2. Normal subgroups of $\mathrm{GL}_n D$ for a division ring D. The Dieudonné determinant. Systems of linear equations.

In this section, D denotes a *division ring* (or a skew field), i.e., D is an associative ring with 1, and $\mathrm{GL}_1 D = D \setminus \{0\}$. Commutative division rings are fields.

Remark. The center C of a division ring D is a field. If D is finite-dimensional (as vector space) over C then:

the dimension, $\dim_C D$ is a perfect square;

when C is the real numbers, $\dim_C D = 1$ or 4 (Frobenius);

when C is finite or algebraically closed, $C = D$.

The fact that every finite division ring is commutative is due to Wedderburn.

Normal subgroups

First we generalize Theorem 1.4:

Theorem 2.1. For any $n \geq 2$, every $\alpha \in \mathrm{GL}_n D$ is $\beta\gamma$, where β is a product of n^2 elementary matrices, and $\gamma = \begin{pmatrix} d & 0 \\ 0 & 1_{n-1} \end{pmatrix}$, with $d \in \mathrm{GL}_1 D$.

Proof. If $n = 2$, then by 3 row addition operations we reduce the last column of α to $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Then we kill the first entry in the second row by a row addition operation.

Proceeding by induction on n, assume now that $n \geq 3$. By n row addition operations we reduce the last column of α to that of 1_n. Then, by $n-1$ row addition operations reduce the last row to that of 1_n. Total number of addition operations used for the reduction is $2n - 1$. QED.

Corollary 2.2. For every $n \geq 2$, $\mathrm{E}_n D$ is a normal subgroup of $\mathrm{GL}_n D$. Moreover, every commutator in $\mathrm{GL}_n D$ is a product of $4n^2$ elementary matrices hence $\mathrm{E}_n D$ contains the commutator subgroup $[\mathrm{GL}_n D, \mathrm{GL}_n D]$. If $n \geq 3$ or $n = 2$ and D has at least four elements then

$\mathrm{E}_n D = [\mathrm{E}_n D, \mathrm{E}_n D] = [\mathrm{GL}_n D, \mathrm{GL}_n D]$.

Proof. Let $\alpha, \alpha' \in \mathrm{GL}_n D$. We write $\alpha = \beta\gamma$, and $\alpha' = \beta'\gamma'$, where β, β' are products of n^2 elementary matrices, $\gamma = \begin{pmatrix} d & 0 \\ 0 & 1_{n-1} \end{pmatrix}$, $\gamma' = \begin{pmatrix} 1_{n-1} & 0 \\ 0 & d' \end{pmatrix}$, and $d, d' \in \mathrm{GL}_1 D$. Then

$[\alpha, \alpha']$

$= \beta\gamma\beta'\gamma'\gamma^{-1}\beta^{-1}\gamma'^{-1}\beta'^{-1}$

$= \beta(\gamma\beta'\gamma^{-1})(\gamma'\beta^{-1}\gamma'^{-1})\beta'^{-1}$

is a product of $4n^2$ elementary matrices, because the conjugates of elementary matrices by diagonal matrices γ, γ' are elementary matrices, and because $[\gamma, \gamma'] = 1$. Thus, $\mathrm{E}_n D \supset [\mathrm{GL}_n D, \mathrm{GL}_n D]$, hence $\mathrm{E}_n D$ is normal. The rest of the conclusion follows from Lemmas 1.3 and 1.6.

We have to check the condition of Lemma 1.6. In fact, we claim that every $d \in D$ has the form $\gamma a \gamma - a$ where $a \in D, \gamma \in GL_1 D$ (rather than being a sum of such elements). We find a subfield C' of D containing d and at least 3 other elements. For instance, $C' = C[d]$ works unless the center C of D has only two or three elements including d, in which case we can take $C' = C[d']$ with arbitrary d' outside C.

We pick $\gamma \neq 0, \pm 1$ in C'. Then $d = \gamma a \gamma - a = (\gamma^2 - \gamma)a$, for $a = d/(\gamma^2 - 1)$. QED.

Theorem 2.3. Let $n \geq 3$ or $n = 2$ and D has at least 4 elements. Let H be a subgroup of $\mathrm{GL}_n D$ which is normalized by $\mathrm{E}_n D$. Then either $\mathrm{E}_n D \subset H$ or H consists of scalar matrices over the center C of D. Conversely, every subgroup H of $\mathrm{GL}_n D$ which is either central or contains $\mathrm{E}_n D$ is normal.

