Advanced Algebra

Lectures by Laurent Berger
Notes by Alexis Marchand

ENS de Lyon
S1 2018-2019
M1 course

Contents

1 Rings and modules

Notation 1.0.1. *In this course, all rings will be commutative, with a unit element, and will verify* $0 \neq 1$.

1.1 Modules, submodules and homomorphisms

Definition 1.1.1 (Module)**.** *A* module M *on a ring* A *is an abelian group equipped with a law* $(a, m) \in A \times M \longmapsto am \in M$ *s.t.*

(i) $\forall (a, b) \in A^2,\ \forall (m, n) \in M^2,\ (a + b)m = am + bm \quad a(m + n) = am + an.$

(ii) $\forall (a, b) \in A^2,\ \forall m \in M,\ a(bm) = (ab)m.$

(iii) $\forall m \in M,\ 1m = m.$

Example 1.1.2.

(i) *If the ring* A *is a field,* A*-modules are exactly* A*-vector spaces.*

(ii) $\mathbb{Z}$*-modules are exactly abelian groups.*

Remark 1.1.3. *Let* A *be a ring.*

(i) *In general, in an* A*-module* M*, if* $a \in A\backslash\{0\}$ *and* $m \in M$*,* $am = 0$ *does not imply* $m = 0$.

(ii) A*-modules do not have bases in general.*

Definition 1.1.4 (Torsion elements)**.** *Let* M *be an* A*-module. We define:*

$$M_{\text{tor}} = \{m \in M,\ \exists a \in A\backslash\{0\},\ am = 0\}\,.$$

The elements of M_{tor} *are called* torsion elements*. We say that* M *is* torsion-free *if* $M_{\text{tor}} = \{0\}$.

Definition 1.1.5 (Submodule)**.** *Let* M *be an* A*-module. A submodule of* M *is an additive subgroup* N *s.t.* $AN \subseteq N$.

Example 1.1.6. *If* A *is a ring, the submodules of* A *(considered as an* A*-module) are exactly the ideals of* A.

Proposition 1.1.7. *Let* M *be an* A*-module. If* A *is an integral domain, then* M_{tor} *is a submodule of* M.

Definition 1.1.8 (Module homomorphism)**.** *Let* M *and* N *be two* A*-modules. A map* $f : M \to N$ *is said to be a* module homomorphism *if* f *is additive and* A*-linear. The set of module homomorphisms from* M *to* N *is denoted by* $\mathrm{Hom}_A(M, N)$ *or* $\mathrm{Hom}(M, N)$*. It is an* A*-module.*

Example 1.1.9. *Let* M *be an* A*-module.*

(i) *The module* $\mathrm{Hom}_A(A, M)$ *is isomorphic to* M.

(ii) *The module* $\mathrm{Hom}_A(M, A)$ *is called the* dual *of* M*, and it is denoted by* M^* *or* $M^\vee$*. Its elements are called* linear forms.

1.2 Exact sequences

Definition 1.2.1 (Kernel and image). *Let $f : M \to N$ be a module homomorphism. We define* $\operatorname{Ker} f = f^{-1}(\{0\})$ *and* $\operatorname{Im} f = f(M)$. *These are submodules of M and N respectively.*

Definition 1.2.2 (Exact sequence). *Consider three modules L, M, N and two homomorphisms $f : L \to M$ and $g : M \to N$. One can write this as a sequence:*

$$L \xrightarrow{f} M \xrightarrow{g} N.$$

We say that the sequence is exact *if* $\operatorname{Im} f = \operatorname{Ker} g$. *Likewise, for a (possibly infinite sequence) $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \xrightarrow{f_3} \cdots$, we say that the sequence is exact at M_i if $\operatorname{Im} f_{i-1} = \operatorname{Ker} f_i$; and we say that the sequence is exact if it is exact at all positions.*

Example 1.2.3. *A sequence $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ is exact* iff *f is injective, g is surjective and* $\operatorname{Im} f = \operatorname{Ker} g$.

Definition 1.2.4.

(i) *Let M, N_1, N_2 be three A-modules and consider a homomorphism $f : N_1 \to N_2$. We define a module homomorphism:*

$$f_* : \left| \begin{array}{rcl} \operatorname{Hom}_A(M, N_1) & \longrightarrow & \operatorname{Hom}_A(M, N_2) \\ g & \longmapsto & f \circ g \end{array} \right. .$$

(ii) *Let M_1, M_2, N be three A-modules and consider a homomorphism $f : M_1 \to M_2$. We define a module homomorphism:*

$$f^* : \left| \begin{array}{rcl} \operatorname{Hom}_A(M_2, N) & \longrightarrow & \operatorname{Hom}_A(M_1, N) \\ g & \longmapsto & g \circ f \end{array} \right. .$$

Proposition 1.2.5. *Consider a sequence $N' \xrightarrow{f} N \xrightarrow{g} N''$. The following assertions are equivalent:*

(i) *The sequence $0 \to N' \xrightarrow{f} N \xrightarrow{g} N''$ is exact.*

(ii) *For any A-module M, the sequence $0 \to \operatorname{Hom}(M, N') \xrightarrow{f_*} \operatorname{Hom}(M, N) \xrightarrow{g_*} \operatorname{Hom}(M, N'')$ is exact.*

Proposition 1.2.6. *Consider a sequence $M' \xrightarrow{f} M \xrightarrow{g} M''$. The following assertions are equivalent:*

(i) *The sequence $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact.*

(ii) *For any A-module N, the sequence $0 \to \operatorname{Hom}(M'', N) \xrightarrow{g^*} \operatorname{Hom}(M, N) \xrightarrow{f^*} \operatorname{Hom}(M', N)$ is exact.*

1.3 Sums, products and quotients

Definition 1.3.1 (Sums and products). *Let $(M_i)_{i \in I}$ be a family of A-modules.*

(i) *The set $\prod_{i \in I} M_i$ has naturally the structure of an A-module.*

(ii) *We define $\bigoplus_{i \in I} M_i = \left\{ (m_i)_{i \in I} \in \prod_{i \in I} M_i,\ \{i \in I,\ m_i \neq 0\} \text{ is finite} \right\}$.*

Hence, $\bigoplus_{i \in I} M_i$ is a submodule of $\prod_{i \in I} M_i$, and we have $\bigoplus_{i \in I} M_i = \prod_{i \in I} M_i$ iff *I is finite.*

Proposition 1.3.2. *Let $(M_i)_{i \in I}$, $(N_j)_{j \in J}$, M and N be A-modules.*

(i) $\operatorname{Hom}\left(M, \prod_{j\in J} N_j\right) \simeq \prod_{j\in J} \operatorname{Hom}(M, N_j)$.

(ii) $\operatorname{Hom}\left(\bigoplus_{i\in I} M_i, N\right) \simeq \prod_{i\in I} \operatorname{Hom}(M_i, N)$.

(iii) $\operatorname{Hom}\left(\bigoplus_{i\in I} M_i, \prod_{j\in J} M_j\right) \simeq \prod_{(i,j)\in I\times J} \operatorname{Hom}(M_i, N_j)$.

Definition 1.3.3 (Quotient)**.** *Let N be an A-module and M be a submodule of N. We define an equivalence relation $\sim$ on N by $n_1 \sim n_2 \iff (n_1 - n_2) \in M$. The set of equivalence classes is denoted by N/M. It has a unique structure of A-module s.t. the natural projection $\pi : N \to N/M$ is a module homomorphism. Hence, if $i : M \to N$ denotes inclusion, we have an exact sequence:*

$$0 \to M \xrightarrow{i} N \xrightarrow{\pi} N/M \to 0.$$

Proposition 1.3.4 (Universal property of the quotient)**.** *Let N be an A-module and M be a submodule of N. If $f : N \to P$ is a module homomorphism s.t. $M \subseteq \operatorname{Ker} f$, then there is a unique map $\overline{f} : N/M \to P$ s.t. $f = \overline{f} \circ \pi$, where $\pi : N \to N/M$ is the natural projection.*

Corollary 1.3.5. *If we have an exact sequence $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$, then $N \simeq M/\operatorname{Im} f$. In other words, given a module homomorphism $f : M \to N$, we have:*

$$\operatorname{Im} f \simeq M/\operatorname{Ker} f.$$

Definition 1.3.6 (Cokernel)**.** *Given a module homomorphism $f : M \to N$, define:*

$$\operatorname{Coker} f = N/\operatorname{Im} f.$$

We have the following exact sequence:

$$0 \to \operatorname{Ker} f \to M \xrightarrow{f} N \to \operatorname{Coker} f \to 0.$$

Proposition 1.3.7. *Let $f : M \to N$ be a module homomorphism. Consider a submodule X of M and a submodule Y of N. Write $\pi_{M/X} : M \to M/X$ and $\pi_{N/Y} : N \to N/Y$ for the natural projections. If $f(X) \subseteq Y$, then there exists a unique map $\overline{f} : M/X \to N/Y$ s.t.*

$$\pi_{N/Y} \circ f = \overline{f} \circ \pi_{M/X}.$$

1.4 Snake Lemma

Theorem 1.4.1 (Snake Lemma)**.** *Consider the following commutative diagram:*

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Ker} a \arrow[r] \arrow[d] & \operatorname{Ker} b \arrow[r] \arrow[d] & \operatorname{Ker} c \arrow[d] \arrow[dddll, rounded corners, "\delta"] & \\
0 \arrow[r] & A \arrow[r, "u"] \arrow[d, "a"'] & B \arrow[r, "v"] \arrow[d, "b"'] & C \arrow[r] \arrow[d, "c"'] & 0 \\
0 \arrow[r] & A' \arrow[r, "u'"] \arrow[d] & B' \arrow[r, "v'"] \arrow[d] & C' \arrow[r] \arrow[d] & 0 \\
 & \operatorname{Coker} a \arrow[r] & \operatorname{Coker} b \arrow[r] & \operatorname{Coker} c \arrow[r] & 0
\end{tikzcd}$$

Assume that the two horizontal black sequences are exact. Then there is a natural map $\delta : \operatorname{Ker} c \to \operatorname{Coker} a$, and the red sequence is exact.

1.5 Noetherian modules

Notation 1.5.1. *Let M be an A-module. Given a subset $P \subseteq M$, we denote by $(P) = \sum_{m \in P} Am$ the submodule of M generated by P.*

Definition 1.5.2 (Noetherian module)**.**

(i) *An A-module M is said to be* of finite type *(or finitely generated) if there exist $m_1, \ldots, m_r$ s.t. $M = (m_1, \ldots, m_r)$. Equivalently, there exist $r \in \mathbb{N}^*$ and a surjective map $A^r \to M$.*

(ii) *An A-module M is said to be* noetherian *if every submodule of M is of finite type.*

Remark 1.5.3. *The submodules of the A-module A are precisely the ideals of A, so A is noetherian as a ring* iff *A is noetherian as an A-module.*

Proposition 1.5.4. *An A-module M is noetherian* iff *every increasing sequence $(M_n)_{n \in \mathbb{N}}$ of submodules of M is eventually constant.*

Lemma 1.5.5. *Consider an exact sequence $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$. Then M is noetherian* iff *L and N are noetherian.*

Proof. ($\Rightarrow$) This amounts to proving that every submodule of a noetherian module is noetherian and that the image of a noetherian module by a homomorphism is noetherian. ($\Leftarrow$) Assume that L and N are noetherian. Let P be a submodule of M. Then $P \cap f(L)$ is a submodule of $f(L)$, which is noetherian as the image of a noetherian module. Hence, there exist $\ell_1, \ldots, \ell_r \in L$ s.t. $P \cap f(L) = (f(\ell_1), \ldots, f(\ell_r))$. Likewise, there exist $p_1, \ldots, p_s \in P$ s.t. $g(P) = (g(p_1), \ldots, g(p_s))$. Using the fact that the sequence is exact, we now prove that $P = (f(\ell_1), \ldots, f(\ell_r), p_1, \ldots, p_s)$. $\square$

Theorem 1.5.6. *If A is a noetherian ring, then every finitely generated A-module M is noetherian.*

Proof. Suppose that A is a notherian A-module. For $r \in \mathbb{N}^*$, we have an exact sequence $0 \to A \to A^r \to A^{r-1} \to 0$. Using Lemma 1.5.5, we use these exact sequences to prove by induction on r that A^r is noetherian for all $r \in \mathbb{N}^*$. Now, if M is a finitely generated A-module, there exist $r \in \mathbb{N}^*$ and a surjective map $f : A^r \to M$. Hence, $M = f(A^r)$ is noetherian as the image of a noetherian module. $\square$

1.6 Free modules

Definition 1.6.1 (Free module)**.** *Let M be an A-module. If $(m_j)_{j \in J} \in M^J$ is a family of elements of M, we get a map $f : \bigoplus_{j \in J} A \to M$ defined by $f(a_j) = a_j m_j$. We say that $(m_j)_{j \in J}$ is a* basis *of M if the map f is an isomorphism. We say that the module M is* free *if it admits a basis, i.e. if it is isomorphic to $\bigoplus_{j \in J} A$ for some set J.*

Proposition 1.6.2. *If M is a free A-module, then any two bases of M have the same cardinality.*

Proof. By Krull's Theorem, A has a maximal ideal I. If $(m_j)_{j \in J}$ is a basis of M, then M/IM is an A/I-vector space and $(\overline{m}_j)_{j \in J}$ is a basis of this space. As any two bases of a vector space have the same cardinality, this proves the proposition. $\square$

Definition 1.6.3 (Free module of finite type)**.** *We say that an A-module M is* free of finite type *if it admits a finite basis, i.e. if M is isomorphic to A^r for some $r \in \mathbb{N}^*$. The integer r only depends on M, and it is called the* rank *of M.*

1.7 Matrices

Definition 1.7.1 (Matrix of a module homomorphism)**.** *Let M and N be two A-modules that are free of rank r and s. Consider respective bases $(m_1, \dots, m_r)$ of M and $(n_1, \dots, n_s)$ of N. If $f \in \operatorname{Hom}(M, N)$, then the matrix of f is $\operatorname{Mat}(f) = (f_{ij})_{\substack{1\le i\le s\\ 1\le j\le r}} \in M_{s,r}(A)$ defined by:*

$$\forall (i,j) \in \{1,\dots,s\} \times \{1,\dots,r\}\,,\ f(m_j) = \sum_{i=1}^{s} f_{ij} n_i.$$

Proposition 1.7.2. *If $f : M \to N$ and $g : N \to L$ are two homomorphisms between three free A-modules of finite type equipped with bases, then $\operatorname{Mat}(fg) = \operatorname{Mat}(f)\operatorname{Mat}(g)$.*

Proposition 1.7.3. *Let M be a free A-module of rank r equipped with a basis. Consider $f \in \operatorname{Hom}_A(M, M)$ and let $P = \operatorname{Mat}(f)$.*

