Algèbre Avancée

R. Abdellatif

Transcrit par Idriss Mazari

E.N.S Lyon, 2014-2015

I. Avant-Propos

Ces notes ont été rédigées par Idriss Mazari. Les erreurs qui s'y trouvent ne sont donc aucunement du fait de Mme. Abdellatif (http://perso.ens-lyon.fr/ramla.abdellatif/). Elles correspondent au cours d'algèbre du premier semestre du master de mathématiques avancées de l'ENS Lyon.

I-A. Conseils bibliographiques

La liste qui suit nous a été fournie par Mme. Abdellatif :

Algèbre Commutative :

- M.F. Atiyah et I.G. MacDonald, *Introduction to commutative algebra*, Addison-Wesley (1969)
- N. Bourbaki, Chapitres 1 a 4 et 5 a 7 de *Algebre Commutative*, Springer (2006)
- J.W.S. Cassels et A. Frohlich, *Algebraic Number Theory 1*, Academic Press Inc. (1986)
- H. Koch, Number Theory : *Algebraic Numbers and Functions*, AMS Graduate Studies in Mathematics (2000)
- N. Jacobson, *Basic Algebra* (volumes I et II), Freeman and Company (1989)
- S. Lang, *Algebraic Number Theory*, Springer (1994)
- H. Matsumura, *Commutative Ring Theory*, Cambridge University Press (2000)
- P. Samuel, *Théorie algébrique des nombres*, Hermann (1967)
- J-P. Serre, *Corps locaux*, Hermann (1997)
- J.S. Milne, *Algebraic Number Theory*, disponible sur http://www.jmilne.org/math/CourseNotes/ant.html
- P. Colmez, *Les nombres p-adiques et Corps locaux*, disponible sur http://webusers.imj-prg.fr/~pierre.colmez/M2.html

Théorie de Galois :

- E. Artin, *Galois Theory*, Dover Publications (1998)
- N. Bourbaki, Chapitre 5 du *Livre II - Algèbre*, Springer (2006)
- R. Elkik, *Cours dalgèbre*, Ellipses (2002)
- J-P. Escofier, *Théorie de Galois*, 2eème edition, Dunod (2004)
- J-P. Lafon, *Algèbre commutative - Langages géométrique et algeébrique*, Hermann (1997)
- S. Lang, *Algèbre*, 3ème edition, Dunod (2004)
- C. Mutafian, *Équations algébriques et théorie de Galois*, Vuibert (1980)
- P. Samuel, *Théorie algébrique des nombres*, Hermann (1967)
- I. Stewart, *Galois Theory*, 3ème edition, Chapman and Hall (2004)
- A. Chambert-Loir, *Algèbre corporelle*, disponible sur http://www.math.polytechnique.fr/~chambert/teach/algebre.pdf
- A. Kraus, *Cours de théorie de Galois*, disponible sur http://www.galois-group.net/theory/Galois_Kraus.pdf
- J.S. Milne, *Fields and Galois Theory*, disponible sur http://www.jmilne.org/math/CourseNotes/ft.html

I-B. Notations et conventions

- Σ' désigne une somme finie.
- A désigne dans tout le cours un anneau <u>commutatif</u> et <u>unifère</u>, propriétés que partageront tous les anneaux rencontrés [1]

1. Sauf mention du contraire.

- Si A est un anneau commutatif unifère, on note $Spec(A)$ l'ensemble des idéaux premiers de A.
- Si $n \in \mathbb{N}^*$, on note S_n le groupe symétrique de l'ensemble $\{1, \ldots, n\}$ et A_n le groupe alterné.
- Si E est un ensemble, on note S_E l'ensemble des bijections de E dans E.
- Si $P \in k[X]$ est un poynôme, on note $Z(P)$ l'ensemble de ses racines dans une clôture algébrique de k.

Première partie

Algèbre Commutative

II. Produit tensoriel

II-A. Motivation

L'idée est que, étant donnés deux A-modules M et N, on aimerait étudier les applications bilinéaires sur $M \times N$ à valeurs dans un A-module M_1 à travers des applications linéaires. En d'autres termes :

Existe-t-il un A-module P tel que pour tout A-modules P', l'ensemble $\mathcal{L}^2_A(M \times N; P')$ des applications bilinéaires de $M \times N$ dans P' puisse être étudié grâce au A-module $Hom_A(P, P')$?

$$\begin{tikzcd} M \times N \arrow[r, "\mathcal{L}^2"] \arrow[d, "\pi"] & P' \\ P \arrow[ur, "Hom_A"'] & \end{tikzcd}$$

Comme on va le voir, la réponse est oui.