Proof. If H is not central, then it contains a matrix with a nonzero off-diagonal entry. Indeed otherwise H would consist of diagonal matrices. If a diagonal entry d_i of a matrix $\alpha = \mathrm{diag}(d_1, \cdots, d_n) \in H$ is not in C or is different from another entry d_j, then we find $a \in D$ such that $d_i a \neq a d_j$. We have $\beta = [\alpha, a^{ij}] = (d_i a - a d_j)^{ij} \in H$, and β is not diagonal.

So our first conclusion follows from Propositions 1.10 and 1.13.

The second conclusion is clear for central subgroups H. If H is not central, it follows from the inclusions

$[H, \mathrm{GL}_n D] \subset [\mathrm{GL}_n D, \mathrm{GL}_n D] \subset \mathrm{E}_n D \subset H$,

see Corollary 2.2. QED.

The Dieudonné determinant

The main result of this section describe the commutative group $\mathrm{GL}_n(A)/\mathrm{E}_n(A)$ whose subgroups are in (1-1)-correspondence with all non-central normal subgroups of $\mathrm{GL}_n(A)$.

Theorem 2.4 (Dieudonné [Die1, Die2]). The element $d \in \mathrm{GL}_1 D$ in Theorem 2.1 is determined by $\alpha \in \mathrm{GL}_n D$ uniquely modulo $[\mathrm{GL}_1 D, \mathrm{GL}_1 D]$. Thus, we have an isomorphism

$\mathrm{GL}_n D / \mathrm{E}_n D = \mathrm{GL}_1 D / [\mathrm{GL}_1 D, GL_1 D]$,

for every $n \geq 2$.

Proof. By induction on n, we construct homomorphisms (Dieudonné determinants)

$\delta_n : \mathrm{GL}_n D \longrightarrow \mathrm{GL}_1 D / [\mathrm{GL}_1 D, \mathrm{GL}_1 D]$

for all $n \geq 1$ such that $\delta_n(\alpha) = 1$ for every elementary matrix α and such that The Dieudonné determinant. $\delta_n \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix} = \delta_{n-1}(\beta)$

for any $n \geq 2$ and $\beta \in \mathrm{GL}_{n-1} D$. This will prove our theorem.

We define δ_1 to be the canonical projection. Suppose now that $n \geq 2$ and δ_i's are defined for $i \leq n-1$. We will define δ_n for any matrix $\alpha \in \mathrm{GL}_n D$ by reducing it to the form $\begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix}$ and setting $\delta_n(\alpha) = \delta_{n-1}(\beta)$. The problem is that the reduction is not unique.

We define X_k ($k = 1, \ldots, n$) to be the set of matrices $\alpha = (\alpha_{ij}) \in \mathrm{GL}_n D$ with $\alpha_{k,n} \in \mathrm{GL}_1 D$. Clearly, $\mathrm{GL}_n D$ is the union of its subsets X_k. We define δ_n on X_n by

$$\Delta_n \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \delta_1(d)\delta_{n-1}(a - bd^{-1}c) \in \ \mathrm{GL}_1 D / [\ \mathrm{GL}_1 D,\ \mathrm{GL}_1 D],$$

where $d \in \mathrm{GL}_1 D$, $a \in \mathrm{M}_{n-1} D$, b is an $(n-1)$-column, and c is an $(n-1)$-row.

For $k < n$, we define Δ_k on X_k similarly, namely, $\Delta_k(\alpha) = \delta_n(p\alpha)\delta_1(-1)$, where $p = p_k$ is the permutation matrix switching k and n, so $pX_k = X_n$, and where $\alpha \in X_k$.

Our plan now is to show that Δ_i and Δ_j agree on $X_i \cap X_j$ for $i \neq j$, and that the mapping

$\delta_n : \mathrm{GL}_n D \longrightarrow \mathrm{GL}_1 D / [\mathrm{GL}_1 D, \mathrm{GL}_1 D]$

they define jointly is a homomorphism with the desired properties.

But first we establish some properties of Δ_n.

