}t_{ij}(ab) = {}^{t_{ji}(c)}\big[t_{ih}(a), t_{hj}(b)\big] = \big[{}^{t_{ji}(c)}t_{ih}(a), {}^{t_{ji}(c)}t_{hj}(b)\big].$$

Clearly, the commutator on the right hand side again belongs to

$$\big[U(n, A), U^-(n, B)\big] \leqslant \mathrm{EE}(n, A, B).$$

This shows that all of the above relative elementary generators $z_{ij}(ab, c)$, apart maybe from $z_{1n}(ab, c)$ and $z_{n1}(ab, c)$, also belong to $\mathrm{EE}(n, A, B)$. Anyway, there are enough of those inside $\mathrm{EE}(n, A, B)$ to be able to apply Lemma 4: just take any $h \neq 1, n$, then all $z_{ih}(ab, c)$ belong to $\mathrm{EE}(n, A, B)$. □

Now, we are all set to finish the proof of Theorem 3.

Proof. By Lemma 8, the group $\mathrm{EE}(n, A, B)$ contains $E(n, R, AB)$. Also, by the very definition, $\mathrm{EE}(n, A, B)$ contains half of the elementary commutators, namely, those of the form $[t_{ij}(a), t_{ji}(b)]$, where $i < j$, $a \in A$, $b \in B$.

By Lemma 3 it only remains to prove that the other half of the elementary commutators, those of the form $[t_{ij}(a), t_{ji}(b)]$, where $i > j$, $a \in A$, $b \in B$, also belong to $\mathrm{EE}(n, A, B)$. This is done by the switching trick standard in the works on bounded generation (see, for instance, [5, 29, 38]), when by elementary moves the entries a and b are interchanged by rolling them over to a different position. A very similar calculation is also hidden inside the proof of the main Theorem in [21], and it would be interesting to understand the common source of this.

Namely, rewrite the above problematic elementary commutator with $i > j$ as

$$z = \big[t_{ij}(a), t_{ji}(b)\big] = t_{ij}(a) \cdot {}^{t_{ji}(b)}t_{ij}(-a) = t_{ij}(a) \cdot {}^{t_{ji}(b)}\big[t_{ih}(a), t_{hj}(-1)\big].$$

Expanding the conjugation by $t_{ji}(b)$, we see that

$$z = t_{ij}(a)\cdot\big[{}^{t_{ji}(b)}t_{ih}(a), {}^{t_{ji}(b)}t_{hj}(-1)\big] = t_{ij}(a)\cdot[t_{jh}(ab)t_{ih}(a), t_{hj}(-1)t_{hi}(b)\big].$$

Now, the first factor $t_{jh}(ab)$ of the first argument in this last commutator already belongs to the group $E(n, R, AB)$ which is contained in $\mathrm{EE}(n, A, B)$ by the previous lemma. Since $E(n, R, AB)$ is by the very definition normal in the absolute elementary group $E(n, R)$, in the sequel we can argue modulo $E(n, R, AB)$: at the moment, we see anything from $E(n, R, AB)$, we can drop it, since pulling it out from our expression to the right, we still get something from $E(n, R, AB) \leqslant \mathrm{EE}(n, A, B)$.

Thus,

$$z \equiv t_{ij}(a) \cdot \big[t_{ih}(a), t_{hj}(-1)t_{hi}(b)\big] \,(\mathrm{mod}\ E(n, R, AB))\,,$$

and it remains to satisfy ourselves that this last expression belongs to $\mathrm{EE}(n, A, B)$. Using multiplicativity of the commutator w.r.t. the second argument, we see that

$$z \equiv t_{ij}(a) \cdot \big[t_{ih}(a), t_{hj}(-1)\big] \cdot {}^{t_{hj}(-1)}\big[t_{ih}(a), t_{hi}(b)\big] \,(\mathrm{mod}\ E(n, R, AB))\,.$$

Now, the first two factors of the last expression cancel, and if we have chosen h wisely, $[t_{ih}(a), t_{hi}(b)]$ belongs to $\mathrm{EE}(n, A, B)$ by the very definition. The only case, when it cannot be done is $i = n$, so that you cannot roll z forwards. But in that case we would have started rewriting the commutator z differently, as

$$z = \big[t_{ij}(a), t_{ji}(b)\big] = {}^{t_{ij}(a)}t_{ji}(b) \cdot t_{ji}(-b) = {}^{t_{ij}(a)}\big[t_{jh}(b), t_{hi}(1)\big] \cdot t_{ji}(-b),$$

to eventually roll it over backwards.