II-B. Produit tensoriel de deux modules

Définition II.1. *Un <u>produit tensoriel</u> de M et N sur A est une paire (P, π) formée d'un A-module P et d'une application $\pi \in \mathcal{L}^2_A(M \times N; P)$ vérifiant la propriété universelle suivante : Pour tout A-module P', pour tout application A-bilinéaire $\tilde{f}$ de $M \times N$ dans P', il existe une unique application f A-linéaire de P dans P' telle que*

$$\tilde{f} = f \circ \pi.$$

Théorème II.1. *Pour toute paire de A-modules (M, N), il existe un produit tensoriel de M et N sur A. Il est de plus unique à isomorphisme prés.*

Démonstration du théorème. • <u>Existence</u> : On va en fait procéder à la construction explicite d'un produit tensoriel. On considère le A-module libre $A^{(M,N)}$, c'est-à-dire le A-module admettant la base canonique $(e_{m,n})_{m \in M, n \in N}$.

On a une application $\tilde{f}_0 : M \times N \to A^{(M,N)}$ qui associe à (m, n) l'élément $(e_{m,n})$. On va la rendre bilinéaire en quotientant $A^{(M,N)}$ par les relations suivantes : pour tout $(m, m') \in M^2, (n, n') \in N^2, \lambda \in A$

- $e_{m+m',n} = e_{m,n} + e_{m',n}$
- $e_{m,n+n'} = e_{m,n} + e_{m,n'}$
- $e_{\lambda m,n} = \lambda e_{m,n}$
- $e_{m,\lambda n} = \lambda e_{m,n}$

Soit $\mathcal{R}$ le sous-A-module de $A^{(M,N)}$ engendré par ces relations. On définit ainsi le A module $A^{(M,N)}/\mathcal{R}$. L'application $\tilde{f}_0$ induit alors une application bilinéaire de $M \times N$ dans $A^{(M,N)}/\mathcal{R}$. On vérifie ensuite la propriété universelle des produits tensoriels : Soit $\varphi \in \mathcal{L}^2_A(M \times N; P)$, où P est un A-module. Considérons l'application $\tilde{\varphi} : A^{(M \times N)} \to P$ envoyant $e_{m,n}$ sur (m, n). Par construction, cette application est linéaire et se factorise à travers $\mathcal{R}$, et $\varphi = \varphi_0 \circ f_0$ où f_0 est l'application bilinéaire induite par $\tilde{f}_0$. Comme les $\overline{e_{m,n}}$ engendrent $A/\mathcal{R}$ comme A-module, on en déduit que l'application φ_0 factorise φ à travers $A/\mathcal{R}$ de manière unique.

- <u>Unicité</u> Soient (P, π) et (P_0, π_0) deux produits tensoriels de M et N sur A. Montrons qu'ils sont isomorphes. On a les deux diagrammes suivants :

$$\begin{tikzcd} M \times N \arrow[r, "\pi_0"] \arrow[d, "\pi"] & P_0 \\ P \arrow[ur, "\varphi"'] & \end{tikzcd} \quad \text{et} \quad \begin{tikzcd} M \times N \arrow[r, "\pi"] \arrow[d, "\pi_0"] & P \\ P_0 \arrow[ur, "\varphi_0"'] & \end{tikzcd}$$

On en déduit ainsi $(\varphi \circ \varphi_0) \circ \pi_0 = \pi_0$. Comme Id permet l'unique factorisation de π_0 à travers P_0, on en déduit par la propriété universelle que $\varphi \circ \varphi_0 = Id_{P_0}$ et, de même, en échangeant P et P_0, $\varphi_0 \circ \varphi = Id_P$. Ainsi, φ et φ_0 sont deux isomorphismes de A-modules, inverses l'un de l'autre. Le produit tensoriel est donc unique à isomorphisme près.

□

On note le représentant dans les classes d'isomorphismes de A-modules du produit tensoriel de M et N sur A par $M \otimes_A N$. On adoptera également les définitions suivantes.

Définition II.2. • *Un tenseur simple est un tenseur de la forme $m \otimes n$, c'est-à-dire un élément de la forme $\tilde{f}_0(m,n)$.*

• *Un tenseur est un élément de $M \otimes_A N$.*

On peut donc réécrire la propriété universelle du produit tensoriel comme suit : Pour tout A-module P, pour toute application $\tilde{f} \in \mathcal{L}^2(M \times N; P)$ il existe une unique application $f \in Hom_A(M \otimes_A N; P)$ telle que pour tout $(m,n) \in M \times N, \tilde{f}(m,n) = f(m \otimes n)$.

Remarque. 1. Un tenseur n'est en général pas un tenseur simple.

2. Par construction, tout tenseur une combinaison linéaire finie de tenseurs simples.
3. Les tenseurs simples ne forment généralement pas une base de $M \otimes_A N$, dans la mesure où ce module n'a aucune raison d'être libre.