Lemma 2.5. Let $\alpha \in X_n, d' \in \mathrm{GL}_1 D$, and $\beta \in \mathrm{GL}_{n-1} D$. Then $\Delta_n(\begin{pmatrix} \beta & * \\ 0 & d' \end{pmatrix} \alpha) = \delta_{n-1}(\beta)\Delta_n(\alpha)\delta_1(d')$.

Proof. We write $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ as in the definition of Δ_n. Then
$\Delta_n(\begin{pmatrix} \beta & v \\ 0 & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix})$
$= \Delta_n \begin{pmatrix} \beta a + vc & \beta b + vd \\ d'c & d'd \end{pmatrix}$
$= \delta_1(d'd)\delta_{n-1}(\beta a + vc - (\beta b + vd)cd^{-1})$
$= \delta_1(d'd)\delta_{n-1}(\beta a - \beta bd^{-1}c)$
$= \delta_1(d)\delta_1(d')\delta_{k-1}(\beta)\delta_{n-1}(a - bd^{-1}c) = \delta_{n-1}(\beta)\Delta_n(\alpha)\delta_1(d')$. QED.

Corollary 2.6. If a matrix β is obtained from $\alpha = (\alpha_{ij}) \in X_k$ by a row multiplication with a coefficient $\gamma \in \mathrm{GL}_1 D$, then $\delta_k(\beta) = \delta_1(\gamma)\delta_k(\alpha)$.

Proof. Use induction on n and Lemma 1.5. Note all row multiplication operations preserve each X_k. QED.

Now it is easy to check that δ_i and δ_j agree on $X_i \cap X_j$. Namely, let $\alpha = (\alpha_{k,l}) \in X_i \cap X_j$. We have to prove that $\delta_i(\alpha) = \delta_j(\alpha)$. Since row multiplication operation change $\delta_i(\alpha)$ and $\delta_j(\alpha)$ in the same way (see Corollary 2.6), we can assume that $\alpha_{i,n} = \alpha_{j,n} = 1$. Here are two typical cases which involve the relevant in the general case entries.

When $n = 2, i = 1, j = 2, \alpha = \begin{pmatrix} a & 1 \\ b & 1 \end{pmatrix}$ with $a, b \in D$, we have $\Delta_2(\alpha) = \delta_1(a - b)$ and

$$\Delta_1(\alpha) = \Delta_2 \begin{pmatrix} b & 1 \\ a & 1 \end{pmatrix} \delta_1(-1) = \delta_1(b - a)\delta_1(-1) = \delta_1(a - b).$$

When $n = 3, i = 1, j = 2, \alpha = \begin{pmatrix} a & 1 \\ b & 1 \\ c & d \end{pmatrix}$ with a, b, c being 2-rows and $d \in D$, we have

$$\Delta_2(\alpha) = \Delta_3 \begin{pmatrix} a & 1 \\ c & d \\ b & 1 \end{pmatrix} \delta_1(-1) = \delta_2 \begin{pmatrix} a - b \\ c - db \end{pmatrix} \delta_1(-1)$$

and

$$\Delta_1(\alpha) = \Delta_3 \begin{pmatrix} c & d \\ b & 1 \\ a & 1 \end{pmatrix} \delta_1(-1) = \delta_2 \begin{pmatrix} c - da \\ b - a \end{pmatrix} \delta_1(-1).$$

It remains to notice that $\begin{pmatrix} a - b \\ c - db \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & -d \end{pmatrix} \begin{pmatrix} c - da \\ b - a \end{pmatrix}$

and

$$\begin{pmatrix} 0 & -1 \\ 1 & -d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ d-1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$ QED.

Thus, we have a well-defined mapping

$$\delta_n : \mathrm{GL}_n D = \cup X_k \to \mathrm{GL}_1 D/[\mathrm{GL}_1 D, \mathrm{GL}_1 D].$$

By Corollary 2.6, for every $\alpha \in \mathrm{GL}_n D$ and every diagonal matrix $\beta = \mathrm{diag}(d_1, \ldots, d_n)$,

$$\delta_n(\beta\alpha) = \delta_1(d_1 \cdots d_n)\delta_n(\alpha) = \delta_n(\beta)\delta_n(\alpha).$$

Also it is now obvious that
$\delta_n(\beta\alpha) = \delta_n(\alpha) = \delta_n(\beta)\delta_n(\alpha)$
for every elementary matrix β.