But since $[t_{ih}(a), t_{hi}(b)]$ already belongs to $\mathrm{GL}(n, R, AB) \cap \mathrm{EE}(n, A, B)$, conjugation by $t_{hj}(-1)$ does not change anything, since

$${}^{t_{hj}(-1)}\big[t_{ih}(a), t_{hi}(b)\big] = t_{ij}(-a^2b)t_{hj}(-ab) \cdot \big[t_{ih}(a), t_{hi}(b)\big]$$

again belongs to $\mathrm{EE}(n, A, B)$, as claimed. □

§5. Proof of Theorem 2

So far, all results pertained to all commutative rings. However, there is no hope to explicitly compute the values of K_1-functors, or the mutual commutator subgroups $[E(n,A),E(n,B)]$ in similar generality. Starting from this point, we assume that $R=\mathcal{O}_S$ is a Dedekind ring of arithmetic type.

Let K be a global field, i. e. a finite extension either of $\mathbb{Q}$, the *number case*, or of $\mathbb{F}_q(t)$, the *function case*. Further, let S be a finite set of places (non-equivalent valuations) of K, which contains all Archimedian places in the number case. For a non-Archimedian valuation $\mathfrak{p}$ of K we denote by $v_{\mathfrak{p}}$ the corresponding exponent. As usual, $R=\mathcal{O}_S$ denotes the ring consisting of $x\in K$ such that $v_{\mathfrak{p}}(x)\geqslant 0$ for all valuations $\mathfrak{p}$ of K that do not belong to S. Such a ring is called Dedekind ring of arithmetic type determined by the set of places S of the field K. In the number case they are also called Hasse domains. By Dirichlet's unit theorem, the multiplicative group $\mathcal{O}_S^*$ of $\mathcal{O}_S$ is infinite if and only if $|S|\geqslant 2$.

Another important auxiliary result is the following normality theorem, which is a very special case of [44], Theorem 1.

Lemma 9. *Let A and B be two ideals of a Dedekind ring of arithmetic type $R=\mathcal{O}_S$. Assume that the multiplicative group R^* is infinite and that $n\geqslant 3$. Then $\mathrm{EE}(n,A,B)$ is normal in $G(n,A,B)$.*

Now, we are in position to finish the proof of Theorem 2.

Combining Lemma 2, Lemma 8 and Lemma 9, we see that there is a surjective homomorphism

$$\mathrm{SK}_1(n,R,AB)=\mathrm{SL}(n,R,AB)/E(n,R,AB)\longrightarrow \mathrm{SF}(n,A,B)/\,\mathrm{EE}(n,A,B).$$

On the other hand, since $\mathrm{SK}_1(n,R,AB)$ are finite cyclic groups by [3], Theorem F implies this is an isomorphism, or, what is the same, that

$$\mathrm{SL}(n,R,AB)\cap \mathrm{EE}(n,A,B)=E(n,R,AB),$$

On the other hand, by Lemma 3 the relative commutator subgroup $[E(n,A),E(n,B)]$ sits in the sandwich of level AB,

$$E(n,R,AB)\leqslant [E(n,A),E(n,B)]\leqslant \mathrm{SL}(n,R,AB),$$

and it remains to compare it with Theorem 3, which asserts that

$$[E(n,A),E(n,B)]\leqslant \mathrm{EE}(n,A,B).$$

It follows that

$$[E(n,A),E(n,B)] \leqslant \mathrm{SL}(n,R,AB) \cap \mathrm{EE}(n,A,B) = E(n,R,AB).$$

Combining the last inclusions we see that $[E(n,A),E(n,B)]=E(n,R,AB)$ as claimed.