Corollaire II.1. *Il existe donc, pour tout A-module P, un isomorphisme canonique de A-modules*

$$\mathcal{L}^2(M \times N; P) \cong Hom_A(M \otimes_A N; P)$$

II-C. Propriétés élémentaires du produit tensoriel

Dans toute la suite, M, M_1, M_2 et N sont des A-modules.

Proposition II.1. *Le produit tensoriel est commutatif au sens où il existe un isomorphisme de A-modules φ canonique entre $M \otimes_A N$ et $N \otimes_A M$ vérifiant :*

$$\forall (m,n) \in M \times N, \varphi(m \otimes n) = n \otimes m$$

Démonstration de la proposition. Considérons l'application $\tilde{\varphi}$ de $M \times N$ dans $N \otimes_A M$ définie par

$$\tilde{\varphi} : (m,n) \mapsto n \otimes m$$

Par la propriété universelle du produit tensoriel, cette application étant A-bilinéaire, elle induit un homomorphisme de A-modules φ entre $M \otimes_A N$ et $N \otimes_A M$, vérifiant que pour tout tenseur simple $m \otimes n$, $p(m \otimes n) = n \otimes m$. En inversant les rôles de M et N, on obtient l'existence d'un homomorphisme $\psi : N \otimes_A M \to M \otimes_A N$ vérifiant que pour tout $(n,m) \in M \times N, \varphi(n \otimes m) = m \otimes n$. On vérifie alors que ψ et φ sont deux applications réciproques l'une de l'autre.

□

Proposition II.2. *Le produit tensoriel est associatif au sens où, si M, N et P sont trois A-modules, il existe un isomorphisme canoniques de A-modules entre $(M \otimes_A N) \otimes_A P$ et $M \otimes_A (N \otimes_A) P$.*

Démonstration de la proposition. Cette construction est fondamentale, et on la retrouvera souvent : on va procéder en deux étapes.

1. Soit $m \in M$. Considérons l'application

$$\tilde{\varphi_m} : \begin{array}{l} N \times P \longrightarrow (M \otimes_A N) \otimes_A P \\ (n,p) \longrightarrow (m \otimes n) \otimes p \end{array}$$

Cette application est A-bilinéaire par construction du produit tensoriel. Elle induit donc une unique application $\varphi_m \in Hom_A(N \otimes_A P, (M \otimes_A N) \otimes_A P)$ vérifiant que pour tout $(n,p) \in N \times P, \varphi_m(n \otimes p) = (m \otimes n) \otimes p$.

2. Considérons ensuite l'application

$$\begin{array}{rl} \tilde{\varphi}: & M \times (N \otimes_A P) \longrightarrow (M \otimes_A N) \otimes_A P \\ & (m, v) \longrightarrow \varphi_m(v) \end{array}$$

On vérifie que cette application est A-bilinéaire : la linéarité en la seconde variable est évidente, tandis que la relation $\varphi_{\lambda m+m'} = \lambda\varphi_m + \varphi_{m'}$ est une conséquence de la propriété universelle : les deux applications coincident sur les tenseurs simples, elles sont donc égales. On obtient donc une application $\varphi \in Hom_A(M \otimes_A (N \otimes_A P); (M \otimes_A N) \otimes_A P$ vérifiant sur les tenseurs simples $\varphi(m, n \otimes p) = (m \otimes n) \otimes p$. On construit de même une application $\psi \in Hom_A((M \otimes_A N) \otimes_A P; M \otimes_A (N \otimes_A P))$. On vérifie alors que $\psi \circ \varphi$ et $\varphi \circ \psi$ fixent les tenseurs simples : par A-linéarité et génération des A-modules considérés par les tenseurs simples, on en déduit qu'il s'agit de deux isomorphismes de A-modules, ce qui achève la preuve.

□

Proposition II.3. *Il existe un isomorphisme de A-modules canonique entre $M \otimes_A A$ et A.*

Démonstration de la proposition. Considérons l'application suivante :

$$\begin{array}{rl} \tilde{\varphi}: & M \times A \longrightarrow M \\ & (m, a) \longrightarrow a \cdot m \end{array}$$

Elle est, de manière immédiate, A-bilinéaire, et induit donc un homomorphisme de A-modules φ de $M \otimes_A A$ sur M vérifiant la propriété suivante :

$$\forall (a, m) \in A \times M, \varphi(a \otimes m) = a \cdot m$$

Si l'on construit ensuite l'application ψ définie par

$$\begin{array}{rl} \psi: & M \longrightarrow M \otimes_A A \\ & m \longrightarrow m \otimes 1 \end{array}$$

on voit que ψ et φ sont deux applications réciproques l'une de l'autre.

