Chapter II
The Basic Local-Global Principle and Systems of Linear Equations

In this chapter, as in the entirety of this manuscript unless explicitly stated otherwise, rings are commutative and unitary, and homomorphisms between rings preserve the multiplicative identities. In particular, a subring has the same multiplicative identity as the whole ring.

Introduction

Solving systems of linear equations is an omnipresent theme of commutative algebra, in particular in its most developed form for which homological methods are at use. In this chapter, we recall some classical results on this topic, which we will come back to often throughout this work.

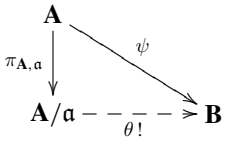
Particular attention is given to the basic local-global principle, the notion of a coherent module and some variants of Cramer's formula.

1 Some Facts Concerning Quotients and Localizations

Let us begin by recalling the following result on quotients. Let $\mathfrak{a}$ be an ideal of a ring $\mathbf{A}$. When needed, the canonical mapping will be denoted by $\pi_{\mathbf{A},\mathfrak{a}} : \mathbf{A} \to \mathbf{A}/\mathfrak{a}$.

The quotient ring $(\mathbf{A}/\mathfrak{a}, \pi_{\mathbf{A},\mathfrak{a}})$ is characterized, *up to unique isomorphism*, by the following universal property.

1.1 Fact (Characteristic property of the quotient by the ideal $\mathfrak{a}$) *A ring homomorphism $\psi : \mathbf{A} \to \mathbf{B}$ is factorized by $\pi_{\mathbf{A},\mathfrak{a}}$ if and only if $\mathfrak{a} \subseteq \operatorname{Ker}\psi$, meaning $\psi(\mathfrak{a}) \subseteq \{0_{\mathbf{B}}\}$. In this case, the factorization is unique.*



homomorphisms vanishing on $\mathfrak{a}$.

© Springer Science+Business Media Dordrecht 2015

H. Lombardi and C. Quitté, *Commutative Algebra: Constructive Methods*,
Algebra and Applications 20, DOI 10.1007/978-94-017-9944-7_II

Explanation regarding the figure. *In a figure of the type found above, everything but the morphism θ corresponding to the dotted arrow is given. The exclamation mark signifies that θ makes the diagram commute and that it is* the unique *morphism with this property.*

We denote by $M/\mathfrak{a}M$ the $\mathbf{A}/\mathfrak{a}$-module obtained from the quotient of the $\mathbf{A}$-module M by the submodule generated by the elements ax for $a \in \mathfrak{a}$ and $x \in M$. This module can thus be defined through the extension of scalars to $\mathbf{A}/\mathfrak{a}$ from the $\mathbf{A}$-module M (see p. 191, and Exercise IV-5).

Let us move on to localizations, which are very analogous to quotients (we will return to this analogy in further detail on p. 635). In this work, when referring to a *monoid* contained within a ring (i.e. a submonoid of a ring) we always assume a subset of the ring which contains 1 and is closed under multiplication.

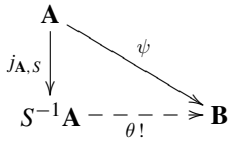
For a given ring $\mathbf{A}$, we denote by $\mathbf{A}^\times$ the multiplicative group of invertible elements, also called the *group of units*.

If S is a monoid, we denote by $\mathbf{A}_S$ or $S^{-1}\mathbf{A}$ the localization of $\mathbf{A}$ at S. Every element of $\mathbf{A}_S$ can be written in the form x/s with $x \in \mathbf{A}$ and $s \in S$.

By definition we have $x_1/s_1 = x_2/s_2$ if there exists an $s \in S$ such that $ss_2x_1 = ss_1x_2$. When needed, we will denote by $j_{\mathbf{A},S} : \mathbf{A} \to \mathbf{A}_S$ the canonical mapping $x \mapsto x/1$.

The localized ring $(\mathbf{A}_S, j_{\mathbf{A},S})$ is characterized, *up to unique isomorphism*, by the following universal property.

1.2 Fact (Characteristic property of the localization at S) *A ring homomorphism $\psi : \mathbf{A} \to \mathbf{B}$ is factorized by $j_{\mathbf{A},S}$ if and only if $\psi(S) \subseteq \mathbf{B}^\times$. When this is the case, the factorization is unique.*



homomorphisms which send S into $\mathbf{B}^\times$.

Similarly, we denote by $M_S = S^{-1}M$ the $\mathbf{A}_S$-module obtained by localization of the $\mathbf{A}$-module M at S. Every element of M_S is of the form x/s with $x \in M$ and $s \in S$. By definition, we have $x_1/s_1 = x_2/s_2$ if there exists an $s \in S$ such that $ss_2x_1 = ss_1x_2$. This module M_S can also be defined through an extension of scalars to $\mathbf{A}_S$ from the $\mathbf{A}$-module M (see p. 191, and Exercise IV-5).

The monoid S contained in a ring $\mathbf{A}$ is called *saturated* when

$$\forall s, t \in \mathbf{A} \quad (st \in S \;\Rightarrow\; s \in S)$$

is satisfied. A saturated monoid is also called a *filter*. A *principal filter* is a filter generated by a single element; that is, it is just the set of divisors of some arbitrary power of that element. We denote by S^{sat} the saturation of the monoid S; it is obtained by adding all elements dividing an element of S. When we saturate a monoid, the

localization remains unchanged.[1] Two monoids S_1 and S_2 are said to be *equivalent* if they have the same saturation. We then write $\mathbf{A}_{S_1} = \mathbf{A}_{S_2}$.

> It is possible to localize by a monoid which contains 0.
> The result is then the *trivial* ring (recall that a ring is trivial if it is reduced to a single element, i.e. if $1 = 0$).

If S is generated by $s \in \mathbf{A}$, i.e. if $S = s^{\mathbb{N}} \stackrel{\text{def}}{=} \{ s^k \mid k \in \mathbb{N} \}$, we denote by $\mathbf{A}_s$ or $\mathbf{A}[1/s]$ the localized ring $S^{-1}\mathbf{A}$, which is isomorphic to $\mathbf{A}[T]/\langle sT - 1 \rangle$.

In a ring, the *conductor* of an ideal $\mathfrak{a}$ into an ideal $\mathfrak{b}$ is the ideal

$$(\mathfrak{b} : \mathfrak{a})_{\mathbf{A}} = \{ a \in \mathbf{A} \mid a\mathfrak{a} \subseteq \mathfrak{b} \}.$$

More generally, if N and P are submodules of an $\mathbf{A}$-module M, we define the *conductor* of N into P as the ideal

$$(P : N)_{\mathbf{A}} = \{ a \in \mathbf{A} \mid aN \subseteq P \}.$$

Recall also that the *annihilator* of an element x from an $\mathbf{A}$-module M is the ideal $\mathrm{Ann}_{\mathbf{A}}(x) = (\langle 0_{\mathbf{A}} \rangle : \langle x \rangle) = \{ a \in \mathbf{A} \mid ax = 0 \}$.

The *annihilator of a module* M is the ideal $\mathrm{Ann}_{\mathbf{A}}(M) = (\langle 0_M \rangle : M)_{\mathbf{A}}$. A module or an ideal is *faithful* if its annihilator is reduced to 0.

The following notations are also useful for a submodule N of M.

$$(N : \mathfrak{a})_M = \{ x \in M \mid x\,\mathfrak{a} \subseteq N \}.$$
$$(N : \mathfrak{a}^\infty)_M = \left\{ x \in M \mid \exists n,\ x\,\mathfrak{a}^n \subseteq N \right\}.$$

The latter submodule is called the *saturation* of N by $\mathfrak{a}$ in M.

We say that an element x of an $\mathbf{A}$-module M is *regular* (if $M = \mathbf{A}$ we also say that x is a *nonzerodivisor*) if the sequence

$$0 \longrightarrow \mathbf{A} \xrightarrow{.x} M$$

is exact; in other words if $\mathrm{Ann}(x) = 0$. If $0_{\mathbf{A}}$ is a regular in $\mathbf{A}$, the ring is trivial.

When the context is unambiguous, we omit the $\mathbf{A}$ or M subscript to simplify the previous notations regarding conductors.

The *total ring of fractions* or *total quotient ring* of $\mathbf{A}$, denoted by $\mathrm{Frac}\,\mathbf{A}$, is the localized ring $\mathbf{A}_S$, where S is the monoid of regular elements of $\mathbf{A}$, denoted by $\mathrm{Reg}\,\mathbf{A}$.

[1] In fact, depending on the specific construction chosen to define localization, we would either have an equality or a canonical isomorphism between the two localizations.

1.3 Fact

1. *The kernel of the natural homomorphism* $j_{\mathbf{A},s} : \mathbf{A} \to \mathbf{A}_s = \mathbf{A}[1/s]$ *is the ideal* $(0 : s^\infty)_\mathbf{A}$. *It is reduced to* 0 *if and only if* s *is regular.*
2. *Similarly, the kernel of the natural homomorphism of* M *to* $M_s = M[1/s]$ *is the* $\mathbf{A}$*-submodule* $(0 : s^\infty)_M$.
3. *The natural homomorphism* $\mathbf{A} \to \operatorname{Frac}\mathbf{A}$ *is injective.*

1.4 Fact *If* $S \subseteq S'$ *are two monoids of* $\mathbf{A}$ *and* M *is an* $\mathbf{A}$*-module, we have two canonical identifications* $(\mathbf{A}_S)_{S'} \simeq \mathbf{A}_{S'}$ *and* $(M_S)_{S'} \simeq M_{S'}$.

2 The Basic Local-Global Principle

We will study the general workings of the local-global principle in commutative algebra in Chap. XV. However, we will encounter it at every turn, under different forms adapted to each situation. In this section, an essential instance of this principle is given as it is so simple and efficient that it would be a pity to go without it any longer.

The local-global principle affirms that certain properties are true if and only if they are true after "sufficiently many" localizations. In classical mathematics we often invoke localization at every maximal ideal. It is a lot of work and seems a bit mysterious, especially from an algorithmic point of view. We will use simpler (and less intimidating) versions in which only a finite number of localizations are used.

Comaximal Localizations and the Local-Global Principle

The following definition corresponds to the intuitive idea that certain (finite) systems of localizations of a ring $\mathbf{A}$ are "sufficiently numerous" to capture all the information contained within $\mathbf{A}$.

2.1 Definition

1. Let $s_1, \dots, s_n$ be elements. if $\langle 1\rangle = \langle s_1, \dots, s_n\rangle$ then $s_1, \dots, s_n$ are said to be *comaximal*.
2. Let $S_1, \dots, S_n$ be monoids. If for every $s_1 \in S_1, \dots, s_n \in S_n$, the s_i's are comaximal then $S_1, \dots, S_n$ are called *comaximal*.

Two Fundamental Examples

1) If $s_1, \dots, s_n$ are comaximal then the monoids they generate are comaximal. Indeed, consider every $s_i^{m_i}$ $(m_i \geqslant 1)$ in the monoids $s_i^{\mathbb{N}}$ and let $a_1, \dots, a_n$ be such that $\sum_{i=1}^n a_i s_i = 1$. By raising the latter equality to the power of $1 - n + \sum_{i=1}^n m_i$ and by conveniently regrouping the terms in the resulting sum, we get an equality of the form $\sum_{i=1}^n b_i s_i^{m_i} = 1$, as required.

2) If $a = a_1 \cdots a_n \in \mathbf{A}$, then the monoids $a^{\mathbb{N}}, 1+a_1\mathbf{A}, \ldots, 1+a_n\mathbf{A}$ are comaximal. Indeed, take an element $b_i = 1 - a_i x_i$ in each monoid $1 + a_i\mathbf{A}$ and an element a^m in the monoid $a^{\mathbb{N}}$. We need to prove that the ideal $\mathfrak{m} = \langle a^m, b_1, \ldots, b_n\rangle$ contains 1. However, modulo $\mathfrak{m}$ we have $1 = a_i x_i$, thus $1 = a\prod_i x_i = ax$, and we finally obtain $1 = 1^m = a^m x^m = 0$. ∎

Here is a characterization from classical mathematics.

2.2 Fact* Let $S_1, \ldots, S_n$ be monoids in a nontrivial ring $\mathbf{A}$ (i.e., $1 \neq_{\mathbf{A}} 0$). The monoids S_i are comaximal if and only if for every prime ideal (resp. for every maximal ideal) $\mathfrak{p}$ one of the S_i is contained within $\mathbf{A}\backslash\mathfrak{p}$.

▷ Let $\mathfrak{p}$ be a prime ideal. If none of the S_i's are contained in $\mathbf{A}\backslash\mathfrak{p}$ then for each i there exists some $s_i \in S_i \cap \mathfrak{p}$. Consequently, $s_1, \ldots, s_n$ are not comaximal.

Conversely, suppose that for every maximal ideal $\mathfrak{m}$ one of the S_i's is contained within $\mathbf{A}\backslash\mathfrak{m}$ and let $s_1 \in S_1, \ldots, s_n \in S_n$ then the ideal $\langle s_1, \ldots, s_n\rangle$ is not contained in any maximal ideal. Thus it contains 1. □

We denote by $\mathbf{A}^{m\times p}$ or $\mathbb{M}_{m,p}(\mathbf{A})$ the $\mathbf{A}$-module of m-by-p matrices with coefficients in $\mathbf{A}$, and $\mathbb{M}_n(\mathbf{A})$ means $\mathbb{M}_{n,n}(\mathbf{A})$. The group of invertible matrices is denoted by $\mathbb{GL}_n(\mathbf{A})$, the subgroup consisting of the matrices of determinant 1 is denoted by $\mathbb{SL}_n(\mathbf{A})$. The subset of $\mathbb{M}_n(\mathbf{A})$ consisting of the projection matrices (i.e. matrices F such that $F^2 = F$) is denoted by $\mathbb{AG}_n(\mathbf{A})$. The acronyms are explained as follows: $\mathbb{GL}$ for linear group, $\mathbb{SL}$ for special linear group and $\mathbb{AG}$ for affine Grassmannian.

2.3 Concrete local-global principle (Basic local-global principle, concrete gluing of solutions of a system of linear equations) *Let $S_1, \ldots, S_n$ be comaximal monoids of $\mathbf{A}$, B a matrix of $\mathbf{A}^{m\times p}$ and C a column vector of $\mathbf{A}^m$. Then the following properties are equivalent.*

1. *The system of linear equations $BX = C$ has a solution in $\mathbf{A}^p$.*
2. *For $i \in [\![1..n]\!]$, the system of linear equations $BX = C$ has a solution in $\mathbf{A}^p_{S_i}$.*

This principle also holds for systems of linear equations with coefficients in an $\mathbf{A}$-module M.

▷ *1 ⇒ 2.* Clearly true.
2 ⇒ 1. For each i, we have $Y_i \in \mathbf{A}^p$ and $s_i \in S_i$ such that $B(Y_i/s_i) = C$ in $\mathbf{A}^m_{S_i}$. This means that we have some $t_i \in S_i$ such that $t_i BY_i = s_i t_i C$ in $\mathbf{A}^m$. Using $\sum_i a_i s_i t_i = 1$, we get a solution in $\mathbf{A}$: $X = \sum_i a_i t_i Y_i$. □

Remark As to the merits, this concrete local-global principle boils down to the following remark when speaking of an integral ring (a ring is said to be *integral* if every element is null or regular[2]). If every s_i is regular and if

[2]This notion is discussed in further detail on p. 197.

$$\frac{x_1}{s_1} = \frac{x_2}{s_2} = \cdots = \frac{x_n}{s_n},$$

then the common value of these fractions, when $\sum_i s_i u_i = 1$, is also equal to

$$\frac{x_1u_1 + \cdots + x_nu_n}{s_1u_1 + \cdots + s_nu_n} = x_1u_1 + \cdots + x_nu_n.$$

This principle could then also be called "the art of shrewdly getting rid of denominators." Arguably, the most remarkable thing is that this holds in full generality, even if the ring is not integral. Our thanks go to Claude Chevalley for introducing arbitrary localizations. In some scholarly works, we find the following reformulation (at the cost of an information loss regarding the concreteness of the result): the $\mathbf{A}$-module $\bigoplus_{\mathfrak{m}} \mathbf{A}_{1+\mathfrak{m}}$ (where $\mathfrak{m}$ ranges over every maximal ideal of $\mathbf{A}$) is faithfully flat. ∎

2.4 Corollary *Let $S_1, \ldots, S_n$ be comaximal monoids of $\mathbf{A}$, $x \in \mathbf{A}$ and $\mathfrak{a}$, $\mathfrak{b}$ be two finitely generated ideals of $\mathbf{A}$. Then, we have the following equivalences.*

1. *$x = 0$ in $\mathbf{A}$ if and only if for $i \in [\![1..n]\!]$, $x = 0$ on $\mathbf{A}_{S_i}$.*
2. *x is regular in $\mathbf{A}$ if and only if for $i \in [\![1..n]\!]$, x is regular in $\mathbf{A}_{S_i}$.*
3. *$\mathfrak{a} = \langle 1 \rangle$ in $\mathbf{A}$ if and only if for $i \in [\![1..n]\!]$, $\mathfrak{a} = \langle 1 \rangle$ in $\mathbf{A}_{S_i}$.*
4. *$\mathfrak{a} \subseteq \mathfrak{b}$ in $\mathbf{A}$ if and only if for $i \in [\![1..n]\!]$, $\mathfrak{a} \subseteq \mathfrak{b}$ in $\mathbf{A}_{S_i}$.*

▷ The proof is left to the reader. □

Remark In fact, as we will see in the local-global principle 6.7, ideals do not need to be finitely generated. ∎

Examples

Let us give some simple examples of applications of the basic concrete local-global principle. A typical application of the first example (Fact 2.5) is where the module M in the statement is a nonzero ideal of a Dedekind ring. A module M is said to be *locally cyclic* if after each localization at comaximal monoids $S_1, \ldots, S_n$, it is generated by a single element.

2.5 Fact *Let $M = \langle a, b \rangle = \langle c, d \rangle$ be a module with two generator sets. Suppose this module is faithful and locally cyclic. Then, there exists a matrix $A \in \mathbb{SL}_2(\mathbf{A})$ such that $[\, a \; b \,]\, A = [\, c \; d \,]$.*

▷ If $A = \begin{bmatrix} x & y \\ z & t \end{bmatrix}$, the cotransposed matrix must be equal to

$$B = \operatorname{Adj} A = \begin{bmatrix} t & -y \\ -z & x \end{bmatrix}.$$

In particular, we mean to solve the following system of linear equations:

$$[\,a\ b\,]\,A = [\,c\ d\,], \quad [\,c\ d\,]\,B = [\,a\ b\,] \qquad (*)$$

where the unknowns are x, y, z, t. Note that $AB = \det(A)\ \mathrm{I}_2$.

Conversely, if this system of linear equations is solved, we will have $[\,a\ b\,] = [\,a\ b\,]\,A\,B$. So $\big(1-\det(A)\big)[\,a\ b\,] = 0$, and since the module is faithful, $\det(A) = 1$.

We have some comaximal monoids S_i such that M_{S_i} is generated by $g_i/1$ for some $g_i \in M$. To solve the system of linear equations it suffices to solve it after localizing at each of the S_i's.

In the ring $\mathbf{A}_{S_i}$, we have the equalities $a = \alpha_i g_i$, $b = \beta_i g_i$, $g_i = \mu_i a + \nu_i b$, thus $\big(1 - (\alpha_i\mu_i + \beta_i\nu_i)\big)\, g_i = 0$.

The module $M_{S_i} = \langle g_i \rangle$ stays faithful, so $1 = \alpha_i\mu_i + \beta_i\nu_i$ in $\mathbf{A}_{S_i}$. Therefore:

$$[\,a\ b\,]\,E_i = [\,g_i\ 0\,] \ \text{ with } \ E_i = \begin{bmatrix} \mu_i & -\beta_i \\ \nu_i & \alpha_i \end{bmatrix} \text{ and } \det(E_i) = 1.$$

Similarly we obtain $[\,c\ d\,]\,C_i = [\,g_i\ 0\,]$ for some matrix C_i with determinant 1 in $\mathbf{A}_{S_i}$. By taking $A_i = E_i\ \mathrm{Adj}(C_i)$ we get $[\,a\ b\,]\,A_i = [\,c\ d\,]$ and $\det(A_i) = 1$ in $\mathbf{A}_{S_i}$. Thus the system of linear equations $(*)$ has a solution in $\mathbf{A}_{S_i}$. □

Our second example is given by the Gauss-Joyal Lemma: point *1* in the following lemma is proven by applying the basic local-global principle. Before stating this result, we first need to recall some definitions.

An element a of a ring is said to be *nilpotent* if $a^n = 0$ some integer $n \in \mathbb{N}$. The nilpotent elements of a ring $\mathbf{A}$ form an ideal called *the nilradical*, or the *nilpotent radical* of the ring. A ring is *reduced* if its nilradical equals 0. More generally, the nilradical of an ideal $\mathfrak{a}$ of $\mathbf{A}$ is the ideal consisting of elements $x \in \mathbf{A}$, such that each x has some power in $\mathfrak{a}$. We denote the nilradical of an ideal $\mathfrak{a}$ of $\mathbf{A}$ by $\sqrt{\mathfrak{a}}$ or by $\mathrm{D}_{\mathbf{A}}(\mathfrak{a})$. We also use $\mathrm{D}_{\mathbf{A}}(x)$ to denote $\mathrm{D}_{\mathbf{A}}(\langle x \rangle)$. An ideal $\mathfrak{a}$ is called *a radical ideal* when it is equal to its nilradical. The ring $\mathbf{A}/\mathrm{D}_{\mathbf{A}}(0) = \mathbf{A}_{\mathrm{red}}$ is *the reduced ring associated with* $\mathbf{A}$.

For some polynomial f of $\mathbf{A}[X_1, \ldots, X_n] = \mathbf{A}[\underline{X}]$, we call the *content* of f and denote by $\mathrm{c}_{\mathbf{A},\underline{X}}(f)$ or $\mathrm{c}(f)$ the ideal generated by the coefficients of f. The polynomial f is said to be *primitive* (in $\underline{X}$) when $\mathrm{c}_{\mathbf{A},\underline{X}}(f) = \langle 1 \rangle$.

When a polynomial f of $\mathbf{A}[X]$ is given in the form $f(X) = \sum_{k=0}^{n} a_k X^k$, we say that n is the *formal degree* of f, and a_n is its *formally leading coefficient*. Finally, if f is null, its formal degree is -1.

2.6 Lemma

1. (Poor man's Gauss-Joyal) *The product of two primitive polynomials is a primitive polynomial.*
2. (Gauss-Joyal) *For $f, g \in \mathbf{A}[\underline{X}]$, there exists a $p \in \mathbb{N}$ such that*

$$\big(\mathrm{c}(f)\mathrm{c}(g)\big)^p \subseteq \mathrm{c}(fg).$$

3. (Nilpotent elements in $\mathbf{A}[\underline{X}]$) *An element f of $\mathbf{A}[\underline{X}]$ is nilpotent if and only if all of its coefficients are nilpotent. In other words, we have the following equality:* $(\mathbf{A}[\underline{X}])_{\mathrm{red}} = \mathbf{A}_{\mathrm{red}}[\underline{X}]$.
4. (Invertible elements in $\mathbf{A}[\underline{X}]$) *An element f of $\mathbf{A}[\underline{X}]$ is invertible if and only if $f(\underline{0})$ is invertible and $f - f(\underline{0})$ is nilpotent. In other words,* $\mathbf{A}[\underline{X}]^\times = \mathbf{A}^\times + \mathrm{D}_{\mathbf{A}}(0)[\underline{X}]$ *and in particular* $(\mathbf{A}_{\mathrm{red}}[\underline{X}])^\times = (\mathbf{A}_{\mathrm{red}})^\times$.

▷ Note that, a priori, we have the following inclusion: $\mathrm{c}(fg) \subseteq \mathrm{c}(f)\mathrm{c}(g)$.
1. For univariate polynomials $f,\ g \in \mathbf{A}[X]$. We have $\mathrm{c}(f) = \mathrm{c}(g) = \langle 1\rangle$. Consider the quotient ring $\mathbf{B} = \mathbf{A}/\mathrm{D}_{\mathbf{A}}\big(\mathrm{c}(fg)\big)$. We need to prove that this ring is trivial. It suffices to do so after localization at comaximal elements, for example at the coefficients of f. That is, we can suppose that some coefficient of f is invertible. Let us give a proof of a sufficiently general example. Suppose

$$f(X) = a + bX + X^2 + cX^3 + \dots \text{ and } g(X) = g_0 + g_1X + g_2X^2 + \dots$$

In the ring $\mathbf{B}$ we have $ag_0 = 0$, $ag_1 + bg_0 = 0$, $ag_2 + bg_1 + g_0 = 0$, thus $bg_0^2 = 0$, then $g_0^3 = 0$, thus $g_0 = 0$. We then have $g = Xh$ and $c(fg) = c(fh)$. Moreover, since the formal degree of h is smaller than that of g, we can conclude by induction on the formal degree that $g = 0$. As $\mathrm{c}(g) = \langle 1\rangle$, the ring is trivial.
2. For univariate polynomials. Consider a coefficient a of f and a coefficient b of g. We prove that ab is nilpotent in $\mathbf{B} = \mathbf{A}/\mathrm{c}(fg)$. This boils down to proving that $\mathbf{C} = \mathbf{B}[1/(ab)]$ is trivial. However, in $\mathbf{C}$, f and g are primitive, so point *1* implies that $\mathbf{C}$ is trivial.
2 and *1. General case.* Point *2.* is proved by induction on the number of variables from the univariate case. Indeed, for $f \in \mathbf{A}[X][Y]$ we have the equality $\mathrm{c}_{\mathbf{A},X,Y}(f) = \langle \mathrm{c}_{\mathbf{A},X}(h) \mid h \in \mathrm{c}_{\mathbf{A}[X],Y}(f)\rangle$. Then we deduce point *1* from it.
3. Note that $f^2 = 0$ implies $\mathrm{c}(f)^p = 0$ for some p from point *2.*
4. The condition is sufficient: in a ring, if x is nilpotent, then $1 - x$ is invertible because $(1-x)(1+x+\cdots+x^n) = 1-x^{n+1}$. Thus if u is invertible and x nilpotent, $u + x$ is invertible. To see that the condition is necessary it suffices to deal with the univariate case (we conclude by induction on the number of variables). Let $fg = 1$ with $f = f(0) + XF(X)$ and $g = g(0) + XG(X)$. We obtain $f(0)g(0) = 1$. Let n be the formal degree of F and m that of G. We must prove that F and G are nilpotent.