Theorem 1 is simply a conjunction of Theorems C, D and 2.

§6. Final remarks

As we already mentioned in the introduction, our main results *fail* when R is the ring of integers of a quadratic imaginary field. However, it should be very easy to verify them for $\mathrm{SL}(n,\mathbb{Z})$, $n \geqslant 3$. In the special case $A = B = I$ this is indeed done by Jens Mennicke [27] and Bogdan Nica [28], see also [36]. They prove that in this case $F(n,I) = E(n,I)$, which amounts to the positive solution of the congruence subgroup problem. In our situation of a Dedekind ring of arithmetic type R with infinite multiplicative group one has $F(n,I)/E(n,I) \cong \mathrm{SK}_1(n,R,I^2)$, for $n = 2$ by Vaserstein [40] and for $n \geqslant 3$ by myself [44].

It would be natural to try to generalise these results to other groups. This is not quite as trivial as it seems, since in most cases many of the preliminary results are not yet there.

Problem 1. *Generalise results of the present paper to Chevalley groups.*

It seems that for Theorem 3 such a generalisation would be mostly an exercise. Most of the requisite commutator calculus was already developed in our joint papers with Roozbeh Hazrat and Zuhong Zhang [14, 15, 49], whereas the elementary calculus at the level of unipotent radicals of parabolic subgroups can be found in the papers by Alexei Stepanov [31–34]. Theorem E is established in [15, 49] and after that it would take 3–4 pages of calculations to prove an analogue of Theorem 3 in this generality.

On the other hand, I am not aware of a full-scale analogue of Theorem C in such generality (however, for small dimensional rings it should mostly follow from the general commutator formula, see [34]). Most importantly, even to establish Theorem 2 one has to first prove an analogue of Theorem F. For Dedekind rings most of the necessary stability results were already established in [3, 26]. But there are some complications in the symplectic case. In exactly the same way as in [44] one can easily prove that the $2'$-parts of the occurring groups are isomorphic. But establishing isomorphism of the 2-parts would require somewhat more detailed calculations in $\mathrm{Sp}(4,R)$.

As we know from the work of Vaserstein and others [22, 23, 40], for Dedekind rings of arithmetic type with infinite multiplicative group the isomorphism

$$F(2, A, B)/\operatorname{EE}(2, A, B) \cong \operatorname{SK}_1(2, R, AB)$$

holds already for $n = 2$. Nevertheless, it would be extremely difficult to fully generalise the main results of the present paper to this case. In fact, computation of commutators in SL_2 over rings becomes quite tricky in the presence of residue fields of 2 or 3 elements. The peculiarities of the SL_2 case are discussed in a great number of papers, notably in the very profound and intricate papers by Douglas Costa and Gordon Keller, see, for instance, [6] and especially [7], which expressly addresses the arithmetic case.

Let us state another question that naturally suggests itself, a generalisation of Lemma 9.

Problem 2. *Let A and B be two ideals of a commutative ring R, $n \geqslant 3$. Prove that $\operatorname{EE}(n, A, B)$ is normal in $G(n, A, B)$.*

It is essentially a minor variation of the (morally) much more general [4], Theorem 3. It seems that is should immediately follow from Suslin's factorisation [37], in the form it was used by Zenon Borewicz and myself [4], § 7, compare also [1]. But it is not the case, some of the factors $v(i, j)$, in the notation of [4], do not obviously belong to $\operatorname{EE}(n, A, B)$. In [4] these recalcitrant factors were subdued by stipulating that the elementary subgroup $E(\sigma)$ was major: for each index i there were two other distinct indices j, h, both of them distinct from i, such that $E(\sigma)$ contained *all* elementary transvections from the copy of $\mathrm{SL}(3, R)$ in the rows and columns i, j, h, not just the ones with parameters in ideals. The special case $A = B = I$ of the problem was solved by Nica [28], Theorem 2. To supress these obstinate factors, he rolls them over to another position, in essentially the same way as above, towards the very end of the proof of Theorem 3. However, now the problem is that by doing so we also switch the ideals A and B.