□

Le même genre d'arguments mène à la proposition ci-dessous, dont la preuve est laissée en exercice.

Proposition II.4. *Le produit tensoriel est distributif au sens suivant :*
Il existe un isomorphisme de A-modules canonique entre $(M_1 \oplus M_2) \otimes_A M$ et $(M_1 \otimes_A M) \oplus (M_2 \otimes_A M)$.

Proposition II.5. *Soient M et N deux A-modules.*

i) Si $(m_i)_{i \in I}$ et $(n_j)_{j \in J}$ sont deux familles génératrices de M et N respectivement, $(m_i \otimes n_j)_{i \in I, j \in J}$ est une famille génératrice de $M \otimes_A N$.

ii) Supposons de plus que M et N sont deux A-modules libres. Si $(m_i)_{i \in I}$ et $(n_j)_{j \in J}$ sont deux bases de M et N respectivement, $(m_i \otimes n_j)_{i \in I, j \in J}$ est une base de $M \otimes_A N$.

Démonstration de la proposition.

1. Il suffit de vérifier que les tenseurs simples peuvent être exprimés comme somme finie de tenseurs de la forme $m_i \otimes n_j$, ce qui est immédiat par A-bilinéarité du produit tensoriel.
2. Il faut vérifier que la famille $(m_i \otimes n_j)_{i \in I, j \in J}$ est libre. Pour cela, on considère $(m_i^*)_{i \in I}$ et $(n_j^*)_{j \in J}$ les bases duales respectives de M et N. Soit $I' \subset I$ et $J' \subset J$ deux sous-familles finies et $(\lambda_{i,j})_{i \in I', j \in J'} \in A^{card(I) \times card(J)}$ tels que

$$\sum_{(i,j) \in I' \times J'} \lambda_{i,j} m_i \otimes n_j = 0$$

Les formes linéaires $m_i^* \cdot n_j^*$ sont A-bilinéaires et induisent donc un homorphisme $\varphi_{i,j} \in Hom_A(M \otimes_A N; A)$ vérifiant $\varphi_{i,j}(m \otimes n) = m_i^*(m) n_j^*(n)$. On en tire donc $\lambda_{i,j} = 0$.

□

Remarque. Cette proposition permet de montrer que tout tenseur n'est pas nécessairement un tenseur simple : considérons M un A-module libre de rang $n \geq 2$. Soit $\{e_1, \ldots, e_n\}$ une base de M. Alors $e_1 \otimes e_1 + e_2 \otimes e_2$ n'est pas un tenseur simple. En effet, supposons par l'absurde qu'il s'écrive $m \otimes n$, avec $m = \sum_{j=1\ldots,n} m_j e_j$ et $n = \sum_{i=1,\ldots,n} n_i e_i$. Alors par la proposition précédente, on a les relations suivantes : $m_1 n_1 = 1, m_2 n_1 = 0, m_1 n_2 = 0, m_2 n_2 = 0$ ce qui est absurde.

Proposition II.6. *Soit M un A-module et I un idéal de A. Il y a un isomorphisme canonique de A-modules entre M/IM et $M \otimes_A (A/I)$.*

Démonstration de la proposition. Considérons l'application $\tilde{\varphi} : M \times (A/I) \to M/IM$ définie par $\tilde{\varphi}(m, \overline{a}) = am \bmod (IM)$. Par définition de la structure de A-module sur M/IM, cette application est A-bilinéaire.Elle induit donc un morphisme $\varphi \in Hom_A(M \otimes_A (A/I); M/IM)$.
Considérons ensuite $\psi : M \to M \otimes_A A/I$ définie par $\varphi(m) = m \otimes \overline{1}$. Son noyau continent I, et elle se factorise donc en une application A-linéaire $\mu : M/IM \to M \otimes_A (A/I)$ vérifiant $\mu(\overline{m}) = m \otimes \overline{1}$. On vérifie que ce sont deux applications inverses l'une de l'autre.

□

Corollaire II.2. *Si I et J sont deux idéaux de A, il existe un isomorphisme canonique entre $(A/I) \otimes_A (A/J)$ et $A/(I+J)$.*

Démonstration du corollaire.

$$\begin{aligned} A/I \otimes_A A/J &\cong (A/I)/(J \cdot A/I) \\ &\cong A/(I+J) \end{aligned}$$

par les théorèmes d'isomorphismes de première année.

□

En particulier, si I et J sont premiers entre eux, $A/I \otimes_A A/J = \{0\}$.

II-D. Exemples de calculs de produits tensoriels

On calcule dans cette section plusieurs produits tensoriels : Soit $n \geq 1$ un entier naturel.