If $n = -1$ or $m = -1$, the result is obvious. We reason by induction on $n + m$ assuming that $n, m \geqslant 0$, F_n and G_m being the formally leading coefficients. By induction hypothesis the result is obtained for the rings $(\mathbf{A}/\langle F_n\rangle)[X]$ and $(\mathbf{A}/\langle G_m\rangle)[X]$. Since $F_nG_m = 0$, we can conclude with the following lemma.
NB: some details are given in Exercise VII-8. □

2.7 Lemma *Let $a, b, c \in \mathbf{A}$. If c is nilpotent modulo a and modulo b, and if $ab = 0$, then c is nilpotent.*

▷ We have $c^n = xa$ and $c^m = yb$ therefore $c^{n+m} = xyab = 0$. □

Remark We can reformulate this lemma in a more structural manner as follows. For two ideals $\mathfrak{a}$, $\mathfrak{b}$ consider the canonical morphism

$$\mathbf{A} \to \mathbf{A}/\mathfrak{a} \times \mathbf{A}/\mathfrak{b}$$

whose kernel is $\mathfrak{a} \cap \mathfrak{b}$. If an element of $\mathbf{A}$ is nilpotent modulo $\mathfrak{a}$ and modulo $\mathfrak{b}$, it is also nilpotent modulo $\mathfrak{a} \cap \mathfrak{b}$, thus also modulo $\mathfrak{ab}$, as $(\mathfrak{a} \cap \mathfrak{b})^2 \subseteq \mathfrak{ab}$. This touches on the "closed covering principle," see p. 640. ∎

Finite Character Properties

The basic concrete local-global principle can be reformulated as a "transfer principle."

2.8 Basic Transfer principle *For some system of linear equations in a ring* $\mathbf{A}$ *the elements* s *such that the system of linear equations has a solution in* $\mathbf{A}[1/s]$ *form an ideal of* $\mathbf{A}$.

Firstly, we invite the reader to prove that this transfer principle is equivalent to the basic concrete local-global principle.

We now provide a detailed analysis of what is going on. The equivalence actually relies on the following notion.

2.9 Definition A property P concerning commutative rings and modules is called a *finite character property* if it is preserved by localization and if, when it holds for $S^{-1}\mathbf{A}$, then it also holds for $\mathbf{A}[1/s]$ for some $s \in S$.

2.10 Fact *Let* P *be a finite character property. Then the concrete local-global principle for* P *is equivalent to the transfer principle for* P. *In other words, the following principles are equivalent.*

1. *If the property* P *is true after localization at every monoid in a family of comaximal monoids, then it is true.*
2. *The set of elements* s *(in a given ring) such that the property* P *is true after localization at* s *is an ideal.*

◗ Let $\mathbf{A}$ be a ring which provides the context for the property P. Now consider the set $I = \{\, s \in \mathbf{A} \mid \mathsf{P} \text{ is true for } \mathbf{A}_s \,\}$.
1 ⇒ *2*. Suppose *1*. Let $s, t \in I$, $a, b \in \mathbf{A}$ and $u = as + bt$. The elements s and t are comaximal in $\mathbf{A}_u$. Since P is closed under localization, P is true for $(\mathbf{A}_u)_s = (\mathbf{A}_s)_u$ and $(\mathbf{A}_u)_t = (\mathbf{A}_t)_u$. By applying *1*, P is true for $\mathbf{A}_u$, i.e., $u = as + bt \in I$.
2 ⇒ *1*. Suppose *2* and let (S_i) be the considered family of comaximal monoids. Since we have a property of finite character, we find in each S_i an element s_i such that P is true after localization at s_i. Since the S_i's are comaximal the s_i's are comaximal elements. By applying *2*, we get $I = \langle 1 \rangle$. Finally, the localization at 1 provides the answer. □

Most of the concrete local-global principles which we will consider in this manuscript apply to finite character properties. One may thus replace any concrete local-global principle with its corresponding transfer principle.

For finite character properties we have an equivalence in classical mathematics between two notions, one concrete and the other abstract. In Chaps. XV and XVII we shall use the concrete version.

2.11 Fact* *Let* P *be a finite character property. Then, in classical mathematics the following properties are equivalent.*

1. *There exist comaximal monoids such that the property* P *is true after localization at each monoid.*
2. *The property* P *is true after localization at every maximal ideal.*

▷ *1* $\Rightarrow$ *2*. Let (S_i) be the family of comaximal monoids under consideration. Since it is a finite character property, we find in each S_i some element s_i such that P is true after localization at s_i. Since the S_i's are comaximal the s_i's are comaximal elements. Let $\mathfrak{m}$ be a maximal ideal. Some s_i is not in $\mathfrak{m}$. The localization at $1+\mathfrak{m}$ is a localization of the localization at s_i. Thus P is true after localization at $1+\mathfrak{m}$.
2 $\Rightarrow$ *1*. For each maximal ideal $\mathfrak{m}$ select an $s_{\mathfrak{m}} \notin \mathfrak{m}$ such that the property P is true after localization at $s_{\mathfrak{m}}$. The set of $s_{\mathfrak{m}}$ generates an ideal which is not contained in any maximal ideal, therefore it is the ideal $\langle 1\rangle$. A finite family of some of these $s_{\mathfrak{m}}$ is then a system of comaximal elements. The family of monoids generated by these elements is suitable. □

We immediately obtain the following corollary.

2.12 Fact* *Let* P *a finite character property. Then the concrete local-global principle for* P *is equivalent (in classical mathematics) to the abstract local-global principle for* P*. In other words, the following principles are equivalent.*

1. *If the property* P *is true after localization at each monoid in a family of comaximal monoids, then it is true.*
2. *If the property* P *is true after localization at every maximal ideal, then it is true.*

Remark Let us give a direct proof of the equivalence from classical mathematics between the transfer principle and the abstract local-global principle for the property P (which we assume is of finite character).

Transfer $\Rightarrow$ *Abstract* Suppose the property is true after localization at every maximal ideal. The ideal given by the transfer principle cannot be strict,[3] otherwise it would be contained in a maximal ideal $\mathfrak{m}$, which contradicts the fact that the property is true after localization at some $s \notin \mathfrak{m}$.

[3] An ideal $\mathfrak{a}$ is said to be strict when $1 \notin \mathfrak{a}$.

Abstract $\Rightarrow$ *Transfer* For each maximal ideal $\mathfrak{m}$ select an $s_{\mathfrak{m}} \notin \mathfrak{m}$ such that the property P is true after localization at $s_{\mathfrak{m}}$. The set of $s_{\mathfrak{m}}$ generates an ideal not contained in any maximal ideal, thus it is the ideal $\langle 1 \rangle$. We can then conclude by the transfer principle: the property is true after localization at 1! ∎

Comment The advantage of localizing at a prime ideal is that the result is a local ring, which has very nice properties (see Chap. IX). The disadvantage is that the proofs which use an abstract local-global principle instead of its corresponding concrete local-global principle are non-constructive to the extent that the only access we have (in a general situation) to the prime ideals is given by Zorn's Lemma. Furthermore even Fact 2.2 is obtained by contradiction, which removes any algorithmic trait from the corresponding "construction."

Some concrete local-global principles do not have a corresponding abstract version as the property they are affiliated with is not of finite character. This is the case with the concrete local-global principles for finitely generated modules and for coherent rings (3.6 and 3.5 respectively).

We will systematically make efficient and constructive use of the basic concrete local-global principle and its consequences. Often, we will draw inspiration from some abstract local-global principle's proof found in classical mathematics. In Chap. XV we will develop a general local-global machinery to fully exploit the classical local-global proofs in a constructive manner. ∎

Abstract Version of the Basic Local-Global Principle

Since we are dealing with a finite character property, classical mathematics provides the following abstract version of the basic local-global principle.

2.13 Abstract local-global principle* (Abstract basic local-global principle: abstract patching of solutions of a system of linear equations) *Let B be a matrix $\in \mathbf{A}^{m\times p}$ and C a column vector of $\mathbf{A}^m$. Then the following properties are equivalent.*

1. *The system of linear equations $BX = C$ has a solution in $\mathbf{A}^p$.*
2. *For every maximal ideal $\mathfrak{m}$ the system of linear equations $BX = C$ has a solution in $(\mathbf{A}_{1+\mathfrak{m}})^p$.*

Forcing Comaximality

Localization at an element $s \in \mathbf{A}$ is a fundamental operation in commutative algebra for forcing the invertibility of s.

Sometimes you may need to make n elements $a_1, \ldots, a_n$ of a ring $\mathbf{A}$ comaximal. To this end we introduce the ring

$$\mathbf{B} = \mathbf{A}[X_1, \ldots, X_n]\big/\big\langle 1 - \textstyle\sum_i a_i X_i \big\rangle = \mathbf{A}[x_1, \ldots, x_n].$$

2.14 Lemma *The kernel of the natural homomorphism $\psi : \mathbf{A} \to \mathbf{B}$ is the ideal $(0 : \mathfrak{a}^\infty)$, where $\mathfrak{a} = \langle a_1, \ldots, a_n \rangle$. In particular, the homomorphism is injective if and only if* $\operatorname{Ann} \mathfrak{a} = 0$.

▷ Let c be an element of the kernel. Considering the isomorphism

$$\mathbf{B}/\langle (x_j)_{j\neq i}\rangle \simeq \mathbf{A}[1/a_i],$$

we have $c =_{\mathbf{A}[1/a_i]} 0$. Thus $c \in (0 : a_i^\infty)$. From this we deduce that $c \in (0 : \mathfrak{a}^\infty)$. Conversely if $c \in (0 : \mathfrak{a}^\infty)$, there exists an r such that $ca_i^r = 0$ for each i, and therefore $\psi(c) = \psi(c)(\sum a_i x_i)^{nr} = 0$. □

3 Coherent Rings and Modules

A Fundamental Notion

A ring $\mathbf{A}$ is called *coherent* if every linear equation

$$LX = 0 \text{ with } L \in \mathbf{A}^{1\times n} \text{ and } X \in \mathbf{A}^{n\times 1}$$

has for solutions the elements of a finitely generated $\mathbf{A}$-submodule of $\mathbf{A}^{n\times 1}$. In other words,

$$\left\{\begin{array}{l} \forall n \in \mathbb{N},\ \forall L \in \mathbf{A}^{1\times n},\ \exists m \in \mathbb{N},\ \exists G \in \mathbf{A}^{n\times m},\ \forall X \in \mathbf{A}^{n\times 1}, \\ \quad LX = 0 \iff \exists Y \in \mathbf{A}^{m\times 1},\ X = GY . \end{array}\right. \tag{1}$$

This means that we have some control over the solution space of the homogeneous system of linear equations $LX = 0$.

Clearly, a finite product of rings is coherent if and only if each factor is coherent.

More generally, given $V = (v_1, \ldots, v_n) \in M^n$ where M is an $\mathbf{A}$-module, the $\mathbf{A}$-submodule of $\mathbf{A}^n$ defined as the kernel of the linear map

$$\check{V} : \mathbf{A}^n \longrightarrow M, \quad (x_1, \ldots, x_n) \longmapsto \textstyle\sum_i x_i v_i$$

is called the *syzygy module between the v_i's*. More specifically, we say that it is the *syzygy module of (the vector) V*. An element $(x_1, \ldots, x_n)$ of this kernel is called a *linear dependence relation* or a *syzygy* between the v_i's. When V is a generator set of M the syzygy module between the v_i's is often called the *(first) syzygy module of M*.

By slight abuse of terminology, we indifferently refer to the term *syzygy* to mean the equality $\sum_i x_i v_i = 0$ or the element $(x_1, \ldots, x_n) \in \mathbf{A}^n$. The $\mathbf{A}$-module M is said to be *coherent* if for every $V \in M^n$ the syzygy module is finitely generated, in other words if we have:

$$\left\{\begin{array}{l} \forall n \in \mathbb{N},\ \forall V \in M^{n\times 1},\ \exists m \in \mathbb{N},\ \exists G \in \mathbf{A}^{m\times n},\ \forall X \in \mathbf{A}^{1\times n}, \\ \quad XV = 0 \iff \exists Y \in \mathbf{A}^{1\times m},\ X = YG . \end{array}\right. \tag{2}$$

A ring $\mathbf{A}$ is then coherent if and only if it is coherent as an $\mathbf{A}$-module.

Notice that we used a transposed notation in Eq. (2) with respect to Eq. (1). This was to avoid writing the sum $\sum_i x_i v_i$ as $\sum_i v_i x_i$ with $v_i \in M$ and $x_i \in \mathbf{A}$. For the remainder of this work, we will generally not use this transposition, as it seems preferable to keep to the usual form $AX = V$ for a system of linear equations, even when the matrices A and V have their coefficients in a module M.

3.1 Proposition *Let M be a coherent $\mathbf{A}$-module.*

Any homogeneous system of linear equations $BX = 0$, where $B \in M^{k\times n}$ and $X \in \mathbf{A}^{n\times 1}$, *has the elements of a finitely generated $\mathbf{A}$-submodule of $\mathbf{A}^{n\times 1}$ as its solution set.*

▷ The general proof is by induction on the number of linear equations k, where the procedure is as follows: solve the first equation, then substitute the obtained general solution into the second equation, and so on. So let us for example do the proof for $k = 2$ and take a closer look at this process. The matrix B is composed of the rows L and L'. We then have a matrix G such that

$$LX = 0 \iff \exists Y \in \mathbf{A}^{m\times 1},\ X = GY.$$

We now need to solve $L'GY = 0$ which is equivalent to the existence of a column vector Z such that $Y = G'Z$ for a suitable matrix G'. Thus $BX = 0$ if and only if X can be expressed as $GG'Z$. □

The above proposition is particularly important for systems of linear equations on $\mathbf{A}$ (i.e. when $M = \mathbf{A}$).

Comment The notion of a coherent ring is then fundamental from an algorithmic point of view in commutative algebra. Usually, this notion is hidden behind that of a *Noetherian* ring,[4] and rarely put forward as we have here. In classical mathematics every Noetherian ring $\mathbf{A}$ is coherent because every submodule of $\mathbf{A}^n$ is finitely generated, and every finitely generated module is coherent for the same reason. Furthermore, we have the Hilbert theorem, which states that *if $\mathbf{A}$ is Noetherian, every finitely generated $\mathbf{A}$-algebra is also a Noetherian ring*, whereas the same statement does not hold if one replaces "Noetherian" with "coherent."

From an algorithmic point of view however, it seems impossible to find a satisfying constructive formulation of Noetherianity which implies coherence (see Exercise 8), and coherence is often the most important property from an algorithmic point of view. Consequently, coherence cannot be implied (as is the case in classical mathematics) when we speak of a Noetherian ring or module.

The classical theorem stating that in a Noetherian ring every finitely generated $\mathbf{A}$-module is Noetherian is often advantageously replaced by the following constructive theorem.[5]

[4] The constructive definition of this notion is given after this comment.

[5] For the non-Noetherian version see Theorem IV-4.3, and for the Noetherian version see [MRR, Corollary 3.2.8 p. 83].

Over a coherent (resp. Noetherian coherent) ring every finitely presented **A***-module is coherent (resp. Noetherian coherent).*

In fact, as this example shows, Noetherianity is often an unnecessarily strong assumption. ∎

The following definition of a Noetherian module is equivalent in classical mathematics to the usual definition but it is much better adapted to constructive algebra (only the trivial ring constructively satisfies the usual definition).

3.2 Definition (*Richman-Seidenberg theory of Noetherianity, [153, 163]*) An **A**-module is called *Noetherian* if it satisfies the following *ascending chain condition*: any ascending sequence of finitely generated submodules has two equal consecutive terms. A ring **A** is called *Noetherian* if it is Noetherian as an **A**-module.

Here is a corollary of Proposition 3.1.

3.3 Corollary (Conductors and coherence) *Let* **A** *be a coherent ring. Then, the conductor of a finitely generated ideal into another is a finitely generated ideal. More generally, if N and P are two finitely generated submodules of a coherent* **A***-module, then $(P : N)$ is a finitely generated ideal.*

3.4 Theorem *An* **A***-module M is coherent if and only if the following two conditions hold.*

1. *The intersection of two arbitrary finitely generated submodules is a finitely generated module.*
2. *The annihilator of an arbitrary element is a finitely generated ideal.*

▷ *The first condition is necessary.* Let $g_1, \ldots, g_n$ be the generators of the first submodule and $g_{n+1}, \ldots, g_m$ be the generators of the second. Taking an element of the intersection reduces to finding a syzygy $\sum_{i=1}^{m} \alpha_i g_i = 0$ between the g_i's. To such a syzygy $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbf{A}^m$ corresponds the element $\varphi(\alpha) = \alpha_1 g_1 + \cdots + \alpha_n g_n = -(\alpha_{n+1} g_{n+1} + \cdots + \alpha_m g_m)$ in the intersection. Thus if S is a generator set for the syzygies between the g_i's, $\varphi(S)$ generates the intersection of the two submodules.

The second condition is necessary by definition.

The two conditions together are sufficient. Here we give the key idea of the proof and leave the details to the reader. Consider the syzygy module of some $L \in M^n$. We perform induction on n. For $n = 1$ the second condition applies and gives a generator set for the syzygies connecting the single element of L.

Suppose that the syzygy module of every $L \in M^n$ is finitely generated and consider some $L' \in M^{n+1}$. Let $k \in [\![1..n]\!]$, we write $L' = L_1 \bullet L_2$ where $L_1 = (a_1, \ldots, a_k)$ and $L_2 = (a_{k+1}, \ldots, a_{n+1})$. Let $M_1 = \langle a_1, \ldots, a_k \rangle$ and $M_2 = \langle a_{k+1}, \ldots, a_{n+1} \rangle$. Taking a syzygy $\sum_{i=1}^{n+1} \alpha_i a_i = 0$ reduces to taking an element of the intersection $M_1 \cap M_2$ (as above). We thus obtain a generator set for the syzygies between the a_i's by taking the union of the three following systems of

syzygies: the system of syzygies between the elements of L_1, the system of syzygies between the elements of L_2, and that which comes from the generator set of the intersection $M_1 \cap M_2$. □

In particular, *a ring is coherent if and only if on the one hand the intersection of the two finitely generated ideals is always a finitely generated ideal, and on the other hand the annihilator of an element is always a finitely generated ideal.*

Examples If $\mathbf{K}$ is a discrete field, every finitely presented algebra over $\mathbf{K}$ is a coherent ring (Theorem VII-1.10). It is also clear that every Bezout domain (cf. p. 201) is a coherent ring. ∎

Local Character of Coherence

Coherence is a local notion in the following sense.

3.5 Concrete local-global principle (Coherent modules) *Consider a ring* $\mathbf{A}$*, let* $S_1, \ldots, S_n$ *be comaximal monoids and* M *an* $\mathbf{A}$*-module.*

1. *The module* M *is coherent if and only if each* M_{S_i} *is coherent.*
2. *The ring* $\mathbf{A}$ *is coherent if and only if each* $\mathbf{A}_{S_i}$ *is coherent.*

▷ Let $a = (a_1, \ldots, a_m) \in M^m$, and $N \subseteq \mathbf{A}^m$ be the syzygy module of a. We find that for any monoid S, N_S is the syzygy module of a in M_S. This brings us to prove the following concrete local-global principle. □

3.6 Concrete local-global principle (Finitely generated modules) *Let* $S_1, \ldots, S_n$ *be comaximal monoids of* $\mathbf{A}$ *and* M *an* $\mathbf{A}$*-module. Then,* M *is finitely generated if and only if each* M_{S_i} *is finitely generated.*

▷ Suppose that M_{S_i} is a finitely generated $\mathbf{A}_{S_i}$-module for each i. Let us prove that M is finitely generated. Let $g_{i,1}, \ldots, g_{i,q_i}$ be elements of M which generate M_{S_i}. Let $x \in M$ be arbitrary. For each i we have some $s_i \in S_i$ and some $a_{i,j} \in \mathbf{A}$ such that:

$$s_i x = a_{i,1} g_{i,1} + \cdots + a_{i,q_i} g_{i,q_i} \quad \text{in} \quad M.$$

When writing $\sum_{i=1}^{n} b_i s_i = 1$, we observe that x is a linear combination of the $g_{i,j}$'s. □

Remark Consider the $\mathbb{Z}$-submodule M of $\mathbb{Q}$ generated by the elements $1/p$ where p ranges over the set of prime numbers. We can easily check that M is not finitely generated but that it becomes finitely generated after localization at any prime ideal. This means that the Concrete local-global principle 3.6 does not have a corresponding "abstract" version, in which the localization at some comaximal monoids would be replaced by the localization at every prime ideal. Actually, the property P for a module to be finitely generated is not a finite character property, as we can see with the module M above and the monoids $\mathbb{Z} \setminus \{0\}$ or $1 + p\mathbb{Z}$. Moreover, the property satisfies the transfer principle, but it so happens here that it is of no use. ∎

About the Equality and the Membership Tests

We now introduce several constructive notions relating to the equality test and the membership test.

A set E is well defined when we have indicated how to construct its elements and when we have constructed an equivalence relation which defines the equality of two elements in a set. We denote by $x = y$ the equality in E, or $x =_E y$ if necessary. The set E is called *discrete* when the following axiom holds

$$\forall x, y \in E \qquad x = y \ \text{ or } \ \neg(x = y).$$

Classically, every set is discrete, as the "or" present in the definition is understood in an abstract manner. Constructively, this same "or" is understood according to the usual language's meaning: at least one of the two alternatives must occur. It is thus an "or" of an algorithmic nature. In short, a set is discrete if we have a test for the equality of two arbitrary elements of this set.

If we want to be more precise and explain in detail what comprises an equality test in the set E, we will say that it is a construction which, from two given elements of E, provides a "yes" or "no" answer to the posed question (are these elements equal?). However, we could not go into much further detail. In constructive mathematics the notions of integers and of construction are basic concepts. They can be explained and commented on, but not strictly speaking "defined." The constructive meaning of the "or" and that of the "there exists" are as such directly dependent of the notion of construction,[6] which we do not attempt to define.

A *discrete field* is simply a ring where the following axiom is satisfied:

$$\forall x \in \mathbf{A} \qquad x = 0 \ \text{ or } \ x \in \mathbf{A}^{\times} \tag{3}$$

The trivial ring is a discrete field.

Remark The Chinese pivot method (often called Gaussian elimination) works algorithmically with discrete fields. This means that the basic linear algebra is explicit over discrete fields. ∎

Note that a discrete field $\mathbf{A}$ is a discrete set if and only if the test "$1 =_{\mathbf{A}} 0$?" is explicit.[7] Sometimes, however, it is known that a ring constructed during an algorithm is a discrete field without knowing whether it is trivial or not.

---

[6] In classical mathematics we may wish to define the notion of construction from the notion of a "correct program." However, what we define in this way is rather the notion of "mechanized construction," and especially in the notion of a "correct program," there is the fact that the program must halt after a finite number of steps. This hides a "there exists," which in constructive mathematics refers in an irreducible manner to the notion of construction. On this matter, see Sect. A-4 of the Annex.

[7] The general notion of a field in constructive mathematics will be defined p. 479. We will then see that if a field is a discrete set, then it is a discrete field.

If $\mathbf{A}$ is a nontrivial discrete field, the statement "M is a free finite dimensional vector space" is more precise than the statement "M is a finitely generated vector space" as in the first case knowing how to extract a basis of the generator set is similar to having a test of linear independence in M.

A subset P of a set E is said to be *detachable* when the following property is satisfied:

$$\forall x \in E \qquad x \in P \text{ or } \neg(x \in P).$$

It amounts to the same to take a detachable part P of E or to take its characteristic function $\chi_P : E \to \{0, 1\}$.

In constructive mathematics, if two sets E and F are correctly defined, then so is the *set of functions from E to F*, which is denoted by F^E. Consequently, the *set of detachable subsets* of a set E is itself correctly defined since it is identified with the set $\{0, 1\}^E$ of characteristic functions over E.

Strongly Discrete Coherent Rings and Modules

A ring (resp. a module) is said to be *strongly discrete* when the finitely generated ideals (resp. the finitely generated submodules) are detachable, i.e. if the quotients by the finitely generated ideals (resp. by the finitely generated submodules) are discrete.

This means that we have a test for deciding whether a linear equation $LX = c$ has a solution or not, and by computing one in the affirmative case.

A key result in constructive algebra and Computer Algebra states that $\mathbb{Z}[X_1, \ldots, X_n]$ is a strongly discrete coherent ring.

More generally, we have the following constructive version of the Hilbert theorem (see [MRR, Adams & Loustaunau]).

If $\mathbf{A}$ is a strongly discrete Noetherian coherent ring, so is any finitely presented $\mathbf{A}$-algebra.

The following proposition is proven similarly to Proposition 3.1.

3.7 Proposition *Over a strongly discrete coherent module M, every system of linear equations $BX = C$ ($B \in M^{k\times n}$, $C \in M^{k\times 1}$, $X \in \mathbf{A}^{n\times 1}$) can be tested. In the affirmative case, a particular solution X_0 can be computed. Furthermore the solutions X are all the elements of $X_0 + N$ where N is a finitely generated $\mathbf{A}$-submodule of $\mathbf{A}^{n\times 1}$.*

4 Fundamental Systems of Orthogonal Idempotents

An element e of a ring is said to be *idempotent* if $e^2 = e$. In this case, $1 - e$ is also an idempotent, called the *complementary idempotent of e*, or the *complement of e*. For two idempotents e_1 and e_2, we have

$$\langle e_1\rangle \cap \langle e_2\rangle = \langle e_1 e_2\rangle, \quad \langle e_1\rangle + \langle e_2\rangle = \langle e_1, e_2\rangle = \langle e_1 + e_2 - e_1 e_2\rangle,$$

where e_1e_2 and $e_1 + e_2 - e_1e_2$ are idempotents. Two idempotents e_1 and e_2 are said to be *orthogonal* when $e_1e_2 = 0$. We then have $\langle e_1\rangle + \langle e_2\rangle = \langle e_1 + e_2\rangle$.

A ring is said to be *connected* if every idempotent is equal to 0 or 1.

In the following, we implicitly use the following obvious fact: for an idempotent e and an element x, e divides x if and only if $x = ex$.