(i) *f is surjective $\iff (\det P) \in A^\times$.*

(ii) *f is injective $\iff (\det P)$ is not a divisor of 0 in A.*

Proof. (ii) ($\Rightarrow$) Suppose that $(\det P)$ is a divisor of 0 in A, i.e. there exists $h \in A\backslash\{0\}$ s.t. $h \det P = 0$. If $h \cdot P = 0$, then $P \cdot {}^t\!\begin{pmatrix} h & 0 & \cdots & 0 \end{pmatrix} = 0$ so $\operatorname{Ker} f \neq \{0\}$. Therefore, assume that $h \cdot P \neq 0$, i.e. there exists $(i,j) \in \{1,\cdots,r\}^2$ s.t. $hP_{ij} \neq 0$. In other words, there is a 1×1 minor of P which is not killed by h. And the only $r \times r$ minor of P is killed by h. Hence P has a largest minor, of size $n < r$, which is not killed by h: call it $\mu = \operatorname{minor}^{j_1,\dots,j_n}_{i_1,\dots,i_n}(P)$, with $h\mu \neq 0$. Take $i_0 \notin \{i_1,\dots,i_n\}$ and let $x = {}^t\!\begin{pmatrix} x_1 & \cdots & x_r \end{pmatrix}$, where $x_i = 0$ if $i \notin \{i_0,\dots,i_r\}$, and $x_{i_k} = (-1)^k h \operatorname{minor}^{j_1,\dots,j_n}_{i_0,\dots,\hat{i}_k,\dots,i_n}(P)$. Note that $x_{i_0} = h\mu \neq 0$, so $x \neq 0$. However, it is easy to check that $Px = 0$. Hence, $\operatorname{Ker} f \neq \{0\}$ and f is not injective. □

Corollary 1.7.4. *If M is a free A-module of finite type and $f \in \operatorname{Hom}_A(M, M)$ is surjective, then f is bijective.*

Corollary 1.7.5. *If there exists an injective map $f \in \operatorname{Hom}_A(A^r, A^s)$, then $r \le s$*

Proof. Suppose for contradiction that $r > s$. Then we can extend f to a map $\widetilde{f} : x \in A^r \longmapsto (f(x), 0) \in A^s \oplus A^{r-s} = A^r$. Hence, $\widetilde{f}$ is injective, but $\det f = 0$, which is a contradiction. □

1.8 Cayley-Hamilton Theorem

Definition 1.8.1 (Characteristic polynomial)**.** *If $P \in M_n(A)$, the* characteristic polynomial *of P is defined by:*

$$\Pi_P = \det(X \operatorname{Id} - P) \in A[X].$$

Remark 1.8.2. *The data of an $A[X]$-module M is equivalent to an A-module M equipped with an A-linear map $f : M \to M$.*

Theorem 1.8.3 (Cayley-Hamilton Theorem)**.** *Consider an A-module M generated by a finite number $m_1,\dots,m_n$ of elements. Let $f \in \operatorname{Hom}_A(M, M)$ and take a matrix $P \in M_n(A)$ s.t. $\forall i \in \{1,\dots,n\}\,,\ f(m_i) = \sum_{j=1}^{n} P_{ij} m_j$. Then $\Pi_P(f) = 0$ on M.*

Proof. View M as an $A[X]$-module by setting $X \cdot m = f(m)$ for $m \in M$. Hence, we have:

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = (X \operatorname{Id} - P) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = {}^t(\operatorname{Com}(X \operatorname{Id} - P))\,(X \operatorname{Id} - P) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \Pi_P(X) \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}.$$

Therefore, $\forall i \in \{1,\dots,n\}\,,\ \Pi_P(f) \cdot m_i = \Pi_P(X) \cdot m_i = 0$. Since $m_1,\dots,m_n$ generate M, $\Pi_P(f) = 0$. □

Remark 1.8.4. *Proving the Cayley-Hamilton Theorem for any module gives the vector space version as a corollary.*

Corollary 1.8.5. *If M is a finitely generated A-module and I is an ideal of A s.t. $IM = M$, then there exists $x \in A$ s.t. $x \equiv 1 \mod I$ and $xM = 0$.*

Proof. Let $m_1, \ldots, m_n$ be a finite generating family for M. Note that there exists $P \in M_n(I)$ s.t. $\forall i \in \{1, \ldots, n\}$, $m_i = \sum_{j=1}^{n} P_{ij} m_j$ (because $IM = M$). Apply the Cayley-Hamilton Theorem to $f = \mathrm{id}_M$ with P as above. We take $x = \Pi_P(1) \in A$; hence $x = \det(\mathrm{Id} - P) \equiv 1 \mod I$ (because $P \in M_n(I)$) and $\forall m \in M$, $xm = \Pi_P(\mathrm{id}_M) \cdot m = 0$. □

1.9 Local rings

Definition 1.9.1 (Local ring)**.** *A ring A is said to be a* local ring *if it admits only one maximal ideal. In this case, if I is the unique maximal ideal of A, the quotient A/I is called the* residue field *of A.*

Lemma 1.9.2. *A ring A is local* iff *$A \backslash A^\times$ is an ideal of A.*

Example 1.9.3.

(i) *A field is local (with maximal ideal $\{0\}$).*

(ii) *$\mathbb{Z}_p$ is local (with maximal ideal $p\mathbb{Z}_p$).*

(iii) *$\mathbb{C}[[X]]$ is local (with maximal ideal $X\mathbb{C}[[X]]$).*

(iv) *Consider a topological space X and choose $x \in X$. Let B be the set of pairs $(\mathcal{U}, f)$, where $\mathcal{U}$ is an open neighbourhood of x and $f : \mathcal{U} \to \mathbb{R}$ is a continuous function. Define an equivalence relation $\mathcal{R}$ on B by $(\mathcal{U}, f)\, \mathcal{R}\, (\mathcal{V}, g)$* iff *there exists an open neighbourhood $\mathcal{W} \subseteq \mathcal{U} \cap \mathcal{V}$ of x s.t. $f_{|\mathcal{W}} = g_{|\mathcal{W}}$. Hence, the quotient $A = B/\mathcal{R}$ is naturally a ring, and it is local.*

Proposition 1.9.4 (Nakayema's Lemma)**.** *Let A be a local ring with maximal ideal I. Consider a finitely generated A-module M. If $m_1, \ldots, m_r$ are elements of M s.t. the A/I-vector space M/IM is generated by $\overline{m}_1, \ldots, \overline{m}_r$, then M is generated by $m_1, \ldots, m_r$.*

Proof. Let $N = Am_1 + \cdots + Am_r$. We have $M = N + IM$, therefore $I \cdot (M/N) = (IM + N)/N = M/N$. By Corollary 1.8.5, there exists $x \equiv 1 \mod I$ s.t. $x \cdot M/N = 0$. Since A is local, $x \in A^\times$ and therefore $M = N$. □

Corollary 1.9.5. *Let A be a local ring with maximal ideal I. If M and N are two A-modules with $M = N + IM$, then $N = M$.*

2 Finitely generated modules over PIDs

2.1 Invariant factors for PIDs

Theorem 2.1.1. *If A is a PID, M is a free A-module of rank r and N is a submodule of M, then N is free of rank $\leq r$.*

Proof. Let $(m_i)_{1 \leq i \leq r}$ be a basis of M. For $i \in \{1, \ldots, r\}$, define $N_i = N \cap (m_1, \ldots, m_i)$. By induction on i, let us show that N_i is free of rank $\leq i$ (the result will follow by taking $i = r$). For $i = 1$, $N_1 \subseteq (m_1)$, and $(m_1) \simeq A$ (as an A-module). Since A is principal, N_1 is of the form $(a_1 m_1)$ for some $a_1 \in A$; hence N_1 is free of rank ≤ 1. Assume the result has been proved up to i. We have $N_{i+1} \subseteq (m_1, \ldots, m_{i+1})$. Consider:

$$I = \left\{ a \in A,\ \exists (b_1, \ldots, b_i) \in A^i,\ (b_1 m_1 + \cdots + b_i m_i + a m_{i+1}) \in N_{i+1} \right\}.$$

I is an ideal of A. As A is principal, I is of the form (a_{i+1}), with $a_{i+1} \in A$. If $a_{i+1} = 0$, then $N_{i+1} = N_i$ is free of rank $\leq i$ by induction. Otherwise, choose $x \in N_{i+1}$ s.t. the coefficient of m_{i+1} in x is a_{i+1}. For every $y \in N_{i+1}$, the coefficient of m_{i+1} in y is some multiple $b \cdot m_{i+1}$ of a_{i+1}, so $y - bx \in N_i$. This implies that $N_{i+1} = N_i + Ax$. But $N_i \cap Ax = \{0\}$, so:

$$N_{i+1} = N_i \oplus Ax.$$

Now, N_{i+1} is free of rank $\leq i+1$ by induction. □

Theorem 2.1.2. *If A is a PID, M is a free A-module of rank r and N is a submodule of M of rank s, then there exists a basis $(m_i)_{1\leq i\leq r}$ of M and $d_1, \ldots, d_s \in A\backslash\{0\}$ s.t.*

(i) *$(d_i m_i)_{1\leq i\leq s}$ is a basis of N.*

(ii) *$d_1 \mid d_2 \mid \cdots \mid d_s$.*

The ideals $(d_1), \ldots, (d_s)$ are determined by M/N; they are called the invariant factors *of M/N.*

Proof. We shall prove the result with the (stronger) assumption that A is euclidean, i.e. there exists a euclidean function $\mathcal{N} : A\backslash\{0\} \to \mathbb{N}$ s.t. for all $a \in A$ and for all $b \in A\backslash\{0\}$, there exist $q, r \in A$ with $a = qb + r$ and either $r = 0$ or $\mathcal{N}(r) < \mathcal{N}(b)$. We use induction on r. We choose respective bases of M and N. Let $P \in M_{r,s}(A)$ be the matrix of the basis of N in terms of the basis of M. Changing bases amounts to multiplying P by invertible matrices on the left and on the right. Hence, it is enough to prove that there exist $X \in GL_r(A)$ and $Y \in GL_s(A)$ s.t.

$$XPY = \begin{bmatrix} \operatorname{diag}(d_1, \ldots, d_s) \\ 0 \end{bmatrix},$$

with $d_1 \mid \cdots \mid d_s$. In other words, it is enough to prove that, by using elementary operations on rows and columns (i.e. permutation of rows or columns, and transvection operations), one can go from P to a matrix of the above form. We may assume that $P \neq 0$ (otherwise we are done) and we let $\mathcal{N}(P) = \min_{\substack{1\leq i\leq r \\ 1\leq j\leq s \\ P_{ij}\neq 0}} \mathcal{N}(P_{ij})$. We can permute rows and columns so that $\mathcal{N}(P) = \mathcal{N}(P_{11})$. Now, if there exists $i \in \{1, \ldots, r\}$ s.t. $P_{11} \nmid P_{i1}$, perform the euclidean division of P_{i1} by P_{11}: $P_{i1} = qP_{11} + r$, with $r \neq 0$. Now perform the operation $L_i \leftarrow L_i - qL_1$; we obtain a new matrix P' with $\mathcal{N}(P') < \mathcal{N}(P)$. After performing such operations a finite number of times, we will have $P_{11} \mid P_{i1}$ for all i; likewise, we can obtain $P_{11} \mid P_{1j}$ for all j. Now perform $L_i \leftarrow L_i - \frac{P_{i1}}{P_{11}} L_1$ for all $i \neq 1$ and $C_j \leftarrow C_j - \frac{P_{1j}}{P_{11}} C_1$ for all $j \neq 1$. We obtain a matrix of the form $\begin{bmatrix} P_{11} & 0 \\ 0 & Q \end{bmatrix}$, with $Q \in M_{r-1,s-1}(A)$. If there exists $(i,j) \in \{1, \ldots, r-1\} \times \{1, \ldots, s-1\}$ s.t. $P_{11} \nmid Q_{ij}$, perform $L_i \leftarrow L_i - qL_1$ as before in order to decrease the norm strictly. Thus, one may assume that $P_{11} \mid Q_{ij}$ for all (i,j). Now, applying the induction hypothesis to $\frac{Q}{P_{11}}$ gives the desired result. □

Vocabulary 2.1.3. *Let A be an integral domain.*

(i) *We say that A is an* elementary divisor domain *(EDD) if for all $P \in M_{r,s}(A)$, there exist $X \in GL_r(A)$ and $Y \in GL_s(A)$ s.t.*

$$XPY = \begin{bmatrix} \operatorname{diag}(d_1, \ldots, d_s) \\ 0 \end{bmatrix},$$

with $d_1 \mid \cdots \mid d_s$.

(ii) *We say that A is a* Bézout domain *if every finitely generated ideal of A is principal.*

Proposition 2.1.4. *If A is an EDD, then A is a Bézout domain.*

Proof. Let $I = (x_1, \ldots, x_r)$ be a finitely generated ideal of A. Consider $P = {}^t\!\begin{pmatrix} x_1 & \cdots & x_r \end{pmatrix} \in M_{r,1}(A)$. Since A is an EDD, there exist $X \in GL_r(A)$, $Y \in GL_s(A)$ and $d \in A$ s.t. $XPY = {}^t\!\begin{pmatrix} d & 0 & \cdots & 0 \end{pmatrix}$. Hence, $I = (d)$. □

Corollary 2.1.5. *Let A be an integral domain. We have the following chain of implications :*

A is a euclidean domain $\Longrightarrow$ A is a PID $\Longrightarrow$ A is an EDD $\Longrightarrow$ A is a Bézout domain.