Therefore
$\delta_n(\beta\alpha) = \delta_n(\beta)\delta_n(\alpha)$
whenever β is product of elementary and diagonal matrices. Using Theorem 2.1 we conclude that δ_n is multiplicative (i.e., group morphism). Finally,
$\delta_n \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix} = \Delta_n \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix} = \delta_{n-1}(\beta)$ by definition. QED.

Systems of linear equations

The system of linear equations over any division ring D can be solved by elementary operations, in the same way as in commutative case. Let

$$\alpha x = b$$

be an arbitrary system of linear equations. Here α is a given m by m matrix over D (the coefficient matrix), b a given column with m entries in D, and x is a column of n distinct unknowns.

We do elementary operations on the augmented matrix (α, b). Namely, to solve the system, we bring α to a diagonal form by row addition operations and column permutation operations.

We can drop any zero row in the augmented matrix because it gives a redundant equation $0 = 0$. If we have a zero row in the coefficient matrix but the correspondind entry in the last column of the augmented matrix is nonzero, then the rest of the augmented matrix is redundant , and our system is equivalent to the equation $0 = 1$, i.e., there are no solutions.

Otherwise, the diagonal form has all diagonal entries nonzero, and they can be all made 1 by row multiplication operations. So the final answer has one of the following four forms:

(a) $0 = 1$ (the system has no solutions);

(b) x is arbitrary (every x is a solution; equivalently, the augmented matrix is the zero matrix);

(c) $y = \beta z + c$ with arbitrary z where z is a set of $r \geq 1$ unknows in x with $r \leq m$ and y is a set of remaining $n - r \geq 1$ unknowns (so the column $\begin{pmatrix} y \\ z \end{pmatrix}$ is a permutation of the column x); when $r = n$ (hence $n \le m$) there is no β and we have exactly one solution $x = c$.

When $b = 0$ i.e., the system is homogeneous, the outcome (a) is impossible If in addition $n > m$, then the system has a nonzero solution. In other words, any $m+1$ columns in D^n are linearly dependent.

As a corollary, we obtain that every finite-dimensional right vector space V over a division ring D is isomorphic to D^n for an unique n (the dimension of V) hence the endomorphism ring of V is isomorphic to $M_n D$ and the isomorphism group of V is isomorphic to $GL_n D$.

Another corollary is that the number r in (c) (the dimension of the affine space of solutions) is determined by the augmented matrix. Namely, r is the dimension of the vector space of solutions to $\alpha x = 0$.

For an arbitrary associative ring A with 1, the right A-modules A^n and A^m could be isomorphic for $n \neq m$. Also solving systems of linear equations over A could be intractable. We consider now three examples when an explicit description of all solutions is possible.

Example 2.7. Let A be a commutative principal ideal domain (PID, e.g., $A = \mathbf{Z}$, the integers). Then every system $\alpha x = b$ can be solved as follows. It is well known [J] that there are matrices $\beta \in \mathrm{GL}_m A$ and $\gamma \in \mathrm{GL}_n A$ such that the m by n matrix $\beta\alpha\gamma$ is diagonal. (Now we cannot always get away with a permutation matrix γ; for Euclidean rings A we can restrict β and γ to $\mathrm{E}_m A$ and $\mathrm{E}_n A$ respectively.)

Our system $\alpha x = b$ is equivalent to $\beta\alpha\gamma(\gamma^{-1}x) = \beta b$ but now every equation involves only one of new variables y_0 and can be easily solved, i.e, simplified to the equation $0 = 1$ or $y_0 = b_0$.. Thus, the answer is either

(a) $0 = 1$ (there are no solutions)

or

(b) $x = \delta z + c$ where δ is an n by r matrix consisting of r columns of the matrix β, the column z consists of r free parameters selected from n new variables $\gamma^{-1}x$, and $0 \le r \le m, n$.

Example 2.8. Let A be an arbitrary associative ring with 1 and $1 \le m \le n$. Let α be a unimodular m by n matrix over A, that is, there is an n by m matrix over A such that $\alpha\beta = 1_m$. We will describe all solutions x for the system $\alpha x = b$ of m linear equations for n variables, with arbitrary column $b \in A^m$.

The general solution is

$$x = \beta b + (1_n - \beta\alpha)y \tag{1}$$

with free parameters $y \in A^n$. (So the solution space for the homogeneous system $\alpha z = 0$ is the column space of the idenpotent matrix $(1_n - \beta\alpha) = (1_n - \beta\alpha)^2$.)