The presence of an idempotent $\neq 0, 1$ means that the ring $\mathbf{A}$ is isomorphic to a product of two rings $\mathbf{A}_1$ and $\mathbf{A}_2$, and that any computation in $\mathbf{A}$ can be split into two "simpler" computations in $\mathbf{A}_1$ and $\mathbf{A}_2$. We describe the situation as follows.

4.1 Fact *For every isomorphism $\lambda : \mathbf{A} \to \mathbf{A}_1 \times \mathbf{A}_2$, there exists a unique element $e \in \mathbf{A}$ satisfying the following properties.*

1. *The element e is idempotent (its complement is denoted by $f = 1 - e$).*
2. *The homomorphism $\mathbf{A} \to \mathbf{A}_1$ identifies $\mathbf{A}_1$ with $\mathbf{A}/\langle e\rangle$ and with $\mathbf{A}[1/f]$.*
3. *The homomorphism $\mathbf{A} \to \mathbf{A}_2$ identifies $\mathbf{A}_2$ with $\mathbf{A}/\langle f\rangle$ and with $\mathbf{A}[1/e]$.*

Conversely, if e is an idempotent and f is its complement, the canonical homomorphism $\mathbf{A} \to \mathbf{A}/\langle e\rangle \times \mathbf{A}/\langle f\rangle$ is an isomorphism.

▷ The element e is defined by $\lambda(e) = (0, 1)$. □

Here are some often useful facts.

4.2 Fact *Let e be an idempotent of $\mathbf{A}$, $f = 1 - e$ and M be an $\mathbf{A}$-module.*

1. *The monoids $e^{\mathbb{N}} = \{1, e\}$ and $1 + f\mathbf{A}$ have the same saturation.*
2. *As an $\mathbf{A}$-module, $\mathbf{A}$ is the direct sum of $\langle e\rangle = e\mathbf{A}$ and $\langle f\rangle = f\mathbf{A}$. The ideal $e\mathbf{A}$ is a ring where e is a neutral element of the multiplication. We then have three isomorphic rings*

$$\mathbf{A}[1/e] = (1 + f\mathbf{A})^{-1}\mathbf{A} \;\simeq\; \mathbf{A}/\langle f\rangle \;\simeq\; e\mathbf{A}.$$

These isomorphisms stem from the three canonical mappings

$$\begin{array}{lll} \mathbf{A} \to \mathbf{A}[1/e] & : & x \mapsto x/1, \\ \mathbf{A} \to \mathbf{A}/\langle f\rangle & : & x \mapsto x \bmod \langle f\rangle, \\ \mathbf{A} \to e\mathbf{A} & : & x \mapsto ex, \end{array}$$

which are surjective and have the same kernel.

3. *We have three isomorphic $\mathbf{A}$-modules $M[1/e] \simeq M/fM \simeq eM$. These isomorphisms stem from the three canonical mappings*

$$\begin{array}{lll} M \to M[1/e] & : & x \mapsto x/1, \\ M \to M/fM & : & x \mapsto x \bmod \langle f\rangle, \\ M \to eM & : & x \mapsto ex, \end{array}$$

which are surjective and have the same kernel.

In addition, care must be taken that the ideal $e\mathbf{A}$, which is a ring with e as its neutral element, is not a subring of $\mathbf{A}$ (unless $e = 1$).

In a ring $\mathbf{A}$ a *fundamental system of orthogonal idempotents* is a list $(e_1, \ldots, e_n)$ of elements of $\mathbf{A}$ which satisfy the following equalities:

$$e_i e_j = 0 \text{ for } i \neq j, \quad \text{and} \quad \sum_{i=1}^{n} e_i = 1.$$

This implies that the e_i's are idempotents. We do not claim that none of them are null.[8]

4.3 Theorem (Fundamental systems of orthogonal idempotents) *Let $(e_1, \ldots, e_n)$ be a fundamental system of orthogonal idempotents of a ring $\mathbf{A}$, and M be an $\mathbf{A}$-module. Note that $\mathbf{A}_i = \mathbf{A}/\langle 1 - e_i \rangle \simeq \mathbf{A}[1/e_i]$. Then:*

$$\begin{array}{rcl} \mathbf{A} & \simeq & \mathbf{A}_1 \times \cdots \times \mathbf{A}_n, \\ M & = & e_1 M \oplus \cdots \oplus e_n M. \end{array}$$

Take note that $e_1 M$ is an $\mathbf{A}$-module and an $\mathbf{A}_1$-module, but that it is not an $\mathbf{A}_2$-module (unless it is null).

The following lemma gives a converse of Theorem 4.3.

4.4 Lemma *Let $(\mathfrak{a}_i)_{i \in [\![1..n]\!]}$ be ideals of $\mathbf{A}$. We have $\mathbf{A} = \bigoplus_{i \in [\![1..n]\!]} \mathfrak{a}_i$ if and only if there exists a fundamental system of orthogonal idempotents $(e_i)_{i \in [\![1..n]\!]}$ such that $\mathfrak{a}_i = \langle e_i \rangle$ for $i \in [\![1..n]\!]$. In this case, the fundamental system of orthogonal idempotents is uniquely determined.*

▷ Assume that $\mathbf{A} = \bigoplus_{i \in [\![1..n]\!]} \mathfrak{a}_i$. We have $e_i \in \mathfrak{a}_i$ such that $\sum_i e_i = 1$, and since $e_i e_j \in \mathfrak{a}_i \cap \mathfrak{a}_j = \{0\}$ for $i \neq j$, we indeed obtain a fundamental system of orthogonal idempotents. Furthermore if $x \in \mathfrak{a}_j$, we have $x = x \sum_i e_i = x e_j$ and thus $\mathfrak{a}_j = \langle e_j \rangle$. The converse is immediate. The uniqueness follows from that of writing an element as a direct sum. □

Next we give two very useful lemmas.

4.5 Lemma (Lemma of the ideal generated by an idempotent) *An ideal $\mathfrak{a}$ is generated by an idempotent if and only if*

$$\mathfrak{a} + \operatorname{Ann} \mathfrak{a} = \langle 1 \rangle.$$

▷ First, if e is idempotent, we have $\operatorname{Ann} \langle e \rangle = \langle 1 - e \rangle$. For the reciprocal implication, let $e \in \mathfrak{a}$ such that $1 - e \in \operatorname{Ann} \mathfrak{a}$. Then $e(1 - e) = 0$, therefore e is idempotent, and for every $y \in \mathfrak{a}$, $y = ye$, thus $\mathfrak{a} \subseteq \langle e \rangle$. □

[8] This is much nicer to obtain uniform statements. Furthermore this is virtually necessary when we do not have at our disposal an equality to zero test for idempotents in the given ring.

4.6 Lemma (Lemma of the finitely generated idempotent ideal) *If $\mathfrak{a}$ is a finitely generated idempotent ideal (i.e., $\mathfrak{a} = \mathfrak{a}^2$) in $\mathbf{A}$, then $\mathfrak{a} = \langle e \rangle$ where $e^2 = e$ is entirely determined by $\mathfrak{a}$.*

▷ We use the determinant trick. Consider a generator set $(a_1, \dots a_q)$ of $\mathfrak{a}$ and the column vector $\underline{a} = {}^t[\, a_1 \ \cdots \ a_q \,]$.

Since $a_j \in \mathfrak{a}^2$ for $j \in [\![1..q]\!]$, there exists a $C \in \mathbb{M}_q(\mathfrak{a})$ such that $\underline{a} = C\,\underline{a}$, so $(\mathrm{I}_q - C)\,\underline{a} = \underline{0}$ and $\det(\mathrm{I}_q - C)\,\underline{a} = \underline{0}$. However, $\det(\mathrm{I}_q - C) = 1 - e$ where $e \in \mathfrak{a}$. Hence $(1-e)\mathfrak{a} = 0$, and we apply Lemma 4.5.

Finally, the uniqueness of e follows immediately from Lemma 4.4. □

Let us finally recall the Chinese remainder theorem, a very efficient tool which hides a fundamental system of orthogonal idempotents. Some ideals $\mathfrak{b}_1, \dots, \mathfrak{b}_\ell$ of a ring $\mathbf{A}$ are called *comaximal* when $\mathfrak{b}_1 + \cdots + \mathfrak{b}_\ell = \langle 1 \rangle$.

4.7 Chinese Remainder Theorem *Let $(\mathfrak{a}_i)_{i \in [\![1..n]\!]}$ be pairwise comaximal ideals in $\mathbf{A}$ and $\mathfrak{a} = \bigcap_i \mathfrak{a}_i$.*

Then $\mathfrak{a} = \prod_i \mathfrak{a}_i$, and the canonical mapping $\mathbf{A}/\mathfrak{a} \to \prod_i \mathbf{A}/\mathfrak{a}_i$ is an isomorphism. Now, there exist $e_1, \dots, e_n$ in $\mathbf{A}$ such that $\mathfrak{a}_i = \mathfrak{a} + \langle 1 - e_i \rangle$ and the $\pi_{\mathbf{A},\mathfrak{a}}(e_i)$'s form a fundamental system of orthogonal idempotents of $\mathbf{A}/\mathfrak{a}$.

As a corollary we obtain the following result.

4.8 Lemma (Kernels' Lemma) *Let $P = P_1 \cdots P_\ell \in \mathbf{A}[X]$ and an $\mathbf{A}$-linear map $\varphi : M \to M$ satisfying $P(\varphi) = 0$. Assume the P_i's are pairwise comaximal and let $K_i = \mathrm{Ker}\,\big(P_i(\varphi)\big)$, $Q_i = \prod_{j \neq i} P_j$. Then we have*

$$K_i = \mathrm{Im}\big(Q_i(\varphi)\big),\ M = \bigoplus_{j=1}^{\ell} K_j \ \text{ and } \ \mathrm{Im}\big(P_i(\varphi)\big) = \mathrm{Ker}\,\big(Q_i(\varphi)\big) = \bigoplus_{j \neq i} K_i.$$

▷ Consider the ring $\mathbf{B} = \mathbf{A}[X]/\langle P \rangle$. The module M can be seen as a $\mathbf{B}$-module by the operation $(Q, y) \mapsto Q \cdot y = Q(\varphi)(y)$. We then apply the Chinese remainder theorem and Theorem 4.3.

This proof summarizes the following computation. From the equalities $U_{ij} P_i + U_{ji} P_j = 1$, we get the equalities $U_i P_i + V_i Q_i = 1$ together with an equality $\sum_i W_i Q_i = 1$. Let $p_i = P_i(\varphi)$, $q_i = Q_i(\varphi)$, and so on.

Then, all obtained endomorphisms commute and we obtain the equalities $p_i q_i = 0$, $u_i p_i + v_i q_i = \mathrm{Id}_M$, $\sum_i w_i q_i = \mathrm{Id}_M$. The claimed result readily follows. □

5 A Little Exterior Algebra

That a homogeneous system of n linear equations with n unknowns
admits (over a discrete field) a nontrivial solution
if and only if the determinant of the system is zero,
here is a fact of utmost importance whose scope we
will never finish measuring.
Anonymous

Eliminate, eliminate, eliminate
Eliminate the eliminators of elimination theory!
Mathematical poem (extract)
S. Abhyankar

Some simple examples illustrating these ideas are given in this section.

Free Submodules as Direct Summands (Splitting Off)

Let $k \in \mathbb{N}$. A *free module of rank k* is by definition an $\mathbf{A}$-module isomorphic to $\mathbf{A}^k$. If k is not specified, we will say *free module of finite rank*.

When $\mathbf{A}$ is a discrete field we speak of a *finite dimensional vector space* or a *finite rank vector space* interchangeably.

The modules whose structure is the simplest are the free modules of finite rank. We are thus interested in the possibility of constructing an arbitrary module M in the form $L \oplus N$ where L is a free module of finite rank. A (partial) answer to this question is given by the exterior algebra.

5.1 Proposition (Splitting Off) *Let $a_1, \ldots, a_k$ be elements of an $\mathbf{A}$-module M, then the following properties are equivalent.*

1. *The submodule $L = \langle a_1, \ldots, a_k \rangle$ of M is free with basis $(a_1, \ldots, a_k)$ and is a direct summand of M.*
2. *There exists a k-multilinear alternating form $\varphi : M^k \to \mathbf{A}$ which satisfies the equality $\varphi(a_1, \ldots, a_k) = 1$.*

▷ *1 ⇒ 2*. If $L \oplus N = M$, if $\pi : M \to L$ is the projection parallel to N, and if $\theta_j : L \to \mathbf{A}$ is the j-th coordinate form for the basis $(a_1, \ldots, a_k)$, we define

$$\varphi(x_1, \ldots, x_k) = \det\Big(\big(\theta_j(\pi(x_i))\big)_{i,j\in[\![1..k]\!]}\Big).$$

2 ⇒ 1. We define the linear map $\pi : M \to M$ as

$$\pi(x) = \sum\nolimits_{j=1}^{k} \varphi(\underbrace{a_1, \ldots, x, \ldots, a_k}_{(x \text{ is in position } j)})\, a_j.$$

We immediately have $\pi(a_i) = a_i$ and $\operatorname{Im}\pi \subseteq L := \langle a_1, \dots, a_k\rangle$, thus $\pi^2 = \pi$ and $\operatorname{Im}\pi = L$. Finally, if $x = \sum_j \lambda_j a_j = 0$, then $\varphi(a_1, \dots, x, \dots, a_k) = \lambda_j = 0$ (with x in position j). □

Special case: for $k = 1$ we say that the element a_1 of M is *unimodular* when there exists a linear form $\varphi : M \to \mathbf{A}$ such that $\varphi(a_1) = 1$. The vector $b = (b_1, \dots, b_n) \in \mathbf{A}^n$ is unimodular if and only if the b_i's are comaximal. In this case we also say that the sequence $(b_1, \dots, b_n)$ is *unimodular*.

The Rank of a Free Module

As we will see, the rank of a free module is a well-determined integer if the ring is nontrivial. In other words, two $\mathbf{A}$-modules $M \simeq \mathbf{A}^m$ and $P \simeq \mathbf{A}^p$ with $m \neq p$ can only be isomorphic if $1 =_{\mathbf{A}} 0$.

We will use the notation $\operatorname{rk}_{\mathbf{A}}(M) = k$ (or $\operatorname{rk}(M) = k$ if $\mathbf{A}$ is clear from the context) to indicate that a (supposedly free) module has rank k.

A scholarly proof consists to say that, if $m > p$, the m-th exterior power of P is $\{0\}$ whereas that of M is isomorphic to $\mathbf{A}$ (this is essentially the proof for Corollary 5.23).

The same proof can be presented in a more elementary way as follows. First recall the basic Cramer formula. If B is a square matrix of order n, we denote by $\widetilde{B}$ or $\operatorname{Adj} B$ the *cotransposed* matrix (sometimes called *adjoint*). The elementary form of Cramer's identities is then expressed as:

$$A\ \operatorname{Adj}(A) = \operatorname{Adj}(A)\ A = \det(A)\ \mathrm{I}_n. \tag{4}$$

This formula, in combination with the product formula

$$\det(AB) = \det(A)\det(B),$$

has a couple of implications regarding square matrices. First, that a square matrix A is invertible on one side if and only if A is invertible if and only if its determinant is invertible. Second, that the inverse of A is equal to $(\det A)^{-1} \operatorname{Adj} A$.

We now consider two $\mathbf{A}$-modules $M \simeq \mathbf{A}^m$ and $P \simeq \mathbf{A}^p$ with $m \geqslant p$ and a surjective linear map $\varphi : P \to M$. Therefore there exists a linear map $\psi : M \to P$ such that $\varphi \circ \psi = \mathrm{Id}_M$. This corresponds to two matrices $A \in \mathbf{A}^{m\times p}$ and $B \in \mathbf{A}^{p\times m}$ with $AB = \mathrm{I}_m$. If $m = p$, the matrix A is invertible with inverse B and φ and ψ are reciprocal isomorphisms. If $m > p$, we have $AB = A_1B_1$ with square A_1 and B_1 respectively obtained from A and B by filling in with zeros ($m - p$ columns for A_1, $m - p$ rows for B_1).

$$A_1 = \left[\begin{array}{c|c} \begin{matrix}0\\ \vdots\\ 0\end{matrix} & A \end{array}\right], \qquad B_1 = \left[\begin{array}{c} 0 \cdots 0 \\ \hline B \end{array}\right], \qquad A_1B_1 = \mathrm{I}_m.$$

Thus $1 = \det \mathrm{I}_m = \det(AB) = \det(A_1B_1) = \det(A_1)\det(B_1) = 0$.

In this proof we clearly see the commutativity of the ring appear (which is truly necessary). Let us summarize.

5.2 Proposition *Let two* $\mathbf{A}$*-modules* $M \simeq \mathbf{A}^m$ *and* $P \simeq \mathbf{A}^p$ *and a surjective linear map* $\varphi : P \to M$.

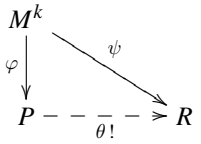
1. *If* $m = p$, *then* φ *is an isomorphism. In other words, in a module* $\mathbf{A}^m$ *every generator set of* m *elements is a basis.*
2. *If* $m > p$, *then* $1 =_{\mathbf{A}} 0$, *and if the ring is nontrivial,* $m > p$ *is impossible.*

In the following, this important classification theorem will often appear as a corollary of more subtle theorems, as for example Theorems IV-5.1 or IV-5.2.

Exterior Powers of a Module

Terminology Recall that any determinant of a square matrix extracted from A on certain rows and columns is called a *minor* of A. We speak of a *minor of order* k when the extracted square matrix is in $\mathbb{M}_k(\mathbf{A})$. When A is a square matrix, a *principal minor* is a minor corresponding to a matrix extracted on the same set of indices for both the rows and the columns. For example if $A \in \mathbb{M}_n(\mathbf{A})$, the coefficient of X^k in the polynomial $\det(\mathrm{I}_n + XA)$ is the sum of the principal minors of order k of A. Finally, a principal minor in the north-west position, i.e. obtained by extracting the matrix on the first lines and first columns, is called a *dominant principal minor*. ∎

Let M be an $\mathbf{A}$-module. A k-multilinear alternating map $\varphi : M^k \to P$ is called a k-th *exterior power* of the $\mathbf{A}$-module M if every multilinear alternating map $\psi : M^k \to R$ is uniquely expressible in the form $\psi = \theta \circ \varphi$, where θ is an $\mathbf{A}$-linear map from P to R.



k-multilinear alternating maps

linear maps.

Clearly $\varphi : M^k \to P$ is unique in the categorical sense, i.e. that for every other exterior power $\varphi' : M^k \to P'$ there is a unique linear map $\theta : P \to P'$ which makes the suitable diagram commutative, and that θ is an isomorphism.

We then denote P by $\bigwedge^k M$ or $\bigwedge^k_{\mathbf{A}} M$ and $\varphi(x_1, \ldots, x_k)$ by $\lambda_k(x_1, \ldots, x_k)$ or $x_1 \wedge \cdots \wedge x_k$.

The existence of a k-th exterior power for every module M results from general considerations analogous to those that we will detail for the tensor product on p. 186 in Sect. IV-4.

The simplest theory of exterior powers, analogous to the elementary theory of the determinant, shows that if M is a free module with a basis of n elements $(a_1, \ldots, a_n)$, then $\bigwedge^k M$ is zero if $k > n$, and otherwise it is a free module whose basis is the $\binom{n}{k}$ k-vectors $a_{i_1} \wedge \cdots \wedge a_{i_k}$, where $(i_1, \ldots, i_k)$ ranges over the set of strictly increasing k-tuples of elements of $[\![1..n]\!]$.

In particular, $\bigwedge^n M$ is free and of rank 1 with $a_1 \wedge \cdots \wedge a_n$ as its basis.

To every $\mathbf{A}$-linear map $\alpha : M \to N$ corresponds a unique $\mathbf{A}$-linear map $\bigwedge^k \alpha : \bigwedge^k M \to \bigwedge^k N$ satisfying the equality

$$\big(\bigwedge^k \alpha\big)(x_1 \wedge \cdots \wedge x_k) = \alpha(x_1) \wedge \cdots \wedge \alpha(x_k)$$

for every k-vector $x_1 \wedge \cdots \wedge x_k$ of $\bigwedge^k M$. The linear map $\bigwedge^k \alpha$ is called the k-th *exterior power* of the linear map α.

Moreover we have $\big(\bigwedge^k \alpha\big) \circ \big(\bigwedge^k \beta\big) = \bigwedge^k(\alpha \circ \beta)$ when $\alpha \circ \beta$ is defined. In short, each $\bigwedge^k(\bullet)$ is a functor.

If M and N are free with respective bases $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_m)$, and if α admits the matrix H on its bases, then $\bigwedge^k \alpha$ admits the matrix denoted by $\bigwedge^k H$ on the corresponding bases of $\bigwedge^k M$ and $\bigwedge^k N$. The coefficients of this matrix are all the minors of order k of the matrix H.

Determinantal Ideals

5.3 Definition Let $G \in \mathbf{A}^{n\times m}$ and $k \in [\![1..\min(m,n)]\!]$, *the determinantal ideal of order k of the matrix G* is the ideal, denoted by $\mathcal{D}_{\mathbf{A},k}(G)$ or $\mathcal{D}_k(G)$, generated by the minors of order k of G. For $k \leqslant 0$ we set by convention $\mathcal{D}_k(G) = \langle 1\rangle$, and for $k > \min(m,n)$, $\mathcal{D}_k(G) = \langle 0\rangle$.

These conventions are natural because they allow us to obtain in full generality the following equalities.

- If $H = \begin{array}{|c|c|}\hline \mathrm{I}_r & 0 \\ \hline 0 & G \\ \hline \end{array}$, for all $k \in \mathbb{Z}$ we have $\mathcal{D}_k(G) = \mathcal{D}_{k+r}(H)$.
- If $H = \begin{array}{|c|c|}\hline 0 & 0 \\ \hline 0 & G \\ \hline \end{array}$, for all $k \in \mathbb{Z}$ we have $\mathcal{D}_k(H) = \mathcal{D}_k(G)$.

5.4 Fact *For every matrix G of type $n \times m$ we have the inclusions*

$$\{0\} = \mathcal{D}_{1+\min(m,n)}(G) \subseteq \cdots \subseteq \mathcal{D}_1(G) \subseteq \mathcal{D}_0(G) = \langle 1\rangle = \mathbf{A} \tag{5}$$

More precisely for all $k, r \in \mathbb{N}$ we have one inclusion

$$\mathcal{D}_{k+r}(G) \subseteq \mathcal{D}_k(G)\,\mathcal{D}_r(G) \tag{6}$$

Indeed, every minor of order $h+1$ is expressed as a linear combination of minors of order h, and the inclusion (6) is obtained via the Laplace expansion of the determinant.

5.5 Fact *Let $G_1 \in \mathbf{A}^{n\times m_1}$, $G_2 \in \mathbf{A}^{n\times m_2}$ and $H \in \mathbf{A}^{p\times n}$.*

1. *If* $\operatorname{Im} G_1 \subseteq \operatorname{Im} G_2$, *then for any integer k we have* $\mathcal{D}_k(G_1) \subseteq \mathcal{D}_k(G_2)$.
2. *For any integer k, we have* $\mathcal{D}_k(HG_1) \subseteq \mathcal{D}_k(G_1)$.
3. *The determinantal ideals of a matrix* $G \in \mathbf{A}^{n\times m}$ *only depend on the equivalence class of the submodule image of G (i.e., they only depend on* $\operatorname{Im} G$, *up to automorphism of the module* $\mathbf{A}^n$*).*
4. *In particular, if* φ *is a linear map between free modules of finite rank, the determinantal ideals of a matrix of* φ *do not depend on the chosen bases. We denote them by* $\mathcal{D}_k(\varphi)$ *and we call them the* determinantal ideals of the linear map φ.

▷ *1.* Each column of G_1 is a linear combination of columns of G_2. We conclude with the multilinearity of the determinant.
2. Same reasoning by replacing the columns with the rows.
Finally, *3* implies *4* and results from the two preceding items. □

Remark A determinantal ideal is therefore essentially attached to a finitely generated submodule M of a free module L. However, it is the structure of the inclusion $M \subseteq L$ and not only the structure of M which intervenes to determine the determinantal ideals. For example $M = 3\mathbb{Z} \times 5\mathbb{Z}$ is a free $\mathbb{Z}$-submodule of $L = \mathbb{Z}^2$ and its determinantal ideals are $\mathcal{D}_1(M) = \langle 1\rangle$, $\mathcal{D}_2(M) = \langle 15\rangle$. If we replace 3 and 5 with 6 and 10 for example, we obtain another free submodule, but the structure of the inclusion is different since the determinantal ideals are now $\langle 2\rangle$ and $\langle 60\rangle$. ■

5.6 Fact *If G and H are matrices such that GH is defined, then, for all* $n \geqslant 0$ *we have*

$$\mathcal{D}_n(GH) \subseteq \mathcal{D}_n(G)\,\mathcal{D}_n(H) \tag{7}$$

▷ The result is clear for $n = 1$. For $n > 1$, we reduce to the case $n = 1$ by noting that the minors of order n of G, H and GH represent the coefficients of the matrices "n-th exterior power of G, H and GH" (taking into account the equality $\bigwedge^n(\varphi\psi) = \bigwedge^n \varphi \circ \bigwedge^n \psi$). □

The following equality is immediate.

$$\mathcal{D}_n(\varphi \oplus \psi) = \sum\nolimits_{k=0}^{n} \mathcal{D}_k(\varphi)\,\mathcal{D}_{n-k}(\psi) \tag{8}$$

The Rank of a Matrix

5.7 Definition A linear map φ between free modules of finite rank is said to be

- *of rank* $\leqslant k$ if $\mathcal{D}_{k+1}(\varphi) = 0$,
- *of rank* $\geqslant k$ if $\mathcal{D}_k(\varphi) = \langle 1\rangle$,
- *of rank k* if it is both of rank $\geqslant k$ and of rank $\leqslant k$.

We will use the notations $\mathrm{rk}(\varphi) \geqslant k$ and $\mathrm{rk}(\varphi) \leqslant k$, in accordance with the preceding definition, without presupposing that $\mathrm{rk}(\varphi)$ is defined. Only the notation $\mathrm{rk}(\varphi) = k$ will mean that the rank is defined.

We will later generalize this definition to the case of linear maps between finitely generated projective modules: see the Notation X-6.5 as well as Exercises X-21, X-22 and X-23.