2.2 Finitely generated modules over PIDs

Proposition 2.2.1. *If A is a PID and M is a finitely generated A-module, then there exist $n, m \in \mathbb{N}$ and nonzero elements $e_1, \ldots, e_m \in A \backslash A^\times$ with $e_1 \mid \cdots \mid e_m$ s.t.*

$$M \simeq A^n \oplus A/e_1A \oplus \cdots \oplus A/e_mA.$$

Proof. Since M is finitely generated, there exists a surjective map $f : A^r \to M$, with $r \in \mathbb{N}$. Let $N = \operatorname{Ker} f$. By Theorem 2.1.2, there is a basis $(g_i)_{1 \le i \le r}$ of A^r and nonzero elements $d_1, \ldots, d_s$ of A s.t. $d_1 \mid \cdots \mid d_s$ and:

$$N = d_1 g_1 A \oplus \cdots \oplus d_s g_s A.$$

Note that $M = \operatorname{Im} f \simeq A^r / \operatorname{Ker} f = A^r/N$. Therefore:

$$M \simeq \frac{g_1 A \oplus \cdots \oplus g_r A}{d_1 g_1 A \oplus \cdots \oplus d_s g_s A} \simeq A^{r-s} \oplus A/d_1A \oplus \cdots \oplus A/d_sA.$$

But $A/d_iA = \{0\}$ if $d_i \in A^\times$; we obtain the result by throwing away the indices i s.t. $d_i \in A^\times$. □

Proposition 2.2.2. *If M is a finitely generated module over a PID A, then the module M/M_{tor} is free of finite rank. Moreover, the integer n in Proposition 2.2.1 is the rank of M/M_{tor}. In particular, a torsion-free finitely generated module over a PID is free of finite rank.*

Proposition 2.2.3. *Let A be a PID and $d_1, \ldots, d_m$, $e_1, \ldots, e_n$ be nonzero elements of $A \backslash A^\times$ s.t. $d_1 \mid \cdots \mid d_m$, $e_1 \mid \cdots \mid e_n$, and $A/d_1A \oplus \cdots \oplus A/d_mA \simeq A/e_1A \oplus \cdots \oplus A/e_nA$. Then $m = n$ and $(d_i) = (e_i)$ for all $i \in \{1, \ldots, m\}$.*

Proof. Since A is a PID, prime elements are the same as irreducible elements; hence, if $p \in A$ is prime, then (p) is maximal and A/pA is a field. Moreover, for $d \in A \backslash A^\times$, $\frac{A/dA}{p \cdot (A/dA)} \simeq \frac{A}{pA + dA}$ is A/pA if $p \mid d$, $\{0\}$ otherwise. Hence, for any prime element $p \in A$, $\frac{A/d_1A \oplus \cdots \oplus A/d_mA}{p \cdot (A/d_1A \oplus \cdots \oplus A/d_mA)}$ is an (A/pA)-vector space whose dimension is the number of d_i that are divisible by p. Since $A/d_1A \oplus \cdots \oplus A/d_mA \simeq A/e_1A \oplus \cdots \oplus A/e_nA$, we have, for every prime element p:

$$|\{i \in \{1, \ldots, m\}\,,\ p \mid d_i\}| = |\{j \in \{1, \ldots, n\}\,,\ p \mid e_j\}|\,.$$

Now choose a prime element p s.t. $p \mid d_1$. Then $p \mid d_1 \mid d_2 \mid \cdots \mid d_m$, so $|\{j \in \{1, \ldots, n\}\,,\ p \mid e_j\}| = m$, and $n \ge m$. By symmetry, $n = m$ and $p \mid e_1 \mid \cdots \mid e_m$. Now if p divides some $d \in A$, then $p \cdot (A/dA) \simeq A/\left(\frac{d}{p}\right)A$. Here, this gives $A/\left(\frac{d_1}{p}\right)A \oplus \cdots \oplus A/\left(\frac{d_m}{p}\right)A \simeq A/\left(\frac{e_1}{p}\right)A \oplus \cdots \oplus A/\left(\frac{e_m}{p}\right)A$, which allows us to prove the result by induction. □

Theorem 2.2.4. *If A is a PID and M is a finitely generated A-module, then there exist $n, m \in \mathbb{N}$ and nonzero elements $e_1, \ldots, e_m \in A \backslash A^\times$ with $e_1 \mid \cdots \mid e_m$ s.t.*

$$M \simeq A^n \oplus A/e_1A \oplus \cdots \oplus A/e_mA.$$

The integers n and m and the ideals (e_i) are uniquely determined by M.

Remark 2.2.5. *Let A be a PID, $d \in A$. The module A/dA may be decomposed as follows: if $d = up_1^{\alpha_1} \cdots p_r^{\alpha_r}$, with the p_i distinct prime elements, $\alpha_i \in \mathbb{N}^*$ and $u \in A^\times$, then by the Chinese Remainder Theorem:*

$$A/dA \simeq A/p_1^{\alpha_1}A \oplus \cdots \oplus A/p_r^{\alpha_r}A.$$

However, one can prove that $A/p^\alpha A$ is indecomposable if p is prime and $\alpha \in \mathbb{N}^*$.

Definition 2.2.6 (Primary parts)**.** *If A is a PID and M is an A-module, then for any prime element $p \in A$, we define the p-*primary part *of M by:*

$$M(p) = \{m \in M,\ \exists \alpha \in \mathbb{N},\ p^\alpha m = 0\}\,.$$

$M(p)$ is a submodule of M.

Remark 2.2.7. *Let A be a PID and $M = A/dA$. Write $d = up_1^{\alpha_1} \cdots p_r^{\alpha_r}$, with the p_i distinct prime elements, $\alpha_i \in \mathbb{N}^*$ and $u \in A^\times$. Then for all $j \in \{1, \ldots, r\}$, $M(p_j) \simeq A/p_j^{\alpha_j} A$. Hence, $M = \bigoplus_{p \text{ prime}} M(p)$.*

Corollary 2.2.8. *If A is a PID and M is a finitely generated A-module, then $M(p) = 0$ for all but finitely many prime elements p, and there exists $n \in \mathbb{N}$ s.t.*

$$M \simeq A^n \oplus \left(\bigoplus_{p \text{ prime}} M(p) \right).$$

Moreover, for every prime element p, there exist $\alpha_1(p) \leq \cdots \leq \alpha_{m(p)}(p)$ s.t.

$$M(p) \simeq \bigoplus_{i=1}^{m(p)} A/p^{\alpha_i(p)} A.$$

The integers n, $m(p)$, $\alpha_i(p)$ are uniquely determined by M.

2.3 Applications: finitely generated abelian groups, reduction of endomorphisms

Theorem 2.3.1. *Let G be a finitely generated abelian group. Then there exist $n, m \in \mathbb{N}$ and integers $d_1, \ldots, d_m \geq 2$ with $d_1 \mid \cdots \mid d_m$ s.t.*

$$G \simeq \mathbb{Z}^n \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z}.$$

Proof. An abelian group is a $\mathbb{Z}$-module, so Theorem 2.2.4 applies. $\square$

Theorem 2.3.2. *Let V be a finite-dimensional vector space over a field k. Let $f \in \operatorname{End}(V)$. Note that V can be seen as a $k[X]$-module by setting $X \cdot v = f(v)$ for $v \in V$.*

(i) *There exist polynomials $D_1, \ldots, D_m \in k[X]$ with $D_1 \mid \cdots \mid D_m$ s.t.*

$$V \simeq k[X]/(D_1) \oplus \cdots \oplus k[X]/(D_m).$$

Note that $k[X]/(D_i)$ is a cyclic subspace for f, for all $i \in \{1, \ldots, m\}$.

(ii) *The ideals $(D_1), \ldots, (D_m)$ are the nonunit invariant factors of $(X \operatorname{Id} - M) \in M_d(k[X])$, where M is the matrix of f in a basis of V.*

Proof. (i) The $k[X]$-module V is finitely generated because V is a finitely generated k-module. Moreover, according to the Cayley-Hamilton Theorem (Theorem 1.8.3), $M = M_{\text{tor}}$, which gives the result using Theorem 2.2.4. (ii) Let $v_1, \ldots, v_d$ be a basis of V, let $M = (m_{ij})_{1 \leq i,j \leq d} = \operatorname{Mat}(f)$. Consider a free $k[X]$-module W of rank d; write $W = \bigoplus_{i=1}^d k[X]\omega_i$ for some $(\omega_1, \ldots, \omega_d) \in W^d$. For $i \in \{1, \ldots, d\}$, set:

$$n_i = X\omega_i - \sum_{j=1}^d m_{ji}\omega_j \in W.$$

Consider $N = (n_1, \ldots, n_d) \subseteq W$. Now, define a map $\pi : W \to V$ by $\pi\left(\sum_{i=1}^d P_i(X)\omega_i\right) = \sum_{i=1}^d P_i(f)v_i$. The map π is $k[X]$-linear, and we claim that the sequence $0 \to N \to W \xrightarrow{\pi} V \to 0$ is exact. The surjectivity of π is clear since $\pi(\omega_i) = v_i$ for $i \in \{1, \ldots, d\}$. Moreover, for $i \in \{1, \ldots, d\}$, $\pi(n_i) = 0$ because $M = \operatorname{Mat}(f)$. Hence, $N \subseteq \operatorname{Ker}\pi$. Conversely, let $w \in \operatorname{Ker}\pi$. As $w \in W$, there exist $n \in N$ and $(a_1, \ldots, a_d) \in k^d$ s.t. $w = n + \sum_{i=1}^d a_i\omega_i$. But $w \in \operatorname{Ker}\pi$, and $n \in N \subseteq \operatorname{Ker}\pi$, so $0 = \pi\left(\sum_{i=1}^d a_i\omega_i\right) = \sum_{i=1}^d a_i v_i$. Hence, $a_i = 0$ for all $i \in \{1, \ldots, d\}$, and $w = n \in N$. This proves that the sequence $0 \to N \to W \xrightarrow{\pi} V \to 0$ is exact. Therefore, $V \simeq W/N$, so N is free of rank d and $N = \bigoplus_{i=1}^d k[X]\left(X\omega_i - \sum_{j=1}^d m_{ji}\omega_j\right)$. Now, note that $(X \operatorname{Id} - M)$ is the matrix of $\left(X\omega_i - \sum_{j=1}^d m_{ji}\omega_j\right)_{1 \leq i \leq d} \in W^d$ in the basis $(\omega_i)_{1 \leq i \leq d}$. $\square$

Remark 2.3.3. *With the notations of Theorem 2.3.2, D_m is the minimal polynomial of f and $D_1 \cdots D_m$ is its characteristic polynomial.*

Corollary 2.3.4. *Let k be a field and $A, B \in M_d(k)$. Then A and B are similar* iff $(X \operatorname{Id} - A)$ *and* $(X \operatorname{Id} - B)$ *are equivalent in $M_d(k[X])$.*

Corollary 2.3.5 (Jordan normal form of an endomorphism)**.** *Let V be a finite-dimensional vector space over an algebraically closed field k. Let $f \in \operatorname{End}(V)$. Then there exist $\lambda_1, \ldots, \lambda_s \in k$ s.t. $V = \bigoplus_{i=1}^s V_{\lambda_i}$, with V_{λ_i} stable by f and s.t. the matrix of the endomorphism induced by f in some basis of V_{λ_i} is:*

$$\begin{pmatrix} \lambda_i & 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \lambda_i \end{pmatrix}.$$

Proof. View V as a $k[X]$ module and use Corollary 2.2.8. Use the fact that the matrix above is the matrix of multiplication by X in the basis $\left((X-\lambda)^i\right)_{0 \leq i \leq \alpha - 1}$ of $k[X]/(X-\lambda)^\alpha$. □

2.4 Projective modules

Definition 2.4.1 (Projective module)**.** *A module P is said to be* projective *if for every surjective linear map $f : N_1 \to N_2$ between modules, the induced map $f_* : \operatorname{Hom}(P, N_1) \to \operatorname{Hom}(P, N_2)$ is also surjective.*

Example 2.4.2. *Free modules are always projective.*

Definition 2.4.3 (Split sequence)**.** *Consider an exact sequence $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$. The following assertions are equivalent:*

(i) *There exists a linear map $r : P \to N$ s.t. $g \circ r = \mathrm{id}_P$.*

(ii) *There exists $P' \subseteq N$ s.t. $N = f(M) \oplus P'$.*

In this case, we say the the sequence is split*.*

Proof. (i) $\Rightarrow$ (ii) Take $P' = r(P)$. (ii) $\Rightarrow$ (i) Note that g induces an isomorphism $\widetilde{g} : P' \to P$, so take $r = \widetilde{g}^{-1} : P \to P' \subseteq N$. □

Theorem 2.4.4. *Let P be a module over a ring A. The following assertions are equivalent:*

(i) *P is projective.*

(ii) *Every exact sequence $0 \to M \to N \to P \to 0$ is split.*

(iii) *There exists an A-module R s.t. $P \oplus R$ is free.*

Proof. (i) $\Rightarrow$ (ii) Consider an exact sequence $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$. Note that $g : N \to P$ is surjective, and P is projective, so $g_* : \operatorname{Hom}(P, N) \to \operatorname{Hom}(P, P)$ is surjective. Hence, there exists $r \in \operatorname{Hom}(P, N)$ s.t. $g_*(r) = \mathrm{id}_P$, i.e. $g \circ r = \mathrm{id}_P$. Hence, the sequence is split. (ii) $\Rightarrow$ (iii) Note that every module is the quotient of a free module, because every module has a (possibly infinite) generating family. Therefore, there exists a free module L and a surjective map $g : L \to P$. Hence, we get an exact sequence $0 \to \operatorname{Ker} g \to L \xrightarrow{g} P \to 0$. Since this exact sequence splits, we get $L = r(P) \oplus \operatorname{Ker} g \simeq P \oplus \operatorname{Ker} g$, with $r : P \to N$ s.t. $g \circ r = \mathrm{id}_P$. (iii) $\Rightarrow$ (i) Let R be an A-module s.t. $L = R \oplus P$ is free. Consider a surjective map $g : N_1 \to N_2$. We know that L is projective (because L is free), so the induced map $\operatorname{Hom}(L, N_1) \to \operatorname{Hom}(L, N_2)$ is surjective. But $\operatorname{Hom}(L, N_1) \simeq \operatorname{Hom}(R, N_1) \oplus \operatorname{Hom}(P, N_1)$ and $\operatorname{Hom}(L, N_2) \simeq \operatorname{Hom}(R, N_2) \oplus \operatorname{Hom}(P, N_2)$, so the map $\operatorname{Hom}(P, N_1) \to \operatorname{Hom}(P, N_2)$ is also surjective and P is projective. □

Remark 2.4.5. *If P is a finitely generated projective module, the above proof shows the existence of a module R s.t. $P \oplus R$ is free of finite rank. In particular, over a PID, a module is projective and finitely generated* iff *it is free of finite rank.*

Example 2.4.6. *The following modules are projective but not free:*

(i) *$\mathbb{Z}/2\mathbb{Z}$ is a projective $\mathbb{Z}/6\mathbb{Z}$-module that is not free (because $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$).*

(ii) *If M and N are free A- and B-modules respectively, then $M \times N$ is a projective $A \times B$ module, and it is free* iff $\operatorname{rk}_A M = \operatorname{rk}_B N$.