Indeed, an easy direct computation shows that every x of the above form is a solution for the system. Conversely, for any solution x we have

$$x = \beta b + 1_n(x - \beta b) = \beta b + (1_n - \beta\alpha + \beta\alpha)(x - \beta b) = \beta b + (1_n - \beta\alpha)(x - \beta b)$$

$$= \beta b + (1_n - \beta\alpha)y$$

with $y = x - \beta b$.

In particular, when $m = n$ and $\alpha \in GL_n A$ we obtain the unique solution $x = \alpha^{-1} b$ of the system.

In the case when A is commutative and $m = 1 < n$, there is an alternative parameterization [VS] of all solutions. Namely, in this case, choosing any i, j such that $1 \leq i < j \leq n$ we get a solution $z = e_i a_j - e_j a_i$ to $\alpha z = 0$ where $\alpha = (a_k)$ and e_k is the k-th column of 1_n. Every solution z to this homogeneous equation is a linear combination of these special solutions. (It suffices to show this for the columns of the matrix $1_n - \beta\alpha$ which is an easy exercise) So every solution to $\alpha x = b$ is the sum of βb and the linear combination z.

Example 2.9. Example 2.7 can be extended to noncommutative PIDs (including the division rings) and ever to more general rings A, namely, the right Bézout domains (see Exersice 23 in Section 1).

Now we describe how to solve any system $\alpha x = b$ over such a ring A where α is a given m by n matrix over A and $b \in A^m$. As in Example 2.7, we reduce the system to an equivalent system where every equation involves only one unknown.

If $m = n = 1$, there are the following three possible outcomes:

when $\alpha = b = 0$, every x is a solution;

when $b \notin \alpha A$, there are no solutions;

when $\alpha \neq 0$ and $b \in \alpha A$, there is exactly one solution.

Next we consider that case when $m = 1 = n-1$. We write $\alpha = (a, b)$ and $aA + bA = cA$ with $c \in A$. Then we write

$$a = ca_0, b = cb_0, c = ac_9 + bd_0$$

with $a_0, b_0, c_0, d_0 \in A$.

The case $b = 0$ can be dealt with as above, so we assume that $b \neq 0$ hence $c \neq 0$ and $a_0 c_0 + b_0 d_0 = 1$. Then we write similarly $(1 - c_0 a_0, -c_0 b_0) = e(u, v)$ with $e, u, v \in A$ and unimodular u, v. So $uu' + vv' = 1$ for some $u', v' \in A$.

Note that $(1 - c_0 a_0, -c_0 b_0) \begin{pmatrix} c_0 \\ d_0 \end{pmatrix} = 0$ hence

$$\begin{pmatrix} a_0 & b_0 \\ u & v \end{pmatrix} \begin{pmatrix} c_0 & u' \\ d_0 & v' \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

A row addition operation replaces the right-hand side by 1_2 (and changes u', v'). Thus,

$$\begin{pmatrix} a_0 & b_0 \\ u & v \end{pmatrix} \begin{pmatrix} c_0 & u' \\ d_0 & v' \end{pmatrix} = 1_2.$$

We want to conclude that these two matrices are inverse to each other (i.e.,both belong to $\mathrm{GL}_2 A$). This is true in the case when A is a division ring because in this case the matrices can be made diagonal by additional operations (see Exercise 22 below). In general, A can be embedded into a division ring (see Exercise 23 in Section 1) once we check the Ore condition (see Exercise 24 in Section 1)

Now we can rewrite our linear equation $(a, b)x = b$ as $(c, 0)y = b$ with $(c, 0) = (a, b) \begin{pmatrix} c_0 & u' \\ d_0 & v' \end{pmatrix}$ and $y = \begin{pmatrix} a_0 & b_0 \\ u & v \end{pmatrix} x$, so by invertible change of variables we are reduced to the case $m = n = 1$.

If $m = 1$ and $n > 2$, we proceed by induction on the number n of variables. We can multiply the row α by an invertible matrix of the form $\begin{pmatrix} 1_{n-2} & 0 \\ 0 & \beta \end{pmatrix}$ with $\beta \in \mathrm{GL}_2 A$ to kill the last entry in α.

