1. Normal subgroups of $\mathbf{GL}_n F$ for a field F. Generators for $\mathbf{E}_n A$.

Let F be a field, $n \geq 1$ an integer, $\mathrm{GL}_n F$ the group of all invertible $n \times n$ matrices with entries in F. It is well-known, that an $n \times n$ matrix α is invertible if and only if its determinant $\det(\alpha)$ is invertible, i.e., $\det(\alpha) \in \mathrm{GL}_1 F = F \setminus \{0\}$.

Our main goal here is to answer the following question: Which subgroups of $\mathrm{GL}_n F$ are normal?

First of all, the kernel $\mathrm{SL}_n F$ of det: $\mathrm{GL}_n F \to \mathrm{GL}_1 F$ is normal (as any kernel is). More generally, any subgroup H of $\mathrm{GL}_n F$ containing $\mathrm{SL}_n F$ is normal because it is the inverse image of the normal subgroup $\det(H)$ of commutative $\mathrm{GL}_1 F$. So we have a family of normal subgroups H parameterized by all subgroups of the multiplicative group $\mathrm{GL}_1 F$.

Recall that every finite subgroup of $\mathrm{GL}_1 F$ is cyclic. So in the case of a finite F with q elements, the number of normal subgroups H in this family equals the number of divisors of $q - 1$.

Secondly, we will see soon (Corollary 1.2 below) that the center of the group $\mathrm{GL}_n F$ consists of all scalar matrices $\lambda 1_n$, where $\lambda \in \mathrm{GL}_1 F$. Since every central subgroup is normal, we get another family of of normal subgroups H parameterized by all subgroups of the multiplicative group $\mathrm{GL}_1 F$.

Our main result in this section (due to Dickson [Dic1] for an arbitrary field, while for some fields this had been known previously [Dic2]) is that there are no other normal H, i.e.,that every normal subgroup H of $\mathrm{GL}_n F$ either contains $\mathrm{SL}_n F$ or is contained in the center $\mathrm{G}_n(F, 0)$ with the following two exceptions: $n = 2, q = 2$ or 3, $H = [\mathrm{SL}_2 F, \mathrm{SL}_2 F]$ (the commutator subgroup). See Theorem 1.8 below.

For any associative ring A with 1, we denote by $\mathrm{GL}_n A$ the group of all invertible $n \times n$ matrices with entries in A. In other words, $\mathrm{GL}_n A$ is the multiplicative group of the ring $\mathrm{M}_n A$ of all $n \times n$ matrices over A.

A matrix α is *elementary* if $\alpha = a^{i,j}$ (where $a \in A, i \neq j$) differs from the identity matrix 1_n by one entry a at a off-diagonal position (i, j). The identity matrix 1_n is the trivial elementary matrix (with $a = 0$). Multiplication by an elementary matrix on right (left) is a column (row) addition operation. For any subset B of A, we denote by $\mathrm{E}_n B$ the subgroup of $\mathrm{GL}_n A$ generated by all elementary matrices $b^{i,j}$ with $b \in B, i \neq j$.

Lemma 1.1. For any ring A with 1 and any $n \geq 2$, a matrix $\alpha \in \mathrm{M}_n A$ commutes with all elementary matrices $1^{i,j}$ if and only if α is a scalar matrix $c1_n$. Such a matrix α commutes with all elementary matrices $a^{i,j}$ if and only if α is a scalar matrix $c1_n$ with c in the center C of the ring A.

Proof. The "if" parts are obvious. Let $\alpha = (\alpha_{i,j})$ commute with all elementary matrices $1^{i,j}$. Considering the positions (1,1) and (1,2) in $1^{1,2}\alpha = \alpha 1^{1,2}$, we obtain that $\alpha_{2,1} = 0$ and $\alpha_{1,1} = \alpha_{2,2}$. Similarly, all other off-diagonal entries of α are zeros and all diagonal entries are the same.

Let now a scalar matrix $\alpha = c1_n$ commute with all elementary matrices $a^{1,2}$. Considering the position (1,2) in $a^{1,2}\alpha = \alpha a^{1,2}$, we conclude that $ac = ca$ for $a \in A$, i.e., c belongs to the center of the ring A. QED.

Corollary 1.2. The centralizer of $\mathrm{E}_n A$ in $\mathrm{GL}_n A$ coincides with the center $\mathrm{G}_n(A, 0)$ of $\mathrm{GL}_n A$, and it coincides with $(\mathrm{GL}_1 C)1_n$ where C is the center of the ring A.

For any two elements g, h of a group G, we set $[g, h] = ghg^{-1}h^{-1}$. The commutator subgroup $[G, G]$ of G is defined as the subgroup of G generated by all commutators. It is a normal subgroup. A group G is called *perfect* if $G = [G, G]$.

Lemma 1.3. For any ring A with 1 and any integer $n \geq 3$, the group $\mathrm{E}_n A$ is perfect.