Let us mention another possible generalisation. Let P be a proper standard parabolic subgroup of $\mathrm{GL}(n, R)$. We can define the corresponding subgroup of $\operatorname{EE}(n, A, B)$ as follows

$$\operatorname{EE}_P(n, A, B) = \big\langle U_P(A), U_P^-(B) \big\rangle,$$

where $U_P(A)$ and $U_P^-(B)$ are the intersections of $U(n,A)$ and $U^-(n,B)$ with the unipotent radicals U_P and U_P^- of P and its opposite standard parabolic P^-, respectively. In the definition of $\mathrm{EE}(n,A,B)$ itself $P = B(n,R)$ is the standard Borel subgroup. However, in many cases it is technically much more expedient to work with the maximal standard parabolics instead.

Problem 3. *Let A and B be two ideals of a commutative ring R, and P be a standard parabolic subgroup of $\mathrm{GL}(n,R)$, $n \geqslant 3$. Generalise Theorem 3 and other related results from $\mathrm{EE}(n,A,B)$ to $\mathrm{EE}_P(n,A,B)$.*

As we have already mentioned, some of the requisite preliminary facts were already established by Stepanov in [31–33], in a more general context. After that it should be more or less straightforward to carry over to this more general setting also the calculations in § 4.

Observe, that $\mathrm{EE}_P(n,A,B)$ could be used to prove the main results of the present paper instead of $\mathrm{EE}(n,A,B)$. The corresponding minimal congruence subgroup is $\mathrm{SF}_P(n,A,B)$ defined by the following congruences on its matrices $g = (g_{ij})$. As above, $g_{ij} \in A$ or $g_{ij} \in B$, respectively, when (i,j) corresponds to a position inside the unipotent radical U_P or U_P^-, whereas $g_{ij} \equiv \delta_{ij} \pmod{AB}$ for positions inside the Levi factor L_p. As established in [44], the corresponding factor $\mathrm{SF}_P(n,A,B)/\mathrm{EE}_P(n,A,B)$ still equals $\mathrm{SK}_1(n,R,AB)$.

The author cordially thanks Roozbeh Hazrat, Alexei Stepanov, and Zuhong Zhang for ongoing discussion of this circle of ideas and long-standing cooperation over the last decades. In July–September 2019 we started to specifically discuss arithmetic case with Boris Kunyavsky and Eugene Plotkin, in connection with our work on bounded generation. The present paper is a spin-off of our discussions in "Biblioteka Cafe", and then in "Manneken Pis" on Kazanskaya on September 16. I very much appreciate also the very pertinent questions by Pavel Gvozdevsky and Sergei Sinchuk, which prompted me to generalise Theorem 3 and some of the previous results, especially those of [49].

References

1. A. Bak, A. Stepanov, *Dimension theory and nonstable* K*-theory for net groups.* — Rend. Sem. Mat. Univ. Padova, **106** (2001), 207–253.
2. H. Bass, K*-theory and stable algebra.* — Inst. Hautes Études Sci. Publ. Math. (1964), No. 22, 5–60.