Comment The reader is cautioned that there is no universally accepted definition for "matrix of rank k" in the literature. When reading another book, one must first ascertain the definition adopted by the author. For example in the case of an integral ring $\mathbf{A}$, we often find the rank defined as that of the matrix over the quotient field of $\mathbf{A}$. Nevertheless a matrix of rank k in the sense of Definition 5.7 is generally of rank k in the sense of other authors. ∎

The following concrete local-global principle is an immediate consequence of the basic local-global principle.

5.8 Concrete local-global principle (Rank of a matrix) *Let $S_1, \ldots, S_n$ be comaximal monoids of $\mathbf{A}$ and B be a matrix $\in \mathbf{A}^{m\times p}$. Then the following properties are equivalent.*

1. *The matrix is of rank $\leqslant k$ (resp. of rank $\geqslant k$) over $\mathbf{A}$.*
2. *For $i \in [\![1..n]\!]$, the matrix is of rank $\leqslant k$ (resp. of rank $\geqslant k$) over $\mathbf{A}_{S_i}$.*

Generalized Pivot Method

Terminology

1) Two matrices are said to be *equivalent* if we can pass from one to the other by left- and right-multiplying by invertible matrices.
2) Two square matrices in $\mathbb{M}_n(\mathbf{A})$ are said to be *similar* when they represent the same endomorphism of $\mathbf{A}^n$ over two bases (distinct or not), in other words when they are conjugate with respect to the action $(G, M) \mapsto GMG^{-1}$ of $\mathbb{GL}_n(\mathbf{A})$ over $\mathbb{M}_n(\mathbf{A})$.
3) An *elementary row operation* on a matrix of n rows consists in replacing a row L_i with a row $L_i + \lambda L_j$ where $i \neq j$.

We also denote this by $L_i \leftarrow L_i + \lambda L_j$. This corresponds to the left-multiplication by a matrix, said to be *elementary*, denoted by $\mathrm{E}_{i,j}^{(n)}(\lambda)$ (or, if the context allows it, $\mathrm{E}_{i,j}(\lambda)$). This matrix is obtained from I_n by means of the same elementary row operation.

The right-multiplication by the same matrix $\mathrm{E}_{i,j}(\lambda)$ corresponds to the *elementary column operation* (for a matrix having n columns) which transforms the matrix I_n into $\mathrm{E}_{i,j}(\lambda)$: $C_j \leftarrow C_j + \lambda C_i$.
4) The subgroup of $\mathbb{SL}_n(\mathbf{A})$ generated by the elementary matrices is called the *elementary group* and it is denoted by $\mathbb{E}_n(\mathbf{A})$. Two matrices are said to be *elementarily equivalent* when we can pass from one to the other via elementary row and column operations. ∎

5.9 Invertible minor lemma (Generalized pivot) *If a matrix $G \in \mathbf{A}^{q\times m}$ has an invertible minor of order $k \leqslant \min(m, q)$, it is equivalent to a matrix*

$$\begin{bmatrix} \mathrm{I}_k & 0_{k,m-k} \\ 0_{q-k,k} & G_1 \end{bmatrix},$$

where $\mathcal{D}_r(G_1) = \mathcal{D}_{k+r}(G)$ for all $r \in \mathbb{Z}$.

▷ By eventually permuting the rows and the columns we bring the invertible minor to the top left. Next, by right-multiplying (or left-multiplying) by an invertible matrix, we reduce to the form

$$G' = \begin{bmatrix} \mathrm{I}_k & A \\ B & C \end{bmatrix},$$

then by elementary row and column operations, we obtain

$$G'' = \begin{bmatrix} \mathrm{I}_k & 0_{k,m-k} \\ 0_{q-k,k} & G_1 \end{bmatrix}.$$

Finally, $\mathcal{D}_r(G_1) = \mathcal{D}_{k+r}(G'') = \mathcal{D}_{k+r}(G)$ for all $r \in \mathbb{Z}$. □

As an immediate consequence we obtain the freeness lemma.

5.10 Freeness lemma *Consider a matrix $G \in \mathbf{A}^{q\times m}$ of rank $\leqslant k$ with $1 \leqslant k \leqslant \min(m, q)$. If the matrix G has an invertible minor of order k, then it is equivalent to the matrix*

$$\mathrm{I}_{k,q,m} = \begin{bmatrix} \mathrm{I}_k & 0_{k,m-k} \\ 0_{q-k,k} & 0_{q-k,m-k} \end{bmatrix}.$$

In this case, the image, the kernel and the cokernel of G are free, respectively of ranks k, $m-k$ and $q-k$. Moreover the image and the kernel have free summands.

If $i_1, \ldots, i_k$ (resp. $j_1, \ldots, j_k$) are the indexes of rows (resp. of columns) of the invertible minor, then the columns $j_1, \ldots, j_k$ form a basis of the module Im G, *and* Ker G *is the module of vectors annihilated by the linear forms corresponding to the rows $i_1, \ldots, i_k$.*

▷ With the notations of the previous lemma we have $\mathcal{D}_1(G_1)=\mathcal{D}_{k+1}(G)=0$, so $G_1 = 0$. The rest is left to the reader. □

The matrix $\mathrm{I}_{k,q,m}$ is called a *standard simple matrix*. We denote the matrix $\mathrm{I}_{k,n,n}$ by $\mathrm{I}_{k,n}$ and we call it a *standard projection matrix*.

5.11 Definition A linear map between free modules of finite rank is said to be *simple* if it can be represented by a matrix $\mathrm{I}_{k,q,m}$ over suitable bases. Similarly a matrix is said to be *simple* when it is equivalent to a matrix $\mathrm{I}_{k,q,m}$.

Generalized Cramer Formula

We study in this subsection some generalizations of the usual Cramer formulas. We will exploit these in the following paragraphs.

For a matrix $A \in \mathbf{A}^{m\times n}$ we denote by $A_{\alpha,\beta}$ the matrix extracted on the rows $\alpha = \{\alpha_1, \ldots, \alpha_r\} \subseteq [\![1..m]\!]$ and the columns $\beta = \{\beta_1, \ldots, \beta_s\} \subseteq [\![1..n]\!]$.

Suppose that the matrix A is of rank $\leqslant k$. Let $V \in \mathbf{A}^{m\times 1}$ be a column vector such that the bordered matrix $[\, A \mid V \,]$ is also of rank $\leqslant k$. Let us call A_j the j-th column of A. Let $\mu_{\alpha,\beta} = \det(A_{\alpha,\beta})$ be the minor of order k of the matrix A extracted on the rows $\alpha = \{\alpha_1, \ldots, \alpha_k\}$ and the columns $\beta = \{\beta_1, \ldots, \beta_k\}$. For $j \in [\![1..k]\!]$ let $\nu_{\alpha,\beta,j}$ be the determinant of the same extracted matrix, except that the column j has been replaced with the extracted column of V on the rows α. Then, we obtain for each pair (α, β) of multi-indices a Cramer identity:

$$\mu_{\alpha,\beta}\, V = \sum\nolimits_{j=1}^{k} \nu_{\alpha,\beta,j}\, A_{\beta_j} \tag{9}$$

due to the fact that the rank of the bordered matrix $[\, A_{1..m,\beta} \mid V \,]$ is $\leqslant k$. This can be read as follows:

$$\begin{aligned}
\mu_{\alpha,\beta}\, V &= \begin{bmatrix} A_{\beta_1} & \ldots & A_{\beta_k} \end{bmatrix} \cdot \begin{bmatrix} \nu_{\alpha,\beta,1} \\ \vdots \\ \nu_{\alpha,\beta,k} \end{bmatrix} \\
&= \begin{bmatrix} A_{\beta_1} & \ldots & A_{\beta_k} \end{bmatrix} \cdot \mathrm{Adj}(A_{\alpha,\beta}) \cdot \begin{bmatrix} v_{\alpha_1} \\ \vdots \\ v_{\alpha_k} \end{bmatrix} \\
&= A \cdot (\mathrm{I}_n)_{1..n,\beta} \cdot \mathrm{Adj}(A_{\alpha,\beta}) \cdot (\mathrm{I}_m)_{\alpha,1..m} \cdot V
\end{aligned} \tag{10}$$

This leads us to introduce the following notation.

5.12 Notation We denote by $\mathcal{P}_\ell$ the set of parts of $[\![1..\ell]\!]$ and $\mathcal{P}_{k,\ell}$ the set of parts of $[\![1..\ell]\!]$ with k elements. For $A \in \mathbf{A}^{m\times n}$ and $\alpha \in \mathcal{P}_{k,m}$, $\beta \in \mathcal{P}_{k,n}$

$$\mathrm{Adj}_{\alpha,\beta}(A) := (\mathrm{I}_n)_{1..n,\beta} \cdot \mathrm{Adj}(A_{\alpha,\beta}) \cdot (\mathrm{I}_m)_{\alpha,1..m}.$$

For example with the matrix

$$A = \begin{bmatrix} 5 & -5 & 7 & 4 \\ 9 & -1 & 2 & 7 \\ 13 & 3 & -3 & 10 \end{bmatrix},$$

and the parts $\alpha = \{1, 2\}$ and $\beta = \{2, 3\}$, we obtain

$$A_{\alpha,\beta} = \begin{bmatrix} -5 & 7 \\ -1 & 2 \end{bmatrix}, \ \mathrm{Adj}(A_{\alpha,\beta}) = \begin{bmatrix} 2 & -7 \\ 1 & -5 \end{bmatrix} \text{ and } \mathrm{Adj}_{\alpha,\beta}(A) = \begin{bmatrix} 0 & 0 & 0 \\ 2 & -7 & 0 \\ 1 & -5 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

When $\mathcal{D}_{k+1}([\, A \mid V \,]) = 0$, equality (10) is written as follows.

$$\mu_{\alpha,\beta}\, V \ = \ A \cdot \mathrm{Adj}_{\alpha,\beta}(A) \cdot V \tag{11}$$

We thus obtain the following equality, under the assumption that A is of rank $\leqslant k$.

$$\mu_{\alpha,\beta}\, A \ = \ A \cdot \mathrm{Adj}_{\alpha,\beta}(A) \cdot A \tag{12}$$

The Cramer's identities (11) and (12) provide the congruences which are not subject to any hypothesis: it suffices for example to read (11) in the quotient ring $\mathbf{A}/\mathcal{D}_{k+1}([\, A \mid V \,])$ to obtain the congruence (13).

5.13 Lemma (Generalized Cramer formula) *Without any assumption on the matrix A or the vector V, we have for $\alpha \in \mathcal{P}_{k,m}$ and $\beta \in \mathcal{P}_{k,n}$ the following congruences.*

$$\mu_{\alpha,\beta}\, V \equiv A \cdot \mathrm{Adj}_{\alpha,\beta}(A) \cdot V \quad \mod \ \mathcal{D}_{k+1}([\, A \mid V \,]), \tag{13}$$

$$\mu_{\alpha,\beta}\, A \equiv A \cdot \mathrm{Adj}_{\alpha,\beta}(A) \cdot A \quad \mod \ \mathcal{D}_{k+1}(A). \tag{14}$$

A simple special case is the following where $k = m \leqslant n$.

$$\mu_{1..m,\beta}\, \mathrm{I}_m \ = \ A \cdot \mathrm{Adj}_{1..m,\beta}(A) \quad (\beta \in \mathcal{P}_{m,n}). \tag{15}$$

This equality is in fact a direct consequence of the basic Cramer's identity (4). Similarly we obtain

$$\mu_{\alpha,1..n}\, \mathrm{I}_n \ = \ \mathrm{Adj}_{\alpha,1..n}(A) \cdot A \quad (\alpha \in \mathcal{P}_{n,m},\ n \leqslant m) \tag{16}$$

A Magic Formula

An immediate consequence of the Cramer's identity (12) is the less usual identity (17) given in the following theorem. Similarly the equalities (18) and (19) easily result from (15) and (16).

5.14 Theorem *Let $A \in \mathbf{A}^{m\times n}$ be a matrix of rank k. We thus have an equality $\sum_{\alpha\in\mathcal{P}_{k,m},\beta\in\mathcal{P}_{k,n}} c_{\alpha,\beta}\, \mu_{\alpha,\beta} = 1$. Let*

$$B \ = \ \textstyle\sum_{\alpha\in\mathcal{P}_{k,m},\beta\in\mathcal{P}_{k,n}} c_{\alpha,\beta}\ \mathrm{Adj}_{\alpha,\beta}(A).$$

1. *We have*
$$A \cdot B \cdot A = A. \tag{17}$$
Consequently $A\,B$ is a projection matrix of rank k and the submodule $\operatorname{Im} A = \operatorname{Im} AB$ *is a direct summand in* $\mathbf{A}^m$.
2. *If $k = m$, then*
$$A \cdot B = \mathrm{I}_m. \tag{18}$$
3. *If $k = n$, then*
$$B \cdot A = \mathrm{I}_n. \tag{19}$$

The following identity, which we will not use in this work, is even more miraculous.

5.15 Proposition (Prasad and Robinson) *With the assumptions and the notations of Theorem 5.14, if we have*

$$\forall \alpha, \alpha' \in \mathcal{P}_{k,m},\ \forall \beta, \beta' \in \mathcal{P}_{k,n}\ \ c_{\alpha,\beta}\, c_{\alpha',\beta'} = c_{\alpha,\beta'}\, c_{\alpha',\beta},$$

then
$$B \cdot A \cdot B = B. \tag{20}$$

Generalized Inverses and Locally Simple Maps

Let E and F be two $\mathbf{A}$-modules, and $\varphi : E \to F$ be a linear map. We can see this as some sort of generalized system of linear equations (a usual system of linear equations corresponds to the free modules of finite rank case). Informally such a system of linear equations is considered to be "well-conditioned" if there is a systematic way to solve the equation $\varphi(x) = y$ for x from a given y, when such a solution exists. More precisely, we ask if there exists a linear map $\psi : F \to E$ satisfying $\varphi\big(\psi(y)\big) = y$ each time there exists a solution x. This amounts to asking $\varphi\big(\psi\big(\varphi(x)\big)\big) = \varphi(x)$ for all $x \in E$.

This clarifies the importance of the Eq. (17) and leads to the notion of a generalized inverse.

The terminology regarding generalized inverses does not seem fully fixed. We adopt that of [Lancaster & Tismenetsky].

In the book [Bhaskara Rao], the author uses the term "reflexive g-inverse."

5.16 Definition Let E and F be two $\mathbf{A}$-modules, and $\varphi : E \to F$ be a linear map. A linear map $\psi : F \to E$ is called a *generalized inverse* of φ if we have

$$\varphi \circ \psi \circ \varphi = \varphi \quad \text{and} \quad \psi \circ \varphi \circ \psi = \psi. \tag{21}$$

A linear map is said to be *locally simple* when it has a generalized inverse.

The following fact is immediate.

5.17 Fact *When ψ is a generalized inverse of φ, we have:*

– *$\varphi\,\psi$ and $\psi\,\varphi$ are projections,*
– $\operatorname{Im}\varphi = \operatorname{Im}\varphi\,\psi$, $\operatorname{Im}\psi = \operatorname{Im}\psi\,\varphi$, $\operatorname{Ker}\varphi = \operatorname{Ker}\psi\,\varphi$, $\operatorname{Ker}\psi = \operatorname{Ker}\varphi\,\psi$,
– *$E = \operatorname{Ker}\varphi \oplus \operatorname{Im}\psi$ and $F = \operatorname{Ker}\psi \oplus \operatorname{Im}\varphi$,*
– $\operatorname{Ker}\varphi \simeq \operatorname{Coker}\psi$ *and* $\operatorname{Ker}\psi \simeq \operatorname{Coker}\varphi$.

Moreover φ and ψ provide by restriction reciprocal isomorphisms φ_1 and ψ_1 between $\operatorname{Im}\psi$ *and* $\operatorname{Im}\varphi$. *In matrix form we obtain:*

$$\begin{array}{c} \\ \operatorname{Im}\varphi \\ \operatorname{Ker}\psi \end{array}\!\!\begin{array}{c} \begin{array}{cc} \operatorname{Im}\psi & \operatorname{Ker}\varphi \end{array} \\ \begin{bmatrix} \varphi_1 & 0 \\ 0 & 0 \end{bmatrix} \end{array} = \varphi, \qquad \begin{array}{c} \\ \operatorname{Im}\psi \\ \operatorname{Ker}\varphi \end{array}\!\!\begin{array}{c} \begin{array}{cc} \operatorname{Im}\varphi & \operatorname{Ker}\psi \end{array} \\ \begin{bmatrix} \psi_1 & 0 \\ 0 & 0 \end{bmatrix} \end{array} = \psi.$$

Remarks

1) If we have a linear map ψ_0 satisfying as in Theorem 5.14 the equality $\varphi\,\psi_0\,\varphi = \varphi$, we obtain a generalized inverse of φ by stating $\psi = \psi_0\,\varphi\,\psi_0$. In other words, a linear map φ is locally simple if and only if there exists a ψ satisfying $\varphi\,\psi\,\varphi = \varphi$.
2) A simple linear map between free modules of finite rank is locally simple (immediate verification).
3) Theorem 5.14 informs us that a linear map which has rank k in the sense of Definition 5.7 is locally simple. ∎

5.18 Fact *Let $\varphi : \mathbf{A}^n \to \mathbf{A}^m$ be a linear map. The following properties are equivalent.*

1. *The linear map φ is locally simple.*
2. *There exists a $\varphi^\bullet : \mathbf{A}^m \to \mathbf{A}^n$ such that*
$$\mathbf{A}^n = \operatorname{Ker}\varphi \oplus \operatorname{Im}\varphi^\bullet \text{ and } \mathbf{A}^m = \operatorname{Ker}\varphi^\bullet \oplus \operatorname{Im}\varphi.$$
3. *The submodule $\operatorname{Im}\varphi$ is a direct summand in $\mathbf{A}^m$.*

▷ *1 ⇒ 2.* If ψ is a generalized inverse of φ, we can take $\varphi^\bullet = \psi$.
2 ⇒ 3. Obvious.
3 ⇒ 1. If $\mathbf{A}^m = P \oplus \operatorname{Im}\varphi$, denote by $\pi : \mathbf{A}^m \to \mathbf{A}^m$ the projection over $\operatorname{Im}\varphi$ parallel to P. For each vector e_i of the canonical basis of $\mathbf{A}^m$ there exists an element a_i of $\mathbf{A}^n$ such that $\varphi(a_i) = \pi(e_i)$. We define $\psi : \mathbf{A}^m \to \mathbf{A}^n$ as $\psi(e_i) = a_i$. Then, $\varphi \circ \psi = \pi$ and $\varphi \circ \psi \circ \varphi = \pi \circ \varphi = \varphi$, and $\psi \circ \varphi \circ \psi$ is a generalized inverse of φ. □

The notion of a locally simple linear map is a local notion in the following sense.

5.19 Concrete local-global principle (Locally simple linear maps) *Let $S_1, \ldots, S_n$ be comaximal monoids of a ring $\mathbf{A}$. Let $\varphi : \mathbf{A}^m \to \mathbf{A}^q$ be a linear map. If every $\varphi_{S_i} : \mathbf{A}^m_{S_i} \to \mathbf{A}^q_{S_i}$ is simple, then φ is locally simple. More generally φ is locally simple if and only if all the φ_{S_i}'s are locally simple.*

ᗡ Let us focus on the second statement. To prove that φ is locally simple amounts to finding a ψ which satisfies $\varphi\psi\varphi = \varphi$. This is a system of linear equations in the coefficients of the matrix of ψ and we can therefore apply the basic Concrete local-global principle 2.3. □

The terminology of a locally simple linear map is justified by the previous local-global principle and by the converse given in item *8* of Theorem 5.26 (also see the locally simple map lemma in the local ring case, p. 484).

Grassmannians

The following theorem serves as an introduction to the grassmannian varieties. It results from Fact 5.18 and Theorem 5.14.

5.20 Theorem (Finitely generated submodules as direct summands of a free module) *Let* $M = \langle C_1, \dots, C_m \rangle$ *be a finitely generated submodule of* $\mathbf{A}^n$ *and* $C = [\, C_1 \ \cdots \ C_m \,] \in \mathbf{A}^{n\times m}$ *be the corresponding matrix.*

1. *The following properties are equivalent.*
   a. *The matrix* C *is locally simple.*
   b. *The module* M *is a direct summand of* $\mathbf{A}^n$.
   c. *The module* M *is the image of a matrix* $F \in \mathbb{AG}_n(\mathbf{A})$.
2. *The following properties are equivalent.*
   a. *The matrix* C *is of rank* k.
   b. *The module* M *is image of a matrix* $F \in \mathbb{AG}_n(\mathbf{A})$ *of rank* k.

The "variety" of vector lines in a $\mathbf{K}$-vector space of dimension $n+1$ is, intuitively, of dimension n, as a vector line essentially depends on n parameters (a nonzero vector, up to a multiplicative constant, that makes $(n+1)-1$ independent parameters). We call this variety the projective space of dimension n over $\mathbf{K}$.

Furthermore, passing from a field $\mathbf{K}$ to an arbitrary ring $\mathbf{A}$, the correct generalization of a "vector line in $\mathbf{K}^{n+1}$" is "the image of a projection matrix of rank 1 in $\mathbf{A}^{n+1}$." This leads to the following definitions.

5.21 Definition

1. We define the space $\mathbb{AG}_{n,k}(\mathbf{A}) \subseteq \mathbb{AG}_n(\mathbf{A})$ as the set of projection matrices of rank k and $\mathbb{G}_{n,k}(\mathbf{A})$ as the set of submodules of $\mathbf{A}^n$ which are images of matrices of $\mathbb{AG}_{n,k}(\mathbf{A})$.
2. The space $\mathbb{G}_{n+1,1}(\mathbf{A})$ is again denoted by $\mathbb{P}^n(\mathbf{A})$ and we call it the *projective space of dimension n over* $\mathbf{A}$.
3. We denote by $\mathbb{G}_n(\mathbf{A})$ the space of all the submodules that are direct summands of $\mathbf{A}^n$ (i.e., images of a projection matrix).

The above definition is a little unsatisfactory, insofar as we have not explained how the set $\mathbb{G}_{n,k}(\mathbf{A})$ is structured. Only this structure makes it worthy of the label "space."

A partial answer is given by the observation that $\mathbb{G}_{n,k}$ is a functor. More precisely, to every homomorphism $\varphi : \mathbf{A} \to \mathbf{B}$ we associate a natural map $\mathbb{G}_{n,k}(\varphi) : \mathbb{G}_{n,k}(\mathbf{A}) \to \mathbb{G}_{n,k}(\mathbf{B})$, so that

$$\mathbb{G}_{n,k}(\mathrm{Id}_{\mathbf{A}}) = \mathrm{Id}_{\mathbb{G}_{n,k}(\mathbf{A})}, \text{ and } \mathbb{G}_{n,k}(\psi \circ \varphi) = \mathbb{G}_{n,k}(\psi) \circ \mathbb{G}_{n,k}(\varphi),$$

when $\psi \circ \varphi$ is defined.

Injectivity and Surjectivity Criteria

Two famous propositions are contained in the following theorem.

5.22 Theorem *Let $\varphi : \mathbf{A}^n \to \mathbf{A}^m$ be a linear map with matrix A.*

1. *The map φ is surjective if and only if φ is of rank m, i.e. here $\mathcal{D}_m(\varphi) = \langle 1 \rangle$ (we then say that A is* unimodular*).*
2. (McCoy's theorem) *The map φ is injective if and only if $\mathcal{D}_n(\varphi)$ is faithful, i.e. if the annihilator of $\mathcal{D}_n(\varphi)$ is reduced to* $\{0\}$.

▷ *1.* If φ is surjective, it admits a right inverse ψ, and Fact 5.6 gives $\langle 1 \rangle = \mathcal{D}_m(\mathrm{I}_m) \subseteq \mathcal{D}_m(\varphi)\mathcal{D}_m(\psi)$, so $\mathcal{D}_m(\varphi) = \langle 1 \rangle$. Conversely, if A is of rank m, Eq. (18) shows that A admits a right inverse, and φ is surjective.
2. Assume that $\mathcal{D}_n(A)$ is faithful. By equality (16), if $AV = 0$, then $\mu_{\alpha,1..n}V = 0$ for all the generators $\mu_{\alpha,1..n}$ of $\mathcal{D}_n(A)$, and so $V = 0$.
For the converse, we will prove by induction on k the following property: *if k column vectors $x_1, \ldots, x_k$ are linearly independent, then the annihilator of the vector $x_1 \wedge \cdots \wedge x_k$ is reduced to* 0. For $k = 1$ it is trivial. To pass from k to $k+1$ we proceed as follows. Let z be a scalar that annihilates $x_1 \wedge \cdots \wedge x_{k+1}$. For $\alpha \in \mathcal{P}_{k,m}$, we denote by $d_\alpha(y_1, \ldots, y_k)$ the minor extracted on the index rows of α for the column vectors $y_1, \ldots, y_k$ of $\mathbf{A}^m$. Since $z(x_1 \wedge \cdots \wedge x_{k+1}) = 0$, and by the Cramer formulas, we have the equality

$$z\left(d_\alpha(x_1, \ldots, x_k)x_{k+1} - d_\alpha(x_1, \ldots, x_{k-1}, x_{k+1})x_k + \cdots\right) = 0,$$

so $z\, d_\alpha(x_1, \ldots, x_k) = 0$.

As this is true for any α, this gives $z(x_1 \wedge \cdots \wedge x_k) = 0$, and by the induction hypothesis, $z = 0$. □

Remark Theorem 5.22 can also be read in the following way.

1. The linear map $\varphi : \mathbf{A}^n \to \mathbf{A}^m$ is surjective if and only if the map $\bigwedge^m \varphi : \mathbf{A}^{\binom{n}{m}} \to \mathbf{A}$ is surjective.
2. The linear map $\varphi : \mathbf{A}^n \to \mathbf{A}^m$ is injective if and only if the map $\bigwedge^n \varphi : \mathbf{A} \to \mathbf{A}^{\binom{m}{n}}$ is injective. ■

5.23 Corollary *Let $\varphi : \mathbf{A}^n \to \mathbf{A}^m$ be an $\mathbf{A}$-linear map.*

1. *If φ is surjective and $n < m$, the ring is trivial.*
2. *If φ is injective and $n > m$, the ring is trivial.*

Remark A more positive, equivalent, but probably even more bewildering formulation of the results of the previous corollary is the following.

1. If φ is surjective, then X^m divides X^n in $\mathbf{A}[X]$.
2. If φ is injective, then X^n divides X^m in $\mathbf{A}[X]$.