- $$\begin{aligned} \mathbb{Z}^n \otimes_{\mathbb{Z}} \mathbb{Q} &\cong (\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q})^n \\ &\cong \mathbb{Q}^n \end{aligned}$$

- $$\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$$

- $$(\mathbb{Q}/\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = \{0\}$$

  En effet,
  $$\overline{q} \otimes \overline{k} = \frac{\overline{q}}{n} \otimes n\overline{k} = 0$$
  Le point essentiel est ici que $\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$ et que $\mathbb{Z}/n\mathbb{Z}$ est un module de torsion.

- $$\mathbb{Q} \otimes_{\mathbb{Z}} \cong \mathbb{R}$$

- $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ est un $\mathbb{R}$-module libre de rang 4. Il est donc isomorphe à $\mathbb{C}^2$.

II-E. Changements de bases et produit tensoriel d'algèbres

Dans toute la suite, A, B et C désigneront trois anneaux commutatifs. Considérons $f : A \to B$ un morphisme d'anneaux. Il permet de munir B d'une structure de A-module et, conséquemment, de munir tout B-module d'une structure de A-module. On appelle cette opération la restriction des scalaires. Réciproquement, si l'on considère un A-module, peut-on le munir, de manière naturelle, d'une structure de B-module ? Le produit tensoriel nous permet de répondre par l'affirmative à cette question, grâce au théorème suivant :

Théorème II.2. *Soit M un A-module et B un A-module. Il existe une unique structure de B-module sur $M \otimes_A B$ compatible avec la structure de A-module sur $M \otimes_A B$ et vérifiant*

$$\forall (b, b', m) \in B \times B \times M,\ b \cdot m \otimes b' = m \otimes (bb') \tag{1}$$

Le B-module ainsi obtenu est appelé <u>extension des scalaires de M à B</u>.

Démonstration du théorème. • <u>Unicité :</u> Un module est uniquement déterminé par sa structure abélienne et son action. Ici, la structurede groupe abélien est fixée par construction du A-module $M \otimes_A B$, et l'action de B sur ce groupe est donnée par l'équation 1.

• <u>Existence :</u> Il faut définir l'action de B sur $M \otimes_A B$. Pour cela, fixons $b \in B$ et considérons l'application suivante :

$$\begin{array}{rl} \tilde{\mu_b} : & M \times B \longrightarrow M \otimes_A B \\ & (m, b') \longrightarrow m \otimes b'b \end{array}$$

Elle est A-bilinéaire et induit donc une application $\mu_b \in Hom_A(M \otimes_A B; M \otimes_A B)$. On pose ensuite pour tout tenseur v et pour tout $b \in B$ $b \cdot v := \mu_b(v)$. On vérifie que cette action définit une structure convenable.

□

La preuve de la proposition suivante est laissée en exercice :

Proposition II.7. *Si M est un A-module libre de base $(e_i)_{i \in I}$, $M \otimes_A B$ est un B-module libre de base $(e_i \otimes A)_{i \in I}$.*

Passons à présent au produit tensoriel d'algèbres :

Proposition II.8. *Soient B et C deux algèbres sur A commutatives. Il existe une unique structure de A-algèbre sur $B \otimes_A C$ vérifiant*

$$\forall ((b, b'), (c, c')) \in B^2 \times C^2, (b \otimes c) \cdot (b' \otimes c') = (bb') \otimes (cc') \tag{2}$$

Son morphisme structural est donné par l'application qui à $a \in A$ associe $a \cdot (1 \otimes 1)$.

III. Propriétés fonctorielles du produit tensoriel

III-A. Catégories et foncteurs

III-A- 1. Notion de catégorie

Définition III.1. *Une catégorie $\mathcal{C}$ est*

- *Une famille d'objets $Ob(\mathcal{C})$.*
- *Pour toute paire (A, B) d'objets de $\mathcal{C}$, un ensemble de flèches (aussi appelées morphisme) noté $Hom_{\mathcal{C}}(A; B)$.*
- *Pour tout triplet (A, B, C) d'objets de $\mathcal{C}$, une loi de composition $\circ : Hom_{\mathcal{C}}(A; B) \times Hom_{\mathcal{C}}(B, C) \to Hom_{\mathcal{C}}(A; C)$ vérifiant les propriétés suivantes :*
  - *i) $Hom_{\mathcal{C}}(A; B)$ et $Hom_{\mathcal{C}}(A'; B')$ sont disjoints sauf si $A = A$ et $B = B'$.*
  - *ii) Pour tout objet A de $\mathcal{C}$, il existe un morphisme $id_A \in Hom_{\mathcal{C}}(A; A)$ se comportant comme l'identité à droite (resp. à gauche) relativement à $\circ$ pour les éléments de $Hom_{\mathcal{C}}(B; A)$ (resp. pour les éléments de $Hom_{\mathcal{C}}(A; B)$).*
  - *iii) $\circ$, lorsqu'elle est bien définie, est associative.*

Exemple . • La catégorie des ensembles, notée *Ens*, dont les objets sont les ensembles et les morphismes les applications ensemblistes. La loi de composition est la loi de composition usuelle.