Proof. It follows from the identity $[a^{i,j}, 1^{j,k}] = a^{i,k}$ where $a \in A, i \neq j \neq k \neq i$. QED.

Now we return to the case when A is a field.

Theorem 1.4. For any field F and any n, we have $\mathrm{E}_n F = \mathrm{SL}_n F$. Moreover every matrix in $\mathrm{SL}_n F$ is a product of n^2 elementary matrices.

Proof. It is clear that the determinant of an elementary matrix is 1. Conversely, given any $\alpha = (\alpha_{i,j}) \in \mathrm{SL}_n F$, we can prove that it is a product of n^2 elementary matrices by induction on n as follows (the case $n = 1$ being trivial with the number of elementary matrices equal to 0). If a off-diagonal entry in the last row or column of α is nonzero, then by one addition operation we can arrange the (n, n)-entry to be 1. After this, we can reduce the last column of α to the last column of 1_n by at most $n - 1$ row addition operations. Next by at most $n - 1$ row addition operations we can reduce the last row of α to the last row of 1_n.

Thus, by at most $2n - 1$ addition operations we can reduce α to a matrix of the form $\begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix}$ with $\beta \in \mathrm{SL}_{n-1} F$. By the induction hypothesis, β is a product of $(n-1)^2$ elementary matrices, hence α is a product of $2n - 1 + (n-1)^2 = n^2$ elementary matrices.

If all off-diagonal entries in the last row and column of α are zero, then we write

$$\alpha = \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1_{n-2} & 0 & 0 \\ 0 & \gamma & 0 \\ 0 & 0 & 1/\gamma \end{pmatrix}$$

with $\beta \in \mathrm{SL}_{n-1}(F), \gamma = 1/\alpha_{n,n}$ and we again done by induction on n using the following identity known as the Whitehead lemma which holds for an arbitrary ring A and an arbitrary $\gamma \in \mathrm{GL}_1 A$:

$$(\mathbf{1.5}) \qquad \begin{pmatrix} \gamma & 0 \\ 0 & 1/\gamma \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1/\gamma & 1 \end{pmatrix} \begin{pmatrix} 1 & \gamma - 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1/\gamma - 1 \\ 0 & 1 \end{pmatrix}.$$

QED.

The group $\mathrm{E}_2 F$ is not perfect for the fields $F = \mathbf{Z}/2\mathbf{Z}$ and $F = \mathbf{Z}/3\mathbf{Z}$. Therefore the group $\mathrm{E}_2 A$ is not perfect for any ring A with 1 which has an ideal of index 2 or 3 (e.g., $A = \mathbf{Z}$, the integers). Using (1.5), we can prove that $\mathrm{E}_2 A$ is perfect for some rings.

Lemma 1.6. Let A be a ring with 1 such that the additive group A is gemerated by the set $\{\gamma a \gamma - a : \gamma \in GL_1 A, a \in A\}$. Then the group $\mathrm{E}_2 A$ is perfect.

Proof. By (1.5), $g = \begin{pmatrix} \gamma & 0 \\ 0 & 1/\gamma \end{pmatrix} \in \mathrm{E}_2 A$ hence

$(\gamma a \gamma - a)^{1,2} = [g, a^{1,2}] \in [\mathrm{E}_2 A, \mathrm{E}_2 A]$

and

$(\gamma a \gamma - a)^{2,1} = [g^{-1}, a^{2,1}] \in [\mathrm{E}_2 A, \mathrm{E}_2 A]$.

Now use the identity

(1.7) $(a-b)^{1,2} = a^{1,2}(b^{1,2})^{-1}$. QED.

Theorem 1.8 (L. Dickson). Let F be a field, and let $n \geq 2$ be an integer. In the case when $n = 2$ assume that F has at least 4 elements. Then every non-central subgroup H of $\mathrm{GL}_n F$ which is normalized by elementary matrices, contains $\mathrm{SL}_n F$.

Corollary 1.9. Under the conditions of Theorem 1.8, the group $\mathrm{SL}_n F$ modulo its center is a simple group.

To prove Theorem 1.8, we do some computations for an arbitrary ring A with 1.

Proposition 1.10. Let H be a subgroup of $\mathrm{GL}_n A$ which is normalized by all elementary matrices, and $n \geq 3$. Assume that H contains a non-central matrix with a off-diagonal entry equal to 0. Then H contains $\mathrm{E}_n B$ for a nonzero ideal B of A.

Proof. Set $B = \{b \in A : b^{1,2} \in H\}$. The identity (1.7) shows that B is an additive subgroup of A. The identities

(1.11) $[a^{i,j}, b^{j,k}] = (ab)^{i,k}$ $(i \neq j \neq k \neq i)$

show that B is an ideal of A.

We have to prove that $B \neq 0$. Let $\alpha = (\alpha_{i,j})$ be a non-central matrix in H.

Case 1: α is an elementary matrix, i.e. $\alpha = a^{i,j}$ with $a \neq 0$ and $i \neq j$. The identities (1.11) show that $a \in B$, so B is a nonzero ideal.