Now we proceed by induction on the number m of equation. First we solve the first equation. If it has no solution, the system has no solutions. Otherwise, after an invertible linear change of variables, the equation has the form $x_1 = c_0$. Eliminating x_1 from the other equations, we are reduced to a smaller system, one variable and one equation less.

The final answer, as in commutative case, has one of the following forms:

(a) $0 = 1$ (there are no solutions)

or

(b) $x = \delta z + c$ where δ is an n by r matrix consisting of r columns of an invertible matrix β, the column z consists of $r \geq 0$ free parameters selected from n new variables and $0 \leq r \leq m, n$.

In the case (b), we have an 1-1 correspondence between the set of solutions and A^r.

Example 2.9. For an arbitrary associative ring A with 1 and an arbitrary system $\alpha x = b$ of linear equations, we have no method of findind a solution or describing all solutions. What is clear, that given a solution x every solution has the form $x + z$ where z is a solution to the homogeneous system $\alpha z = 0$. The set Z of all such z is an A-submodule of A^n. In Examples 2.7 and 2.9, this submodule Z was free.

In Example 2.8, Z was stably free. Namely Z was the column space of the idenpotent matrix $1_n - \beta\alpha$ and $A^n = (1_n - \beta\alpha)A^m \oplus \alpha\beta A^n$ the second summand being a free A-module $A^m \subset A^n$ consisting of columns with that last $n - m$ being 0. (Here is an example when the solution space Z is not free: A is the ring of real-valued continuous function on the sphere $x^2 + y^2 + z^2 = 1$ and Z is given by the linear equation $xu + yv + zw = 0$ for unknown $u, v, w \in A$.)

In general, Z is not free nor stably free. When A is right Noetherean, Z is finitely generated, i.e., a finite set of solutions span all solutions. Another interesting case is when every finitely generated right ideal of A has two generators (see Example 22 in Section 1). Then Z has $2n$ generators.

Exercises.

1. For the Hamilton quaternions $D = \mathbf{H}$, prove that the δ_1 is the norm. That is, check that every quaternion of norm 1 belongs to $[\mathrm{GL}_1 D,\ \mathrm{GL}_1 D]$ (in fact, it is a commutator). The Hamilton quaternions can be defined as the 4-tuples $a+bi+cj+dk$ of real numbers a, b, c, d with the obvious addition and an associative multiplication determined by $i^2 = j^2 = -1, ij = k = -ji$.

We can define an involution on D by $(a + bi + cj + dk)^* = a - bi - cj - dk$. Show that $(x - y)^* = x^* - y^*$ and $(xy)^* = y^* x^*$ for all $x, y \in D$.

We can define the norm N on D by $N(x) = x^* x$. Show that $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$ for any $a, b, c, d \in D$ and that the multiplicative inverse of $x \neq 0$ is $x^*/N(x)$.

We can consider D as a two-dimensional left vector $\mathbf{C} + \mathbf{C}j$ space over the subfield

$\mathbf{C} = \mathbf{R} + \mathbf{R}i$. Namely,

$$a + bi + cj + dk = (a + bi) + (c + di)j.$$

Check that the right multiplication by a quaternion $c_1 + c_2 j$ has the matrix $\begin{pmatrix} c_1 & c_2 \\ -c_3^* & c_1^* \end{pmatrix}$ where $c_1, c_2 \in \mathbf{C}$ and that the norm of $c_1 + c_2 j$ is the determinant of the matrix.

2. Construct a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2 D$ over a division ring D such that $ad - bc = 0$.

3. Construct a matrix $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2 D$ over a division ring D with $ad - bc = 1$ but α is not invertible.

4. Let D be a division ring, $n \geq 2$, and let α be a nonzero matrix in $\mathrm{M}_n D$ which is not invertible. Prove that by row and column addition operations, α can be reduced to a diagonal matrix of the form $\begin{pmatrix} 1_m & 0 \\ 0 & 0 \end{pmatrix}$. Prove that the number m here (the rank of α) does not depend on reduction. (For $\alpha \in \mathrm{GL}_n D$, the rank is n.)

5. Let D be a division ring. Prove that a matrix $\alpha \in \mathrm{M}_n D$ is similar (i.e., conjugated) to an elementary matrix if and only if α has the form $\alpha = 1_n + vu$ where u is an n-row over D, v is an n-column over D, and $uv = 0$,

6. For any ring A with 1 and any $x, y \in \mathrm{GL}_1 A$, check that $x(y^2 - 1)$ is a sum of elements of the form $\gamma a \gamma - a$ with $a \in A, \gamma \in \mathrm{GL}_1 A$.