(iii) *Let $A = \mathbb{Z}\left[\sqrt{-5}\right]$, $P = \left(3, 1+\sqrt{-5}\right) \subseteq A$, $R = \left(3, 1-\sqrt{-5}\right)$. We have $P + R = A$, $P \cap R = 3A$. Therefore, we have an exact sequence $0 \to 3A \to P \oplus R \to A \to 0$. This sequence is split because A is projective over itself. Hence, $P \oplus R \simeq A^2$, so P and R are projective. However, P and R are not free.*

(iv) *Let $A = \mathcal{C}^0(\mathbb{S}^n, \mathbb{R})$. Choose an orthonormal basis of $\mathbb{R}^{n+1}$ and let $\hat{x}_0, \ldots, \hat{x}_n : \mathbb{R}^{n+1} \to \mathbb{R}$ denote the associated coordinate functions. For $i \in \{0, \ldots, n\}$, set $x_i = \hat{x}_i \circ j \in A$, where $j : \mathbb{S}^n \to \mathbb{R}^{n+1}$ is the inclusion. Now let $e = (x_0, \ldots, x_n) \in A^{n+1}$ and $P = \{v \in A^{n+1}, \langle v \mid e \rangle = 0\}$. The A-module P is projective because $A^{n+1} = P \oplus Ae$. If P is free, then it must be of rank n, so there must exist $v_1, \ldots, v_n \in A^{n+1}$ s.t. $P = Av_1 \oplus \cdots \oplus Av_n$. Therefore, $A^{n+1} = Av_1 \oplus \cdots \oplus Av_n \oplus Ae$. By fixing $s \in \mathbb{S}^n$ and applying the map $f \in A \mapsto f(s) \in \mathbb{R}$, we get $\mathbb{R}^{n+1} = \mathbb{R}v_1(s) \oplus \cdots \oplus \mathbb{R}v_n(s) \oplus \mathbb{R}e(s)$. In particular, $v_1(s) \neq 0$ for every $s \in \mathbb{S}^n$, and $v_1(s) \in s^\perp$, so v_1 is a nonvanishing continuous vector field on $\mathbb{S}^n$. This is impossible when n is even, due to the Hairy Ball Theorem.*

3 Tensor products

3.1 Universal property of the tensor product

Theorem 3.1.1 (Existence of the tensor product)**.** *Let M and N be two A-modules. There exists an A-module $M \otimes N$ (sometimes written $M \otimes_A N$) together with a bilinear map $t : M \times N \to M \otimes N$ satisfying the following universal property: for any A-module P, the map $f \in \operatorname{Hom}(M \otimes N, P) \longmapsto f \circ t \in \operatorname{Bil}(M \times N, P)$ is an isomorphism of A-modules. Moreover, the module $M \otimes N$ is uniquely determined by this property, i.e. if X is an A-module together with a bilinear map $u : M \times N \to X$ satisfying the same universal property, then there exists a unique isomorphism $\varphi : X \to M \otimes N$ s.t. $t = \varphi \circ u$.*

Proof. Let L be the free A-module whose basis is $([m,n])_{(m,n) \in M \times N}$, i.e. $L = \bigoplus_{(m,n) \in M \times N} A[m,n]$. Let R be the submodule of L generated by elements of the form $[a_1 m_1 + a_2 m_2, n] - a_1 [m_1, n] - a_2 [m_2, n]$ or $[m, b_1 n_1 + b_2 n_2] - b_1 [m, n_1] - b_2 [m, n_2]$ for $a_1, a_2, b_1, b_2 \in A$, $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$. Set $M \otimes N = L/R$ and define $m \otimes n$ to be the class of $[m,n]$ in L/R for $(m,n) \in M \times N$. Hence, define a bilinear map $t : (m,n) \in M \times N \longmapsto m \otimes n \in M \otimes N$. If P is an A-module, the map $\Psi : f \in \operatorname{Hom}(M \otimes N, P) \longmapsto f \circ t \in \operatorname{Bil}(M \times N, P)$ is A-linear; let us prove that it is an isomorphism. The injectivity comes from the fact that $(m \otimes n)_{(m,n) \in M \times N}$ is a generating family for $M \otimes N$. For the surjectivity, let $g \in \operatorname{Bil}(M \times N, P)$. Define $\widetilde{f} : L \to P$ by $\widetilde{f}([m,n]) = g(m,n)$ for $(m,n) \in M \times N$. We have $R \subseteq \operatorname{Ker} \widetilde{f}$ because g is bilinear; therefore, there exists $f : M \otimes N \to P$ s.t. $\widetilde{f} = f \circ \pi$, where $\pi : L \to L/R = M \otimes N$ is the projection. Hence, $g = f \circ t$. This proves that $(M \otimes N, t)$ satisfies the universal property. Let (X, u) be another pair satisfying the same universal property. Since $t \in \operatorname{Hom}(M \times N, M \otimes N)$, there exists $f \in \operatorname{Hom}(X, M \otimes N)$ s.t. $t = f \circ u$. Likewise, there exists $g \in \operatorname{Hom}(M \otimes N, X)$ s.t. $u = g \circ t$. Note that $f \circ g \circ t = t$, so $f \circ g = \mathrm{id}_{M \otimes N}$ by the universal property. Likewise, $g \circ f = \mathrm{id}_X$, so $f : X \to M \otimes N$ is an isomorphism and $t = f \circ u$. $\square$

Example 3.1.2.

(i) $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = 0$ *because* $\forall (a,b) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Q}$, $a \otimes b = na \otimes \frac{b}{n} = 0$.

(ii) $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(m \wedge n)\mathbb{Z}$.

(iii) $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z} = \mathbb{Q}$.

(iv) $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}$.

Remark 3.1.3. *Let M and N be two A-modules.*

(i) *If* $\mathrm{Bil}(M \times N, P) = 0$ *for every A-module P, then $M \otimes N = 0$.*

(ii) *If M is generated by $(m_i)_{i \in I}$ and N is generated by $(n_j)_{j \in J}$, then $M \otimes N$ is generated by $(m_i \otimes n_j)_{(i,j) \in I \times J}$. In particular, if M and N are finitely generated, then so is $M \otimes N$.*

Vocabulary 3.1.4. *Let M and N be two A-modules. Elements of the form $m \otimes n \in M \otimes N$, for $(m,n) \in M \times N$, are called* simple tensors. *If $x \in M \otimes N$, the* rank *of x is the smallest integer r s.t. x can be written as the sum of r simple tensors.*

Proposition 3.1.5. *Let $M, N, P, (M_i)_{i \in I}$ be A-modules.*

(i) $M \otimes N = N \otimes M$.

(ii) $M \otimes A = M$.

(iii) $\left(\bigoplus_{i \in I} M_i\right) \otimes N = \bigoplus_{i \in I} (M_i \otimes N)$.

(iv) $\mathrm{Hom}\,(M \otimes N, P) = \mathrm{Hom}\,(M, \mathrm{Hom}\,(N, P))$.

(v) $(M \otimes N) \otimes P = M \otimes (N \otimes P)$.

Remark 3.1.6. *If M, N, P are A-modules, we shall write $M \otimes N \otimes P = (M \otimes N) \otimes P = M \otimes (N \otimes P)$. The A-module $M \otimes N \otimes P$ has a universal property w.r.t. multilinear maps on $M \times N \times P$.*

Corollary 3.1.7. *The tensor product of two free A-modules is a free A-module.*

Corollary 3.1.8. *The tensor product of two projective A-modules is a projective A-module.*

Proof. If M and N are projective A-modules, then there exist A-modules M' and N' s.t. $M \oplus M'$ and $N \oplus N'$ are free. Therefore $(M \oplus M') \otimes (N \oplus N')$ is free. But:

$$(M \oplus M') \otimes (N \oplus N') = (M \otimes N) \oplus (M \otimes N') \oplus (M' \otimes N) \oplus (M' \otimes N').$$

Therefore, $M \otimes N$ is projective. □

3.2 Tensor products, exact sequences and quotients

Proposition 3.2.1. *If $M' \to M \to M'' \to 0$ is an exact sequence and N is a module, then the following sequence is exact:*

$$M' \otimes N \to M \otimes N \to M'' \otimes N \to 0.$$

In particular, $\frac{M}{\operatorname{Im} M'} \otimes N = \frac{M \otimes N}{\operatorname{Im}(M' \otimes N)}$.

Proof. Let P be an A-module. Applying Proposition 1.2.6, we see that the sequence:

$$0 \to \mathrm{Hom}\,(M'', \mathrm{Hom}(N,P)) \to \mathrm{Hom}\,(M, \mathrm{Hom}(N,P)) \to \mathrm{Hom}\,(M', \mathrm{Hom}(N,P))$$

is exact. But this sequence can be rewritten as:

$$0 \to \mathrm{Hom}\,(M'' \otimes N, P) \to \mathrm{Hom}\,(M \otimes N, P) \to \mathrm{Hom}\,(M' \otimes N, P).$$

Proposition 1.2.6 applied in the other direction now tells us that $M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$ is exact. □

Remark 3.2.2. *Even if a linear map $M' \to M$ between A-modules is injective, the induced map $M' \otimes N \to M \otimes N$ may not be injective for an A-module N. For example, the inclusion $2\mathbb{Z} \to \mathbb{Z}$ is injective but the induced map $2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$ is zero.*

Corollary 3.2.3. *Let M be an A-module. If I is an ideal of A, then:*

$$A/I \otimes M = M/IM.$$

Proof. We have an exact sequence $I \xrightarrow{j} A \xrightarrow{\pi} A/I \to 0$, which induces an exact sequence $I \otimes M \xrightarrow{\widetilde{j}} M \xrightarrow{\widetilde{\pi}} A/I \otimes M \to 0$. Since $\operatorname{Im} \widetilde{j} = IM$, we obtain $A/I \otimes M = M/IM$. $\square$

Corollary 3.2.4. *If I and J are two ideals of A, then:*

$$A/I \otimes A/J = A/(I+J).$$

Corollary 3.2.5. *If $K \xrightarrow{i} M \to P \to 0$ and $L \xrightarrow{j} N \to Q \to 0$ are two exact sequences, then the following sequence is exact:*

$$(K \otimes N) \oplus (M \otimes L) \xrightarrow{i \otimes \mathrm{id} \oplus \mathrm{id} \otimes j} M \otimes N \longrightarrow P \otimes Q \longrightarrow 0.$$

In particular, $\frac{M}{\operatorname{Im} K} \otimes \frac{N}{\operatorname{Im} L} = \frac{M \otimes N}{\operatorname{Im}(K \otimes N) + \operatorname{Im}(M \otimes L)}$.

Definition 3.2.6 (Flat module)**.** *An A-module P is said to be* flat *if for every injective map $M' \to M$, the induced map $P \otimes M' \to P \otimes M$ is still injective.*

Example 3.2.7. *Any free module is flat.*

Proposition 3.2.8. *Projective modules are flat.*

Proof. Use the fact that projective modules are direct summands of free modules. $\square$

3.3 Tensor products of homomorphisms

Definition 3.3.1 (Tensor product of homomorphisms)**.** *If $f : M_1 \to M_2$ and $g : N_1 \to N_2$ are homomorphisms of A-modules, then there exists a unique homomorphism $(f \otimes g) : M_1 \otimes N_1 \to M_2 \otimes N_2$ s.t.*

$$\forall\, (m,n) \in M_1 \times N_1,\ (f \otimes g)\,(m \otimes n) = f(m) \otimes g(n).$$

Remark 3.3.2. *Let M_1, M_2, N_1, N_2 be A-modules. The tensor product of homomorphisms defines a bilinear map $\widetilde{h} : \operatorname{Hom}(M_1, M_2) \times \operatorname{Hom}(N_1, N_2) \longrightarrow \operatorname{Hom}(M_1 \otimes N_1, M_2 \otimes N_2)$, which induces a linear map:*

$$h : \operatorname{Hom}(M_1, M_2) \otimes \operatorname{Hom}(N_1, N_2) \longrightarrow \operatorname{Hom}(M_1 \otimes N_1, M_2 \otimes N_2)\,.$$

In general, h has no reason to be either injective or surjective, but we shall see some cases in which it is.

Proposition 3.3.3. *Let M_1, M_2, N_1, N_2 be A-modules. Assume that M_1 and N_1 (resp. M_1 and M_2) are free of finite rank. Then the map $h : \operatorname{Hom}(M_1, M_2) \otimes \operatorname{Hom}(N_1, N_2) \longrightarrow \operatorname{Hom}(M_1 \otimes N_1, M_2 \otimes N_2)$ is an isomorphism.*

Proof. Prove it firstly for $M_1 = N_1 = A$ (resp. $M_1 = M_2 = A$). $\square$

Remark 3.3.4. *Let M_1, M_2, N_1, N_2 be free A-modules of finite rank equipped with bases. Let $f \in \operatorname{Hom}(M_1, M_2)$ and $g \in \operatorname{Hom}(N_1, N_2)$. If $A = (a_{ij})_{\substack{1 \le i \le n \\ 1 \le j \le p}} = \operatorname{Mat}(f)$ and $B = \operatorname{Mat}(g)$, then in appropriate bases of $M_1 \otimes N_1$ and $M_2 \otimes N_2$, we have:*

$$\operatorname{Mat}(f \otimes g) = \begin{bmatrix} a_{11}B & \cdots & a_{1p}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \cdots & a_{np}B \end{bmatrix}.$$

This matrix will be denoted by $A \otimes B$.

Corollary 3.3.5. *Let M be a free A-module of finite rank. Then, for any A-module N, the map:*

$$h : M^\vee \otimes N \longrightarrow \mathrm{Hom}\,(M, N)$$

is an isomorphism.

Proposition 3.3.6. *Let V and W be two vector spaces over a field k. We have an isomorphism $\psi : V^\vee \otimes W \to \mathrm{Hom}\,(V, W)$. If $f \in \mathrm{Hom}\,(V, W)$, then the rank of f as a linear map is equal to the rank of $\psi^{-1}(f) \in V^\vee \otimes W$ (c.f. Vocabulary 3.1.4).*

Proof. Let $t = \psi^{-1}(f)$. Let us show that $\mathrm{rk}\, f = \mathrm{rk}\, t$. ($\leq$) Write $t = \sum_{i=1}^r f_i \otimes w_i$, with $r = \mathrm{rk}\, t$, $f_1, \ldots, f_r \in V^\vee$, $w_1, \ldots, w_r \in W$. Then:

$$\forall v \in V,\ f(v) = \sum_{i=1}^r f_i(v) w_i.$$

Therefore, $\mathrm{Im}\, f \subseteq \mathrm{Vect}\,(w_1, \ldots, w_r)$ and $\mathrm{rk}\, f \leq r = \mathrm{rk}\, t$. ($\geq$) Let $(w_i)_{1 \leq i \leq r}$ be a basis of $\mathrm{Im}\, f$. For $i \in \{1, \ldots, r\}$, let $p_i : \mathrm{Im}\, f \to \mathbb{R}$ be the i-th coordinate function associated to the basis $(w_i)_{1 \leq i \leq r}$. Hence, $t = \sum_{i=1}^r (p_i \circ f) \otimes w_i$, so $\mathrm{rk}\, t \leq r = \mathrm{rk}\, f$. □

Proposition 3.3.7. *Let M_1, M_2, N_1, N_2 be A-modules. Assume that M_1 and N_1 (resp. M_1 and M_2) are finitely generated and projective. Then the map $h : \mathrm{Hom}\,(M_1, M_2) \otimes \mathrm{Hom}\,(N_1, N_2) \longrightarrow \mathrm{Hom}\,(M_1 \otimes N_1, M_2 \otimes N_2)$ is an isomorphism.*

Proof. Use Proposition 3.3.3 and the fact that finitely generated projective modules are direct summands of free modules of finite type. □

Remark 3.3.8. *If M is a finitely generated, projective module, then we have an isomorphism $M^\vee \otimes M \simeq \mathrm{End}(M)$. On $M^\vee \otimes M$, there is a linear* trace *map* $\mathrm{tr} : M^\vee \otimes M \to \mathbb{R}$ *induced by the bilinear map $(f, x) \in M^\vee \times M \longmapsto f(x) \in \mathbb{R}$. Hence, with the isomorphism $M^\vee \otimes M \simeq \mathrm{End}(M)$, we have a trace map $\mathrm{tr} : \mathrm{End}(M) \to \mathbb{R}$, which is a generalisation of the trace for endomorphisms of free modules of finite rank.*

3.4 Extension of scalars

Definition 3.4.1 (Restriction of scalars)**.** *Let $f : A \to B$ be a ring homomorphism (e.g. an inclusion map). Any B-module N can be seen as an A-module by setting $a \cdot n = f(a) \cdot n$, for $a \in A$ and $n \in N$.*

Definition 3.4.2 (Extension of scalars)**.** *Let $f : A \to B$ be a ring homomorphism. The ring B itself can be seen as an A-module by restriction of scalars; therefore, $B \otimes_A M$ is an A-module, that can also be seen as a B-module by setting $b \cdot (b' \otimes m) = (bb') \otimes m$ for $b, b' \in B$ and $m \in M$.*

Example 3.4.3. *Let M be a $\mathbb{Z}$-module and assume that $M = \mathbb{Z}^r \oplus M_{\mathrm{tors}}$ for some $r \in \mathbb{N}$. Then $\mathbb{Q} \otimes_{\mathbb{Z}} M$ is the $\mathbb{Q}$-vector space $\mathbb{Q}^r$.*

Proposition 3.4.4. *Let $f : A \to B$ be a ring homomorphism. If M is an A-module and N is a B-module, then:*

$$\mathrm{Hom}_A(M, N) \simeq \mathrm{Hom}_B\,(B \otimes_A M, N) \qquad \text{(as } B\text{-modules).}$$

Lemma 3.4.5. *Let $f : A \to B$ be a ring homomorphism. If M is an A-module and N is a B-module, then:*

$$M \otimes_A N \simeq (B \otimes_A M) \otimes_B N \qquad \text{(as } B\text{-modules).}$$

Corollary 3.4.6. *Let $f : A \to B$ be a ring homomorphism. If P is a flat A-module, then $B \otimes_A P$ is a flat B-module.*

3.5 Tensor product of algebras over a ring

Vocabulary 3.5.1 (A-algebra)**.** *If $f : A \to B$ is a ring homomorphism, we say that B is an A-algebra.*

Proposition 3.5.2. *If M and N are two A-algebras, then $M \otimes_A N$ is also an A-algebra.*

Example 3.5.3. *If B is an A-algebra, then:*

$$B \otimes_A A[X] = B[X].$$

In particular, $A[X] \otimes_A A[Y] = A[X, Y]$.