3. H. Bass, J. Milnor, J.-P. Serre, *Solution of the congruence subgroup problem for* SL_n $(n \geqslant 3)$ *and* Sp_{2n} $(n \geqslant 2)$. — Publ. Math. Inst. Hautes Etudes Sci., **33** (1967), 59–137.
4. Z. I. Borewicz, N. A. Vavilov, *The distribution of subgroups in the full linear group over a commutative ring*. — Proc. Steklov Inst. Math. **3** (1985), 27–46.
5. D. Carter, G. E. Keller, *Bounded elementary generation of* $\mathrm{SL}_n(\mathcal{O})$. — Amer. J. Math. **105** (1983), 673–687.
6. D. L. Costa, G. E. Keller, *The* $\mathrm{E}(2, A)$ *sections of* $\mathrm{SL}(2, A)$. — Ann. Math., **134**, No. 1 (1991), 159–188.
7. D. L. Costa, G. E. Keller, *Power residue symbol and the central sections of* $\mathrm{SL}(2, A)$. — K-Theory, **15**, No. 1 (1998), 33–98.
8. A. J. Hahn, O. T. O'Meara, *The classical groups and* K*-theory*. Springer, Berlin et al., 1989.
9. R. Hazrat, A. Stepanov, N. Vavilov, Zuhong Zhang, *The yoga of commutators*. — J. Math. Sci. **179**, No. 6 (2011), 662–678.
10. R. Hazrat, A. Stepanov, N. Vavilov, Zuhong Zhang, *Commutator width in Chevalley groups*. — Note di Matematica **33**, No. 1 (2013), 139–170.
11. R. Hazrat, A. Stepanov, N. Vavilov, Zuhong Zhang, *The yoga of commutators, further applications*. — J. Math. Sci. **200**, No. 6 (2014), 742–768.
12. R. Hazrat, N. Vavilov, *Bak's work on* K*-theory of rings* (*with an appendix by Max Karoubi*). — J. K-Theory **4**, No. 1 (2009), 1–65.
13. R. Hazrat, N. Vavilov, Zuhong Zhang, *Relative commutator calculus in unitary groups, and applications*. — J. Algebra, **343** (2011), 107–137.
14. R. Hazrat, N. Vavilov, Zuhong Zhang, *Relative commutator calculus in Chevalley groups*. — J. Algebra, **385** (2013), 262–293.
15. R. Hazrat, N. Vavilov, Zuhong Zhang, *Generation of relative commutator subgroups in Chevalley groups*. — Proc. Edinburgh Math. Soc., **59** (2016), 393–410.
16. R. Hazrat, N. Vavilov, Zuhong Zhang, *Multiple commutator formulas for unitary groups*. — Israel Journal Math., **219**, No. 1 (2017), 287–330.
17. R. Hazrat, N. Vavilov, Zuhong Zhang, *The commutators of classical groups*. — J. Math. Sci., **222**, No. 4 (2017), 466–515.
18. R. Hazrat, Zuhong Zhang, *Generalized commutator formula*. — Commun. Algebra, **39**, No. 4 (2011), 1441–1454.
19. R. Hazrat, Zuhong Zhang, *Multiple commutator formula*. — Israel J. Math., **195** (2013), 481–505.
20. W. van der Kallen, *A group structure on certain orbit sets of unimodular rows*. — J. Algebra **82** (1983), 363–397.
21. A. Lavrenov, S. Sinchuk *A Horrocks-type theorem for even orthogonal* K_2, `arXiv:1909.02637 v1 [math.GR] 5 Sep 2019`, pp. 1–23.
22. A. Leutbecher, *Euklidischer Algorithmus und die Gruppe* GL_2. — Math. Ann., **231** (1978), 269–285.
23. B. Liehl, *On the group* SL_2 *over orders of arithmetic type*. — J. reine angew. Math., **323** (1981), 153–171.
24. A. W. Mason, *On subgroups of* $\mathrm{GL}(n, A)$ *which are generated by commutators*. II. — J. reine angew. Math., **322** (1981), 118–135.