7. Find an associative ring A with $1 \neq 0$ such that the group $\mathrm{GL}_n A$ is perfect for each $n \geq 1$.

8. An associative ring A with $1 \neq 0$ is called *local* if $A \backslash \mathrm{GL}_1 A$ is an ideal of A. Let $\mathrm{rad}(A)$ denote this ideal (in the next section we define the Jacobson ideal $\mathrm{rad}(A)$ for any ring A).

Prove that for any local ring A the factor ring $A/\mathrm{rad}(A)$ is a division ring.

9. Prove that a matrix $\alpha \in \mathrm{M}_n A$ over a local ring A is invertible if and only if its reduction modulo $\mathrm{rad}(A)$ is invertible.

10. Prove that a factor ring $\mathbf{Z}/m\mathbf{Z}$ of the integers $\mathbf{Z}$ is local if and only if m is divisible by exactly one prime number.

11. Let A be an associative ring with 1, and let $A[[x]]$ be the ring of formal series over A in x (commuting with A), Prove that $A[[x]]$ is local if and only if A is a local.

12. Prove Theorem 2.1 with the division ring D there replaced by an arbitrary local ring.

13. Prove Corollary 2.2 with the division ring D there replaced by an arbitrary local ring A; in the case $n = 2$ assume that $A/\mathrm{rad}(A)$ has at least 4 elements.

14. Let A be an associative ring with $1 \neq 0$, Let X_k $(k = 1, \ldots, n)$ be the set of matrices $\alpha = (\alpha_{ij}) \in \mathrm{GL}_n A$ with $\alpha_{k,n} \in \mathrm{GL}_1 A$. Assume that $n \geq 2$. Prove that $\mathrm{GL}_n A$ is the union of X_k if and only if A is local.

15. Prove Theorem 2.4 with the division ring D there replaced by an arbitrary local ring.

16. Is there an associative ring A with $1 \neq 0$ which is not local but still has the following property: $1 + x \in \mathrm{GL}_1 A$ for every $x \in A \backslash \mathrm{GL}_1 A$?

17. Prove that the direct product of two nonzero rings is not local.

18. Prove that a factor ring of a local ring is either local or 0.

19. Prove that the matrix ring M_2A is never a local ring.

20. For a local ring A, check that the condition of Lemma 1.6 holds if and only if $A/\mathrm{rad}(A)$ has at least 4 elements. (Hint: use Exercise 6 above.)

21. For a local ring A, check that $\mathrm{E}_2A = [\mathrm{E}_2A, \mathrm{GL}_2A]$ when $A/\mathrm{rad}(A)$ has 3 elements.

22. Let A be a local ring, $x, y \in A$, and $xy = 1$. Prove that $yx = 1$. More generally, let $n \geq 1; x, y \in \mathrm{M}_nA; xy = 1_n$. Prove that $yx = 1_n$.

23. Let D be a division ring, $n \geq 1$. Prove that every matrix $\alpha \in \mathrm{GL}_nD$ can be written as $\alpha = \beta\pi\gamma$ where $\beta \in \mathrm{GL}_nD$ is an upper triangular matrix with ones along the main diagonal, $\pi \in \mathrm{GL}_nD$ is a permutation matrix, and $\gamma \in \mathrm{GL}_nD$ is an upper triangular matrix. Prove that the permutation matrix π is determined by α. (In the case when D commutative, this decomposition is a particular case of the Bruhat decomposition.)

24. Let D be a division ring, $n \geq 2$, $\alpha \in \mathrm{GL}_nD$, and $\lambda + i, \mu_i \in \mathrm{GL}_1D$. Assume that $\delta_n(\alpha) = \delta_1(\prod_{i=1}^n \lambda_i, \mu_i)$ in $\mathrm{GL}_1D/[\mathrm{GL}_1D,\ \mathrm{GL}_1D]$. Assume also that α is not central. Prove that α is similar to $\beta\gamma$ where β is a lower triangular matrix with $\lambda_1, \ldots, \lambda_n$ along the diagonal, γ is an upper triangular matrix with $\mu_1, \ldots, \mu_{n-1}, \mu_n\varepsilon$ along the diagonal with $\varepsilon \in [\mathrm{GL}_1D,\ \mathrm{GL}_1D]$.