Case 2: α has the form $\alpha = \begin{pmatrix} c1_{n-1} & 0 \\ u & c \end{pmatrix}$ with $c \in C$, the center of A. Pick a nonzero entry u_j in the row u and $k \leq n-1$ distinct from j. Then $[\alpha, 1^{j,k}] = (u_j)^{n,k} \in H$, so we are reduced to Case 1.

Case 3: $\alpha = \begin{pmatrix} \beta & 0 \\ u & 1 \end{pmatrix}$. Because of Case 2, we can assume that $\beta \neq 1_{n-1}$. If β and 1_{n-1} differ in row i, then $[1^{n,i}, \alpha] = \begin{pmatrix} 1_{n-1} & 0 \\ w & 1 \end{pmatrix} \in H$ with $w \neq 0$ being the difference of the k-th rows of 1_{n-1} and β^{-1}. So we are reduced to Case 2.

Case 4: $\alpha_{1,n} = 0$. If α commutes with all $a^{n,j}$ where $a \in A, j \leq n-1$, then we have Case 2. Suppose that α does not commute with an elementary matrix $a^{n,j}$. Then

$1_n \neq [a^{n,j}, \alpha] = \begin{pmatrix} 1_{n-1} & 0 \\ u & 1 \end{pmatrix} \in H$, so we are reduced to Case 2 with $c = 1$.

General case, i.e., $\alpha_{i,j} = 0$ for some $i \neq j$. Then $(\gamma\alpha\gamma^{-1})_{1,n} = 0$ for a permutation matrix γ. The group $\gamma H \gamma^{-1}$ is normalized by $\gamma E_n A \gamma^{-1} = E_n A$ and contains a non-central matrix $\gamma\alpha\gamma^{-1}$. By Case 4, $E_n B \subset \gamma H \gamma^{-1}$ for a nonzero ideal B of A. Therefore $E_n B = \gamma^{-1} E_n B \gamma \subset H$. QED.

Corollary 1.12. Let H be a subgroup of $\mathrm{GL}_n A$ which is normalized by all elementary matrices, and $n \geq 3$. Assume that H contains a matrix α such that $Ab = A$ or $bA = A$ for an off-diagonal entry b of α. Then $\mathrm{E}_n B \subset H$ for a nonzero ideal B of A.

Proof. Without loss of generality, we can assume that $b = \alpha_{1,n}$. If $Ab = A$, then we write $\alpha_{2,n} = ab$ with $a \in A$. The matrix $\beta = (\beta_{i,j}) = a^{1,2}\alpha(-a)^{1,2} \in H$ is not scalar and $\beta_{2,n} = 0$, so we are done by Proposition 1.10.

If $bA = A$, we write $\alpha_{1,2} = ba$ with $a \in A$. The matrix $\beta = (\beta_{i,j}) = (-a)^{1,2}\alpha a^{1,2} \in H$ is not scalar and $\beta_{2,n} = 0$, so we are done by Proposition 1.10. QED.

Proof of Theorem 1.8. For any field $A = F$ and for any $b \in A$ we have either $b = 0$ or $Ab = bA = A$. So $B = A$ for any nonzero ideal B of A. Therefore Theorem 1.8 with $n \geq 3$ is covered by Proposition 1.10 and Corollary 1.12.

Assume now that $n = 2$. Since the condition of Lemma 1.6 holds when $F = A$ has at least 4 elements and since every non-central subgroup H in Theorem 1.8 contains a matrix which is not diagonal, we obtain the desired conclusion from the following result involving more general rings A :

Proposition 1.13. Under the conditions of Lemma 1.6, let H be a subgroup of $\mathrm{GL}_2 A$ which is normalized by $\mathrm{E}_2 A$. Suppose that H contains a matrix with an off-diagonal entry in $\mathrm{GL}_1 A$. Then $\mathrm{E}_2 A \subset H$.

Proof. We consider the set $H_{1,2}$ of (1,2)-entries of all matrices in H. Since

$$\delta = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{E}_2 A$$

and since

$$\delta \begin{pmatrix} a & b \\ c & d \end{pmatrix} \delta^{-1} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix},$$

it is clear that $H_{1,2} = -H_{2,1}$. Let $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H$ with $b \in \mathrm{GL}_1 A$. Then

$$\beta = (b^{-1}a)^{2,1} \alpha (-b^{-1}a)^{2,1} = \begin{pmatrix} 0 & b \\ c' & d' \end{pmatrix} \in H$$

hence $c' \in \mathrm{GL}_1 A$. Let us show that $H_{1,2} = A$. In fact we claim more: for any $z \in A$ there is $z' \in A$ such that $\begin{pmatrix} 1 & z \\ z' & 1 + z'z \end{pmatrix} \in H$. Indeed,

$$\begin{pmatrix} 1 & z \\ z' & 1 + z'z \end{pmatrix} = [\beta, (-z)^{2,1}] \in H$$

with $z' = -c'zb^{-1}$.