In some way, this is closer to the formulation found in classical mathematics: if the ring is nontrivial, then $m \leqslant n$ in the first case (resp. $n \leqslant m$ in the second case).

The advantage of our formulations is that they work in all cases, without the need to assume that we know how to decide if the ring is trivial or not. ∎

5.24 Corollary *If $\varphi : \mathbf{A}^n \to \mathbf{A}^m$ is injective, the same applies for every exterior power of φ.*

▷ The annihilator of $\mathcal{D}_n(\varphi)$ is reduced to 0 by the previous theorem. There exists a ring $\mathbf{B} \supseteq \mathbf{A}$ such that the generators of $\mathcal{D}_n(\varphi)$ become comaximal in $\mathbf{B}$ (Lemma 2.14). The $\mathbf{B}$-linear map $\varphi_1 : \mathbf{B}^n \to \mathbf{B}^m$ obtained by extending φ to $\mathbf{B}$ is thus of rank n and admits a left inverse ψ (item *3* of Theorem 5.14), i.e. $\psi \circ \varphi_1 = \mathrm{Id}_{\mathbf{B}^n}$. Therefore

$$\textstyle\bigwedge^k \psi \circ \bigwedge^k \varphi_1 = \mathrm{Id}_{\wedge^k \mathbf{B}^n}.$$

Thus the matrix of $\bigwedge^k \varphi_1$ is injective, and since it is the same matrix as that of $\bigwedge^k \varphi$, the linear map $\bigwedge^k \varphi$ is injective. □

Characterization of Locally Simple Maps

The following lemma places a bijective correspondence between the fundamental systems of orthogonal idempotents and the non-decreasing sequences of idempotents for divisibility.

5.25 Lemma *Let $(e_{q+1} = 0, e_q, \ldots, e_1, e_0 = 1)$ be a list of idempotents such that e_i divides e_{i+1} for $i = 0, \ldots, q$. Then, the elements $r_i := e_i - e_{i+1}$, for $i \in [\![0..q]\!]$, form a fundamental system of orthogonal idempotents. Conversely, every fundamental system of orthogonal idempotents $(r_0, \ldots, r_q)$ defines such a list of idempotents by letting*

$$e_j = \textstyle\sum_{k \geqslant j} r_k \text{ for } j \in [\![0..q+1]\!].$$

▷ It is clear that $\sum_i r_i = 1$. For $0 \leqslant i < q$, we have $e_{i+1} = e_i e_{i+1}$.

Hence $(e_i - e_{i+1})e_{i+1} = 0$, i.e. $(r_q + \cdots + r_{i+1}) \cdot r_i = 0$. We can now easily deduce that $r_i r_j = 0$ for $j > i$. □

We denote by $\mathrm{Diag}(a_1, \ldots, a_n)$ the diagonal matrix of order n whose coefficient in position (i, i) is the element a_i.

In the following theorem some of the idempotents r_i in the fundamental system of orthogonal idempotents can very well be equal to zero. For example if the ring is connected and nontrivial, all but one are equal to zero.

5.26 Theorem (Locally simple matrix) *Let $G \in \mathbf{A}^{m\times n}$ be the matrix of $\varphi : \mathbf{A}^n \to \mathbf{A}^m$ and $q = \inf(m, n)$.*

The following properties are equivalent.

1. *The linear map φ is locally simple.*
2. *The submodule $\mathrm{Im}\,\varphi$ is a direct summand of $\mathbf{A}^m$.*
3. *$\mathrm{Im}\,\varphi$ is a direct summand of $\mathbf{A}^m$ and $\mathrm{Ker}\,\varphi$ is a direct summand of $\mathbf{A}^n$.*
4. *There exists a linear map $\varphi^\bullet : \mathbf{A}^m \to \mathbf{A}^n$ with $\mathbf{A}^n = \mathrm{Ker}\,\varphi \oplus \mathrm{Im}\,\varphi^\bullet$ and $\mathbf{A}^m = \mathrm{Ker}\,\varphi^\bullet \oplus \mathrm{Im}\,\varphi$.*
5. *Each determinantal ideal $\mathcal{D}_k(\varphi)$ is idempotent.*
6. *There exists a (unique) fundamental system of orthogonal idempotents $(r_0, r_1, \ldots, r_q)$ such that on each localized ring $\mathbf{A}[1/r_k]$ the map φ is of rank k.*
7. *Each determinantal ideal $\mathcal{D}_k(\varphi)$ is generated by an idempotent e_k. Then let $r_k = e_k - e_{k+1}$. The r_k's form a fundamental system of orthogonal idempotents. For every minor μ of order k of G, on the localized ring $\mathbf{A}[1/(r_k\,\mu)]$ the linear map φ becomes simple of rank k.*
8. *The linear map φ becomes simple after localization at suitable comaximal elements.*
9. *Each determinantal ideal $\mathcal{D}_k(\varphi)$ is generated by an idempotent e_k and the matrix of φ becomes equivalent to the matrix $\mathrm{Diag}(e_1, e_2, \ldots, e_q)$, eventually filled-in with zeros (for both rows and columns), after localization at suitable comaximal elements.*
10. * *The linear map φ becomes simple after localization at any arbitrary maximal ideal.*

▷ The equivalence of items *1*, *2*, *3*, *4* is already clear (see Facts 5.17 and 5.18). Furthermore, we trivially have $7 \Rightarrow 6 \Rightarrow 5$ and $9 \Rightarrow 5$.

Since $q = \inf(m, n)$, we have $\mathcal{D}_{q+1}(\varphi) = 0$.

1 $\Rightarrow$ *5*. We have $GHG = G$ for some matrix H and we apply Fact 5.6.

5 $\Rightarrow$ *7*. The fact that each $\mathcal{D}_k(\varphi)$ is generated by an idempotent e_k results from Fact 4.6. The fact that $(r_0, \ldots, r_q)$ is a fundamental system of orthogonal idempotents results from Lemma 5.25 (and Fact 5.4).

As $r_k e_{k+1} = 0$, over the ring $\mathbf{A}[1/r_k]$, and thus over the ring $\mathbf{A}[1/(\mu r_k)]$, where μ is a minor of order k, every minor of order $k+1$ of the matrix G is null. Thus, by the Freeness lemma 5.10, G is simple of rank k.

7 $\Rightarrow$ *9*. Over $\mathbf{A}[1/r_k]$ and so over $\mathbf{A}[1/(\mu r_k)]$ (μ a minor of order k), we have $\mathrm{Diag}(e_1, \ldots, e_q) = \mathrm{Diag}(1, \ldots, 1, 0, \ldots, 0)$ with 1 appearing k times.

7 $\Rightarrow$ *8*. Let $t_{k,j}$ be the minors of order k of G. The localizations are those at $t_{k,j} r_k$. We must verify that they are comaximal. Each e_k is in the form $\sum t_{k,j} v_{k,j}$, so $\sum_{k,j} v_{k,j}(t_{k,j} r_k) = \sum_k e_k r_k = \sum r_k = 1$.

8 $\Rightarrow$ *1.* By application of the local-global principle 5.19 since every simple map is locally simple.
8 $\Rightarrow$ *10.* (In classical mathematics.) Because the complement of a maximal ideal always contains at least one element in a system of comaximal elements (we can assume that the ring is nontrivial).
10 $\Rightarrow$ *8.* (In classical mathematics.) For each maximal ideal $\mathfrak{m}$ we obtain a $s_{\mathfrak{m}} \notin \mathfrak{m}$ and a matrix $H_{\mathfrak{m}}$ such that we have $GH_{\mathfrak{m}}G = G$ in $\mathbf{A}[1/s_{\mathfrak{m}}]$. The ideal generated by the $s_{\mathfrak{m}}$'s is not contained in any maximal ideal and so it is the ideal $\langle 1\rangle$. Thus there is a finite number of these $s_{\mathfrak{m}}$'s which are comaximal.

Let us finish by giving a direct proof for the implication *6* $\Rightarrow$ *1.*

On the ring $\mathbf{A}[1/r_k]$ the matrix G is of rank k so there exists a matrix B_k satisfying $GB_kG = G$ (Theorem 5.14). This means that on the ring $\mathbf{A}$ we have a matrix H_k in $\mathbf{A}^{n\times m}$ satisfying $r_kH_k = H_k$ and $r_kG = GH_kG$. We then take $H = \sum_k H_k$ and obtain $G = GHG$. □

The equivalence of items *1* to *9* has been established constructively, whilst item *10* only implies the previous ones in classical mathematics.

Trace, Norm, Discriminant, Transitivity

We denote by $\mathrm{Tr}(\varphi)$ and $\mathrm{C}_\varphi(X)$ the trace and the *characteristic polynomial* of an endomorphism φ of a free module of finite rank (we take as characteristic polynomial of a matrix $F \in \mathbb{M}_n(\mathbf{A})$ the polynomial $\det(X\mathrm{I}_n - F)$, which has the advantage of being monic).

5.27 Notation

- If $\mathbf{A} \subseteq \mathbf{B}$ and if $\mathbf{B}$ is a free $\mathbf{A}$-module of finite rank, we denote $\mathrm{rk}_{\mathbf{A}}(\mathbf{B})$ by $[\,\mathbf{B} : \mathbf{A}\,]$.
- For $a \in \mathbf{B}$ we then denote by $\mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(a)$, $\mathrm{N}_{\mathbf{B}/\mathbf{A}}(a)$ and $\mathrm{C}_{\mathbf{B}/\mathbf{A}}(a)(X)$ the trace, the determinant and the characteristic polynomial of the multiplication by a, seen as an endomorphism of the $\mathbf{A}$-module $\mathbf{B}$.

5.28 Lemma *Assume that* $\mathbf{A} \subseteq \mathbf{B}$ *and that* $\mathbf{B}$ *is a free* $\mathbf{A}$*-module of finite rank* m*.*

1. *Let* E *be a free* $\mathbf{B}$*-module of finite rank* n*. If* $\underline{e} = (e_i)_{i\in[\![1..m]\!]}$ *is a basis of* $\mathbf{B}$ *over* $\mathbf{A}$ *and* $\underline{f} = (f_j)_{j\in[\![1..n]\!]}$ *a basis of* E *over* $\mathbf{B}$*, then* $(e_i f_j)_{i,j}$ *is a basis of* E *over* $\mathbf{A}$*. Consequently,* E *is free over* $\mathbf{A}$ *and*

$$\mathrm{rk}_{\mathbf{A}}(E) = \mathrm{rk}_{\mathbf{B}}(E) \times \mathrm{rk}_{\mathbf{A}}(\mathbf{B}).$$

2. *If* $\mathbf{B} \subseteq \mathbf{C}$ *and if* $\mathbf{C}$ *is a free* $\mathbf{B}$*-module of finite rank, we have*

$$[\,\mathbf{C} : \mathbf{A}\,] = [\,\mathbf{C} : \mathbf{B}\,]\,[\,\mathbf{B} : \mathbf{A}\,].$$

Remark Let $\mathbf{C} = \mathbf{A}[Y]/\langle Y^3\rangle = \mathbf{A}[y]$, a free $\mathbf{A}$-algebra of rank 3. Since $y^4 = 0$, $\mathbf{B} = \mathbf{A} \oplus \mathbf{A}y^2$ is a sub-algebra of $\mathbf{C}$, free over $\mathbf{A}$, whose rank (equal to 2) does not divide the rank of $\mathbf{C}$ (equal to 3). The equality $[\,\mathbf{C} : \mathbf{A}\,] = [\,\mathbf{C} : \mathbf{B}\,][\,\mathbf{B} : \mathbf{A}\,]$ does not apply because $\mathbf{C}$ is not free over $\mathbf{B}$. ∎

5.29 Theorem (Transitivity formulas for the trace, the determinant and the characteristic polynomial) *Under the same assumptions, let $u_{\mathbf{B}} : E \to E$ be a $\mathbf{B}$-linear map. We denote by $u_{\mathbf{A}}$ this map when considered as an $\mathbf{A}$-linear map. We then have the equalities:*

$$\det(u_{\mathbf{A}}) = \mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(\det(u_{\mathbf{B}})\big),\ \mathrm{Tr}(u_{\mathbf{A}}) = \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}\big(\mathrm{Tr}(u_{\mathbf{B}})\big),$$
$$\mathrm{C}_{u_{\mathbf{A}}}(X) = \mathrm{N}_{\mathbf{B}[X]/\mathbf{A}[X]}\big(\mathrm{C}_{u_{\mathbf{B}}}(X)\big).$$

▷ We use the notations of Lemma 5.28. Let u_{kj} be the elements of $\mathbf{B}$ defined by $u(f_j) = \sum_{k=1}^{n} u_{kj} f_k$. Then the matrix M of $u_{\mathbf{A}}$ with respect to the basis $(e_i f_j)_{i,j}$ is expressed as a block matrix

$$M = \begin{bmatrix} M_{11} & \cdots & M_{1n} \\ \vdots & & \vdots \\ M_{n1} & \cdots & M_{nn} \end{bmatrix},$$

where M_{kj} represents the $\mathbf{A}$-linear map $b \mapsto bu_{kj}$ of $\mathbf{B}$ in $\mathbf{B}$ to with respect to the basis $\underline{e}$. This provides the desired equality regarding the trace of u_A since

$$\begin{aligned} \mathrm{Tr}(u_{\mathbf{A}}) &= \sum_{i=1}^{n} \mathrm{Tr}(M_{ii}) = \sum_{i=1}^{n} \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(u_{ii}) \\ &= \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}\Big(\sum_{i=1}^{n} u_{ii}\Big) = \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}\big(\mathrm{Tr}(u_{\mathbf{B}})\big). \end{aligned}$$

As for the equality for the determinant, note that the matrices M_{ij} pairwise commute (M_{ij} is the matrix of the multiplication by u_{ij}). We can then apply the following Lemma 5.30, which gives us:

$$\det(M) = \det(\Delta) \quad \text{with} \quad \Delta = \sum\nolimits_{\sigma \in \mathrm{S}_n} \varepsilon(\sigma) M_{1\sigma_1} M_{2\sigma_2} \dots M_{n\sigma_n}.$$

However, Δ is none other than the matrix of the multiplication by the element $\sum_{\sigma \in \mathrm{S}_n} \varepsilon(\sigma) u_{1\sigma_1} u_{2\sigma_2} \dots u_{n\sigma_n}$, i.e., by $\det(u_{\mathbf{B}})$, thus:

$$\det(u_{\mathbf{A}}) = \det(M) = \mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(\det(u_{\mathbf{B}})\big).$$

Finally, the equality for the characteristic polynomial is deduced from the one for determinants by using the fact that $\mathrm{C}_{u_{\mathbf{A}}}(X)$ is the determinant of the endomorphism $X\mathrm{Id}_{E[X]} - u_{\mathbf{A}}$ of the $\mathbf{A}[X]$-module $E[X]$ whereas $\mathrm{C}_{u_{\mathbf{B}}}(X)$ is that of the same map seen as an endomorphism of the $\mathbf{B}[X]$-module $E[X]$. □

In a noncommutative ring, two elements a and b are said to be *permutable* or *commuting* if $ab = ba$.

5.30 Lemma *Let $(N_{ij})_{i,j}$ be a family of n^2 pairwise commuting square matrices, and N the square matrix of order mn:*

$$N = \begin{bmatrix} N_{11} & \cdots & N_{1n} \\ \vdots & & \vdots \\ N_{n1} & \cdots & N_{nn} \end{bmatrix}.$$

Then: $\det(N) = \det\left(\sum_{\sigma\in \mathrm{S}_n} \varepsilon(\sigma)\, N_{1\sigma_1} N_{2\sigma_2} \dots N_{n\sigma_n}\right)$.

▷ Let Δ be the $n \times n$ matrix defined by $\Delta = \sum_{\sigma\in \mathrm{S}_n} \varepsilon(\sigma) N_{1\sigma_1} N_{2\sigma_2} \dots N_{n\sigma_n}$. Thus we must prove that $\det(N) = \det(\Delta)$.

Let us treat the special cases $n = 2$ then $n = 3$. We replace $\mathbf{A}$ with $\mathbf{A}[Y]$ and N_{ii} by $N_{ii} + Y\mathrm{I}_m$, which has the advantage of making some determinants regular in $\mathbf{A}[Y]$. It suffices to establish the equalities with these new matrices, as we finish by making $Y = 0$.

The key-element of the proof for $n = 2$ resides in the following equality:

$$\begin{bmatrix} N_{11} & N_{12} \\ N_{21} & N_{22} \end{bmatrix} \begin{bmatrix} N_{22} & 0 \\ -N_{21} & \mathrm{I}_m \end{bmatrix} = \begin{bmatrix} N_{11}N_{22} - N_{12}N_{21} & N_{12} \\ 0 & N_{22} \end{bmatrix}.$$

We then consider the LHS and RHS determinants

$$\det(N)\det(N_{22}) = \det(N_{11}N_{22} - N_{12}N_{21})\det(N_{22}),$$

next we simplify by $\det(N_{22})$ (which is regular) to obtain the result.

Case $n = 3$ uses the equality:

$$\begin{bmatrix} N_{11} & N_{12} & N_{13} \\ N_{21} & N_{22} & N_{23} \\ N_{31} & N_{32} & N_{33} \end{bmatrix} \begin{bmatrix} N_{22}N_{33} - N_{23}N_{32} & 0 & 0 \\ N_{31}N_{23} - N_{21}N_{33} & \mathrm{I}_m & 0 \\ N_{21}N_{32} - N_{22}N_{31} & 0 & \mathrm{I}_m \end{bmatrix} = \begin{bmatrix} \Delta & N_{12} & N_{13} \\ 0 & N_{22} & N_{23} \\ 0 & N_{32} & N_{33} \end{bmatrix},$$

which leads to

$$\det(N)\det(N_{22}N_{33} - N_{23}N_{32}) = \det(\Delta)\det\begin{bmatrix} N_{22} & N_{23} \\ N_{32} & N_{33} \end{bmatrix}.$$

Case $n = 2$ provides $\det(N_{22}N_{33} - N_{23}N_{32}) = \det\begin{bmatrix} N_{22} & N_{23} \\ N_{32} & N_{33} \end{bmatrix}$. We simplify by this determinant and obtain $\det(N) = \det(\Delta)$.

The general case is left as an exercise (see Exercise 28). □

5.31 Corollary *Let $\mathbf{A} \subseteq \mathbf{B} \subseteq \mathbf{C}$ be three rings with $\mathbf{C}$ free of finite rank over $\mathbf{B}$ and $\mathbf{B}$ free of finite rank over $\mathbf{A}$. We then have:*

$$\mathrm{N}_{\mathbf{C}/\mathbf{A}} = \mathrm{N}_{\mathbf{B}/\mathbf{A}} \circ \mathrm{N}_{\mathbf{C}/\mathbf{B}}, \quad \mathrm{Tr}_{\mathbf{C}/\mathbf{A}} = \mathrm{Tr}_{\mathbf{B}/\mathbf{A}} \circ \mathrm{Tr}_{\mathbf{C}/\mathbf{B}},$$
$$\mathrm{C}_{\mathbf{C}/\mathbf{A}}(c)(X) = \mathrm{N}_{\mathbf{B}[X]/\mathbf{A}[X]}\big(\mathrm{C}_{\mathbf{C}/\mathbf{B}}(c)(X)\big) \quad (c \in \mathbf{C}).$$

Gram Determinants and Discriminants

5.32 Definition Let M be an $\mathbf{A}$-module, $\varphi : M \times M \to \mathbf{A}$ be a symmetric bilinear form and $(\underline{x}) = (x_1, \ldots, x_k)$ be a list of elements of M. We call the matrix

$$\mathrm{Gram}_{\mathbf{A}}(\varphi, \underline{x}) \stackrel{\text{def}}{=} \big(\varphi(x_i, x_j)\big)_{i,j\in[\![1..k]\!]}$$

the *Gram matrix of* $(x_1, \ldots, x_k)$ *for* φ. Its determinant is called the *Gram determinant of* $(x_1, \ldots, x_k)$ *for* φ and is denoted by $\mathrm{gram}_{\mathbf{A}}(\varphi, \underline{x})$.

If $\mathbf{A}y_1 + \cdots + \mathbf{A}y_k \subseteq \mathbf{A}x_1 + \cdots + \mathbf{A}x_k$ we have an equality

$$\mathrm{gram}(\varphi, y_1, \ldots, y_k) = \det(A)^2 \,\mathrm{gram}(\varphi, x_1, \ldots, x_k),$$

where A is a $k \times k$ matrix which expresses the y_j's in terms of the x_i's.

We now introduce an important case of a Gram determinant, the discriminant. Recall that two elements a, b of a ring $\mathbf{A}$ are said to be *associated* if there exists a $u \in \mathbf{A}^\times$ such that $a = ub$. In the literature such elements are also referred to as *associates*.

5.33 Proposition and definition *Let* $\mathbf{C} \supseteq \mathbf{A}$ *be an* $\mathbf{A}$*-algebra which is a free* $\mathbf{A}$*-module of finite rank and* $x_1, \ldots, x_k, y_1, \ldots, y_k \in \mathbf{C}$.

1. *We call the determinant of the matrix*

$$\big(\mathrm{Tr}_{\mathbf{C}/\mathbf{A}}(x_i x_j)\big)_{i,j\in[\![1..k]\!]}$$

   the discriminant *of* $(x_1, \ldots, x_k)$. *We denote it by* $\mathrm{disc}_{\mathbf{C}/\mathbf{A}}(x_1, \ldots, x_k)$ *or* $\mathrm{disc}(x_1, \ldots, x_k)$.
2. *If* $\mathbf{A}y_1 + \cdots + \mathbf{A}y_k \subseteq \mathbf{A}x_1 + \cdots + \mathbf{A}x_k$ *we have*

$$\mathrm{disc}(y_1, \ldots, y_k) = \det(A)^2 \,\mathrm{disc}(x_1, \ldots, x_k),$$

   where A *is a* $k \times k$ *matrix which expresses the* y_j*'s in terms of the* x_i*'s.*
3. *In particular, if* $(x_1, \ldots, x_n)$ *and* $(y_1, \ldots, y_n)$ *are two bases of the* $\mathbf{A}$*-algebra* $\mathbf{C}$*, the elements* $\mathrm{disc}(x_1, \ldots, x_n)$ *and* $\mathrm{disc}(y_1, \ldots, y_n)$ *are multiplicatively congruent modulo the squares of* $\mathbf{A}^\times$*. We call the corresponding equivalence class the* discriminant of the extension $\mathbf{C}/\mathbf{A}$. *We denote it by* $\mathrm{Disc}_{\mathbf{C}/\mathbf{A}}$.
4. *If* $\mathrm{Disc}_{\mathbf{C}/\mathbf{A}}$ *is regular and* $n = [\,\mathbf{C} : \mathbf{A}\,]$*, a system* $u_1, \ldots, u_n$ *in* $\mathbf{C}$ *is an* $\mathbf{A}$*-basis of* $\mathbf{C}$ *if and only if* $\mathrm{disc}(u_1, \ldots, u_n)$ *and* $\mathrm{Disc}_{\mathbf{C}/\mathbf{A}}$ *are associated elements.*

For example when $\mathbf{A} = \mathbb{Z}$ the discriminant of the extension is a well-defined integer, whereas if $\mathbf{A} = \mathbb{Q}$, the discriminant is characterized on the one hand by its sign, and on the other hand by the list of prime numbers contained therein with an odd power.

5.34 Proposition *Let* $\mathbf{B}$ *and* $\mathbf{C}$ *be two free* $\mathbf{A}$*-algebras of ranks* m *and* n*, respectively, and consider the product algebra* $\mathbf{B} \times \mathbf{C}$*.*

Given a list $(\underline{x}) = (x_1, \ldots, x_m)$ *of elements of* $\mathbf{B}$ *and a list* $(\underline{y}) = (y_1, \ldots, y_n)$ *of elements of* $\mathbf{C}$*, we have:*

$$\operatorname{disc}_{(\mathbf{B}\times\mathbf{C})/\mathbf{A}}(\underline{x}, \underline{y}) = \operatorname{disc}_{\mathbf{B}/\mathbf{A}}(\underline{x}) \times \operatorname{disc}_{\mathbf{C}/\mathbf{A}}(\underline{y}).$$

In particular, $\operatorname{Disc}_{(\mathbf{B}\times\mathbf{C})/\mathbf{A}} = \operatorname{Disc}_{\mathbf{B}/\mathbf{A}} \times \operatorname{Disc}_{\mathbf{C}/\mathbf{A}}$.