25. Let D be a division ring, $n \geq 2$. Show that for every matrix $\alpha \in \mathrm{M}_nD$ there are invertible matrices $\beta, \gamma \in \mathrm{GL}_nD$ such that all diagonal entries of the matrix $\beta\alpha\gamma$ are zeros.

26. Let D be a division ring, $n \geq 1$. Show that every matrix $\alpha \in \mathrm{M}_nD$ is a sum of two invertible matrices except for the case when $\mathrm{card}(D) = 2, n = 1$, and $\alpha = 1$.

27. Let A be a commutative ring with 1. Let $a, b \in A$ and $Aa + Ab = A$. Show that $Aa \cap Ab = Aab$.

28. Let A be a finitely-dimensional associate algebra with 1 over a field (i.e., the center of A contains a field F as a subring and A is finite-dimensional as an F-vector space). Assume A has no zero divisors. Prove that A is a division ring.

29. Let F be a field, A be a 4-dimensional vector space over$F$ with the basis $1, i, j, k$. Make an associative ring from A defining the multiplication by $i^2 = j^2 = -1, ij = -ji = k$, and F belongs to the center of A. Prove that A is a division ring if and only if the sum of 4 squares is anisotropic over F (i.e., the sum of 4 squares in F is zero only if each square is zero).

In the case when A is a division ring, prove that every $a + bi + cj + dk \in A$ with $a^2 + b^2 + c^2 + d^2 = 1$ is a commutator in the multiplicative group GL_1A (cf., Exercise 1).

30. Let α be an m by n matrix over a division ring D. Let S be a maximal set of linearly independent rows of α, and let S' be a maximal set of linearly independent columns of α. Prove that $\mathrm{card}(S) = \mathrm{card}(S')$ (= the rank of α, cf., Exercise 4).

31. Solve the following systems of linear equations for 2 unknowns x, y over the Hamilton quaternions D (see Exercise 1):

(a) $\begin{cases} ix + y = 1, \\ x + iy = 2. \end{cases}$

(b) $\begin{cases} ix + y = 1, \\ -x + iy = 2. \end{cases}$

(c) $\begin{cases} ix + y = 1, \\ -x + iy = i. \end{cases}$

32. Solve for $x, y, z \in \mathbf{Z}$ the linear equation $8x - 4y + 6z = 2$.

33. Solve for $x, y \in A$ the linear equation $zx + (e^z - 1)y = z^2$ over the ring A of entire functions in z.

34. Solve for $x, y \in A$ the linear equation $2^{1/2}x + 3^{1/3}y = 1$ over the ring A of all algebraic integers.

35. Solve for $f, g \in A$ the linear equation $(d/dx)f + xg = x^2$ in the ring A of differential operators with polynomial coefficients in x.

36. Solve for $x, y \in M_2(\mathbf{Z})$ the linear equation

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} x + \begin{pmatrix} 5 & 1 \\ 7 & 0 \end{pmatrix} y = \begin{pmatrix} 6 & 1 \\ 3 & 2 \end{pmatrix}.$$

37. Let D be a division ring and $n \geq 1$. Consider D^n as a left module over $M_n D$. Prove that this module is simple (there are no proper submodules) and that its endomorphism rind is D.

38. Let V be a right module over an associative ring A with 1. Prove that its endomorphism ring is a division ring if V is simple (has exactly two submodules, namely 0 and V).

39. Let A be a commutative ring with 1, $m < n$, and α a unimodular m by n matrix over A. Let Z be the set of z such that $\alpha z = 0$. Choosing any $m+1$ columns of α we get a solution $z \in Z$ in terms of the m by m minors of this submatrix (with $n - m - 1$ variables being 0).

Prove that every solution $z \in Z$ is a linear combination of these special solutions, i.e., they span Z.

In the case $m = 1$, this parameterization is given in [VS] as mentioned in Example 2.8 above.

40. (Open problem) Is there a commutative Bézout domain A with 1 and a matrix in $M_2 A$ which cannot be reduced to a digonal matrix by multiplying it on the right and left with invertible matrices?

41. Prove that if A is a Bézout domain then for every n every finitely generated right ideal of the matrix ring $\mathrm{M}_n A$ is principal.