Now we want to prove that the intersection of H with $A^{2,1}$ contains all $(\gamma a \gamma - a)^{2,1}$ with $\gamma \in GL_1 A, a \in A$.

We have

$$\alpha = \begin{pmatrix} 1 & \gamma \\ c & 1 + c\gamma \end{pmatrix}, \alpha' = \begin{pmatrix} 1 & 1 \\ c' & 1 + c' \end{pmatrix} \in H$$

for some $c, c' \in A$. So

$$\beta = (1/\gamma)^{2,1} \alpha (-1/\gamma)^{2,1} = \begin{pmatrix} 0 & \gamma \\ -1/\gamma & * \end{pmatrix} \in H$$

and

$$\beta' = 1^{2,1} \alpha' (-1)^{2,1} = \begin{pmatrix} 0 & 1 \\ -1 & * \end{pmatrix} \in H.$$

Therefore

$$(\gamma a\gamma - a)^{2,1} = \begin{pmatrix} 1 & -a \\ \gamma a\gamma & 1 - a\gamma a\gamma \end{pmatrix} \begin{pmatrix} 1 & -a \\ a & 1 - a^2 \end{pmatrix}^{-1} = [\beta, a^{1,2}][\beta', a^{1,2}] \in H.$$

Thus, $A^{1,2} \subset H$, hence $A^{2,1} \subset H$ and $\mathrm{E}_2 A \subset H$. QED.

Remark 1. When F consists of 2 elements, the group $\mathrm{SL}_2 F = \mathrm{GL}_2 F$ has order 6 and is isomorphic to the symmetric group S_3. (To see this, consider the action of $\mathrm{GL}_2 F$ on nonzero vectors on the palne F^2. The action is transitive.) Its commutator subgroup is the only nontrivial proper normal subgroup. It has order 3 and consists of the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Remark 2. When F consists of 3 elements, the group $\mathrm{PSL}_2 F = \mathrm{SL}_2 F/\{\pm 1_2\}$ has order 12 and is isomorphic to the alternating group A_4. (To see this, consider the action of $\mathrm{PSL}_2 F$ on the lines passing the origin in the palne F^2. The action is transitive.) The group $\mathrm{SL}_2 F$ has four normal subgroups: $\{1_2\}, \{\pm 1_2\}$, $[\mathrm{SL}_2 F,\ \mathrm{SL}_2 F]$. $\mathrm{SL}_2 F$. These subgroups are also normal in $\mathrm{GL}_2 F$, so $\mathrm{GL}_2 F$, has five normal subgroups. The commutator subgroup $[\mathrm{SL}_2 F,\ \mathrm{SL}_2 F]$ is a cyclic group of order 6 generated by $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$. We have $[\mathrm{SL}_2 F,\ \mathrm{GL}_2 F] = [\mathrm{GL}_2 F,\ \mathrm{GL}_2 F] = \mathrm{SL}_2 F$.

Remark 3. Our Corollary 1.9 is Theorem 6.14 of [J]. Our elementary matrix $a^{i,j}$ is is denoted by $T_{ij}(a)$ in [J] and $B_{i,j,a}$ in [Dic1].

For the rest of section we consider finite generation of the group $\mathrm{E}_n A$. First of all, if A is any associative ring with 1 and X any subset of A, the relations (1.7) (1.11) show that $\mathrm{E}_n X = \mathrm{E}_n X'$ where X' is the subring of A generated by X and $\mathrm{E}_n(A, X) = \mathrm{E}_n(A, B)$ where B is an ideal of A generated by X, provided that $n \geq 3$.

Therefore, we get

Proposition 1.14. For any associative ring A and any $n \geq 3$, the group $\mathrm{E}_n A$ is finitely generated if and only if the ring A is finitely generated.

More precisely, if for a ring A and any $n \geq 2$, the group $\mathrm{E}_n A$ is generated by m matrices then the ring A is generated by $2mn^2$ element which are the matrix entries of the generators and their inverses.

Conversely, if an associative ring A is generated by d elements and $n \geq 3$ then it is clear that the group $\mathrm{E}_n A$ is generated by $d(n^2 - n)$ elementary matrices.

We will improve the latter bound for rings A with 1 proving, in particular, that the group $\mathrm{E}_n A$ is generated by 2 elements for sufficiently large n (depending on d). By Steinberg [Ste], for any finite field F and any $n \geq 2$, the group $\mathrm{E}_n F = \mathrm{SL}_n F$ is generated by 2 elements. It is also known to be true when F is any factor ring of the integers (we will show this below).

We will use the following refinement of Case 3 of Proposition 1.10.