▷ The proof is left to the reader. □

5.35 Proposition *Let* $\mathbf{B} \supseteq \mathbf{A}$ *be a free* $\mathbf{A}$*-algebra of finite rank* p*.*
We consider

- *a* $\mathbf{B}$*-module* E*,*
- *a symmetric* $\mathbf{B}$*-bilinear form* $\varphi_{\mathbf{B}} : E \times E \to \mathbf{B}$*,*
- *a basis* $(\underline{b}) = (b_i)_{i\in[\![1..p]\!]}$ *of* $\mathbf{B}$ *over* $\mathbf{A}$*, and*
- *a family* $(\underline{e}) = (e_j)_{j\in[\![1..n]\!]}$ *of* n *elements of* E*.*

Let $(\underline{b} \star \underline{e})$ *be a family* $(b_i e_j)$ *of* np *elements of* E *and* $\varphi_{\mathbf{A}} : E \times E \to \mathbf{A}$ *be the symmetric* $\mathbf{A}$*-bilinear form defined by:*

$$\varphi_{\mathbf{A}}(x, y) = \operatorname{Tr}_{\mathbf{B}/\mathbf{A}}\big(\varphi_{\mathbf{B}}(x, y)\big).$$

We then have the following transitivity formula:

$$\operatorname{gram}(\varphi_{\mathbf{A}}, \underline{b} \star \underline{e}) = \operatorname{disc}_{\mathbf{B}/\mathbf{A}}(\underline{b})^n \times \operatorname{N}_{\mathbf{B}/\mathbf{A}}\big(\operatorname{gram}(\varphi_{\mathbf{B}}, \underline{e})\big).$$

▷ In the following the indices i, i', k, j, j' satisfy $i, i', k \in [\![1..p]\!]$ and $j, j' \in [\![1..n]\!]$. Let us agree to sort $\underline{b} \star \underline{e}$ in the following order:

$$\underline{b} \star \underline{e} = b_1e_1, \ldots, b_pe_1, b_1e_2, \ldots, b_pe_2, \ldots, b_1e_n, \ldots, b_pe_n.$$

For $x \in \mathbf{B}$, let $\mu_x : \mathbf{B} \to \mathbf{B}$ be the multiplication by x and $m(x)$ be the matrix of μ_x with respect to the basis $(b_i)_{i\in[\![1..p]\!]}$ of $\mathbf{B}$ over $\mathbf{A}$. Thus we define an isomorphism m of the ring $\mathbf{B}$ into a commutative subring of $\mathbb{M}_p(\mathbf{A})$. If we let $m_{ki}(x)$ be the coefficients of the matrix $m(x)$, we then have:

$$\mu_x(b_i) = b_i x = \sum\nolimits_{k=1}^{p} m_{ki}(x) b_k,$$

with $\operatorname{N}_{\mathbf{B}/\mathbf{A}}(x) = \det\big(m(x)\big)$. By letting $\varphi_{jj'} = \varphi_{\mathbf{B}}(e_j, e_{j'}) \in \mathbf{B}$, we have

$$\varphi_{\mathbf{A}}(b_i e_j b_{i'} e_{j'}) = \operatorname{Tr}_{\mathbf{B}/\mathbf{A}}\big(\varphi_{\mathbf{B}}(b_i e_j b_{i'} e_{j'})\big) = \operatorname{Tr}_{\mathbf{B}/\mathbf{A}}(b_i b_{i'} \varphi_{jj'}).$$

By using the equality $b_{i'}\varphi_{jj'} = \sum_{k=1}^{p} m_{ki'}(\varphi_{jj'})\, b_k$, we have with $\mathrm{Tr} = \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}$:

$$\mathrm{Tr}(b_i b_{i'} \varphi_{jj'}) = \mathrm{Tr}\Big(\sum\nolimits_{k=1}^{p} b_i\, m_{ki'}(\varphi_{jj'})\, b_k\Big) = \sum\nolimits_{k=1}^{p} \mathrm{Tr}(b_i b_k)\, m_{ki'}(\varphi_{jj'}). \qquad (*)$$

We define $\beta \in \mathbb{M}_p(\mathbf{A})$ by $\beta_{ik} = \mathrm{Tr}_{\mathbf{B}/\mathbf{A}}(b_i b_k)$. The right-hand sum in $(*)$ is none other than the coefficient of a product of matrices: $\big(\beta \cdot m(\varphi_{jj'})\big)_{ii'}$. The Gram determinant of $\underline{b} \star \underline{e}$ for $\varphi_{\mathbf{A}}$ is therefore an $np \times np$ matrix comprised of n^2 blocks of $p \times p$ matrices. Here is that matrix if we let $\phi_{jj'} = m(\varphi_{jj'})$ to simplify the expression:

$$\begin{bmatrix} \beta\phi_{11} & \beta\phi_{12} & \dots & \beta\phi_{1n} \\ \beta\phi_{21} & \beta\phi_{22} & \dots & \beta\phi_{2n} \\ \vdots & & & \vdots \\ \beta\phi_{n1} & \beta\phi_{n2} & \dots & \beta\phi_{nn} \end{bmatrix} = \begin{bmatrix} \beta & 0 & \dots & 0 \\ 0 & \beta & \dots & \vdots \\ \vdots & & \ddots & 0 \\ 0 & & \dots & \beta \end{bmatrix} \begin{bmatrix} \phi_{11} & \phi_{12} & \dots & \phi_{1n} \\ \phi_{21} & \phi_{22} & \dots & \phi_{2n} \\ \vdots & & & \vdots \\ \phi_{n1} & \phi_{n2} & \dots & \phi_{nn} \end{bmatrix}.$$

By taking the determinants we obtain

$$\mathrm{gram}(\varphi_{\mathbf{A}}, \underline{b} \star \underline{e}) = \det(\beta)^n \cdot \det \begin{bmatrix} \phi_{11} & \phi_{12} & \dots & \phi_{1n} \\ \phi_{21} & \phi_{22} & \dots & \phi_{2n} \\ \vdots & & & \vdots \\ \phi_{n1} & \phi_{n2} & \dots & \phi_{nn} \end{bmatrix}.$$

By using the fact that the matrices ϕ_{jl} pairwise commute, we find that the right-determinant is equal to

$$\det\Big(\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \phi_{1\sigma_1} \phi_{2\sigma_2} \dots \phi_{n\sigma_n}\Big) = \det m\Big(\det(\varphi_{jl})\Big) = \mathrm{N}_{\mathbf{B}/\mathbf{A}}\Big(\mathrm{gram}(\varphi_{\mathbf{B}}, \underline{e})\Big),$$

as required. □

5.36 Theorem (Transitivity formula for the discriminants) *Let* $\mathbf{A} \subseteq \mathbf{B} \subseteq \mathbf{C}$, *with* $\mathbf{B}$ *free over* $\mathbf{A}$, $\mathbf{C}$ *free over* $\mathbf{B}$, $[\,\mathbf{C} : \mathbf{B}\,] = n$ *and* $[\,\mathbf{B} : \mathbf{A}\,] = m$. *Let* $(\underline{b}) = (b_i)_{i \in [\![1..m]\!]}$ *be a basis of* $\mathbf{B}$ *over* $\mathbf{A}$, $(\underline{c}) = (c_j)_{j \in [\![1..n]\!]}$ *be a basis of* $\mathbf{C}$ *over* $\mathbf{B}$ *and let* $(\underline{b} \star \underline{c})$ *be the basis* $(b_i c_j)$ *of* $\mathbf{C}$ *over* $\mathbf{A}$. *Then:*

$$\begin{aligned} \mathrm{disc}_{\mathbf{C}/\mathbf{A}}(\underline{b} \star \underline{c}) &= \mathrm{disc}_{\mathbf{B}/\mathbf{A}}(\underline{b})^{[\,\mathbf{C}:\mathbf{B}\,]}\, \mathrm{N}_{\mathbf{B}/\mathbf{A}}\big(\mathrm{disc}_{\mathbf{C}/\mathbf{B}}(\underline{c})\big), \\ \textit{and so} \quad \mathrm{Disc}_{\mathbf{C}/\mathbf{A}} &= \mathrm{Disc}_{\mathbf{B}/\mathbf{A}}^{[\,\mathbf{C}:\mathbf{B}\,]}\, \mathrm{N}_{\mathbf{B}/\mathbf{A}}(\mathrm{Disc}_{\mathbf{C}/\mathbf{B}}). \end{aligned}$$

▷ Direct application of Proposition 5.35. □

6 Basic Local-Global Principle for Modules

This section's results will not be used before Chap. V.

We are about to give a slightly more general version of the basic local-global principle 2.3. This new principle concerns arbitrary **A**-modules and linear maps, whilst the basic principle can be considered as the special case where the modules are free and of finite rank. The proof is essentially the same as that of the basic principle.

Beforehand, we start with a brief review of exact sequences and we establish some elementary properties of the localization regarding modules.

Complexes and Exact Sequences

When we have successive linear maps

$$M \xrightarrow{\alpha} N \xrightarrow{\beta} P \xrightarrow{\gamma} Q\ ,$$

we say that they form a *complex* if the composition of any two successive linear maps is null. We say that the sequence is *exact in* N if $\operatorname{Im}\alpha = \operatorname{Ker}\beta$. The entire sequence is said to be exact if it is exact in N and P. This extends to sequences of arbitrary length.

This "abstract" language has an immediate counterpart in terms of systems of linear equations when we are dealing with free modules of finite rank. For example if $N = \mathbf{A}^n$, $P = \mathbf{A}^m$ and if we have an exact sequence

$$0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \xrightarrow{\gamma} Q \to 0\ ,$$

The linear map β is represented by a matrix associated with a system of m linear equations with n unknowns, the module M, isomorphic to $\operatorname{Ker}\beta$, represents the defect of injectivity of β and the module Q, isomorphic to $\operatorname{Coker}\beta$, represents its defect of surjectivity of β.

An exact complex of the type

$$0 \to M_m \xrightarrow{u_m} M_{m-1} \longrightarrow \cdots\cdots\cdots \xrightarrow{u_1} M_0 \to 0$$

with $m \geqslant 3$ is called a *long exact sequence (of length m)*.

If $m = 2$, we say that we have a *short exact sequence*. In this case M_2 can be identified with a submodule of M_1, and, modulo this identification, M_0 can be identified with M_1/M_2.

An important fact to note is that every long exact sequence of length m "can be decomposed into" $m-1$ short exact sequences according to the following schema.

$$\begin{array}{ccccccccc}
0 \to & E_2 & \xrightarrow{\iota_2} & M_1 & \xrightarrow{u_1} & M_0 & \to 0 \\
0 \to & E_3 & \xrightarrow{\iota_3} & M_2 & \xrightarrow{v_2} & E_2 & \to 0 \\
\vdots & & & & & & \vdots \\
0 \to & E_{m-1} & \xrightarrow{\iota_{m-1}} & M_{m-2} & \xrightarrow{v_{m-2}} & E_{m-2} & \to 0 \\
0 \to & M_m & \xrightarrow{u_m} & M_{m-1} & \xrightarrow{v_{m-1}} & E_{m-1} & \to 0
\end{array}$$

with $E_i = \operatorname{Im} u_{i+1} \subseteq M_i$ for $i \in [\![2..m-1]\!]$, the ι_k's canonical injections, and the v_k's obtained from the u_k's by restricting the range to $\operatorname{Im} u_k$.

An important theme of commutative algebra is provided by the transformations that preserve, or do not preserve, exact sequences.

Here are two basic examples, which use the modules of linear maps.

Let $\mathrm{L}_{\mathbf{A}}(M, P)$ be the $\mathbf{A}$-module of $\mathbf{A}$-linear maps from M to P and $\mathrm{End}_{\mathbf{A}}(M)$ designate $\mathrm{L}_{\mathbf{A}}(M, M)$ (with its ring structure generally noncommutative). The *dual module* of M, $\mathrm{L}_{\mathbf{A}}(M, \mathbf{A})$, will in general be denoted by $M^\star$.

6.1 Fact *If* $0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P$ *is an exact sequence of* $\mathbf{A}$*-modules, and if* F *is an* $\mathbf{A}$*-module, then the sequence*

$$0 \to \mathrm{L}_{\mathbf{A}}(F, M) \longrightarrow \mathrm{L}_{\mathbf{A}}(F, N) \longrightarrow \mathrm{L}_{\mathbf{A}}(F, P)$$

is exact.

▷ *Exactness in* $\mathrm{L}_{\mathbf{A}}(F, M)$. Let $\varphi \in \mathrm{L}_{\mathbf{A}}(F, M)$ such that $\alpha \circ \varphi = 0$. Then, since the first sequence is exact in M, for all $x \in F$, $\varphi(x) = 0$, so $\varphi = 0$.

Exactness in $\mathrm{L}_{\mathbf{A}}(F, N)$. Let $\varphi \in \mathrm{L}_{\mathbf{A}}(F, N)$ such that $\beta \circ \varphi = 0$. Then, since the first sequence is exact in N, for all $x \in F$, $\varphi(x) \in \operatorname{Im} \alpha$.

Let $\alpha_1 : \operatorname{Im} \alpha \to M$ be the inverse of the bijection α (regarding the codomain of α as $\operatorname{Im} \alpha$) and $\psi = \alpha_1 \varphi$.

We then obtain the equalities $\mathrm{L}_{\mathbf{A}}(F, \alpha)(\psi) = \alpha \, \alpha_1 \, \varphi = \varphi$. □

6.2 Fact *If* $N \xrightarrow{\beta} P \xrightarrow{\gamma} Q \to 0$ *is an exact sequence of* $\mathbf{A}$*-modules and if* F *is an* $\mathbf{A}$*-module, then the sequence*

$$0 \to \mathrm{L}_{\mathbf{A}}(Q, F) \longrightarrow \mathrm{L}_{\mathbf{A}}(P, F) \longrightarrow \mathrm{L}_{\mathbf{A}}(N, F)$$

is exact.

▷ *Exactness in* $\mathrm{L}_{\mathbf{A}}(Q, F)$. If $\varphi \in \mathrm{L}_{\mathbf{A}}(Q, F)$ satisfies $\varphi \circ \gamma = 0$, then, since γ is surjective, $\varphi = 0$.

Exactness in $\mathrm{L}_{\mathbf{A}}(P, F)$. If $\varphi : P \to F$ satisfies $\varphi \circ \beta = 0$, then $\operatorname{Im} \beta \subseteq \operatorname{Ker} \varphi$ and φ is factorized by $P/\operatorname{Im} \beta \simeq Q$, that is $\varphi = \psi \circ \gamma$ for a linear map $\psi : Q \to F$, i.e. $\varphi \in \operatorname{Im} \mathrm{L}_{\mathbf{A}}(\gamma, F)$. □

6.3 Fact *Let* $\beta : N \to P$ *be a linear map and* $\gamma : P \to \operatorname{Coker} \beta$ *be the canonical projection.*

1. *The canonical map* ${}^{\mathrm{t}}\gamma : (\operatorname{Coker} \beta)^\star \to P^\star$ *induces an isomorphism of* $(\operatorname{Coker} \beta)^\star$ *on* $\operatorname{Ker} {}^{\mathrm{t}}\beta$.
2. *If the canonical linear maps* $N \to N^{\star\star}$ *and* $P \to P^{\star\star}$ *are isomorphisms, then the canonical surjection of* $N^\star$ *in* $\operatorname{Coker} {}^{\mathrm{t}}\beta$ *provides by duality an isomorphism of* $(\operatorname{Coker} {}^{\mathrm{t}}\beta)^\star$ *on* $\operatorname{Ker} \beta$.

▷ *1.* We apply Fact 6.2 with $F = \mathbf{A}$.
2. We apply item *1* to the linear map ${}^{\mathrm{t}}\beta$ by identifying N and $N^{\star\star}$, as well as P and $P^{\star\star}$, and thus also β and ${}^{\mathrm{t}}({}^{\mathrm{t}}\beta)$. □

Remark It is possible to slightly weaken the assumption by requiring that the linear map $P \to P^{\star\star}$ be injective. ■

Localization and Exact Sequences

6.4 Fact *Let S be a monoid of a ring* $\mathbf{A}$.

1. *If M is a submodule of N, we have the canonical identification of M_S with a submodule of N_S and of $(N/M)_S$ with N_S/M_S.*
   In particular, for every ideal $\mathfrak{a}$ of $\mathbf{A}$*, the* $\mathbf{A}$*-module $\mathfrak{a}_S$ is canonically identified with the ideal $\mathfrak{a}\mathbf{A}_S$ of $\mathbf{A}_S$.*
2. *If $\varphi : M \to N$ is an* $\mathbf{A}$*-linear map, then:*
   a. $\mathrm{Im}(\varphi_S)$ *is canonically identified with* $\big(\mathrm{Im}(\varphi)\big)_S$,
   b. $\mathrm{Ker}(\varphi_S)$ *is canonically identified with* $\big(\mathrm{Ker}(\varphi)\big)_S$,
   c. $\mathrm{Coker}(\varphi_S)$ *is canonically identified with* $\big(\mathrm{Coker}(\varphi)\big)_S$.
3. *If we have an exact sequence of* $\mathbf{A}$*-modules*
   $$M \xrightarrow{\varphi} N \xrightarrow{\psi} P\ ,$$
   then the sequence of $\mathbf{A}_S$-modules
   $$M_S \xrightarrow{\varphi_S} N_S \xrightarrow{\psi_S} P_S$$
   is also exact.

6.5 Fact *If $M_1, \ldots, M_r$ are submodules of N and $M = \bigcap_{i=1}^r M_i$, then by identifying the modules $(M_i)_S$ and M_S with submodules of N_S we obtain $M_S = \bigcap_{i=1}^r (M_i)_S$.*

6.6 Fact *Let M and N be two submodules of an* $\mathbf{A}$*-module P,* with *N finitely generated. Then, the conductor ideal $(M_S : N_S)$ is identified with $(M : N)_S$, via the natural maps of $(M : N)$ in $(M_S : N_S)$ and $(M : N)_S$.*

This is particularly applied to the annihilator of a finitely generated ideal.

Local-Global Principle for Exact Sequences of Modules

6.7 Concrete local-global principle (For exact sequences) *Let $S_1, \ldots, S_n$ be comaximal monoids of* $\mathbf{A}$*, M, N, P be* $\mathbf{A}$*-modules and $\varphi : M \to N$, $\psi : N \to P$ be two linear maps. We write $\mathbf{A}_i$ for $\mathbf{A}_{S_i}$, M_i for M_{S_i} etc. The following properties are equivalent.*

1. *The sequence* $M \xrightarrow{\varphi} N \xrightarrow{\psi} P$ *is exact.*
2. *For each* $i \in [\![1..n]\!]$, *the sequence* $M_i \xrightarrow{\varphi_i} N_i \xrightarrow{\psi_i} P_i$ *is exact.*

As a consequence, φ *is injective (resp. surjective) if and only if for each* $i \in [\![1..n]\!]$, φ_i *is injective (resp. surjective)*

▷ We have seen that *1* ⇒ *2* in Fact 6.4.

Assume *2*. Let $\mu_i : M \to M_i$, $\nu_i : N \to N_i$, $\pi_i : P \to P_i$ be the canonical homomorphisms. Let $x \in M$ and $z = \psi\big(\varphi(x)\big)$. We thus have

$$0 = \psi_i\big(\varphi_i(\mu_i(x))\big) = \pi_i\big(\psi(\varphi(x))\big) = \pi_i(z),$$

for some $s_i \in S_i$, $s_i z = 0$ in P. We conclude that $z = 0$ by using the comaximality of the S_i's: $\sum_i u_i s_i = 1$. Now let $y \in N$ such that $\psi(y) = 0$. For each i there exists some $x_i \in M_i$ such that $\varphi_i(x_i) = \nu_i(y)$.

We write $x_i =_{M_i} a_i/s_i$ with $a_i \in M$ and $s_i \in S_i$. The equality $\varphi_i(x_i) = \nu_i(y)$ means that for some $t_i \in S_i$ we have $t_i\varphi(a_i) = t_i s_i y$ in N. If $\sum_i v_i t_i s_i = 1$, we can deduce that $\varphi\big(\sum_i v_i t_i a_i\big) = y$. Thus $\operatorname{Ker}\psi$ is indeed included in $\operatorname{Im}\varphi$. □

6.8 Abstract local-global principle* (For exact sequences) *Let* M, N, P *be* $\mathbf{A}$*-modules, and* $\varphi : M \to N$ *and* $\psi : N \to P$ *be two linear maps. The following properties are equivalent.*

1. *The sequence* $M \xrightarrow{\varphi} N \xrightarrow{\psi} P$ *is exact.*
2. *For every maximal ideal* $\mathfrak{m}$ *the sequence* $M_\mathfrak{m} \xrightarrow{\varphi_\mathfrak{m}} N_\mathfrak{m} \xrightarrow{\psi_\mathfrak{m}} P_\mathfrak{m}$ *is exact.*

As a consequence, φ *is injective (resp. surjective) if and only if for every maximal ideal* $\mathfrak{m}$, $\varphi_\mathfrak{m}$ *is injective (resp. surjective).*

▷ The property $x = 0$ for an element x of a module is a finite character property. Similarly for the property $y \in \operatorname{Im}\varphi$. Thus, even if the property "the sequence is exact" is not of finite character, it is a conjunction of finite character properties, and we can apply Fact* 2.11 to deduce the abstract local-global principle from the concrete local-global principle. □

Let us finally mention a concrete local-global principle for monoids.

6.9 Concrete local-global principle (For monoids) *Let* $S_1, \ldots, S_n$ *be comaximal monoids of* $\mathbf{A}$, V *be a monoid. The following properties are equivalent.*

1. *The monoid* V *contains* 0.
2. *For* $i \in [\![1..n]\!]$, *the monoid* V *seen in* $\mathbf{A}_{S_i}$ *contains* 0.

▷ For each i we have some $v_i \in V$ and some $s_i \in S_i$ such that $s_i v_i = 0$. Let $v = \prod_i v_i \in V$. Then, v is zero in the $\mathbf{A}_{S_i}$'s, thus in $\mathbf{A}$. □

Exercises and Problems

1 Exercise We recommend the reader to do the proofs which are not given, are sketched, are left to the reader, etc… In particular, consider the following cases.

- Check Facts 1.2 to 1.4.
- Prove Corollary 2.4.
- In Lemma 2.6 compute suitable exponents for the items *2*, *3* and *4*, by making the proof completely explicit.
- Prove Corollary 3.3. Give a more detailed proof of Theorem 3.4. Check the details in the proof of the local-global principle 3.5. Prove Proposition 3.7.
- Check Facts 6.4 to 6.6. For Fact 6.5 we use the exact sequence $0 \to M \to N \to \bigoplus_{i=1}^{r} N/M_i$ which is preserved by localization.

2 Exercise *(Also see Exercise VII-8)*

1. *(Invertible elements in* $\mathbf{B}[T]$*, cf. Lemma 2.6)*
   Let two polynomials $f = \sum_{i=0}^{n} a_i T^i$, $g = \sum_{j=0}^{m} b_j T^j$ with $fg = 1$. Show that the coefficients a_i, $i \geqslant 1$, b_j, $j \geqslant 1$ are nilpotent elements and that $a_n^{m+1} = 0$.
2. *(Characteristic polynomial of a nilpotent matrix)*
   Let $A \in \mathbb{M}_n(\mathbf{B})$ be a nilpotent matrix and $\mathrm{C}_A(T) = T^n + \sum_{k=0}^{n-1} a_k T^k$ be its characteristic polynomial.
   a. Show that the coefficients a_i are nilpotent elements.
   b. Precisely, if $A^e = 0$, then $\mathrm{Tr}(A)^{(e-1)n+1} = 0$ and

$$a_i^{e_i} = 0 \quad \text{where} \quad e_i = (e-1)\tbinom{n}{i} + 1 \quad (i = 0, \dots, n-1).$$

3 Exercise Let $x = (x_1, \dots, x_n) \in \mathbf{A}^n$ be a vector and $s \in \mathbf{A}$.

1. If x is unimodular in $\mathbf{A}/\langle s \rangle$ and in $\mathbf{A}[1/s]$, it is unimodular in $\mathbf{A}$.
2. Let $\mathfrak{b}$ and $\mathfrak{c}$ be two ideals of $\mathbf{A}$. If x is unimodular modulo $\mathfrak{b}$ and modulo $\mathfrak{c}$, then it is also unimodular modulo $\mathfrak{bc}$.

4 Exercise *(A typical application of the basic local-global principle)* Let $x = (x_1, \dots, x_n) \in \mathbf{A}^n$ be *unimodular*. For $d \geqslant 1$, we denote by $\mathbf{A}[X_1, \dots, X_n]_d$ the $\mathbf{A}$-submodule of the homogeneous polynomials of degree d and

$$I_{d,x} = \left\{ f \in \mathbf{A}[\underline{X}]_d \mid f(x) = 0 \right\}, \ \mathbf{A}\text{-submodule of } \mathbf{A}[\underline{X}].$$

1. If $x_1 \in \mathbf{A}^\times$, every $f \in I_{d,x}$ is a linear combination of the $x_1 X_j - x_j X_1$ with homogeneous polynomials of degree $d-1$ for coefficients.
2. Generally, every $f \in I_{d,x}$ is a linear combination of the $(x_k X_j - x_j X_k)$ with homogeneous polynomials of degree $d-1$ for coefficients.
3. Let $I_x = \bigoplus_{d \geqslant 1} I_{d,x}$. Show that $I_x = \{ F \mid F(tx) = 0 \}$ (where t is a new indeterminate). Show that I_x is *saturated*, i.e., if $X_j^m F \in I_x$ for some m and for each j, then $F \in I_x$.

5 Exercise *(Variations of the Gauss-Joyal Lemma 2.6)* Show that the following statements are equivalent (each statement is universal, i.e., valid for all polynomials and every commutative ring $\mathbf{A}$):

1. $\mathrm{c}(f) = \mathrm{c}(g) = \langle 1\rangle \;\Rightarrow\; \mathrm{c}(fg) = \langle 1\rangle$,
2. $(\exists i_0, j_0 \;\; f_{i_0} = g_{j_0} = 1) \;\Rightarrow\; \mathrm{c}(fg) = \langle 1\rangle$,
3. $\exists p \in \mathbb{N}, \;\; \big(\mathrm{c}(f)\mathrm{c}(g)\big)^p \subseteq \mathrm{c}(fg)$,
4. *(Gauss-Joyal)* $\mathrm{D}_{\mathbf{A}}\big(\mathrm{c}(f)\mathrm{c}(g)\big) = \mathrm{D}_{\mathbf{A}}\big(\mathrm{c}(fg)\big)$.

6 Exercise *(Norm of a primitive polynomial through the use of a null ring)* Let $\mathbf{B}$ be a free $\mathbf{A}$-algebra of finite rank, $\underline{X} = (X_1, \ldots, X_n)$ be indeterminates, $Q \in \mathbf{B}[\underline{X}]$ and $P = \mathrm{N}_{\mathbf{B}[\underline{X}]/\mathbf{A}[\underline{X}]}(Q) \in \mathbf{A}[\underline{X}]$. Show that if Q is primitive, then so is P. *Hint:* check that $\mathbf{A} \cap \mathrm{c}_{\mathbf{B}}(P) = \mathrm{c}_{\mathbf{A}}(P)$, consider the subring $\mathbf{A}' = \mathbf{A}/\mathrm{c}_{\mathbf{A}}(P)$ of $\mathbf{B}' = \mathbf{B}/\mathrm{c}_{\mathbf{B}}(P)$ and the $\mathbf{A}'$-linear map "multiplication by Q," $m_Q : \mathbf{B}'[\underline{X}] \to \mathbf{B}'[\underline{X}], \;\; R \mapsto QR$.

7 Exercise Show that a coherent ring $\mathbf{A}$ is strongly discrete if and only if the test "$1 \in \langle a_1, \ldots, a_n\rangle$?" is explicit for every finite sequence $(a_1, \ldots, a_n)$ in $\mathbf{A}$.

8 Exercise *(An example of a coherent Noetherian ring with a non-coherent quotient.)* Consider the ring $\mathbb{Z}$ and an ideal $\mathfrak{a}$ generated by an infinite sequence of elements, all zeros besides eventually one, which is then equal to 3 (for example we place a 3 the first time, if it ever occurs, that a zero of the Riemann zeta function[9] has real part not equal to $1/2$). If we are able to provide a finite system of generators for the annihilator of 3 in $\mathbb{Z}/\mathfrak{a}$, we are able to say whether the infinite sequence is identically zero or not. This would mean that there exists a sure method to solve conjectures of the Riemann type.