Example 3.5.4. *If X is a topological space, then:*

$$\mathbb{C} \otimes_{\mathbb{R}} \mathcal{C}^0 (X, \mathbb{R}) = \mathcal{C}^0 (X, \mathbb{C}) .$$

Example 3.5.5. *Let X and Y be two topological spaces. Then there exists a map:*

$$m : \mathcal{C}^0 (X, \mathbb{R}) \otimes_{\mathbb{R}} \mathcal{C}^0 (Y, \mathbb{R}) \longrightarrow \mathcal{C}^0 (X \times Y, \mathbb{R}) ,$$

given by $m(f \otimes g)(x, y) = f(x)g(y)$, and this map is injective.

Example 3.5.6. *Let K and L be two finite extensions of a field F of characteristic 0. By the Primitive Element Theorem, there exists $\alpha \in L$ s.t. $L = F(\alpha)$. If μ_α is the minimal polynomial of α over F, then $L = F[X]/ (\mu_\alpha)$, so:*

$$K \otimes_F L = K[X]/ (\mu_\alpha) .$$

Hence, if $\mu_\alpha = P_1 \cdots P_r$, where $P_1, \ldots, P_r$ are irreducible over K, then:

$$K \otimes_F L = \bigoplus_{1 \leq i \leq r} K[X]/ (P_i) .$$

Thus, $K \otimes_F L$ can be written as a direct sum of extensions of K.

3.6 Flat modules

Definition 3.6.1 (Flat module)**.** *An A-module P is said to be* flat *if for every injective map $M' \to M$, the induced map $P \otimes M' \to P \otimes M$ is still injective.*

Proposition 3.6.2.

(i) *Projective modules are flat.*

(ii) *If P_1 and P_2 are two flat modules, then $P_1 \oplus P_2$ and $P_1 \otimes P_2$ are flat.*

Proposition 3.6.3. *Let P be a flat A-module.*

(i) *If I is an ideal of A, then the map $I \otimes P \to IP$ is an isomorphism.*

(ii) *If A is an integral domain, then P is torsion-free.*

Definition 3.6.4 (Flat module for a specific module)**.** *Let M and P be two modules. We say that P is* flat for M *if for every submodule $M' \subseteq M$, the map $M' \otimes P \to M \otimes P$ is injective.*

Remark 3.6.5. *A module is flat* iff *it is flat for every module.*

Lemma 3.6.6. *If a module P is flat for a module M, then it is also flat for every quotient of M.*

Proof. Write an exact sequence $0 \to K \to M \xrightarrow{\pi} N \to 0$. We want to show that P is flat for N. Hence, let $N' \subseteq N$ be a submodule; set $M' = \pi^{-1} (N')$. We have the following commutative diagram (with the horizontal and vertical sequences exact):

$$
\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & K \arrow[r] \arrow[d, "="'] & M' \arrow[r, "\pi"] \arrow[d, "\subseteq"'] & N' \arrow[r] \arrow[d, "\subseteq"'] & 0 \\
0 \arrow[r] & K \arrow[r] & M \arrow[r, "\pi"] & N \arrow[r] & 0
\end{tikzcd}
$$

After taking the tensor product with P, we obtain:

$$
\begin{tikzcd}
 & 0 \arrow[d] & & \\
P \otimes K \arrow[r] \arrow[d, "="'] & P \otimes M' \arrow[r] \arrow[d] & P \otimes N' \arrow[r] \arrow[d] & 0 \\
P \otimes K \arrow[r] & P \otimes M \arrow[r] & P \otimes N \arrow[r] & 0
\end{tikzcd}
$$

Note that the arrow $P \otimes M' \to P \otimes M$ is injective because P is flat for M by assumption. Now, using this diagram, we show that the arrow $P \otimes N' \to P \otimes N$ is also injective as wanted. $\square$

Lemma 3.6.7. *If a module P is flat for two modules M_1 and M_2, then it is also flat for $M_1 \oplus M_2$.*

Proof. Let $M = M_1 \oplus M_2$ and let M' be a submodule of M. Write $M'_1 = M' \cap M_1$ and $M'_2 = M' \cap M_2$. We have the following commutative diagram (with the horizontal and vertical sequences exact):

$$
\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & M'_1 \arrow[r] \arrow[d, "\subseteq"'] & M' \arrow[r] \arrow[d, "\subseteq"'] & M'_2 \arrow[r] \arrow[d, "\subseteq"'] & 0 \\
0 \arrow[r] & M_1 \arrow[r] & M \arrow[r] & M_2 \arrow[r] & 0
\end{tikzcd}
$$

After taking the tensor product with P, we obtain:

$$
\begin{tikzcd}
 & 0 \arrow[d] & & 0 \arrow[d] & \\
 & P \otimes M'_1 \arrow[r] \arrow[d] & P \otimes M' \arrow[r] \arrow[d] & P \otimes M'_2 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & P \otimes M_1 \arrow[r] & P \otimes M \arrow[r] & P \otimes M_2 \arrow[r] & 0
\end{tikzcd}
$$

Note that the arrows $P \otimes M'_1 \to P \otimes M_1$ and $P \otimes M'_2 \to P \otimes M_2$ are injective because P is flat for M_1 and M_2 by assumption; moreover, the arrow $P \otimes M_1 \to P \otimes M$ is injective because $P \otimes M = P \otimes (M_1 \oplus M_2) = (P \otimes M_1) \oplus (P \otimes M_2)$. Now, using this diagram, we show that the arrow $P \otimes M' \to P \otimes M$ is also injective as wanted. $\square$

Lemma 3.6.8. *If a module P is flat for each module in a family $(M_i)_{i \in I}$, then it is also flat for $\bigoplus_{i \in I} M_i$.*

Proof. Note that by induction, Lemma 3.6.7 gives the result when I is finite. Now, write $M = \bigoplus_{i \in I} M_i$ and let $M' \subseteq M$ be a submodule. Let $f : P \otimes M' \to P \otimes M$ be the map induced by the inclusion $M' \subseteq M$. Let $x' \in \operatorname{Ker} f$; we want to show that $x' = 0$. Write:

$$x' = \sum_{i=1}^{r} p_i \otimes m_i,$$

with $p_1, \ldots, p_r \in P$, $m_1, \ldots, m_r \in M'$. Let $M'' = (m_1, \ldots, m_r) \subseteq M'$ and set $x'' = \sum_{i=1}^r p_i \otimes m_i \in P \otimes M''$. The inclusion $M'' \subseteq M'$ induces a map $j : P \otimes M'' \to P \otimes M'$ and we have $x' = j(x'')$. Moreover, as M'' is finitely generated, there exists a finite subset $J \subseteq I$ s.t. $M'' \subseteq \bigoplus_{j \in J} M_j = M_{\text{finite}}$. Since M_{finite} is a direct summand of M, the map $P \otimes M_{\text{finite}} \to P \otimes M$ is injective; moreover, by Lemma 3.6.7, the map $P \otimes M'' \to P \otimes M_{\text{finite}}$ is injective. Hence, by composition, the map $i : P \otimes M'' \to P \otimes M$ is injective. Therefore, since $i(x'') = f(x') = 0$, we obtain $x'' = 0$, and $x' = j(x'') = 0$ as wanted. □

Theorem 3.6.9. *Let P be an A-module. The following assertions are equivalent:*

(i) *P is flat.*

(ii) *P is flat for A, i.e. the map $I \otimes P \to P$ is injective for every ideal I of A.*

Proof. Use Remark 3.6.5, Lemma 3.6.8 and Lemma 3.6.6, as well as the fact that every module can be written as the quotient of a free module. □

3.7 Flatness and relations

Definition 3.7.1 (Relations)**.** *Let M be an A-module. A* relation *in M is an equation $\sum_{i=1}^r f_i m_i = 0$, with $f_1, \ldots, f_r \in A$ and $m_1, \ldots, m_r \in M$. This relation is said to be* trivial *if there exist $(a_{ij})_{\substack{1 \le i \le r \\ 1 \le j \le s}} \in A^{r \times s}$ and $y_1, \ldots, y_s \in M$ s.t. $m_i = \sum_{j=1}^s a_{ij} y_j$ for all i and $0 = \sum_{i=1}^r f_i a_{ij}$ for all j.*

Example 3.7.2. *Consider $A = k[X, Y]$, where k is a field. The relation $Y \cdot X - X \cdot Y = 0$ is trivial in A but not in the submodule $M = (X, Y)$.*

Proposition 3.7.3. *An A-module M is flat* iff *every relation in M is trivial.*

Proof. ($\Leftarrow$) Assuming that every relation in M is trivial, show that the map $I \otimes M \to M$ is injective for any ideal $I \subseteq A$ and apply Theorem 3.6.9. ($\Rightarrow$) Assume that M is flat and consider a relation $\sum_{i=1}^r f_i m_i = 0$ in M. Let $I = (f_1, \ldots, f_r) \subseteq A$. We have a natural surjective map $A^r \to I$, of kernel $N = \left\{(a_i)_{1 \le i \le r} \in A^r,\ \sum_{i=1}^r a_i f_i = 0\right\}$. Now, as M is flat, note that the exact sequence $0 \to N \to A^r \to I \to 0$ induces an exact sequence:

$$0 \to M \otimes N \to M^r \xrightarrow{\pi} M \otimes I \to 0$$

Since M is flat, the map $M \otimes I \to M$ is injective, which proves that $\sum_{i=1}^r m_i \otimes f_i = 0$, so $(m_i)_{1 \le i \le r} \in \operatorname{Ker} \pi = \operatorname{Im}(M \otimes N)$. Therefore, there exist $(a_{i1})_{1 \le i \le r}, \ldots, (a_{is})_{1 \le i \le r} \in N$ and $y_1, \ldots, y_s \in M$ s.t. $\sum_{j=1}^s y_j \otimes (a_{1j}, \ldots, a_{rj}) = (m_i)_{1 \le i \le r}$. Hence, the relation $\sum_{i=1}^r f_i m_i = 0$ is trivial. □

3.8 Symmetric products

Notation 3.8.1. *If M is an A-module, we write $T^k(M) = \underbrace{M \otimes \cdots \otimes M}_{k \text{ times}}$. For any A-module P, we have a bijection $k\text{-Lin}\left(M^k, P\right) \simeq \operatorname{Hom}\left(T^k(M), P\right)$.*

Definition 3.8.2 (Symmetric multilinear map)**.** *Let M and P be two A-modules. A multilinear map $f \in k\text{-Lin}\left(M^k, P\right)$ is said to be* symmetric *if:*

$$\forall (m_1, \ldots, m_k) \in M^k,\ \forall \sigma \in \mathfrak{S}_k,\ f(m_1, \ldots, m_k) = f\left(m_{\sigma(1)}, \ldots, m_{\sigma(k)}\right).$$

Definition 3.8.3 (Symmetric product)**.** *Let M be an A-module. Let S be the submodule of $T^k(M)$ generated by $\left\{(m_1 \otimes \cdots \otimes m_k) - \left(m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(k)}\right),\ m_1, \ldots, m_k \in M,\ \sigma \in \mathfrak{S}_k\right\}$. We define:*

$$\operatorname{Sym}^k(M) = T^k(M)/S.$$

For $m_1, \ldots, m_k \in M$, we shall denote the image of $m_1 \otimes \cdots \otimes m_k$ in $\operatorname{Sym}^k(M)$ by $m_1 \cdots m_k$ to emphasize commutativity.

Proposition 3.8.4. *Let M and P be two A-module. Then the set of symmetric k-linear maps $M^k \to P$ is in bijection with* $\operatorname{Hom}\left(\operatorname{Sym}^k(M), P\right)$.

Remark 3.8.5. *Let M be an A-module. The map $(v,w) \mapsto v \cdot w$ gives rise to a bilinear map $\operatorname{Sym}^k(M) \times \operatorname{Sym}^\ell(M) \to \operatorname{Sym}^{k+\ell}(M)$. Now, if we define:*

$$\operatorname{Sym}(M) = \bigoplus_{k \in \mathbb{N}} \operatorname{Sym}^k(M),$$

then $\operatorname{Sym}(M)$ *is a ring under the bilinear map defined above, called the* symmetric algebra *of M.*

Proposition 3.8.6. *Let M be an A-module generated by elements $m_1, \ldots, m_n \in M$. Then* $\operatorname{Sym}^k(M)$ *is generated by $\{m_1^{a_1} \cdots m_n^{a_n},\ a_1 + \cdots + a_n = k\}$.*

Lemma 3.8.7. *For $k, n \in \mathbb{N}$, $|\{(a_1, \ldots, a_n) \in \mathbb{N}^n,\ a_1 + \cdots + a_n = k\}| = \binom{n+k-1}{k}$.*

Theorem 3.8.8. *Let M be a free A-module of rank n, equipped with a basis $(m_i)_{1 \le i \le n}$. Then* $\operatorname{Sym}^k(M)$ *is free of rank $\binom{n+k-1}{k}$, with basis $(m_1^{a_1} \cdots m_n^{a_n})_{\substack{(a_1,\ldots,a_n) \in \mathbb{N}^n \\ a_1 + \cdots + a_n = k}}$.*

Proof. Denote $x_1^{a_1} \cdots x_n^{a_n}$ by x^a for $x = (x_i)_{1 \le i \le n} \in M^n$, $a = (a_i)_{1 \le i \le n} \in \mathbb{N}^n$. According to Proposition 3.8.6, it suffices to prove that the family $(m^a)_{\substack{a \in \mathbb{N}^n \\ a_1 + \cdots + a_n = k}}$ is linearly independent. For $a \in \mathbb{N}^n$ with $a_1 + \cdots + a_n = k$, define a multilinear form $f_a \in k\text{-Lin}\left(M^k, A\right)$ by:

$$f_a\left(m_{i_1}, \ldots, m_{i_k}\right) = \begin{cases} 1 & \text{if } \forall \ell \in \{1, \ldots, n\},\ a_\ell = |\{j \in \{1, \ldots, k\},\ i_j = \ell\}| \\ 0 & \text{otherwise} \end{cases}.$$

As $(m_i)_{1 \le i \le n}$ is a basis of M, this defines a (symmetric) k-linear form $f_a : M^k \to A$, which induces a linear map $\widetilde{f}_a : \operatorname{Sym}^k(M) \to A$. For $b \in \mathbb{N}^n$ with $b_1 + \cdots + b_n = k$, we have $\widetilde{f}_a\left(m^b\right) = \delta_{ab}$. Now, if $(\lambda_b)_{\substack{b \in \mathbb{N}^n \\ b_1 + \cdots + b_n = k}}$ is a family of scalars s.t.

$$\sum_{b_1 + \cdots + b_n = k} \lambda_b m^b = 0,$$

then, for all $a \in \mathbb{N}^n$ with $a_1 + \cdots + a_n = k$, we have $\lambda_a = \widetilde{f}_a\left(\sum_{b_1 + \cdots + b_n = k} \lambda_m b^m\right) = 0$. This shows the independence of $(m^a)_{\substack{a \in \mathbb{N}^n \\ a_1 + \cdots + a_n = k}}$. ☐

Corollary 3.8.9. *Let M be a free A-module of rank n, equipped with a basis $(m_i)_{1 \le i \le n}$. Then:*

$$\operatorname{Sym}(M) \simeq A\left[X_1, \ldots, X_n\right],$$

and the isomorphism is given by $m_1^{a_1} \cdots m_n^{a_n} \mapsto X_1^{a_1} \cdots X_n^{a_n}$.