Proposition 1.15. Let A be an associative ring with 1, A' a subring containing 1, $n \geq 3$, H a subgroup of $\mathrm{GL}_n A$. Assume that H is normalized by $\mathrm{E}_n A$ and that H contains a matrix $\alpha = (\alpha_{i,j})$ which coincides with the identity matrix 1_n in a row or a column. Then $E_n B' \subset H$ where B' is the subring of A generated by all $a_1\alpha_{i,j}a_2$ with $i \neq j$ and $a_1, a_2 \in A'$ together with all $a_1(\alpha_{i,i}-1)a_2$ with $a_1, a_2 \in A'$.

Proof. Without loss of generality we can assume that either $\alpha = \begin{pmatrix} \beta & 0 \\ u & 0 \end{pmatrix}$ or $\alpha = \begin{pmatrix} \beta & v \\ 0 & 0 \end{pmatrix}$ with $\beta \in \mathrm{GL}_{n-1}A$.

These two cases are similar so let $\alpha = \begin{pmatrix} \beta & 0 \\ u & 0 \end{pmatrix} \in H$ with $\beta = (\beta_{i,j}) \in \mathrm{GL}_{n-1}A$ and an $(n-1)$-row u.

Set $B = \{a \in A : a^{1.2} \in H\}$. By (1.7) (1.11), B is a subring of $A, BA' + A'B \subset B$, and $\mathrm{E}_n B \in H$. So it suffices to show that $\alpha_{i,j} \in B$ for all $i \neq j$ and that $\alpha_{i,i} - 1 \in B$ for all $i \leq n-1$.

We have $(\alpha_{i,j})^{n,i} = (\beta_{i,j})^{n,i} = [[1^{n,i}, \alpha], 1^{j,i}] \in H$ when $i, j \leq n-1$ and $i \neq j$, hence $\alpha_{i,j} \in B$. When $i \leq n-1$, we have $(\alpha_{i,i}-1)^{n,j} = [[1^{n,1}, \alpha], 1^{i,j}]$ where $j \neq i, j \leq n-1$, hence $\alpha_{i,i} - 1 \in B$.

Thus, B contains all entries of the matrix $\beta - 1_{n-1}$. Similarly, B contains all entries of the matrix $\beta^{-1} - 1_{n-1}$.

It remains to show that $u_i \in B$ for all $i \leq n-1$. Without loss of generality, we can assume that $i = 1$. We have $\gamma = [(-1)^{1,2}, \alpha] = (-1)^{1,2}\begin{pmatrix} 1_{n-1} + v'u' & 0 \\ u_1 u' & 1 \end{pmatrix} \in H$ where $\begin{pmatrix} v' \\ u_1 \end{pmatrix}$ is the first column of α and u' is the second row of β^{-1}.

Since $v'u' = 0$, we have

$$\begin{pmatrix} 1_{n-1} + v'u' & 0 \\ 0 & 1 \end{pmatrix} [\begin{pmatrix} 1_{n-1} & v' \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1_{n-1} & 0 \\ u' & 1 \end{pmatrix}].$$

Since

$$\begin{pmatrix} 1_{n-1} & 0 \\ u' & 1 \end{pmatrix} (-1)^{n,2} \in H$$

and

$$\begin{pmatrix} 1_{n-1} & v' \\ 0 & 1 \end{pmatrix} (-1)^{1,n} \in H,$$

we conclude that $\delta = [(-1)^{n,2}, (-1)^{1,n}][\begin{pmatrix} 1_{n-1} & v' \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1_{n-1} & 0 \\ u' & 1 \end{pmatrix}] \in H$.

We used that H is normalized by $1^{1,n}$ and $1^{n,2}$.

Since

$$[(-1)^{n,2}, (-1)^{1,n}] = [(-1)^{1,n}, (-1)^{n,2}]^{-1} = (-1)^{1,2},$$

we obtain that $\delta = (-1)^{1,2}\begin{pmatrix} 1_{n-1} + v'u' & 0 \\ 0 & 1 \end{pmatrix} [\begin{pmatrix} 1_{n-1} & v' \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1_{n-1} & 0 \\ u' & 1 \end{pmatrix}] \in H$,

hence $\mu = \delta^{-1}\alpha = \begin{pmatrix} 1_{n-1} & 0 \\ u_1 u' & 1 \end{pmatrix} \in H$.

Recall that $u' = (u'_j)$ is the second row of β^{-1}, so $u'w = 1$ for the second row $w = (w_i)$ of β. Also recall that we have shown that $\mathrm{E}_n(x) \in H$ for every entry x of $\beta - 1_{n-1}$.

Therefore, for any distinct $i, j \leq n-1$ we have $[\mu, (w_j)^{j,i}] = (u_1 u'_j w_j)^{n,i} \in H$, hence $u_1 u'_j w_j \ni B$. Taking the sum over j, we obtain that $u_1 \in B$. QED.