Comment As every reasonable constructive definition of Noetherianity seems to demand that a Noetherian ring's quotient remains Noetherian, and given the above "counterexample," we cannot hope to have a constructive proof of the theorem of classical mathematics which states that every Noetherian ring is coherent. ∎

9 Exercise *(Idempotents of $\mathbf{A}[X]$)* Prove that every idempotent of $\mathbf{A}[X]$ is an idempotent of $\mathbf{A}$.

10 Exercise Let u and v be two idempotents and x be an element of $\mathbf{A}$.
The element $1 - (1-u)(1-v) = u + v - uv$ is denoted by $u \vee v$.

1. Show that $x \in u\mathbf{A} \;\Leftrightarrow\; ux = x$. In particular, $u\mathbf{A} = v\mathbf{A} \;\Leftrightarrow\; u = v$.
2. The element uv is the least common multiple of u and v amongst the idempotents of $\mathbf{A}$ (i.e., if w is an idempotent, $w \in u\mathbf{A} \cap v\mathbf{A} \;\Leftrightarrow\; w \in uv\mathbf{A}$). Actually, we even have $u\mathbf{A} \cap v\mathbf{A} = uv\mathbf{A}$. We write $u \wedge v = uv$.
3. Prove the equality $u\mathbf{A} + v\mathbf{A} = (u \vee v)\mathbf{A}$. Infer that $u \vee v$ is the greatest common divisor of u and v amongst the idempotents of $\mathbf{A}$ (in fact an arbitrary element of $\mathbf{A}$ divides u and v if and only if it divides $u \vee v$).

[9] Here we enumerate the zeros $a_n + ib_n$ with $b_n > 0$ by order of magnitude.

4. By a sequence of elementary operations, transform the matrix $\mathrm{Diag}(u, v)$ into the matrix $\mathrm{Diag}(u \vee v, u \wedge v)$.
   From it, deduce that the two $\mathbf{A}$-modules $u\mathbf{A} \oplus v\mathbf{A}$ and $(u \vee v)\mathbf{A} \oplus (u \wedge v)\mathbf{A}$ are isomorphic.
5. Show that the two rings $\mathbf{A}/\langle u\rangle \times \mathbf{A}/\langle v\rangle$ and $\mathbf{A}/\langle u \vee v\rangle \times \mathbf{A}/\langle u \wedge v\rangle$ are isomorphic.

11 Exercise Let $\mathbf{A}$ be a ring and $(e_1, \ldots, e_n)$ be a fundamental system of orthogonal idempotents of $\mathrm{Frac}\,\mathbf{A} = \mathbf{K}$. We write $e_i = a_i/d$ with $a_i \in \mathbf{A}$ and $d \in \mathrm{Reg}\,\mathbf{A}$. We then have $a_i a_j = 0$ for $i \neq j$ and $\sum_i a_i$ regular.

1. Establish a converse.
2. Show that $\mathbf{K}[1/e_i] \simeq \mathrm{Frac}\left(\mathbf{A}/\mathrm{Ann}_{\mathbf{A}}(a_i)\right)$ and $\mathbf{K} \simeq \prod_i \mathrm{Frac}\left(\mathbf{A}/\mathrm{Ann}_{\mathbf{A}}(a_i)\right)$.

12 Exercise *(Separating the irreducible components)*
1. Let $\mathbf{A} = \mathbb{Q}[x, y, z] = \mathbb{Q}[X, Y, Z]/\langle XY, XZ, YZ\rangle$ and $\mathbf{K} = \mathrm{Frac}\,\mathbf{A}$. What are the zeros of $\mathbf{A}$ in $\mathbb{Q}^3$ (i.e. $(x, y, z) \in \mathbb{Q}^3$ such that $xy = yz = zx = 0$)? Give a reduced form of the elements of $\mathbf{A}$. Show that $x + y + z \in \mathrm{Reg}\,\mathbf{A}$. Show that the elements $\dfrac{x}{x+y+z}$, $\dfrac{y}{x+y+z}$ and $\dfrac{z}{x+y+z}$ form a fundamental system of orthogonal idempotents in $\mathbf{K}$. Show that $\mathbf{K} \simeq \mathbb{Q}(X) \times \mathbb{Q}(Y) \times \mathbb{Q}(Z)$.
2. Let $\mathbf{B} = \mathbb{Q}[u, v, w] = \mathbb{Q}[U, V, W]/\langle UVW\rangle$ and $\mathbf{L} = \mathrm{Frac}\,\mathbf{B}$.
What are the zeros of $\mathbf{B}$ in $\mathbb{Q}^3$? Give a reduced form of the elements of $\mathbf{B}$. Show that $\mathbf{L} \simeq \mathbb{Q}(U, V) \times \mathbb{Q}(V, W) \times \mathbb{Q}(W, U)$.

13 Exercise *(Idempotent and elementary group)* Let $a \in \mathbf{A}$ be an idempotent. For $b \in \mathbf{A}$, give a matrix $A \in \mathbb{E}_2(\mathbf{A})$ and an element $d \in \mathbf{A}$ such that $A \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}$. In particular, explain why $\langle a, b\rangle = \langle d\rangle$.
Moreover, prove that if b is regular (resp. invertible) modulo a, then d is regular (resp. invertible). Finally, if b is idempotent, $d = a \vee b = a + b - ab$.

14 Exercise Let $(r_1, \ldots, r_m)$ be a finite family of idempotents in a ring $\mathbf{A}$. Let $s_i = 1 - r_i$ and, for a subset I of $[\![1..m]\!]$, let $r_I = \prod_{i\in I} r_i \prod_{i\notin I} s_i$.
1. Show that the diagonal matrix $D = \mathrm{Diag}(r_1, \ldots, r_m)$ is similar to a matrix $D' = \mathrm{Diag}(e_1, \ldots, e_m)$ where the e_i's are idempotents which satisfy: e_i divides e_j if $j > i$. You can start with the $n = 2$ case and use Exercise 10. Show that $\langle e_k\rangle = \mathcal{D}_k(D)$ for all k.
2. Show that we can write $D' = PDP^{-1}$ with P a *generalized permutation matrix*, i.e. a matrix which can be written as $\sum_j f_j P_j$ where the f_j's form a fundamental system of orthogonal idempotents and each P_j is a permutation matrix. generalized permutation—Suggestions:

- The r_I's form a fundamental system of orthogonal idempotents. The diagonal matrix $r_I D$ has the element r_I as its coefficient in position (i, i) if $i \in I$ and 0 otherwise. The matrix P_I then corresponds to a permutation bringing the coefficients r_I to the head of the list. Finally, $P = \sum_I r_I P_I$. Note that the test "$r_I = 0$?" is not necessary!

- We can also treat the $m = 2$ case: find $P = e\begin{bmatrix}1&0\\0&1\end{bmatrix} + f\begin{bmatrix}0&1\\1&0\end{bmatrix}$ with $f = r_2 s_1$, $e = 1 - f$, and $D' = \mathrm{Diag}(r_1 \vee r_2, r_1 \wedge r_2)$.
  Next we treat the $m > 2$ case step by step.

15 Exercise Recall the proof of the Chinese Remainder Theorem (p. 34) and explicitly give the idempotents.

16 Exercise *(Elementary Group: first steps)* $\mathbb{M}_2(\mathbf{A})$ case.

1. Let $a \in \mathbf{A}$. Determine a matrix $P \in \mathbb{E}_2(\mathbf{A})$ such that $P\begin{bmatrix}a\\0\end{bmatrix} = \begin{bmatrix}0\\a\end{bmatrix}$. Same for $\begin{bmatrix}\varepsilon a\\0\end{bmatrix} \mapsto \begin{bmatrix}a\\0\end{bmatrix}$ where $\varepsilon \in \mathbf{A}^\times$.

2. Write the matrices $\begin{bmatrix}0&-1\\1&0\end{bmatrix}$ and $\begin{bmatrix}-1&0\\0&-1\end{bmatrix}$ as elements of $\mathbb{E}_2(\mathbf{A})$.

3. Show that every triangular matrix of $\mathbb{SL}_2(\mathbf{A})$ is in $\mathbb{E}_2(\mathbf{A})$.

4. Let $u = \begin{bmatrix}x\\y\end{bmatrix}$, $v = \begin{bmatrix}y\\x\end{bmatrix}$, $w = \begin{bmatrix}-y\\x\end{bmatrix}$ with $x, y \in \mathbf{A}$. Show that $v \in \mathbb{GL}_2(\mathbf{A}) \cdot u$ and $w \in \mathbb{E}_2(\mathbf{A}) \cdot u$, but not necessarily $v \in \mathbb{SL}_2(\mathbf{A}) \cdot u$. For example, if x, y are two indeterminates over a ring $\mathbf{k}$, $\mathbf{A} = \mathbf{k}[x, y]$ and $v = Au$, with $A \in \mathbb{GL}_2(\mathbf{A})$, then $\big(\det(A)\big)(0, 0) = -1$. Consequently, we have $\det(A) \in -1 + \mathrm{D}_{\mathbf{k}}(0)\langle x, y\rangle$ (Lemma 2.6), therefore $\det(A) = -1$ if $\mathbf{k}$ is reduced. In addition, if $\det(A) = 1$, then $2 = 0$ in $\mathbf{k}$. As a result, $v \in \mathbb{SL}_2(\mathbf{A}) \cdot u$ if and only if $2 = 0$ in $\mathbf{k}$.

17 Exercise *(Elementary group: next steps)*

1. Let $A \in \mathbb{M}_{n,m}(\mathbf{A})$ with an invertible coefficient and $(n, m) \neq (1, 1)$. Determine matrices $P \in \mathbb{E}_n(\mathbf{A})$ and $Q \in \mathbb{E}_m(\mathbf{A})$ such that $PAQ = \begin{bmatrix}1&0_{1,m-1}\\0_{n-1,1}&A'\end{bmatrix}$. Example: with $a \in \mathbf{A}^\times$ give P for $P\begin{bmatrix}a\\0\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix}$ (Exercise 16 item *1*).

2. Let $A \in \mathbb{M}_2(\mathbf{A})$ with an invertible coefficient. Compute matrices P and $Q \in \mathbb{E}_2(\mathbf{A})$ such that: $PAQ = \begin{bmatrix}1&0\\0&\delta\end{bmatrix}$ with $\delta = \det(A)$.

Every matrix $A \in \mathbb{SL}_2(\mathbf{A})$ with an invertible coefficient belongs to $E E_2(\mathbf{A})$. Make the following cases explicit:

$$\begin{bmatrix}a&0\\0&a^{-1}\end{bmatrix}, \qquad \begin{bmatrix}0&a\\-a^{-1}&0\end{bmatrix}, \qquad \text{with } a \in \mathbf{A}^\times.$$

Write the following matrices (with $a \in \mathbf{A}^\times$) in $\mathbb{E}_2(\mathbf{A})$:

$$\begin{bmatrix}a&b\\0&a^{-1}\end{bmatrix}, \quad \begin{bmatrix}a&0\\b&a^{-1}\end{bmatrix}, \quad \begin{bmatrix}0&a\\-a^{-1}&b\end{bmatrix}, \quad \begin{bmatrix}b&a\\-a^{-1}&0\end{bmatrix}.$$

3. Prove that if $A = \mathrm{Diag}(a_1, a_2, \ldots, a_n) \in \mathbb{SL}_n(\mathbf{A})$, then $A \in \mathbb{E}_n(\mathbf{A})$.

4. Show that every triangular matrix $A \in \mathbb{SL}_n(\mathbf{A})$ belongs to $\mathbb{E}_n(\mathbf{A})$.

18 Exercise *(Division matrices D_q of determinant 1)* A "general division" $a = bq - r$ can be expressed with matrices:

$$\begin{bmatrix} 0 & 1 \\ -1 & q \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ r \end{bmatrix}.$$

This leads to the introduction of the matrix $D_q = \begin{bmatrix} 0 & 1 \\ -1 & q \end{bmatrix} \in \mathbb{SL}_2(\mathbf{A})$.

Show that $\mathbb{E}_2(\mathbf{A})$ is the monoid generated by the D_q matrices.

19 Exercise Let $\mathbf{A}$ be a ring and $A, B \in \mathbb{M}_n(\mathbf{A})$. Assume that we have some $i \in \mathbf{A}$ with $i^2 = -1$ and that $2 \in \mathbf{A}^\times$. Show that the matrices of $\mathbb{M}_{2n}(\mathbf{A})$

$$M = \begin{bmatrix} A & -B \\ B & A \end{bmatrix} \text{ and } M' = \begin{bmatrix} A + iB & 0 \\ 0 & A - iB \end{bmatrix}$$

are *elementarily similar*, (i.e., $\exists P \in \mathbb{E}_{2n}(\mathbf{A})$, $PMP^{-1} = M'$).
Hint: first treat the $n = 1$ case.

20 Exercise For $d \in \mathbf{A}^\times$ and $\lambda \in \mathbf{A}$ compute the matrix

$$\mathrm{Diag}(1, \ldots, d, \ldots, 1) \cdot \mathrm{E}_{ij}(\lambda) \cdot \mathrm{Diag}(1, \ldots, d^{-1}, \ldots, 1).$$

Show that the subgroup of diagonal matrices of $\mathbb{GL}_n(\mathbf{A})$ normalizes $\mathbb{E}_n(\mathbf{A})$.

21 Exercise *(A freeness lemma, or a Splitting Off: reader's choice)* Let $F \in \mathbb{AG}_n(\mathbf{A})$ be a projector with an invertible principal minor of order k. Show that F is similar to a matrix $\begin{bmatrix} \mathrm{I}_k & 0 \\ 0 & F' \end{bmatrix}$ where $F' \in \mathbb{AG}_{n-k}(\mathbf{A})$.

The finitely generated projective module $P \stackrel{\text{def}}{=} \mathrm{Im}\, F \subseteq \mathbf{A}^n$ admits a free direct summand with k columns of F for its basis.

22 Exercise Let $A \in \mathbf{A}^{n \times m}$ be of rank 1. Construct $B \in \mathbf{A}^{m \times n}$ such that $ABA = A$ and verify that AB is a projector of rank 1. Compare your solution with that which would result from the proof of Theorem 5.14.

23 Exercise *This exercise constitutes an abstraction of the computations that led to Theorem* 5.14. Consider an $\mathbf{A}$-module E "with enough linear forms", i.e. if $x \in E$ satisfies $\mu(x) = 0$ for all $\mu \in E^\star$, then $x = 0$. This means that the canonical map from E to its bidual, $E \to E^{\star\star}$, is injective. This condition is satisfied if E is a *reflexive* module, i.e. $E \simeq E^{\star\star}$, e.g. a finitely generated projective module, or a free module of finite rank.

For $x_1, \dots, x_n \in E$, denote by $\bigwedge_r(x_1, \dots, x_n)$ the ideal of $\mathbf{A}$ generated by the evaluations of every r-multilinear alternating form of E at every r-tuplet of elements of $\{x_1, \dots, x_n\}$.

Assume that $1 \in \bigwedge_r(x_1, \dots, x_n)$ *and* $\bigwedge_{r+1}(x_1, \dots, x_n) = 0$.

We want to prove that the submodule $\sum \mathbf{A}x_i$ is a direct summand in E by explicitly giving a projector $\pi : E \to E$ whose image is this submodule.

1. *(Cramer's formulas)* Let f be an r-multilinear alternating form over E. Show, for $y_0, \dots, y_r \in \sum \mathbf{A}x_i$, that

$$\sum_{i=0}^{r} (-1)^i f(y_0, \dots, y_{i-1}, \widehat{y_i}, y_{i+1}, \dots, y_r)\, y_i = 0.$$

   Or, for $y, y_1, \dots, y_r \in \sum \mathbf{A}x_i$, that

$$f(y_1, \dots, y_r)\, y = \sum_{i=1}^{r} f(y_1, \dots, y_{i-1}, y, y_{i+1}, \dots, y_r)\, y_i.$$

2. Give n linear forms $\alpha_i \in E^\star$ such that the linear map

$$\pi : E \to E,\ x \mapsto \textstyle\sum_i \alpha_i(x) x_i$$

   is a projector onto $\sum \mathbf{A}x_i$. We define $\psi : \mathbf{A}^n \to E$ by $e_i \mapsto x_i$ and $\varphi : E \to \mathbf{A}^n$ by $\varphi(x) = \big(\alpha_1(x), \dots, \alpha_n(x)\big)$. Arrange for $\pi = \psi \circ \varphi$ and $\pi \circ \psi = \psi$, so that $\psi \circ \varphi \circ \psi = \psi$.
3. *(New proof of Theorem 5.14)* Let $A \in \mathbf{A}^{m \times n}$ be a matrix of rank r. Show that there exists a $B \in \mathbf{A}^{n \times m}$ such that $ABA = A$.

24 Exercise Let $A \in \mathbf{A}^{n \times m}$ and $B \in \mathbf{A}^{m \times n}$.

1. We have the following commutativity formula:

$$\det(\mathrm{I}_m + XBA) = \det(\mathrm{I}_n + XAB).$$

First proof First treat the case where $m = n$, for example by the method of undetermined coefficients. If $m \neq n$, A and B can be completed with rows and columns of 0's to turn them into square matrices A_1 and B_1 of size $q = \max(m, n)$ as in the proof given p. 36. Then check that $\det(\mathrm{I}_m + XBA) = \det(\mathrm{I}_q + XB_1A_1)$ and $\det(\mathrm{I}_n + XAB) = \det(\mathrm{I}_q + XA_1B_1)$.

Second proof Consider an undetermined X and the matrices

$$B' = \begin{bmatrix} XB & \mathrm{I}_m \\ \mathrm{I}_n & 0_{n,m} \end{bmatrix} \quad \text{and} \quad A' = \begin{bmatrix} A & \mathrm{I}_n \\ \mathrm{I}_m & -XB \end{bmatrix}.$$

Compute $A'B'$ and $B'A'$.

2. What can be deduced about the characteristic polynomials of AB and BA?

25 Exercise *(Binet-Cauchy formula)* We use the notations on p. 42. For two matrices $A \in \mathbf{A}^{n \times m}$ and $B \in \mathbf{A}^{m \times n}$, prove that we have the Binet-Cauchy formula:

$$\det(BA) = \sum\nolimits_{\alpha\in\mathcal{P}_{m,n}} \det(B_{1..m,\alpha})\det(A_{\alpha,1..m}).$$

First proof Use the formula $\det(\mathrm{I}_m + XBA) = \det(\mathrm{I}_n + XAB)$ (Exercise 24). Then consider the coefficient of X^m in each of the polynomials $\det(\mathrm{I}_m + XBA)$ and $\det(\mathrm{I}_n + XAB)$.

Second proof The matrices A and B represent linear maps $u : \mathbf{A}^m \to \mathbf{A}^n$ and $v : \mathbf{A}^n \to \mathbf{A}^m$.

Then consider the matrices of $\bigwedge^m u$, $\bigwedge^m v$ and $\bigwedge^m (v\circ u)$ with respect to the bases naturally associated with the canonical bases of $\mathbf{A}^n$ and $\mathbf{A}^m$.

Conclude by writing $\bigwedge^m (v\circ u) = \bigwedge^m v \circ \bigwedge^m u$.

Third proof In the product BA insert between B and A a diagonal matrix D having indeterminates λ_i for coefficients, and see which is the coefficient of $\lambda_{i_1}\cdots\lambda_{i_m}$ in the polynomial $\det(BDA)$ (to do this take $\lambda_{i_1} = \cdots = \lambda_{i_m} = 1$ and let the other be null). Conclude by letting all the λ_i's be equal to 1.

26 Exercise Let $u \in \mathrm{End}_{\mathbf{A}}(\mathbf{A}^n)$. For $k \in [\![0..n]\!]$, let $u_k = \bigwedge^k (u)$.
Show that $\det(u_k) = \det(u)^{\binom{n-1}{k-1}}$ and that

$$\det(u_k)\det(u_{n-k}) = \det(u)^{\binom{n}{k}}.$$

27 Exercise For $A \in \mathbf{A}^{n\times r}$ prove that the following properties are equivalent.

1. The matrix A is injective and locally simple.
2. There exists a matrix $B \in \mathbf{A}^{r\times n}$ such that $BA = \mathrm{I}_r$.
3. The determinantal ideal $\mathcal{D}_r(A) = \langle 1\rangle$.

Hint: See Theorems 5.14, 5.22 and 5.26.

28 Exercise Treat the general case in the proof of Lemma 5.30.

29 Exercise If $\mathrm{gram}_{\mathbf{A}}(\varphi, x_1, \ldots, x_n)$ is invertible, the submodule $\mathbf{A}x_1 + \cdots + \mathbf{A}x_n$ is free with $(x_1, \ldots, x_n)$ as its basis.

1 Problem *(Gauss' pivot, $ABA = A$, and linear rationality)* Let $\mathbf{K}$ be a discrete field. If $x \in \mathbf{K}^n$ is a nonzero vector, its *pivot index* i is the least index i such that $x_i \neq 0$. We say that the coefficient x_i is the *pivot* of x. The *height* $h(x)$ of x is the integer $n - i + 1$ and it is agreed that $h(0) = 0$. For example, for $n = 4$ and $x = \begin{bmatrix} 0\\ 1\\ *\\ * \end{bmatrix}$, the pivot index of x is $i = 2$, and $h(x) = 3$. The following notions of "staggering" are relative to this height h.

We say that a matrix $A \in \mathbb{M}_{n,m}(\mathbf{K})$ *has staggered columns* if the nonzero columns of A have distinct heights; we say that it is *strictly staggered* if, additionally, the rows at the pivot indices are vectors of the canonical basis of $\mathbf{K}^m$ (these vectors are necessarily distinct). Here is a strictly staggered matrix (0 has been replaced by a dot):

$$\begin{bmatrix} \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & a_{24} & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & a_{43} & a_{44} & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ a_{71} & a_{72} & a_{73} & a_{74} & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ a_{91} & a_{92} & a_{93} & a_{94} & a_{95} & \cdot \end{bmatrix}.$$

1. Let $A \in \mathbb{M}_{n,m}(\mathbf{K})$ be strictly staggered; we define $\overline{A} \in \mathbb{M}_{n,m}(\mathbf{K})$ by annihilating the nonpivot coefficients (the a_{ij}'s in the above exercise) and $B = {}^{\mathrm{t}}\overline{A} \in \mathbb{M}_{m,n}(\mathbf{K})$. Check that $ABA = A$.

Describe the projectors AB, BA and the decomposition $\mathbf{K}^n = \operatorname{Im} AB \oplus \operatorname{Ker} AB$.
2. Let $A \in \mathbb{M}_{n,m}(\mathbf{K})$ be an arbitrary matrix. How do you obtain $Q \in \mathbb{GL}_m(\mathbf{K})$ such that $A' = AQ$ is strictly staggered? How do you compute $B \in \mathbb{M}_{m,n}(\mathbf{K})$ satisfying $ABA = A$?
3. Let $A \in \mathbb{M}_{n,m}(\mathbf{K})$ and $y \in \mathbf{K}^n$. Assume that the system of linear equations $Ax = y$ admits a solution x on an overring of $\mathbf{K}$. Show that it admits a solution on $\mathbf{K}$.
4. Let $\mathbf{K}_0 \subseteq \mathbf{K}$ be a subfield and E, F be two complementary $\mathbf{K}$-linear subspaces of $\mathbf{K}^n$. Assume that E and F are generated by vectors with components in $\mathbf{K}_0$. Show that $\mathbf{K}_0^n = (E \cap \mathbf{K}_0^n) \oplus (F \cap \mathbf{K}_0^n)$.

Let $E \subseteq \mathbf{K}^n$ be a $\mathbf{K}$-linear subspace. We say that E *is* $\mathbf{K}_0$*-rational* if it is generated by vectors with components in $\mathbf{K}_0$.
5. Let F be a complementary subspace of E in $\mathbf{K}^n$ generated by vectors of the canonical basis of $\mathbf{K}^n$: $\mathbf{K}^n = E \oplus F$ and $\pi : \mathbf{K}^n \twoheadrightarrow E$ be the associated projection.

a. Show that E is $\mathbf{K}_0$-rational if and only if $\pi(e_j) \in \mathbf{K}_0^n$ for every vector e_j of the canonical basis.
b. Deduce the existence of a smaller field of rationality for E.
c. What is the field of rationality of the image in $\mathbf{K}^n$ of a strictly staggered matrix?

2 Problem

1. Partial factorization algorithm. Given two integers a and b prove that we can "efficiently" compute a finite family of pairwise coprime positive integers p_i such that $a = \pm \prod_{i=1}^n p_i^{\alpha_i}$ and $b = \pm \prod_{i=1}^n p_i^{\beta_i}$.
2. Consider a system of linear equations $AX = B$ in $\mathbb{Z}$ which admits an infinity of solutions in $\mathbb{Q}^m$. To know if it admits a solution in $\mathbb{Z}^m$ we can try a local-global method. Start by determining a solution in $\mathbb{Q}$, which is a vector $X \in \mathbb{Q}^m$. Find an integer d such that $dX \in \mathbb{Z}^m$, such that X has coefficients in $\mathbb{Z}[1/d]$. It then suffices to construct a solution in each localized ring $\mathbb{Z}_{1+p\mathbb{Z}}$ for the prime p's which divide d and to apply the Concrete local-global principle 2.3. To know if there is a solution in $\mathbb{Z}_{1+p\mathbb{Z}}$ and to construct one, we can use the pivot method, provided we take as pivot an element of the matrix (or rather the remaining part of the matrix) which

divides every other coefficient, i.e. a coefficient wherein p appears with a minimum exponent.

The drawback of this method is that it requires factorizing d, which can render it unfeasible.

However, we can slightly modify the method in order to avoid having to completely factorize d. We will use the partial factorization algorithm. Start as if d were a prime number. More precisely work with the ring $\mathbb{Z}_{1+d\mathbb{Z}}$. Check whether a coefficient of the matrix is comaximal to d. If one is found, use it as your pivot. Otherwise no coefficient of the matrix is comaximal to d and (by using if necessary the partial factorization algorithm) we have one of the following three cases:

- d divides all the coefficients of the matrix, in which case, either it also divides the coefficients of B and it is reduced to a simpler problem, or it does not divide any coefficient of B and the system of linear equations has no solution,
- d is written as a product of pairwise comaximal factors $d = d_1 \cdots d_k$ with $k \geqslant 2$, in which case we can then work with the localizations at the monoids $(1 + d_1\mathbb{Z}), \ldots, (1 + d_k\mathbb{Z})$,
- d is written as a pure power of some d' dividing d, which, with d' in place of d, brings us to a similar but simpler problem.