3.9 Alternating products

Definition 3.9.1 (Alternating multilinear map)**.** *Let M and P be two A-modules. A multilinear map $f \in k\text{-Lin}\left(M^k, P\right)$ is said to be* alternating *if:*

$$\forall\left(m_1, \ldots, m_k\right) \in M^k,\ \left(\exists i \neq j,\ m_i = m_j\right) \Longrightarrow f\left(m_1, \ldots, m_k\right) = 0.$$

Lemma 3.9.2. *Let M and P be two A-modules. If a k-linear map $f : M^k \to P$ is alternating, then it is* antisymmetric*, i.e.*

$$\forall\left(m_1, \ldots, m_k\right) \in M^k,\ \forall \sigma \in \mathfrak{S}_k,\ f\left(m_1, \ldots, m_k\right) = \varepsilon(\sigma) f\left(m_{\sigma(1)}, \ldots, m_{\sigma(k)}\right).$$

Remark 3.9.3. *The converse of Lemma 3.9.2 is false in general, but it becomes true if we assume that* $2 \in A^\times$.

Definition 3.9.4 (Alternating product)**.** *Let M be an A-module. Let L be the submodule of $T^k(M)$ generated by $\{m_1 \otimes \cdots \otimes m_k,\ m_1, \ldots, m_k \in M,\ \exists i \neq j,\ m_i = m_j\}$. We define:*

$$\Lambda^k(M) = T^k(M)/L.$$

For $m_1, \ldots, m_k \in M$, we shall denote the image of $m_1 \otimes \cdots \otimes m_k$ in $\Lambda^k(M)$ by $m_1 \wedge \cdots \wedge m_k$ to emphasize anticommutativity.

Proposition 3.9.5. *Let M and P be two A-module. Then the set of alternating k-linear maps $M^k \to P$ is in bijection with* $\mathrm{Hom}\left(\Lambda^k(M), P\right)$.

Lemma 3.9.6. *Let M be an A-module that is generated by n elements. Then $\Lambda^k(M) = 0$ as soon as $k > n$.*

Theorem 3.9.7. *Let M be a free A-module of rank n, equipped with a basis $(m_i)_{1 \leq i \leq n}$. Then $\Lambda^k(M)$ is free of rank $\binom{n}{k}$, with basis $(m_{i_1} \wedge \cdots \wedge m_{i_k})_{1 \leq i_1 < \cdots < i_k \leq n}$.*

Proof. It is clear that $(m_{i_1} \wedge \cdots \wedge m_{i_k})_{1 \leq i_1 < \cdots < i_k \leq n}$ generates $\Lambda^k(M)$; it remains to prove that this family is linearly independent. To do this, we use the same strategy as in Theorem 3.8.8: it suffices to construct a linear form $f_{i_1,\ldots,i_k} : \Lambda^k(M) \to A$ for each sequence $1 \leq i_1 < \cdots < i_k \leq n$ s.t. $f_{i_1,\ldots,i_k}(m_{j_1} \wedge \cdots \wedge m_{j_k}) = \delta_{i_1 j_1} \cdots \delta_{i_k j_k}$ for all $1 \leq j_1 < \cdots < j_k \leq n$. In the particular case where $k = n$, we take the linear form $f_{i_1,\ldots,i_k}$ on $\Lambda^k(M)$ induced by the alternating k-linear form $\det_{(m_{i_1},\ldots,m_{i_k})} : M^k \to A$. Now, assume that $k < n$. For $1 \leq i_1 < \cdots < i_k \leq n$, choose $1 \leq i_{k+1} < \cdots < i_n \leq n$ s.t. $\{1, \ldots, n\} = \{i_\ell,\ \ell \in \{1, \ldots, n\}\}$ and set $y = m_{i_{k+1}} \wedge \cdots \wedge m_{i_n} \in \Lambda^{n-k}(M)$. Now, $x \mapsto x \wedge y$ defines a linear map $\theta : \Lambda^k(M) \to \Lambda^n(M)$, which sends $m_{j_1} \wedge \cdots \wedge m_{j_k}$ to $\pm m_1 \wedge \cdots \wedge m_n$ if $\{j_1, \ldots, j_k\} = \{i_1, \ldots, i_k\}$, 0 otherwise. Hence, by composing this map by the determinant, we obtain the desired map. □

Notation 3.9.8. *Let M be an A-module. Then any map $f \in \mathrm{End}(M)$ induces a map $T^k(f) \in \mathrm{End}\left(T^k(M)\right)$, which induces maps $\mathrm{Sym}^k(f) \in \mathrm{End}\left(\mathrm{Sym}^k(M)\right)$ and $\Lambda^k(f) \in \mathrm{End}\left(\Lambda^k(M)\right)$.*

Proposition 3.9.9. *Let M be a free A-module of rank n, equipped with a basis $(m_i)_{1 \leq i \leq n}$. Let $f \in \mathrm{End}(M)$. Then the matrix of $\Lambda^k(f)$ in the basis $(m_{i_1} \wedge \cdots \wedge m_{i_k})_{1 \leq i_1 < \cdots < i_k \leq n}$ is the matrix of $k \times k$ minors of* $\mathrm{Mat}(f)$.

4 Localisation

4.1 Local rings

Definition 4.1.1 (Local ring)**.** *A ring A is said to be a* local ring *if one of the following two equivalent conditions is satisfied:*

(i) *A has a unique maximal ideal.*

(ii) *$A \backslash A^\times$ is an ideal of A.*

In this case, if I is the unique maximal ideal of A, the quotient A/I is called the residue field *of A. If M is an A-module, then $M/IM = M \otimes_A A/I$ is an (A/I)-vector space.*

Proposition 4.1.2. *Let A be a local ring with maximal ideal I.*

(i) *If M is a finitely generated A-module s.t. $M = IM$, then $M = 0$.*

(ii) *If M is a finitely generated A-module and $m_1, \ldots, m_r \in M$ are s.t. $\overline{m}_1, \ldots, \overline{m}_r \in M/IM$ generate M/IM, then $m_1, \ldots, m_r$ generate M.*

Theorem 4.1.3. *If M is a finitely generated flat module over a local ring A, then M is free.*

Proof. Let $x_1, \ldots, x_n \in M$ whose images in M/IM form a basis of the vector space M/IM over A/I. By Proposition 4.1.2, $x_1, \ldots, x_n$ generate M; it remains to prove that they are linearly independent over A. We shall prove by induction on $r \in \{1, \ldots, n\}$ that $x_1, \ldots, x_r$ are linearly independent, using the fact that every relation in M is trivial (Proposition 3.7.3). If $r = 1$, let $f_1 \in A$ s.t. $f_1 x_1 = 0$. Since this relation is trivial, there exist $y_1, \ldots, y_s \in M$, $a_1, \ldots, a_s \in A$ s.t. $x_1 = a_1 y_1 + \cdots + a_s y_s$ and $f_1 a_j = 0$ for all j. But $\overline{x}_1 \neq 0$, so there exists j s.t. $a_j \notin I$. Therefore, $a_j \in A^\times$, and $f_1 = 0$. This proves the claim for $r = 1$. Assume we have proved the claim for $(r-1)$. Let $f_1, \ldots, f_r \in A$ s.t. $f_1 x_1 + \cdots + f_r x_r = 0$. Since this relation is trivial, there exist $y_1, \ldots, y_s \in M$ and $(a_{ij})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}} \in A^{r \times s}$ s.t. $x_i = \sum_{j=1}^s a_{ij} y_j$ for all i and $0 = \sum_{i=1}^r f_i a_{ij}$ for all j. Now, there exists (i,j) s.t. $a_{ij} \notin I$; we may assume that $a_{11} \notin I$, i.e. $a_{11} \in A^\times$. Now, we get:

$$f_2 \left(x_2 - \frac{a_{21}}{a_{11}} x_1 \right) + \cdots + f_r \left(x_r - \frac{a_{r1}}{a_{11}} x_1 \right) = 0.$$

By induction, we obtain $f_2 = \cdots = f_r = 0$ because $\left(\overline{x_2 - \frac{a_{21}}{a_{11}} x_1} \right), \ldots, \left(\overline{x_r - \frac{a_{r1}}{a_{11}} x_1} \right)$ are linearly independent in M/IM. Therefore, $f_1 = 0$, which proves the claim by induction. □

Corollary 4.1.4. *Over a local ring, a finitely generated module is projective* iff *it is flat* iff *is is free.*

4.2 Localisation of rings

Remark 4.2.1. *If A is an integral domain, then we know how to construct a field* $\mathrm{Frac}(A)$ *equipped with an injective map $j : A \to \mathrm{Frac}(A)$, s.t. for any ring B and for any morphism $\varphi : A \to B$ with $\varphi(A \backslash \{0\}) \subseteq B^\times$, there exists a unique morphism $\psi : \mathrm{Frac}(A) \to B$ s.t. $\varphi = \psi \circ j$.*

Definition 4.2.2. *Let A be a ring and let S be a multiplicative subset of A containing 1 and not containing 0. Define an equivalence relation on $A \times S$ by:*

$$(a_1, s_1) \sim (a_2, s_2) \iff \exists t \in S,\ t(a_1 s_2 - a_2 s_1) = 0.$$

Denote $S^{-1}A = A \times S / \sim$ and write $\frac{a}{s}$ for the class of (a, s) in $S^{-1}A$.

Proposition 4.2.3. *Let A be a ring and let S be a multiplicative subset of A containing 1 and not containing 0. Then the formulas $\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}$ and $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}$ are well-defined on $S^{-1}A$ and make $S^{-1}A$ an A-algebra via the map $\phi_S : a \in A \longmapsto \frac{a}{1} \in S^{-1}A$.*

Proposition 4.2.4. *Let A be a ring and let S be a multiplicative subset of A containing 1 and not containing 0. Then, for any ring B and for any morphism $f : A \to B$ with $\varphi(S) \subseteq B^\times$, there exists a unique morphism $g : S^{-1}A \to B$ s.t. $f = g \circ \phi_S$.*

Lemma 4.2.5. *Let A be a ring and let S be a multiplicative subset of A containing 1 and not containing 0. Consider the canonical map $\phi_S : A \to S^{-1}A$. We have:*

$$\mathrm{Ker}\, \phi_S = \{a \in A,\ \exists s \in S,\ as = 0\}.$$

Example 4.2.6.

(i) *Let A be an integral domain. Then $S = A \backslash \{0\}$ is a multiplicative subset, $S^{-1}A = \mathrm{Frac}(A)$ and ϕ_S is injective.*

(ii) *Let A be a ring and $\mathfrak{p}$ be a prime ideal of A. Then $S = A \backslash \mathfrak{p}$ is a multiplicative subset, and the ring $S^{-1}A$ is denoted by $A_\mathfrak{p}$.*

(iii) *Let A be a ring and $f \in A$ be an element that is not nilpotent. Then $S = \{f^n,\ n \in \mathbb{N}\}$ is a multiplicative subset, the ring $S^{-1}A$ is denoted by A_f and we have $A_f = A[X]/(Xf - 1)$ (which we denote by $A\left[\frac{1}{f}\right]$).*

(iv) *Let K and L be two fields. If $A = K \times L$ and $S = K \times L^\times$, then $S^{-1}A = L$ and $\phi_S : K \times L \to L$ is the projection on L.*

Proposition 4.2.7. *If $\mathfrak{p}$ is a prime ideal of a ring A, then $A_\mathfrak{p}$ is a local ring, with maximal ideal $\mathfrak{m} = \left\{\frac{a}{s},\ a \in \mathfrak{p},\ s \in S\right\}$. Moreover, we have:*

$$A_\mathfrak{p}/\mathfrak{m} = \mathrm{Frac}\,(A/\mathfrak{p})\,.$$

Proof. It is clear that $\mathfrak{m}$ is an ideal of $A_\mathfrak{p}$. Let us prove that $\mathfrak{m} = A_\mathfrak{p} \backslash A_\mathfrak{p}^\times$. ($\supseteq$) Let $\frac{a}{s} \in A_\mathfrak{p}\backslash\mathfrak{m}$, with $a \in A\backslash\mathfrak{p}$ and $s \in S$. Then $a \in S$, so $\frac{s}{a} \in A_\mathfrak{p}$ and $\frac{a}{s} \cdot \frac{s}{a} = 1$, i.e. $\frac{a}{s} \in A_\mathfrak{p}^\times$. ($\subseteq$) Let $\frac{a}{s} \in A_\mathfrak{p}^\times$. Then there exists $\frac{b}{t} \in A_\mathfrak{p}$ s.t. $\frac{a}{s} \cdot \frac{b}{t} = 1$, i.e. there exists $r \in S$ s.t. $r(ab - st) = 0$. Thus, $rab = rst \in S = A\backslash\mathfrak{p}$, and $\mathfrak{p}$ is an ideal so $a \in A\backslash\mathfrak{p}$. Now, it remains to prove that $A_\mathfrak{p}/\mathfrak{m} = \mathrm{Frac}\,(A/\mathfrak{p})$. To do this, consider the natural projection $\pi : A \to A/\mathfrak{p}$. As $A/\mathfrak{p}$ is an integral domain, it extends to a map $f : A \to \mathrm{Frac}\,(A/\mathfrak{p})$. If $a \in S$, then $\pi(a) \neq 0$, so $f(a) \in \mathrm{Frac}\,(A/\mathfrak{p})^\times$. Therefore, f induces a map $g : A_\mathfrak{p} \to \mathrm{Frac}\,(A/\mathfrak{p})$; we easily check that this map is surjective. And $\mathrm{Ker}\, g$ is a maximal ideal of $A_\mathfrak{p}$ because $\mathrm{Im}\, g$ is a field, so $\mathrm{Ker}\, g = \mathfrak{m}$. ☐

4.3 Localisation of modules

Definition 4.3.1. *Let A be a ring and let S be a multiplicative subset of A containing 1 and not containing 0. If M is an A-module, define an equivalence relation on $M \times S$ by:*

$$(m_1, s_1) \sim (m_2, s_2) \iff \exists t \in S,\ t\,(m_1 s_2 - m_2 s_1) = 0.$$

Denote $S^{-1}M = M \times S/\sim$ and write $\frac{m}{s}$ for the class of (m, s) in $S^{-1}M$.