Corollary 1.16. Let A be an associative ring with 1, A' a subring containing 1, $n \geq 3$, H a subgroup of $\mathrm{GL}_n A$. Assume that H is normalized by $\mathrm{E}_n A$ and that H contains a matrix $\alpha = (\alpha_{i,j})$ such that $\alpha_{1,1}) = 1, \alpha_{n,1}) = 0$, and $(\alpha^{-1})_{n,n}) = 1$. Then $E_n(B') \subset H$ where B' is the subring of A generated by all $a_1 \alpha_{i,j} a_2$ with $i \neq j$ and $a_1, a_2 \in A'$ together with all $a_1(\alpha_{i,i} - 1)a_2$ with $a_1, a_2 \in A'$.

Proof. We apply Proposition 1.15 to the matrix $\beta = [(-1)^{1,n}, \alpha] = 1^{1,n}, (1_n + vu) \in H$ where v is the first column of α and u is the last row of α^{-1}. Note that the last row of β coincides with the last row of 1_n and that the $\beta_{i,n} = \alpha_{i,1} = v_i$ for $2 \leq i \leq n-1$. We obtain that $(u_i)^{1,2} \in H$ for $2 \leq i \leq n-1$.

Now we apply Proposition 1.15 to the matrix

$$\gamma = \prod_{i=2}^{n-1} (-u_i)^{i,1} \alpha.$$

The first column of γ is the same as the first column of 1_n, and the ring generated by all entries of $\gamma - 1_n$ together with all v_i $(2 \leq i \leq n-1)$ is the same as the ring generated by all entries of $\alpha - 1_n$. QED.

Theorem 1.17. Let A be an associative ring with 1 which is generated by 1 together with d elements. Then

(a) the group $\mathrm{E}_n A$ is generated by 2 elements for all $n \geq 2$ when $d = 0$, i.e.., A is a factor ring of the integers;

(b) the group $\mathrm{E}_n A$ is generated by $m+2$ elements provided that
$n \geq 3$ and $m(n^2 - n - 1) \geq d$;

(c) the group $\mathrm{E}_n A$ is generated by $m+2$ elements when
$n \geq 7$ and $(n-5)^2/4 + m(n^2 - n - 1) \geq d$;
in particular, $\mathrm{E}_n A$ is generated by 2 elements when $n \geq 7$ and $(n-5)^2/4 \geq d$.

Proof. Let $\alpha = (\alpha_{i,j}) \in \mathrm{E}_n A$ be the monomial matrix defined by $\alpha_{i,i+1} = 1$ for $i = 1, \ldots, n-1, \alpha_{n,1} = (-1)^{n-1}$, and $\alpha_{i,j} = 0$ when $j \neq i+1$ and $(i,j) \neq (n,1)$.

(a) If $d = 0$, we claim that $\mathrm{E}_n A$ is generated by α and $1^{1,2}$. Indeed, let H be the subgroup generated by α and $1^{1,2}$.

When $n = 2$ we have $1^{2,1} = \alpha(-1)^{1,2}\alpha^{-1} \in H$, hence $H = \mathrm{E}_2 A$ because the ring A is generated by 1.

Let now $n \geq 3$. Then $1^{i,i+1} = \alpha^{1-i} 1^{1,2} \alpha^{i-1} \in H$ for $i = 1, \ldots, n-1$ and $(-1^{n-1})^{n,1} = \alpha^{1-n} 1^{1,2} \alpha^{n-1} \in H$.

Using the relations (1.7), (1,11), we obtain that H contains all elementary matrices, hence $H = \mathrm{E}_n A$.

(b) Our $m+2$ generators are going to be the monomial matrix α, the elementary matrix $1^{1,2}$, and m matrices of the form $\beta_k \gamma_k$ with $1 \leq k \leq m$ where each β_k is a lower diagonal matrix with 1 along the diagonal and $(n,1)$-entry 0 and each β_k is an upper diagonal matrix with 1 along the diagonal.

We place d generators of the ring A as entries of the matrices β_k, γ_k. Note that for each k the subring of A generated by the entries of β_k and γ_k is the same as the the subring of A generated by the entries of $\beta_k\gamma_k$. Therefore it suffices to show that the subgroup H_k of E_nA generated by the three matrices $\alpha, 1^{1,2}$, and $\beta_k\gamma_k$ contains E_nB_k where B_k is the subring of A generated by the entries of $\beta_k\gamma_k$.

By (a), H contains E_nA' where A' is the subring of A generated by 1. Now we apply Corollary 1.16 to each matrix $\beta_k\gamma_k$ and conclude that $\mathrm{E}_nA_k \subset H$ where B_k is the subring of A generated by all entries of $\beta_k\gamma_k - 1_n$.

It remains to observe that A_k is also the subring of of A generated by all entries of $\beta_k - 1_n$ and $\gamma_k - 1_n$.