25. A. W. Mason, W. W. Stothers, *On subgroups of* $\mathrm{GL}(n, A)$ *which are generated by commutators.* — Invent. Math., **23** (1974), 327–346.
26. H. Matsumoto, *Sur les sous-groupes arithmétiques des groupes semi-simples déployés.* — Ann. Sci. École Norm. Sup., Ser. 4, **2**, No. 1 (1969), 1–62.
27. J. L. Mennicke, *A remark on the congruence subgroup problem.* — Math. Scand., **86**, No. 2 (2000), 206–222.
28. B. Nica, *A true relative of Suslin's normality theorem.* — Enseign. Math., **61**, No. 1–2 (2015), 151–159.
29. B. Nica, *On bounded elementary generation for* SL_n *over polynomial rings.* `arXiv:1901.00587v1 [math.GR] 3 Jan 2019`, 1–6.
30. J.-P. Serre, *Le probleme des groupes de congruence pour* SL_2. — Ann. Math., **92**, No. 3 (1970), 489–527.
31. A. Stepanov, *Elementary calculus in Chevalley groups over rings.* — J. Prime Res. Math., **9** (2013), 79–95.
32. A. V. Stepanov, *Structure theory of Chevalley groups over rings.* Habilitation St Petersburg State Univ., (2013), 1–113.
33. A. V. Stepanov, *Non-abelian* K*-theory for Chevalley groups over rings,* J. Math. Sci., **209**, No. 4 (2015), 645–656.
34. A. Stepanov, *Structure of Chevalley groups over rings via universal localization.* — J. Algebra, **450** (2016), 522–548.
35. A. Stepanov, N. Vavilov, *Decomposition of transvections: a theme with variations.* — K-Theory, **19**, No. 2 (2000), 109–153.
36. B. Sury, T. N. Venkataramana, *Generators for all principal congruence subgroups of* $\mathrm{SL}(n, \mathbb{Z})$ *with* $n \geqslant 3$. — Proc. Amer. Math. Soc., **122**, No. 2 (1994), 355–358.
37. A. A. Suslin, *The structure of the special linear group over polynomial rings.* — Math. USSR Izv., **11**, No. 2 (1977), 235–253.
38. O. I. Tavgen, *Bounded generation of Chevalley groups over rings of* S*-integer algebraic numbers.* — Izv. Acad. Sci. USSR, **54**, No. 1 (1990), 97–122.
39. J. Tits, *Systèmes générateurs de groupes de congruence.* — C. R. Acad. Sci. Paris, Sér A, **283** (1976), 693–695.
40. L. N. Vaserstein, *On the group* SL_2 *over Dedekind rings of arithmetic type.* — Mat. Sb., **89**, No. 2 (1972), 313–322.
41. L. N. Vaserstein, *On the normal subgroups of the* GL_n *of a ring.* — Algebraic K-Theory, Evanston 1980, Lecture Notes in Math., vol. 854, Springer, Berlin et al., 1981, pp. 454–465.
42. L. N. Vaserstein, A. A. Suslin, *Serre's problem on projective modules over polynomial rings, and algebraic K-theory.* — Math. USSR Izv., **10** (1978), 937–1001.
43. N. Vavilov, *Parabolic subgroups of the full linear group over a Dedekind ring of arithmetical type.* — J. Sov. Math., **20** (1982), 2546–2555.
44. N. Vavilov, *On the group* SL_n *over a Dedekind domain of arithmetic type,* Vestn. Leningr. Univ., Mat. Mekh. Astron., 1983, No. 2, 5–10.
45. N. Vavilov, *Unrelativised standard commutator formula,* Zapiski Nauchnyh Seminarov POMI. **470** (2018), 38–49.
46. N. A. Vavilov, A. V. Stepanov, *Standard commutator formula.* — Vestnik St. Petersburg State Univ., Ser. 1, **41**, No. 1 (2008), 5–8.

47. N. A. Vavilov, A. V. Stepanov, *Standard commutator formulae, revisited,* Vestnik St. Petersburg State Univ., Ser.1, **43**, No. 1 (2010), 12–17.
48. N. A. Vavilov, A. V. Stepanov, *Linear groups over general rings* I. *Generalities.* — J. Math. Sci., **188**, No. 5 (2013), 490–550.
49. N. Vavilov, Zuhong Zhang, *Generation of relative commutator subgroups in Chevalley groups,* II. — Proc. Edinburgh Math. Soc., , (2019).
50. Hong You, *On subgroups of Chevalley groups which are generated by commutators.* — J. Northeast Normal Univ., No. 2 (1992), 9–13.

St. Petersburg State University
E-mail: nikolai-vavilov@yandex.ru

Поступило 7 октября 2019 г.