- Si A est un anneau commutatif, on note $A - mod$ la catégorie des A-modules à gauche, dont les objets sont les A-modules à gauche, les morphismes les applications A-linéaires et la loi de composition est la loi usuelle.
- $\mathcal{C}^0(\mathbb{R}^n)$ la catégorie dont les objets sont les ouverts et les morphismes les applications continues entre ouverts.

Définition III.2. *Soit $\mathcal{C}$ une catégorie. Pour toute paire (A, B) d'objets de $\mathcal{C}$, on dit que $f \in Hom_{\mathcal{C}}(A; B)$ est un isomorphisme s(il existe $g \in Hom_{\mathcal{C}}(B; A)$ tel que*

i) $f \circ g = id_B$

ii) $g \circ f = id_A$

Si $B = A$, on parle d'automorphisme.

Exercice . Montrer que l'ensemble $(End_{\mathcal{C}}(A) := Hom_{\mathcal{C}}(A; A), \circ)$ est un monoide, puis que l'ensemble des automorphismes de A est un groupe, en général non abélien.

Solution . C'est immédiat.

Définition III.3. *Soit $\mathcal{C}$ une catégorie. Un objet P de $\mathcal{C}$ est dit :*

- *initial si pour tout objet A de $\mathcal{C}$,$|Hom_{\mathcal{C}}(P; A)| = 1$.*
- *final si pour tout objet A de $\mathcal{C}$, $|Hom_{\mathcal{C}}(A; P)| = 1$.*

On dit alors que P est de type initial ou de type final.

Exemple . • Le groupe trivial est un objet initial dans la catégorie *Gr* des groupes.

- $\mathbb{Z}$ est un objet initial dans la catégorie *An* des anneaux.

Exercice . Montrer que si P et P' sont deux objets de même type, il existe un unique isomorphisme entre P et P'.

Solution . Supposons que P et P' soient deux objets initaux. Ainsi, il y a un unique morphisme φ de P dans P' et un unique morphisme ψ de P' dans P. Ainsii, $\varphi \circ \psi$ est un morphisme de P' dans lui-même. Mais $id_{P'}$ est déjà un morphisme de P' dans P'. P' étant initial, on en déduit $\varphi \circ \psi = id_{P'}$.

De même, $\psi \circ \varphi = id_P$. On en déduit donc que φ et ψ sont deux isomorphismes, et qu'ils sont par ailleurs uniques.
Le cas d'objets finaux se traite de manière similaire.

III-A- 2. Notion de foncteur

Définition III.4. *Soient $\mathcal{C}$ et $\mathcal{C}'$ deux catégories. Un <u>foncteur covariant de $\mathcal{C}$ dans $\mathcal{C}'$</u> est une construction $F : \mathcal{C} \to \mathcal{C}'$ envoyant tout objet de $\mathcal{C}$ sur un objet de $\mathcal{C}'$ et tout morphisme $f \in Hom_{\mathcal{C}}(A; B)$ sur un élément $F(f) \in Hom_{\mathcal{C}}(F(A); F(B))$ vérifiant*

1. *Pour tout objet A de $\mathcal{C}$, $F(id_A) = id_{F(A)}$*
2. *Pour toute paire de morphismes $(f, g) \in Hom_{\mathcal{C}}(A; B) \times Hom_{\mathcal{C}}(B; C)$, $F(g \circ f) = F(g) \circ F(f)$*

Un <u>foncteur contravariant de $\mathcal{C}$ dans $\mathcal{C}'$</u> est une construction $F : \mathcal{C} \to \mathcal{C}'$ envoyant tout objet de $\mathcal{C}$ sur un objet de $\mathcal{C}'$ et tout morphisme $f \in Hom_{\mathcal{C}}(A; B)$ sur un élément $F(f) \in Hom_{\mathcal{C}}(F(B); F(A))$ vérifiant

1. *Pour tout objet A de $\mathcal{C}$, $F(id_A) = id_{F(A)}$*
2. *Pour toute paire de morphismes $(f, g) \in Hom_{\mathcal{C}}(A; B) \times Hom_{\mathcal{C}}(B; C)$, $F(g \circ f) = F(f) \circ Fgf)$*

Exemple . • Si M est un A-module fixé, le produit tensoriel par M au dessus de A est un foncteur covariant de la catégorie des A-modules dans elle-même. On le note $(-\otimes_A M, -\otimes_A id_M)$, On se reporte au troisième exercice du Td1.