Check that we can recursively exploit the idea expressed above. Write an algorithm and test it. Examine whether the obtained algorithm runs in a reasonable time.

Some Solutions, or Sketches of Solutions

2 Exercise

1. Assume without loss of generality $a_0 = b_0 = 1$. When you write $fg = 1$, you get

$$0 = a_n b_m,\ 0 = a_n b_{m-1} + a_{n-1} b_m,\ 0 = a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m,$$

and so on up to degree 1.

Then prove by induction over j that $\deg(a_n^j g) \leqslant m - j$.

In particular, for $j = m + 1$, we get $\deg(a_n^{m+1} g) \leqslant -1$, i.e. $a_n^{m+1} g = 0$. Whence $a_n^{m+1} = 0$. Finally, by reasoning modulo $\mathrm{D}_{\mathbf{B}}(0)$, we obtain successively nilpotent a_j's for $j = n - 1, \ldots, 1$.

2a. Consider the polynomials over the commutative ring $\mathbf{B}[A]$:

$$f(T) = \det(\mathrm{I}_n - TA) \ \text{ and } \ g(T) = \det(\mathrm{I}_n + TA + T^2A^2 + \cdots + T^{e-1}A^{e-1}).$$

We have $f(T)g(T) = \det(\mathrm{I}_n - T^e A^e) = 1$. The coefficient of degree $n - i$ of f is $\pm a_i$. Apply *1.*

2b. It suffices to prove that $\mathrm{Tr}(A)^{(e-1)n+1} = 0$, because $a_i = \pm \mathrm{Tr}\left(\bigwedge^{n-i}(A)\right)$.

Consider the determinant defined with respect to a fixed basis $\mathcal{B}$ of $\mathbf{A}^n$. If we take the canonical basis formed by the e_i's, we have an obvious equality

$$\mathrm{Tr}(f) = \det_{\mathcal{B}}(f(e_1), e_2, \ldots, e_n) + \cdots + \det_{\mathcal{B}}\big(e_1, e_2, \ldots, f(e_n)\big).$$

It can be written in the following form:

$$\mathrm{Tr}(f)\det_{\mathcal{B}}(e_1,\dots,e_n)=\det_{\mathcal{B}}(f(e_1),e_2,\dots,e_n)+\cdots+\det_{\mathcal{B}}\big(e_1,e_2,\dots,f(e_n)\big).$$

In this form we can replace the e_i's by any system of n vectors of $\mathbf{A}^n$: both sides are n-multilinear alternating forms (at the e_i's) over $\mathbf{A}^n$, therefore are equal because they coincide on a basis.

Thus, multiplying a determinant by $\mathrm{Tr}(f)$ reduces to replacing it by a sum of determinants in which f acts on each vector.

One deduces that the expression $\mathrm{Tr}(f)^{n(e-1)+1}\det_{\mathcal{B}}(e_1,\dots,e_n)$ is equal to a sum of which each term is a determinant of the form

$$\det_{\mathcal{B}}\big(f^{m_1}(e_1),f^{m_2}(e_2),\dots,,f^{m_n}(e_n)\big),$$

with $\sum_i m_i = n(e-1)+1$, therefore at least one of the exponents m_i is $\geqslant e$.

Remark This solution for the bound $n(e-1)+1$ is due to Gert Almkvist. See on this matter: ZEILBERGER D. *Gert Almkvist's generalization of a mistake of Bourbaki.* Contemporary Mathematics **143** (1993), pp. 609–612. ∎

3 Exercise

1. Let $\mathfrak{a}=\langle x_1,\dots,x_n\rangle$. Obtaining $s^r\in\mathfrak{a}$ (for some r), and $1-as\in\mathfrak{a}$ (for some a). Write $1=a^rs^r+(1-as)(1+as+\cdots)\in\mathfrak{a}$.

2. $\mathfrak{a}+\mathfrak{b}=\langle 1\rangle$, $\mathfrak{a}+\mathfrak{c}=\langle 1\rangle$ and $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}+\mathfrak{c})\subseteq\mathfrak{a}+\mathfrak{bc}$, therefore $\mathfrak{a}+\mathfrak{bc}=\langle 1\rangle$.

4 Exercise

1. Since f is homogeneous, we have $f(tx)=0$ for a new indeterminate t. Whence each $U_i\in\mathbf{A}[X_1,\dots,X_n,t]$ such that $f=\sum_{i=1}^n(X_i-tx_i)U_i$.

By making $t:=x_1^{-1}X_1$, we obtain each $v_i\in\mathbf{A}[X_1,\dots,X_n]$ such that

$$f=\textstyle\sum_{i=2}^n(x_1X_i-x_iX_1)v_i.$$

Finally, since f is homogeneous of degree d, we can replace v_i by its homogeneous component of degree $d-1$.

2. Consider the equality $f=\sum_{k,j}(x_kX_j-x_jX_k)u_{kj}$, where the u_{kj}'s are homogeneous polynomials of degree $d-1$. It is a system of linear equations in the coefficients of the u_{kj}'s. Since this system admits a solution over each localized $\mathbf{A}_{x_i}$ and that the x_i's are comaximal, it admits a solution over $\mathbf{A}$.

3. If $F=\sum_d F_d$ is the decomposition of $F\in\mathbf{A}[X_1,\dots,X_n]$ into homogeneous components, we have $F(tx)=0$ if and only if $F_d(x)=0$ for all d, whence the first item of the question. For the saturation, we prove that if $X_iF\in I_x$ for all i, then $F\in I_x$. But we have $x_iF(tx)=0$. Therefore, by comaximality of the x_i's, we get $F(tx)=0$, i.e. $F\in I_x$.

6 Exercise The polynomial Q, regarded as a polynomial with coefficients in $\mathbf{B}'$, remains primitive and therefore regular (Gauss-Joyal, item *2* of Lemma 2.6). Since m_Q is injective, its determinant $\det(m_Q) = P \in \mathbf{A}'[\underline{X}]$ is regular (Theorem 5.22, item *2*). But P is also null in $\mathbf{A}'[\underline{X}]$. Thus $\mathbf{A}'$ is the null ring, in other words $1 \in \mathrm{c}_{\mathbf{A}}(P)$.

9 Exercise Let $f(X)$ be an idempotent of $\mathbf{A}[X]$. Clearly $e = f(0)$ is idempotent. We want to prove that $f = e$. For this we can reason separately modulo e and modulo $1 - e$.

If $e = 0$, then $f = Xg$. We have $(Xg)(1 - Xg) = 0$, or $1 - Xg$ is regular, thus $g = 0$.

If $e = 1$, consider the idempotent $1 - f$ and we are reduced to the previous case.

10 Exercise For question *5* first prove the result when $uv = 0$. In the general situation, write $u' = 1 - u$ and $v' = 1 - v$. We then have a fundamental system of orthogonal idempotents $(uv, uv', u'v, u'v')$ and by applying the previous special case we see that the two rings are isomorphic to the product $\mathbf{A}/\langle uv'\rangle \times (\mathbf{A}/\langle uv\rangle)^2 \times \mathbf{A}/\langle u'v\rangle$.

11 Exercise

2. We have $\mathbf{K}[1/e_i] \simeq \mathbf{K}/\mathrm{Ann}_{\mathbf{K}}(e_i)$ and $\mathrm{Ann}_{\mathbf{K}}(e_i) = \mathrm{Ann}_{\mathbf{A}}(a_i)\mathbf{K}$. For an element x of $\mathbf{A}$, write $dx = \sum_{i\in[\![1..n]\!]} x_i$ in $\mathbf{K}$, with $x_i = e_i dx = a_i x$. The decomposition is thus entirely in $\mathbf{A}$. Since $dx \equiv x_i \mod \mathrm{Ann}_{\mathbf{A}}(a_i)$ the component $\mathbf{K}/\mathrm{Ann}_{\mathbf{K}}(e_i)$ of the product, when seen as the ideal $e_i\mathbf{K}$, is formed from the elements of the form $a_i x/y$ with $x \in \mathbf{A}$ and y regular in $\mathbf{A}$. But y is regular in $\mathbf{A}$ if and only if each $y_i = a_i y$ is regular modulo $\mathrm{Ann}_{\mathbf{A}}(a_i)$, so that $\mathbf{K}/\mathrm{Ann}_{\mathbf{K}}(e_i)$ is identified with $\mathrm{Frac}(\mathbf{A}/\mathrm{Ann}_{\mathbf{A}}(a_i))$.

12 Exercise

1. The zeros of $\mathbf{A}$ are the three "coordinate axes."

Every element of $\mathbf{A}$ is uniquely written in the form

$$u = a + xf(x) + yg(y) + zh(z),$$

with $f, g, h \in \mathbb{Q}[T]$. This implies that $x + y + z$ is regular because

$$(x + y + z)u = x\big(a + xf(x)\big) + y\big(a + yg(y)\big) + z\big(a + zh(z)\big).$$

So the elements $\dfrac{x}{x+y+z}$, $\dfrac{y}{x+y+z}$ and $\dfrac{z}{x+y+z}$ form a fundamental system of orthogonal idempotents of $\mathbf{K}$. Conclude with Exercise 11 by noting that $\mathrm{Ann}_{\mathbf{A}}(x) = \langle y, z\rangle$, and thus that

$$\mathbf{A}/\mathrm{Ann}_{\mathbf{A}}(x) \simeq \mathbb{Q}[X].$$

2. The zeros of $\mathbf{B}$ are the three "coordinate planes." The fundamental system of orthogonal idempotents in $\mathbf{L}$ is given by $\dfrac{uv}{uv+vw+wu}$, $\dfrac{vw}{uv+vw+wu}$ and $\dfrac{wu}{uv+vw+wu}$.

13 Exercise It suffices to solve the question modulo a and modulo $1-a$.

Modulo a: $\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 0 \\ b \end{bmatrix} \mapsto \begin{bmatrix} b \\ b \end{bmatrix} \mapsto \begin{bmatrix} b \\ 0 \end{bmatrix}$.

Modulo $1-a$, $\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 \\ b \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 0 \end{bmatrix}$. By patching: $d = (1-a)b + a$ with for example the matrix $A = A_2 A_1$, where

$$A_1 = (1-a)\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} + a\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1-a \\ 0 & 1 \end{bmatrix},$$

$$A_2 = (1-a)\begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} + a\begin{bmatrix} 1 & 0 \\ -b & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ a-ab-1 & 1 \end{bmatrix}$$

and

$$A = \begin{bmatrix} 1 & 1-a \\ a-ab-1 & a \end{bmatrix}.$$

18 Exercise The matrix $D_0 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ transforms $\begin{bmatrix} x \\ y \end{bmatrix}$ into $\begin{bmatrix} -y \\ x \end{bmatrix}$, so $D_0^2 = -\mathrm{I}_2$ and $D_0^3 = -D_0 = D_0^{-1}$.

We also have $D_0 = \mathrm{E}_{12}(1)\mathrm{E}_{21}(-1)\mathrm{E}_{12}(1)$, $D_0 D_q = -\mathrm{E}_{12}(q)$ and $D_q D_0 = -\mathrm{E}_{21}(q)$.

21 Exercise Let $(e_1, \ldots, e_n)$ be the canonical basis of $\mathbf{A}^n$ and $(f_1, \ldots, f_n)$ the n columns of F. We can assume that the invertible principal minor is in the north-west position such that $(f_1, \ldots, f_k, e_{k+1}, \ldots, e_n)$ is a basis of $\mathbf{A}^n$.

Since $F(f_j) = f_j$, the matrix of F with respect to this basis is $G \overset{\text{def}}{=} \begin{bmatrix} \mathrm{I}_k & * \\ 0 & * \end{bmatrix}$.

The matrix G is idempotent as well as its transposed G'. Apply to the projector G' the operation that we just subjected to F.

Since $G'(e_j) \in \bigoplus_{i \geqslant k+1} \mathbf{A} e_i$ for $j \geqslant k+1$, the matrix of G' with respect to the new basis is of the form $H = \begin{bmatrix} \mathrm{I}_k & 0 \\ 0 & * \end{bmatrix}$, whence the result because F is similar to ${}^{\mathrm{t}}H$.

22 Exercise We have each $b_{ji} \in \mathbf{A}$ such that $1 = \sum_{i,j} b_{ji} a_{ij}$. Let $B \in \mathbf{A}^{m \times n}$ be defined by $B = (b_{ji})$. Check that $ABA = A$: $(ABA)_{ij} = \sum_{l,k} a_{il} b_{lk} a_{kj}$.

But $\begin{vmatrix} a_{il} & a_{ij} \\ a_{kl} & a_{kj} \end{vmatrix} = 0$, so $(ABA)_{ij} = \sum_{l,k} a_{ij} a_{kl} b_{lk} = a_{ij} \sum_{l,k} a_{kl} b_{lk} = a_{ij}$. Consequently, AB is a projector.

Let us prove that AB is of rank 1. We have $\mathrm{Tr}(AB) = \sum_i (AB)_{ii} = \sum_{i,j} a_{ij} b_{ji} = 1$, thus $\mathcal{D}_1(AB) = 1$. Furthermore, $\mathcal{D}_2(AB) \subseteq \mathcal{D}_2(A) = 0$.

23 Exercise

1. Fix a linear form μ. The map $E^{r+1} \to \mathbf{A}$ defined by

$$(y_0, \ldots, y_r) \mapsto \textstyle\sum_{i=0}^{r} (-1)^i f(y_0, \ldots, y_{i-1}, \widehat{y_i}, y_{i+1}, \ldots, y_r)\, \mu(y_i),$$

where teh symbol $\widehat{y_i}$ denotes the omission of the element, is an $(r+1)$-multilinear alternating form.

According to the hypothesis $\bigwedge_{r+1}(x_1, \ldots, x_n) = 0$ and the injectivity of $E \mapsto E^{\star\star}$, we obtain

$$\textstyle\sum_{i=0}^{r} (-1)^i f(y_0, \ldots, y_{i-1}, \widehat{y_i}, y_{i+1}, \ldots, y_r)\, y_i = 0.$$

Write y instead of y_0 and execute the following operation: in the expression

$$(-1)^i f(y, \ldots, y_{i-1}, \widehat{y_i}, y_{i+1}, \ldots, y_r),$$

bring y between y_{i-1} and y_i. The permutation thus executed necessitates a multiplication by $(-1)^{i-1}$. We then obtain the second equality in which all the signs "have disappeared." For example with $r = 4$, the expression

$$\begin{gathered} f(\widehat{y}, y_1, y_2, y_3, y_4)y - f(y, \widehat{y_1}, y_2, y_3, y_4)y_1 + f(y, y_1, \widehat{y_2}, y_3, y_4)y_2 - \\ f(y, y_1, y_2, \widehat{y_3}, y_4)y_3 + f(y, y_1, y_2, y_3, \widehat{y_4})y_4 = \\ f(y_1, y_2, y_3, y_4)y - f(y, y_2, y_3, y_4)y_1 + f(y, y_1, y_3, y_4)y_2 - \\ f(y, y_1, y_2, y_4)y_3 + f(y, y_1, y_2, y_3)y_4 \end{gathered}$$

is none other than

$$\begin{gathered} f(y_1, y_2, y_3, y_4)y - f(y, y_2, y_3, y_4)y_1 - f(y_1, y, y_3, y_4)y_2 - \\ f(y_1, y_2, y, y_4)y_3 - f(y_1, y_2, y_3, y)y_4. \end{gathered}$$

A faster proof: apply a linear form μ to the last expression above, check that the obtained map $(y, y_1, y_2, y_3, y_4) \mapsto \mu(\ldots)$ is 5-multilinear alternating, and therefore is null by the assumptions.

2. Treat the $r = 3$ case. We have an assumption

$$1 = \sum\nolimits_{ijk} \alpha_{ijk} f_{ijk}(x_i, x_j, x_k), \qquad f_{ijk} \text{ 3-multilinear alternating over } E.$$

Define $\pi : E \to E$ by:

$$\pi(x) = \sum\nolimits_{ijk} \alpha_{ijk}[f_{ijk}(x, x_j, x_k)x_i + f_{ijk}(x_i, x, x_k)x_j + f_{ijk}(x_i, x_j, x)x_k].$$

Clearly, the image of p is contained in the submodule $\sum \mathbf{A}x_i$. In addition, for $x \in \sum \mathbf{A}x_i$, we have

$$f_{ijk}(x, x_j, x_k)x_i + f_{ijk}(x_i, x, x_k)x_j + f_{ijk}(x_i, x_j, x)x_k = f_{ijk}(x_i, x_j, x_k)x.$$

Whence $\pi(x) = x$: the endomorphism $\pi : E \to E$ is a projector onto $\sum \mathbf{A}x_i$. Notice that p is of the form $\pi(x) = \sum_i \alpha_i(x)x_i$ i.e. $\pi = \psi \circ \varphi$ and that $\pi \circ \psi = \psi$.
3. The module E in question is $\mathbf{A}^m$ and the vectors $x_1, \ldots, x_n$ are the columns of A. We have $\psi = A : \mathbf{A}^n \to \mathbf{A}^m$, and if we let $B \in \mathbf{A}^{n\times m}$ be the matrix of $\varphi : \mathbf{A}^m \to \mathbf{A}^n$, we indeed have $ABA = A$. So, the linear map $AB : \mathbf{A}^m \to \mathbf{A}^m$ is a projector having the same image as A.

26 Exercise Let us first see the case where $u = \mathrm{Diag}(\lambda_1, \ldots, \lambda_n)$. We have a basis (e_I) of $\bigwedge^k(\mathbf{A}^n)$ indexed by the subsets $I \subseteq \{1, \ldots, n\}$ of cardinality k:

$$e_I = e_{i_1} \wedge \cdots \wedge e_{i_k} \qquad I = \{i_1 < \cdots < i_k\}.$$

Then, u_k is diagonal with respect to the basis (e_I): $u_k(e_I) = \lambda_I e_I$ with $\lambda_I = \prod_{i\in I} \lambda_i$. It follows that $\det(u_k) = \prod_{\#I=k} \prod_{i\in I} \lambda_i$. It remains to determine, for some j given in $[\![1..n]\!]$, the number of occurrences of λ_j in the above product. In other words, how many subsets I, of cardinality k, contain j? As many as there are subsets of cardinality $k-1$ contained in $\{1, \cdots, n\}\backslash\{j\}$, i.e. $\binom{n-1}{k-1}$. The result is proven for a generic matrix. Thus it is true for any matrix. The second point follows from the equalities

$$\binom{n-1}{k-1} + \binom{n-1}{n-k-1} = \binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}.$$

28 Exercise The general case is treated by induction on n. Consider the polynomial ring $\mathbb{Z}[(x_{ij})]$ with n^2 indeterminates and the universal matrix $A = (x_{ij})$ with coefficients in this ring. Let $\Delta_{1k} \in \mathbb{Z}[(x_{ij})]$ be the cofactor of x_{1k} in A. These cofactors satisfy the identities:

$$\sum_{j=1}^n x_{1j}\Delta_{1j} = \det A, \qquad \sum_{j=1}^n x_{ij}\Delta_{1j} = 0 \quad \text{for } i > 1.$$

Since the N_{kl}'s pairwise commute, the specialization $x_{kl} \mapsto N_{kl}$ is legitimate. Let $N'_{1j} = \Delta_{1j}(x_{kl} \mapsto N_{kl})$, then we have

$$N'_{11} = \textstyle\sum_{\sigma\in \mathrm{S}_{n-1}} \varepsilon(\sigma) N_{2\sigma_2} N_{3\sigma_3} \ldots N_{n\sigma_n}.$$

Let us define N' by:

$$N' = \begin{bmatrix} N'_{11} & 0 & \cdots & 0 \\ N'_{12} & \mathrm{I}_m & & \vdots \\ \vdots & \vdots & \ddots & 0 \\ N'_{1n} & 0 & \cdots & \mathrm{I}_m \end{bmatrix}, \text{ so that } NN' = \begin{bmatrix} \Delta & N_{12} & \cdots & N_{1n} \\ 0 & N_{22} & \cdots & N_{2n} \\ \vdots & & & \vdots \\ 0 & N_{n2} & \cdots & N_{nn} \end{bmatrix}.$$

By taking determinants, we get

$$\det(N)\det(N'_{11}) = \det(\Delta)\det\begin{bmatrix} N_{22} & \cdots & N_{2n} \\ \vdots & & \vdots \\ N_{n2} & \cdots & N_{nn} \end{bmatrix}.$$

The induction hypothesis provides the equalities

$$\det\begin{bmatrix} N_{22} & \cdots & N_{2n} \\ \vdots & & \vdots \\ N_{n2} & \cdots & N_{nn} \end{bmatrix} = \det\Big(\sum_{\sigma\in \mathrm{S}_{n-1}} \varepsilon(\sigma) N_{2\sigma_2} N_{3\sigma_3}\cdots N_{n\sigma_n}\Big) = \det(N'_{11}).$$

Simplification by the regular element $\det(N'_{11})$ gives the equality $\det(N) = \det(\Delta)$.

1 Problem

1. If A_j is a nonzero column of A, we have $BA_j = e_j$ and therefore $ABA_j = A_j$; thus AB is the identity over $\mathrm{Im}\, A$, so $ABA = A$. The matrix AB is lower triangular, and its diagonal coefficients are $0, 1$. The matrix BA is diagonal and its diagonal coefficients are $0, 1$.

$$B = \begin{bmatrix} \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix}, \qquad BA = \begin{bmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix},$$

$$AB = \begin{bmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{24} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{44} & \cdot & a_{43} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ a_{74} & \cdot & a_{73} & \cdot & a_{71} & a_{72} & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ a_{94} & \cdot & a_{93} & \cdot & a_{91} & a_{92} & \cdot & a_{95} & \cdot \end{bmatrix}.$$

The complementary subspace $\mathrm{Ker}\, AB$ of $\mathrm{Im}\, A = \mathrm{Im}\, AB$ in $\mathbf{K}^n$ admits as its basis the e_i's for the indices i of the rows that do not contain a pivot index. In the example, (e_2, e_4, e_7, e_9) is a basis of $\mathrm{Ker}\, AB$.

2. We obtain (Q, A') by Gauss' (classical) pivot method. If the matrix $B' \in M_{n,m}(\mathbf{K})$ satisfies $A'B'A' = A'$, then $AQB'AQ = AQ$, therefore the matrix $B = QB'$ satisfies $ABA = A$.

3. Consider a matrix $B \in \mathbb{M}_{m,n}(\mathbf{K})$ such that $ABA = A$. Then, if $y = Ax$ for some m-vector with coefficients in an overring of $\mathbf{K}$, we have $A(By) = y$, whence the existence of a solution on $\mathbf{K}$, namely By.
4. Let $(u_1, \dots, u_r)$ be a generator set of the $\mathbf{K}$-vector space E, constituted of vectors of $\mathbf{K}_0^n$; similarly for $(v_1, \dots, v_s)$ and F. Let $z \in \mathbf{K}_0^n$, which we want to express in the form $z = x_1u_1 + \cdots + x_ru_r + y_1v_1 + \cdots + y_sv_s$ with each $x_i, y_j \in \mathbf{K}_0$. We thus obtain a $\mathbf{K}_0$-linear system from the unknowns x_i's, y_j's which admits a solution on $\mathbf{K}$, therefore also on $\mathbf{K}_0$.
5.a. If every $\pi(e_j)$ is in $\mathbf{K}_0^n$, then the subspace E, generated by the $\pi(e_j)$'s, is $\mathbf{K}_0$-rational. Conversely, if E is $\mathbf{K}_0$-rational, since F is also $\mathbf{K}_0$-rational, by the previous question we have $\pi(e_j) \in \mathbf{K}_0^n$ for all j.
b. Now trivial: $\mathbf{K}_0$ is the subfield generated by the components of the $\pi(e_j)$ vectors.
c. The field of rationality of a strictly staggered matrix is the subfield generated by the coefficients of the matrix. For example with $E = \operatorname{Im} A \subset \mathbf{K}^5$:

$$A = \begin{array}{c} \\ e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \end{array} \begin{array}{c} \begin{array}{ccc} w_1 & w_2 & w_3 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 \\ a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ b & c & d \end{bmatrix} \end{array},$$

we get $E = \mathbf{K}w_1 \oplus \mathbf{K}w_2 \oplus \mathbf{K}w_3$ and we have $\mathbf{K}^5 = E \oplus F$ with $F = \mathbf{K}e_2 \oplus \mathbf{K}e_5$. Since

$$e_1 - w_1 \in F, \quad e_3 - w_2 \in F, \quad e_4 - w_3 \in F,$$

we have $\pi(e_1) = w_1, \pi(e_3) = w_2, \pi(e_4) = w_3$ and $\pi(e_2) = \pi(e_5) = 0$. The field of rationality of E is $\mathbf{K}_0 = \mathbf{k}(a, b, c, d)$, where $\mathbf{k}$ is the prime subfield of $\mathbf{K}$.

Bibliographic Comments

The Gauss-Joyal Lemma is in [76], which gives it its name. On the general subject of comparison between the ideals $\mathrm{c}(f)\mathrm{c}(g)$ and $\mathrm{c}(fg)$ see [39, 91, 140] and, in this work, Sects. III-2 and III-3 and Proposition XI-3.14.

Regarding the constructive treatment of Noetherianity, see [MRR, 108, 142, 143, 153, 163, 164, 181].

The whole of Sect. 5 can be more or less found in [Northcott]. For example the formula (12) on p. 43 is found in a related form in Theorem 5 on p. 9. Likewise, our Cramer-style magic formula (17) on p. 44 is very similar to Theorem 6 on p. 10: Northcott attaches central importance to the matrix equation $ABA = A$. On this subject, see also [Rao & Mitra] and [57, Díaz-Toca et al.].

Proposition 5.15 is in [Bhaskara Rao] Theorem 5.5.

Concerning Theorem 5.26: in [Northcott] Theorem 18 on p. 115 establishes the equivalence of items *1* and *5* by a method which is not entirely constructive, but Theorem 5 p. 9 would allow us to give an explicit formula for the implication $5 \Rightarrow 1$.

http://www.springer.com/978-94-017-9943-0

Commutative Algebra: Constructive Methods
Finite Projective Modules
Lombardi, H.; Quitté, C.
2015, XLIX, 996 p. 80 illus., Hardcover
ISBN: 978-94-017-9943-0