Proposition 4.3.2. *Let A be a ring and let S be a multiplicative subset of A containing 1 and not containing 0. If M is an A-module, then the formulas $\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{m_1 s_2 + m_2 s_1}{s_1 s_2}$ and $\frac{a_1}{s_1} \cdot \frac{m_2}{s_2} = \frac{a_1 m_2}{s_1 s_2}$ are well-defined on $S^{-1}M$ and make $S^{-1}M$ an $S^{-1}A$-module. Moreover, there is a linear map $m \in M \longmapsto \frac{m}{1} \in S^{-1}M$ whose kernel is $\{m \in M,\ \exists s \in S,\ ms = 0\}$.*

Proposition 4.3.3. *Let A be a ring and let S be a multiplicative subset of A containing 1 and not containing 0. If $u : M \to N$ is an A-linear map between A-modules, then there is an $S^{-1}A$-linear map $S^{-1}u : S^{-1}M \to S^{-1}N$ s.t.*

$$\left(S^{-1}u\right)\left(\frac{m}{s}\right) = \frac{u(m)}{s}.$$

Proposition 4.3.4. *Let A be a ring and let S be a multiplicative subset of A containing 1 and not containing 0. Assume that we have an exact sequence $M' \xrightarrow{f} M \xrightarrow{g} M''$. Then the following sequence is also exact:*

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''.$$

Corollary 4.3.5. *Let A be a ring and let S be a multiplicative subset of A containing 1 and not containing 0. If N and P are two submodules of an A-module M, then:*

$$S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P \qquad \text{and} \qquad S^{-1}(N + P) = S^{-1}N + S^{-1}P.$$

Proof. Note that we have an exact sequence $0 \to N \cap P \to N \oplus P \to N + P \to 0$ and apply Proposition 4.3.4. ☐

Theorem 4.3.6. *Let A be a ring and let S be a multiplicative subset of A containing* 1 *and not containing* 0*. Then, for any A-module M, there is a unique map $\varphi : S^{-1}A \otimes_A M \to S^{-1}M$ s.t. $\varphi\left(\frac{a}{s} \otimes m\right) = \frac{am}{s}$, and this map is an isomorphism. In particular:*

$$S^{-1}A \otimes_A M \simeq S^{-1}M.$$

Proof. The existence and unicity of φ come from the bilinear map $\left(\frac{a}{s}, m\right) \in S^{-1}A \times M \longmapsto \frac{am}{s} \in S^{-1}M$ (check that this map is well-defined by constructing a linear map $M \to \mathrm{Hom}\left(S^{-1}A, S^{-1}M\right)$, which comes from a linear map $M \to \mathrm{Hom}(A, M)$). The map φ is easily seen to be surjective. For the injectivity, prove that every element of $S^{-1}A \otimes_A M$ is equal to a simple tensor. □

Corollary 4.3.7. *Let A be a ring and let S be a multiplicative subset of A containing* 1 *and not containing* 0*. Then $S^{-1}A$ is a flat A-module.*

Proof. If we have an exact sequence of A-modules $0 \to M \to N$, then it induces an exact sequence $0 \to S^{-1}M \to S^{-1}N$ by Proposition 4.3.4, which is equivalent to $0 \to S^{-1}A \otimes_A M \to S^{-1}A \otimes_A N$ by Theorem 4.3.6. □

Remark 4.3.8. *We can generalise Theorem 4.3.6 as follows. If M and N are two A-modules, then there exists a unique map $\varphi : S^{-1}M \otimes_{S^{-1}A} S^{-1}N \to S^{-1}\left(M \otimes_A N\right)$ s.t. $\varphi\left(\frac{m}{s} \otimes \frac{n}{t}\right) = \frac{m \otimes n}{st}$. Moreover, φ is an isomorphism.*

4.4 Localisation of ideals

Remark 4.4.1. *Let A be a ring and let S be a multiplicative subset of A containing* 1 *and not containing* 0*. We denote by $\mathfrak{J}(B)$ the set of ideals of a ring B. Then we have two maps:*

(i) *The* extension map $\mathfrak{E} : I \in \mathfrak{J}(A) \longmapsto S^{-1}I \in \mathfrak{J}\left(S^{-1}A\right)$.

(ii) *The* contraction map $\mathfrak{C} : J \in \mathfrak{J}\left(S^{-1}A\right) \longmapsto \phi_S^{-1}(J) \in \mathfrak{J}(A)$.

Proposition 4.4.2. *Let A be a ring and let S be a multiplicative subset of A containing* 1 *and not containing* 0*. Then, we have:*

$$\mathfrak{E} \circ \mathfrak{C} = \mathrm{id}_{\mathfrak{J}(S^{-1}A)}.$$

In other words, for any ideal $J \subseteq S^{-1}A$, we have $J = S^{-1}\left(\phi_S^{-1}(J)\right)$

Corollary 4.4.3. *Let A be a ring and let S be a multiplicative subset of A containing* 1 *and not containing* 0*. If A is noetherian, then so is $S^{-1}A$.*

Proof. Let $(J_n)_{n\in\mathbb{N}}$ be an increasing sequence of ideals of $S^{-1}(A)$. Then $\left(\mathfrak{C}(J_n)\right)_{n\in\mathbb{N}}$ is an increasing sequence of ideals of A, so there exists $n_0 \in \mathbb{N}$ s.t. $\forall n \geq n_0$, $\mathfrak{C}(J_n) = \mathfrak{C}(J_{n_0})$. As a consequence, $\forall n \geq n_0,\ J_n = \mathfrak{E} \circ \mathfrak{C}(J_n) = \mathfrak{E} \circ \mathfrak{C}(J_{n_0}) = J_{n_0}$. □

4.5 Localisation of morphisms

Proposition 4.5.1. *Let M be an A-module. The following assertions are equivalent:*

(i) $M = 0$.

(ii) $M_{\mathfrak{p}} = 0$ *for every prime ideal* $\mathfrak{p}$ *of* A.

(iii) $M_{\mathfrak{m}} = 0$ *for every maximal ideal* $\mathfrak{m}$ *of* A.

If in addition M is finitely generated, then the previous assertions are also equivalent to:

(iv) $M \otimes_A A/\mathfrak{m} = 0$ *for every maximal ideal* $\mathfrak{m}$ *of* A.

Proof. The implications (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) are clear. Let us prove that (iii) $\Rightarrow$ (i). Assume that $M \neq 0$ and let $x \in M\backslash\{0\}$. Then $\mathrm{Ann}(x) = \{a \in A,\ ax = 0\}$ is a proper ideal of A so it is contained in a maximal ideal $\mathfrak{m}$. Now, if $\phi_{\mathfrak{m}} : M \to M_{\mathfrak{m}}$ is the canonical map, we know that:

$$\mathrm{Ker}\,\phi_{\mathfrak{m}} = \{y \in M,\ \exists a \in A\backslash\mathfrak{m},\ ay = 0\}\,.$$

In particular, $x \notin \mathrm{Ker}\,\phi_{\mathfrak{m}}$ (because $ax = 0 \Rightarrow a \in \mathrm{Ann}(x) \Rightarrow a \in \mathfrak{m}$), so $M_{\mathfrak{m}} \neq 0$. Now, assume that M is finitely generated. It is clear that (i) $\Rightarrow$ (iv), so it suffices to prove that (iv) $\Rightarrow$ (iii). Let $\mathfrak{m}$ be a maximal ideal of A. Recall that $A_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}} = A/\mathfrak{m}$ by Proposition 4.2.7. Thus, by Remark 4.3.8:

$$M_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}} = M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} A_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}} = (M \otimes_A /\mathfrak{m})_{\mathfrak{m}} = 0.$$

By Nakayema's Lemma (Proposition 1.9.4), $M_{\mathfrak{m}} = 0$. ☐

Corollary 4.5.2. *Let $f : M \to N$ be a morphism of A-modules. Then the following assertions are equivalent:*

(i) *$f : M \to N$ is injective (resp. surjective, bijective).*

(ii) *$f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective (resp. surjective, bijective) for every prime ideal $\mathfrak{p}$ of A.*

(iii) *$f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective (resp. surjective, bijective) for every maximal ideal $\mathfrak{m}$ of A.*

Proof. We have an exact sequence:

$$0 \to \mathrm{Ker}\,f \to M \xrightarrow{f} N \to \mathrm{Coker}\,f \to 0.$$

If $\mathfrak{p}$ is a prime ideal, then by Proposition 4.3.4, the following sequence is also exact:

$$0 \to (\mathrm{Ker}\,f)_{\mathfrak{p}} \to M_{\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} N_{\mathfrak{p}} \to (\mathrm{Coker}\,f)_{\mathfrak{p}} \to 0.$$

This proves that $(\mathrm{Ker}\,f)_{\mathfrak{p}} = \mathrm{Ker}\,(f_{\mathfrak{p}})$ and $(\mathrm{Coker}\,f)_{\mathfrak{p}} = \mathrm{Coker}\,(f_{\mathfrak{p}})$. Hence, by Proposition 4.5.1: f is injective iff $\mathrm{Ker}\,f = 0$ iff $(\mathrm{Ker}\,f)_{\mathfrak{p}}$ for every $\mathfrak{p}$ iff $\mathrm{Ker}\,(f_{\mathfrak{p}}) = 0$ for every $\mathfrak{p}$ iff $f_{\mathfrak{p}}$ is injective for every $\mathfrak{p}$. For the surjectivity, use the cokernel instead of the kernel. For maximal ideals, the proof is exactly the same. ☐

4.6 Localisation of finitely presented modules

Definition 4.6.1 (Finitely presented module)**.** *An A-module M is said to be* finitely presented *if one of the following two equivalent conditions is satisfied:*

(i) *There exists an exact sequence $0 \to K \to A^r \to M \to 0$, with K finitely generated, $r \in \mathbb{N}$.*

(ii) *There exists an exact sequence $A^s \to A^r \to M \to 0$, with $r, s \in \mathbb{N}$.*

Remark 4.6.2. *Over a noetherian ring, a module is finitely presented* iff *it is finitely generated.*

Proposition 4.6.3. *Let M and N be two A-modules. Then there is a unique $S^{-1}A$-linear map:*

$$\alpha : S^{-1}\,\mathrm{Hom}_A(M, N) \longrightarrow \mathrm{Hom}_{S^{-1}A}\left(S^{-1}M, S^{-1}N\right),$$

that sends $\frac{1}{s}f$ to the map $\frac{m}{t} \mapsto \frac{f(m)}{st}$. If in addition M is finitely presented, then α is an isomorphism.

Proof. The existence and unicity of α are routine verifications. Assume that M is finitely presented. Then there exist $r, s \in \mathbb{N}$ and an exact sequence $A^s \to A^r \to M \to 0$. We can either localise the sequence at S (using Proposition 4.3.4) and then apply $\mathrm{Hom}\,(\cdot, N)$ (using Proposition 1.2.6) or apply $\mathrm{Hom}\,(\cdot, N)$ and then localise at S. Hence, we obtain two exact sequences, and a commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & S^{-1}\operatorname{Hom}_A(M,N) \arrow[r] \arrow[d, "\alpha"] & S^{-1}\operatorname{Hom}_A(A^r,N) \arrow[r] \arrow[d, "\alpha_r"] & S^{-1}\operatorname{Hom}_A(A^s,N) \arrow[d, "\alpha_s"] \\
0 \arrow[r] & \operatorname{Hom}_{S^{-1}A}(S^{-1}M,S^{-1}N) \arrow[r] & \operatorname{Hom}_{S^{-1}A}(S^{-1}A^r,S^{-1}N) \arrow[r] & \operatorname{Hom}_{S^{-1}A}(S^{-1}A^s,S^{-1}N)
\end{tikzcd}$$

Using the fact that α_r and α_s are isomorphisms, we show that α is an isomorphism by diagram chasing. $\square$

Definition 4.6.4 (Locally free module)**.** *An A-module M is said to be* locally free *if, for every prime ideal $\mathfrak{p}$ of A, $M_\mathfrak{p}$ is free over $A_\mathfrak{p}$.*

Theorem 4.6.5. *Let M be a finitely presented A-module. Then M is projective* iff *M is locally free.*

Proof. ($\Rightarrow$) Assume that M is projective. Let $\mathfrak{p}$ be a prime ideal of A. Then $M_\mathfrak{p} = M \otimes_A A_\mathfrak{p}$ is projective and finitely generated over the local ring $A_\mathfrak{p}$. By Corollary 4.1.4, $M_\mathfrak{p}$ is free over $A_\mathfrak{p}$. ($\Leftarrow$) Assume that M is locally free. Consider a surjective map of A-modules $P \to Q$. We must show that the induced map $\operatorname{Hom}_A(M,P) \longrightarrow \operatorname{Hom}_A(M,Q)$ is also surjective. By Corollary 4.5.2, it suffices to show that the map $(\operatorname{Hom}_A(M,P))_\mathfrak{p} \longrightarrow (\operatorname{Hom}_A(M,Q))_\mathfrak{p}$ is surjective for every prime ideal $\mathfrak{p}$ of A. But since M is finitely presented, Proposition 4.6.3 gives $(\operatorname{Hom}_A(M,P))_\mathfrak{p} = \operatorname{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p},P_\mathfrak{p})$ and $(\operatorname{Hom}_A(M,Q))_\mathfrak{p} = \operatorname{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p},Q_\mathfrak{p})$. But the map $P_\mathfrak{p} \to Q_\mathfrak{p}$ is surjective (by Corollary 4.5.2), and $M_\mathfrak{p}$ is free (and thus projective) over $A_\mathfrak{p}$, so the map $\operatorname{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p},P_\mathfrak{p}) \longrightarrow \operatorname{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p},Q_\mathfrak{p})$ is surjective, which gives the result. $\square$

Corollary 4.6.6. *If M is a finitely presented flat A-module, then M is projective.*

Proof. If $\mathfrak{p}$ is a prime ideal of A, then $M_\mathfrak{p}$ is flat and finitely presented over the local ring $A_\mathfrak{p}$, so it is free by Theorem 4.1.3. Therefore, M is locally free, so it is projective by Theorem 4.6.5. $\square$

5 Integral extensions

5.1 Integral elements

Definition 5.1.1 (Integral elements)**.** *Let A be a subring of a ring B. Let $x \in B$. The following assertions are equivalent:*

(i) *There exists a monic polynomial $P \in A[X]$ s.t. $P(x) = 0$.*

(ii) *$A[x]$ is a finitely generated A-module.*

(iii) *There exists a subring C of B containing A and x that is finitely generated as an A-module.*