- Pour tout anneau commutatif A, on se fixe un A-module M. Considérons la construction suivante : Si N est un A-module, on l'envoit sur $Hom_A(N; M)$.
  Si $f \in Hom_A(N_1; N_2)$, f est envoyé sur l'application envoyant $g \in Hom_A(N_2; M)$ sur $g \circ f \in Hom_A(N_1; M)$. C'est un foncteur contravariant, noté $Hom_A(-; M)$ de la catégorie $\underline{A - mod}$ dans elle-même. On peut définir de la même manière un foncteur covariant, noté $Hom_A(M; -)$.

III-B. Exactitude et platitude

III-B- 1. Suites exactes et suites exactes courtes

Définition III.5. *Soit $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ une suite d'applications A-linéaires. On dit qu'elle est <u>exacte en M_2</u> si* $\ker(g) = im(f)$.
Plus généralement, une suite d'applications A-linéaires

$$M_1 \xrightarrow{f_1} M_2 \to \dots \xrightarrow{f_{n-1}} M_n$$

est dite <u>exacte</u> si elle est exacte en chacun des $M_i, i \in [|2; n-1|]$
Une suite exacte courte est une suite exacte

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$$

telle que f soit injective et g surjective.

Une suite exacte courte est traditionnellement notée

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$$

Exemple . Si M est un A-module et si N est un sous-A-module de M, on a la suite exacte suivante :

$$0 \to N \hookrightarrow M \twoheadrightarrow M/N \to 0$$

III-B- 2. Notion de foncteur exact

Définition III.6. *Soient A et B deux anneaux commutatifs. Un foncteur covariant $F : \underline{A-mod} \to \underline{B-mod}$ est dit <u>exact</u> s'il préserve les suites exactes courtes i.e si pour toute suite exacte courte*

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$$

la suite

$$0 \to F(M_1) \xrightarrow{F(f)} F(M_2) \xrightarrow{F(g)} F(M_3) \to 0$$

est exacte. On définit de manière similaire la notion d'exactitude pour un tenseur contravariant.

Exemple . • Le foncteur $-\otimes_A A$ est exact.

• Le produit tensoriel au dessus de A par n'importe quel A-module n'est en général pas un foncteur exact : l'injectivité des applications peut être mise en défaut.

Définition III.7. *Un foncteur covariant $F : \underline{A-mod} \to \underline{B-mod}$ est dit <u>exact à droite</u>(resp. à gauche) si pour toute suite exacte*

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$$

$$(resp. M_1 \xleftarrow{f} M_2 \xleftarrow{g} M_3 \leftarrow 0)$$

la suite

$$F(M_1) \xrightarrow{F(f)} F(M_2) \xrightarrow{F(g)} F(M_3) \to 0$$

$$(resp. F(M_1) \xleftarrow{F(f)} F(M_2) \xleftarrow{F(g)} F(M_3) \leftarrow 0)$$

est exacte.

Par exemple, si M est un A-module, il a une strcture de groupe abélien. On a donc un foncteur $\underline{A-mod} \to \underline{\mathbb{Z}-mod}$ appelé foncteur d'oubli, dont on peut vérifier qu'il est exact.

Théorème III.1. *Soit A un anneau commutatif unifère et M un A-module. Alors*

- *$Hom_A(M;-)$ est exact à gauche.*
- *$-\otimes_A M$ est exact à droite.*

Démonstration du théorème. Pour vérifier que le foncteur covariant $Hom_A(M;-)$ est exact à droite, donnons-nous une suite exacte

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$$

et considérons la suite

$$0 \to Hom_A(M;M_1) \xrightarrow{f\circ -} Hom_A(M;M_2) \xrightarrow{g\circ -} Hom_A(M;M_3)$$

dont on veut montrer qu'elle est exacte.
L'injectivité de la composition par f est une conséquence immédiate de l'injectivité de f, et la relation $im(f) = \ker(g)$ donne directement l'inclusion $im(f\circ -) \subseteq \ker(g\circ -)$.
Pour établir l'inclusion inverse, considérons $\psi \in Hom_A(M;M_2)$ tel que $g\circ\psi = 0$. Ainsi, $im(\psi) \subset im(f)$. On peut donc considérer une application $\tilde{\psi} : im(\psi) \to M_1$ envoyant x sur son unique antécédent par f. On vérifie immédiatement que $\tilde{\psi}$ est A-linéaire, puis que $\psi = f\circ\tilde{\psi}$.Ceci conlut la preuve.
Pour montrer que le foncteur $-\otimes_A M$ est un foncteur exact à gauche, fixons nous une suite exacte