(c) We set $s = (n-5)/2$ when $n \geq 7$ is odd and $s == (n-6)/2$ when $n \geq 8$ is even. We define the matrix $\gamma_0 \in \mathrm{E}_nA$ by placing $s(n-5-s)$ generators at the positions (i,j) with $4 \leq i \leq s+3$ and $s+6 \leq i \leq n-1$ (if $d < s(n-5-s)$, we place zeros at some of those positions) in the identity matrix 1_n. The remaining generators of the ring, if any, we arrange at matrices β_k, γ_k. as in (b). In the view of (b), it remains to show that the subgroup H of E_nA generated by the monomial matrix α and the matrix $\delta = 1^{1,2}\gamma_0$ contains E_nA'.

Since the matrix γ_0 commutes with the matrices $1^{1,2}, 1^{2,3} = \alpha^{-1}1^{1,2}\alpha$, and $\alpha^{-1}\gamma_0\alpha$, we have $1^{1,3} = [\delta, \alpha^{-1}\delta\alpha] \in H$.

If n is odd, the conjugates of $1^{1,3}$ by powers of α generate E_nA', so $\mathrm{E}_nA' \subset H$.

When n is even, H contains all $1^{i,j}$ with even $i-j$. In particular, $1^{2,n} \in H$. So $1^{1,n} = [\delta, 1^{2,n}] \in H$.

For any n, the conjugates of $1^{n,1}$ by powers of α generate E_nA'. Thus, $\mathrm{E}_nA' \subset H$. GED.

Remarks. Any homomorphism $f : A \to B$ of associative rings with 1 induces homomorphisms $f_n : \mathrm{GL}_nA \to \mathrm{GL}_nB$ for all $n \geq 1$. Notice that $f_n(\mathrm{E}_nA) \subset\mathrm{E}_nB$. When $f(A) = B$, $f_n(\mathrm{E}_nA) =\mathrm{E}_nB$ for all n but $f_n(\mathrm{GL}_nA)$ need not to be the whole group GL_nB. (Consider $\mathbf{Z} \to \mathbf{Z}/5\mathbf{Z}$).

Problems and exercises.

Here are some problems related with this section. Some of them are easy exercises while others are very difficult or even open. Some exercises are about associative rings and intended to prepare the reader for the following sections.

1. Prove that the matrix $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{E}_2A$ (which is a product of 4 elementary matrices by (1.5)) is a product of 3 elementary matrices if and only if $2 = 0$ in the ring A.

2. For any field F show that a matrix in $\mathrm{E}_2F = \mathrm{SL}_2F$ is product of three elementary matrices if and only if the matrix is either non-diagonal or trivial.

3. For every field F and every $n \geq 3$, show that every matrix in $\mathrm{E}_nF = \mathrm{SL}_nF$ is a product of $n^2 - 1$ elementary matrices.

4. For any infinite field F and any $n \geq 2$, show that not every matrix in E_nF is a product of $n^2 - 2$ elementary matrices. (Hint: use the fact that every $m+1$ polynomials in m variables over a field are algebraically dependent.)

5. For any field F and any $n \geq 2$, show that there is a number q such that not every matrix in $\mathrm{E}_n F$ is a product of $n^2 - 2$ elementary matrices provided that F has at least q elements. (Hint: Over a field of q elements, there are $(q-1)(n^2-n)+1$ elementary matrices while the group $\mathrm{SL}_n A$ has order $(q^n-1)(q^n-q^2)\cdots(q^n-q^{n-1}/(q-1))$.)

6. (Open problem) For which finite fields F and integers $n \geq 3$, every matrix in $\mathrm{E}_n F$ is a product of $n^2 - 2$ elementary matrices?

7. For any field F, show that every matrix in $\mathrm{M}_n F$ of rank $k \leq n-1$ can be reduced to $\begin{pmatrix} 1_k & 0 \\ 0 & 0 \end{pmatrix}$ by n^2 row and column addition operations.

8. Prove that $\mathrm{SL}_n \mathbf{Z} = \mathrm{E}_n \mathbf{Z}$ for all n. It is known (Carter-Keller [CK]) that for $n \geq 3$ every matrix in $\mathrm{SL}_n \mathbf{Z}$ is a product of a bounded number (depending on n) of elementary matrices, but this is not true for $n = 2$ (prove it!). In other words, the product A of infinitely many copies of $\mathbf{Z}$ has the following property:
(*) $\mathrm{SL}_n A = \mathrm{E}_n A$ for $n \geq 3$ but $\mathrm{SL}_2 A \neq \mathrm{E}_2 A$.

9. Prove (*) for $A = F[x,y]$ where F is a field (Cohn, Suslin).

10. Prove (*) when A is the ring of all real continuous functions of one variable (Vaserstein).

11. Prove (*) when A is the ring of all real continuous functions of three variables (Thurston-Vaserstein).

12. (Open problem) Is $\mathrm{SL}_2 A = \mathrm{E}_2 A$ when $A = \mathbf{Z}[x, 1/x]$?

13. (Open problem) Given a non-central matrix $\alpha \in \mathrm{SL}_n F$ over a field F, is it true that every non-central matrix in $\mathrm{SL}_n F$ is a product of n matrices, each similar to α?