If these assertions are true, we say that x is integral *over A.*

Proof. (i) $\Rightarrow$ (ii) Suppose that there exists $P = X^d + \sum_{k=0}^{d-1} a_k X^k \in A[X]$ monic s.t. $P(x) = 0$. Then we have:

$$x^d = -\sum_{k=0}^{d-1} a_k x^k.$$

By induction on $n \geq d$, we prove that $x^n \in Ax^{d-1} + \cdots + Ax + A$. Hence, $A[x] \subseteq Ax^{d-1} + \cdots + Ax + A$. (ii) $\Rightarrow$ (iii) Take $C = A[x]$. (iii) $\Rightarrow$ (i) Let C be a finitely generated subring of C containing A and x. Then we can define a map $\mu_x : c \in C \longmapsto cx \in C$. By the Cayley-Hamilton Theorem (Theorem 1.8.3), there exists a monic polynomial $P \in A[X]$ s.t. $P(\mu_x) = 0$. In particular, $P(x) = P(\mu_x) \cdot 1 = 0$. $\square$

Lemma 5.1.2. *Let R be a subring of a ring S and let M be a finitely generated S-module. If S is also finitely generated as an R-module, then M is finitely generated as an R-module.*

Corollary 5.1.3. *Let A be a subring of a ring B. Then the set C of elements of B that are integral over A is a subring of B.*

Proof. We need to prove that the sum and product of two integral elements is integral. Let $x, y \in B$ be two integral elements over A. Then y is integral over $A[x]$, so $A[x, y]$ is a finitely generated $A[x]$-module. And x is integral over A, so $A[x]$ is a finitely generated A-module. By Lemma 5.1.2, $A[x, y]$ is a finitely generated A-module. Moreover, $A[x, y]$ is a subring of B that contains A, $(x + y)$ and (xy), so $(x + y)$ and (xy) are integral over A. $\square$

Definition 5.1.4 (Integral closure)**.** *Let A be a subring of a ring B. The ring C of elements of B that are integral over A is called the* integral closure *(or* normalisation*) of A in B.*

- *If $C = A$, we say that A is* integrally closed *in B.*
- *If $C = B$, we say that B is* integral *over A.*

Vocabulary 5.1.5. *An integral domain is said to be* integrally closed *if it is closed in its field of fractions.*

Proposition 5.1.6. *A factorial domain is integrally closed.*

Example 5.1.7. *If K is a finite extension of $\mathbb{Q}$, we denoted by $\mathcal{O}_K$ the integral closure of $\mathbb{Z}$ in K. The study of $\mathcal{O}_K$ is a topic of algebraic number theory. For example, if $d \in \mathbb{N}_{\geq 2}$ and $K = \mathbb{Q}\left(\sqrt{d}\right)$, then:*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} \oplus \mathbb{Z}\sqrt{d} & \text{if } d \not\equiv 1 \mod 4 \\ \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \mod 4 \end{cases}.$$

5.2 Finiteness of invariants

Definition 5.2.1 (Finitely generated algebra)**.** *Let B be an algebra over a ring A. We say that B is* of finite type *(or finitely generated) as an A-algebra if there exist $b_1, \ldots, b_n \in B$ s.t. $B = A[b_1, \ldots, b_n]$. Equivalently, there exists $n \in \mathbb{N}^*$ and a surjective map $A[X_1, \ldots, X_n] \to B$.*

Remark 5.2.2. *Let B be an algebra over a ring A. If B is finitely generated as an A-module, then it is finitely generated as an A-algebra, but the converse is false.*

Notation 5.2.3. *Let A be an algebra over a field k. If a group G acts k-algebraically on A, we write :*

$$A^G = \{a \in A, \forall g \in G, \ g \cdot a = a\}.$$

Then A^G is a subalgebra of A.

Lemma 5.2.4. *If A is an finitely generated k-algebra, and G is a finite group acting k-algebraically on A, then the ring A is integral over A^G.*

Proof. If $a \in A$, define:

$$P_a = \prod_{g \in G} (X - g \cdot a) \in A^G[X].$$

P_a is monic and $P_a(a) = 0$, so a is integral over A^G. $\square$

Lemma 5.2.5. *If a ring B is integral over A and finitely generated as an A-algebra, then B is finitely generated as an A-module.*

Proof. Write $B = A[x_1, \ldots, x_n]$ and set $B_j = A[x_1, \ldots, x_j]$ for $j \in \{0, \ldots, n\}$. Then $B_{j+1} = B_j[x_{j+1}]$, and x_{j+1} is integral over B_j (because it is over B), so B_{j+1} is a finitely generated B_j-module. By Lemma 5.1.2, we obtain that $B_n = B$ is finitely generated over $B_0 = A$. $\square$

Proposition 5.2.6. *Let B be a finitely generated k-algebra, and let A be a subalgebra of B s.t. B is a finitely generated A-module. Then A is a finitely generated k-algebra.*

Proof. Write $B = k[x_1, \ldots, x_m] = Ay_1 + \cdots + Ay_n$, with $x_1, \ldots, x_n, y_1, \ldots, y_n \in B$. Hence, there exist elements $(a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ and $(a_{ijk})_{1 \le i,j,k \le n}$ in A s.t.

$$x_i = \sum_{j=1}^{n} a_{ij} y_j \qquad \text{and} \qquad y_i y_j = \sum_{k=1}^{n} a_{ijk} y_k.$$

We now set $A_0 = k\left[(a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}}, (a_{ijk})_{1 \le i,j,k \le n}\right]$; this is a subring of A which is a finitely generated k-algebra. We claim that $B = A_0 y_1 + \cdots + y_n$. Firstly, note that (using induction on r), $y_{\ell_1} \cdots y_{\ell_r} \in A_0 y_1 + \cdots + A_0 y_n$ for all indices $\ell_1, \ldots, \ell_r$. Now, if $b \in B$, we can write $b = P(x_1, \ldots, x_m)$ with $P \in k[X_1, \ldots, X_m]$. Hence:

$$b = P\left(\sum_{j=1}^{n} a_{1j} y_j, \ldots, \sum_{j=1}^{n} a_{mj} y_j\right).$$

Expandingt this expression, we obtain $b \in A_0 y_1 + \cdots + A_0 y_n$. Therefore, $B = A_0 y_1 + \cdots + A_0 y_n$ is a finitely generated A_0-module. But A_0 is a noetherian ring, so B is a noetherian A_0-module by Theorem 1.5.6, and $A \subseteq B$, so A is also a finitely generated A_0-module, so it is a finitely generated k-algebra. □

Theorem 5.2.7. *If A is a finitely generated k-algebra, and G is a finite group acting k-algebraically on A, then A^G is finitely generated as a k-algebra.*

Proof. Note that A is a finitely generated A^G-algebra (because it is a finitely generated k-algebra), and it is integral over A^G by Lemma 5.2.4. By Lemma 5.2.5, A is a finitely generated A^G-module. By Proposition 5.2.6, A^G is a finitely generated k-algebra. □

Example 5.2.8. *If $A = k[X_1, \ldots, X_n]$ and $G = \mathfrak{S}_n$ with $\sigma \cdot X_i = X_{\sigma(i)}$, then A^G is the k-algebra generated by the elementary symmetric polynomials.*

5.3 Noether Normalisation Lemma

Definition 5.3.1 (Algebraic independence)**.** *Let B be an algebra over a ring A. Let $b_1, \ldots, b_n \in B$. We say that $b_1, \ldots, b_n$ are* algebraically independent *if:*

$$\forall P \in A[X_1, \ldots, X_n],\ P(b_1, \ldots, b_n) = 0 \Longrightarrow P = 0.$$

Remark 5.3.2. *Algebraic independence is stronger than linear independence.*

Lemma 5.3.3. *We assume that k is an infinite field. If $P \in k[T_1, \ldots, T_k] \backslash \{0\}$, then there exists $t_1, \ldots, t_k \in k$ s.t. $P(t_1, \ldots, t_k) \neq 0$.*

Proof. By induction on k. □

Lemma 5.3.4. *We assume that k is an infinite field. If $R \in k[T_1, \ldots, T_m] \backslash \{0\}$ is homogeneous, then there exist $t_1, \ldots, t_{m-1} \in k$ s.t. $R(t_1, \ldots, t_{m-1}, 1) \neq 0$.*

Proof. Note that $R(T_1, \ldots, T_{m-1}, 1) \in k[T_1, \ldots, T_{m-1}] \backslash \{0\}$ and apply Lemma 5.3.3. □

Lemma 5.3.5. *We assume that k is an infinite field. Let A be a k-algebra. Let $a_1 \ldots, a_m \in A$ and $P \in k[X_1, \ldots, X_m] \backslash \{0\}$ s.t. $A = k[a_1, \ldots, a_m]$ and $P(a_1, \ldots, a_m) = 0$. Then there exist $a'_1, \ldots, a'_{m-1} \in A$ s.t. a_m is integral over $k[a'_1, \ldots, a'_m]$ and $A = k\left[a'_1, \ldots, a'_{m-1}, a_m\right]$.*

Proof. Let $t_1, \dots, t_{m-1} \in k$ (to be chosen later). Set $a_i' = a_i - t_i a_m$ for $i \in \{1, \dots, m-1\}$. Let $B = k\left[a_1', \dots, a_{m-1}'\right]$ and $Q = P\left(a_1' + t_1 X, \dots, a_{m-1}' + t_{m-1} X, X\right) \in B[X]$. We have $A = B\left[a_m\right]$ and $Q\left(a_m\right) = 0$. If d is the (total) degree of P, then Q is of degree at most d and the coefficient of X^d is $P_d\left(t_1, \dots, t_{m-1}, 1\right)$, where P_d is the part of P that is homogeneous of degree d. According to Lemma 5.3.4, it is possible to choose $t_1, \dots, t_{m-1} \in k$ s.t. $P_d\left(t_1, \dots, t_{m-1}, 1\right) \in k^\times$. Hence, Q is a nonzero polynomial whose leading coefficient is a unit of k, and $Q\left(a_m\right) = 0$, so a_m is integral over B. □

Theorem 5.3.6 (Noether Normalisation Lemma)**.** *We assume that k is an infinite field. If A is a finitely generated k-algebra, then there exist $x_1, \dots, x_n \in A$ which are algebraically independent and s.t. A is a finitely generated $k\left[x_1, \dots, x_n\right]$-module. If in addition A is generated by m elements, then we can have $n \leq m$.*

Proof. We proceed by induction on the number m of generators of A. If $m = 0$, then $A = k$ and we are done. Assume the result is proven for $(m-1)$ and write $A = k\left[a_1, \dots, a_m\right]$. If $a_1, \dots, a_m$ are algebraically independent, take $x_i = a_i$. Otherwise, there exists $P \in k\left[X_1, \dots, X_m\right] \backslash \{0\}$ s.t. $P\left(a_1, \dots, a_m\right) = 0$. By Lemma 5.3.5, there exist $a_1', \dots, a_{m-1}' \in A$ s.t. a_m is integral over $B = k\left[a_1', \dots, a_{m-1}'\right]$ and $A = B\left[a_m\right]$. By induction, there exist $x_1, \dots, x_{n-1} \in B$ with $n - 1 \leq m - 1$, $x_1, \dots, x_{n-1}$ algebraically independent and s.t. B is a finitely generated $k\left[x_1, \dots, x_{n-1}\right]$-module. Since $A = B\left[a_m\right]$ with a_m integral over B, A is a finitely generated $k\left[x_1, \dots, x_{n-1}\right]$-module. □

5.4 Hilbert's Nullstellensatz

Lemma 5.4.1. *Let B be an integral domain. Assume that B is integral over a subring A. Then B is a field* iff *A is a field.*

Proof. ($\Leftarrow$) Assume that A is a field. Let $x \in B \backslash \{0\}$. Since x is integral over A, $A[x]$ is a finite dimensional A-vector space. And the map $y \in A[x] \mapsto yx \in A[x]$ is injective because B is an integral domain, so it is surjective, which proves that $x \in B^\times$. ($\Rightarrow$) Assume that B is a field. Let $x \in A \backslash \{0\}$. Then $x \in B^\times$, i.e. $x^{-1} \in B$. Therefore, x^{-1} is integral over A, i.e. there exist $a_0, \dots, a_{n-1} \in A$ s.t.

$$a_0 + a_1 x^{-1} + \cdots + a_{n-1} x^{-(n-1)} + x^{-n} = 0.$$

Therefore, $x^{-1} = -a_0 x^{n-1} - \cdots - a_{n-2} x - a_{n-1} \in A$, so $x \in A^\times$. □

Lemma 5.4.2. *Let A be a finitely generated k-algebra. If A is a field, then A is a finite extension of k.*

Proof. By the Noether Normalisation Lemma (Theorem 5.3.6), A is integral over $k\left[X_1, \dots, X_n\right]$ for some $n \in \mathbb{N}$. By Lemma 5.4.1, $k\left[X_1, \dots, X_n\right]$ is a field (because A is a field); therefore $n = 0$. □

Theorem 5.4.3 (Hilbert's Nullstellensatz)**.** *If k is an algebraically closed field, then the maximal ideals of $k\left[X_1, \dots, X_n\right]$ are the ideals of the form $\left(X_1 - a_1, \dots, X_n - a_n\right)$, with $a_1, \dots, a_n \in k$.*

Proof. Firstly, if $a_1, \dots, a_n \in k$, then $\left(X_1 - a_1, \dots, X_n - a_n\right) = \operatorname{Ker} \varphi$, with:

$$\varphi : P \in k\left[X_1, \dots, X_n\right] \longmapsto P\left(a_1, \dots, a_n\right) \in k.$$

But $\operatorname{Im} \varphi = k$ is a field, so $\operatorname{Ker} \varphi$ is a maximal ideal of $k\left[X_1, \dots, X_n\right]$. Therefore, the ideal $\left(X_1 - a_1, \dots, X_n - a_n\right)$ is maximal for all $a_1, \dots, a_n \in k$. Conversely, consider a maximal ideal I of $k\left[X_1, \dots, X_n\right]$. We have a field $L = k\left[X_1, \dots, X_n\right]/I$, which is also a finitely generated k-algebra. By Lemma 5.4.2, L is a finite extension of k. But k is algebraically closed, so $L = k$. Now, let $a_i \in k$ be the image of X_i in $L = k\left[X_1, \dots, X_n\right]/I$ for $i \in \{1, \dots, n\}$. We have $I \supseteq \left(X_1 - a_1, \dots, X_n - a_n\right)$, and the ideal $\left(X_1 - a_1, \dots, X_n - a_n\right)$ is maximal, so $I = \left(X_1 - a_1, \dots, X_n - a_n\right)$. □

Corollary 5.4.4. *Let k be an algebraically closed field.*

(i) *If* J *is an ideal of* $k[X_1,\ldots,X_n]$*, then the maximal ideals of* $k[X_1,\ldots,X_n]/J$ *are of the form* $\left(\overline{X_1-a_1},\ldots,\overline{X_n-a_n}\right)$*, where* $a_1,\ldots,a_n\in k$ *are s.t.* $P(a_1,\ldots,a_n)=0$ *for every* $P\in J$*.*

(ii) *If* $P_1,\ldots,P_m \in k[X_1,\ldots,X_n]$ *have no common root in* k*, then there exist* $f_1,\ldots,f_m \in k[X_1,\ldots,X_n]$ *s.t.* $f_1P_1+\cdots+f_mP_m=1$*.*

References

[1] M.F. Atiyah and I.G. MacDonald. *Introduction To Commutative Algebra.*

[2] N. Bourbaki. *Algèbre commutative.*

[3] R. Douady and A. Douady. *Algèbre et théories galoisiennes.*

[4] S. Lang. *Algebra.*