14. Prove that every non-central matrix in $\mathrm{SL}_n F$ over a field F is a commutator. What about scalar matrices?

15. Given elements $\lambda_1, \mu_1, \ldots, \lambda_n, \mu_n$ in a field F and a nonscalar matrix $\alpha \in \mathrm{GL}_n F$ such that $\det(\alpha) = \prod_{i=1}^n \lambda_i, \mu_i$ show that there are $\beta, \gamma \in \mathrm{GL}_n F$ such that $\alpha = \beta\gamma$, the eigenvalues of β are λ_i, and the eigenvalues of γ are μ_i.

16. Let A be an associative ring with 1, $a \in A$, and $aA = Aa = A$. Prove that $a \in \mathrm{GL}_1 A$.

17. Let A be an associative ring with 1 and $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2 A$. Prove that $a.d \in \mathrm{GL}_1 A$.

18. Let A be a finitely generated associative ring with 1. Show that for sufficiently large n the ring $\mathrm{M}_n A$ admits two generators.

19. Let F be an infinite field of characteristic $p \neq 0$. Let F' be a field of characteristic $\neq p$. Let $f : \mathrm{SL}_2 F \to \mathrm{GL}_n F'$ be a group morphism (integer $n > 0$ is arbitrary). Prove that f is trivial.

20. Let A be an associative domain with 1 ("domain" means that A has no zero divisors, i.e., if $xy = 0$ in A then either $x = 0$ or $y = 0$). Prove that if $xy = 1$ then $yx = 1$.

21. Let A be a ring with 1, and A^∞ the direct product of infinitely many copies of A. For any n, clearly $\mathrm{GL}_n(A^\infty) = (\mathrm{GL}_n A)^\infty$ so the natural group homomorphism $\mathrm{E}_n(A^\infty) \to$

$(\mathrm{E}_n A)^\infty$ is injective. Show that this homomorphism is surjective if and only if every matrix in $\mathrm{E}_n A$ is a product of a *bounded* number of elementary matrices.

22. Let A be an associative ring with 1. The columns A^n with n entries over A form a free right A-mosule with n free generators. Every finitely generated free right A-mosule is isomorphic to A^n for some $n \geq 0$. (In general, n is not unique.) When every right ideal of A is finitely generated, A is called *Noetherian.* Prove that if A is right Noetherian then every submodule of A^n is finitely generated for every n.

Prove that if for some k every right ideal of A is generated by k elements, then every submodule of A^n is generated by kn elements, for any $n \geq 1$.

There are rings with $k = 1$, known as right principal idea rings (PIRs), e.g., $A = \mathbf{Z}$, the integers, and with $k = 2$, e.g., the rings of algebraic integers and the rings of differential operators with polynomial coefficients.

23. Let A be an associative domain with 1 It is called a *rigt Ore donain* if $aA \cap bA \neq \{0\}$ for any nonzero $a, b \in A$, Clearly, every commutative domain is an Ore domain.

Prove that every right Ore domain is isomorphic to a subring of a division ring.

Prove that every right Noetherian domain (see the previous exercise) is a right Ore domain.

24. Let A be an associative domain with 1. It is called a *right Bézout domain* if for every $a, b \in A$ there is $c \in A$ such that $aA + bA = cA$. Clearly, every right principal ideal domain is a Bézout domain and that every finitely generated right ideal in right Bézout domain is principal. Here are two examples of commutative Bézout domains which are not PIRs: the ring of entire functions, the ring of all algebaic integers.

Prove that every right Bézout domain is an Ore domain (see the previous exercise).

25. An associative ring with 1 is called a *right Euclidean* if there a function f from A to the non-negative integers such that for for any nonzetro $a, b \in A$ there is $q \in A$ such that $f(a - bq) < f(b)$. Here are three examples of commutative Euclidean domains:

$\mathbf{Z}$ is Euclidean with $f(a) = |a|$,

any field F is Euclidean with $f(a) = 1$ for $a \neq 0$ and $f(0) = 0$.

$F[t]$ is Euclidean for any field F with $f(a) = \deg(a) + 1$ for $a \neq 0$ and $f(0) = 0$.

Prove that every right Euclidean ring is a right PIR (see Exercise 22 above).

26. Let A_1 be an associative ring with 1, $n \geq 2$, and $A = \mathrm{M}_n A_1$. Show that every element of A is the sum of elements of the form $\gamma a \gamma - a$ with $a \in A$ and $\gamma \in \mathrm{GL}_1 A = \mathrm{GL} n A$.

27. Let A be an associative ring with 1 and $n \geq 2$. Show that 1_n is the sum of 2 invertible matrices in $\mathrm{M}_n A$ and that every matrix in $\mathrm{M}_n A$ is the sum of 3 invertible matrices (i.e., matrices in $\mathrm{GL}_n A$.)

28. Let A be an associative ring with 1 and $n \geq 1$. Show that every ideal of $\mathrm{M}_n A$ has the form $\mathrm{M}_n B$ where B is an ideal of A.