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$$

et considérons son image sous le foncteur $-\otimes_A M$:

$$M_1\otimes_A M \overset{f\otimes_A id_M}{\to} M_2\otimes_A M \overset{g\otimes_A id_M}{\to} M_3\otimes_A M \to 0$$

La surjectivité de $g\otimes_A id_M$ est évidente et découle immédiatement de la surjectivité de g : l'image de $g\otimes_A id_M$ contient les tenseurs simples de $M_3\otimes_A M$. Or ceux-ci engendrent le A-module $M_3\otimes_A M$. Montrons donc que $\ker(g\otimes_A id_M) = im(f\otimes_A id_M)$. L'inclusion $im(f\otimes_A id_M) \subseteq \ker(g\otimes_A id_M)$ est immédiate : en effet, $(g\otimes_A id_M)\circ(f\otimes_A id_M) = (g\circ f)\otimes id_M$. Établissions l'inclusion réciproque : pour cela, on va ruser, en montrant en fait que l'application $g\otimes_A id_M$ induit un isomorphisme $\tilde{g}$: $(M_3\otimes_A M)/(im(f\otimes_A id_M)) \cong M_3\otimes_A M_3$ (remarquons déjà que, par la première étape, g se factorise à travers le quotient voulu en une application A-linéaire $\tilde{g}$.). Pour cela, on va construire une application réciproque $g' : M_3\times M \to (M_2\otimes_A M)/im(f\otimes_A id_M)$. Considérons $\pi : M_2\otimes_A M \to (M_2\otimes_A M)/(im(f\otimes_A id_M))$ la surjection canonique. Si $(z,m)\in M_3\times M$, on a envie de poser $g'(m,z) = \pi y\otimes m$ où y est un antécédent quelconque de z par g. Il faut donc vérifier que cette application est bien définie, *i.e* qu'elle ne dépend pas du choix de l'antécédent de z par g. Soient donc $y, y' \in M_2$ deux antécédents de z par g. Alors $y - y' \in im(f)$ et donc on peut choisir $x\in M_1$ tel que $f(x) = y - y'$. Ainsi, $\pi((y-y')\otimes m) = 0$, et on peut donc poser $g'(z\otimes m) = \pi(y\otimes m)$ avec y un antécédent quelconque de z par g. Par ailleurs, g' est A-bilinéaire (par construction). Par propriété universelle du produit tensoriel, il existe une unique application $\tilde{g"} \in Hom_A(M_3\otimes_A M; (M_2\otimes_A M)/im(f\otimes_A id_M)$ telle que pour tout $(m_3, m)\in M_3\times M$, $\tilde{g'}(m_3\otimes m) = \pi(n_2\otimes m)$ où n_2 est un antécédent quelconque de m_3 par g.
Remarquons alors que $\tilde{g"}\circ\tilde{g}(\pi(x\otimes m)) = \pi(x\otimes m)$. Ces classes d'équivalence engendrent le A-module $(M_2\otimes_A M)/im(f\otimes_A id_M)$, et donc $\tilde{g"}\circ\tilde{g} = id$. De même, on vérifie que $\tilde{g}\circ\tilde{g"} = Id$. $\tilde{g}$ et $\tilde{g"}$ sont ainsi deux isomorphismes inverses l'un de l'autre.

□

ATTENTION : $-\otimes_A M$ n'est en général pas un foncteur exact. On le vérifie par exemple avec $-\otimes_{\mathbb{Z}}\mathbb{Z}/n\mathbb{Z}$ et la suite exacte

$$0\to\mathbb{Z}\overset{\cdot n}{\to}\mathbb{Z}\twoheadrightarrow\mathbb{Z}/n\mathbb{Z}\to 0$$

le défaut d'exactitude provenant dans ce cas de la présence d'éléments de torsion : En effet, si l'on tensorise au dessus de $\mathbb{Z}$ par $\mathbb{Z}/n\mathbb{Z}$, on obtient la suite (non exacte à priori)

$$0\to\mathbb{Z}/n\mathbb{Z}\overset{0}{\to}\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/n\mathbb{Z}\to 0$$

qui n'est clairement pas exacte.

Définition III.8. *Un A-module M est dit <u>plat</u> si le foncteur $-\otimes_A M$ est exact.*

On prendra bien garde au fait que cette notion est, de manière intrinsèque, liée à l'anneau au dessus duquel on tensorise : par exemple, $\mathbb{Z}/n\mathbb{Z}$ est plat au-dessus de $\mathbb{Z}/n\mathbb{Z}$, mais il ne l'est pas sur $\mathbb{Z}$. De manière générale, tout anneau commutatif unifère est plat sur lui-même.

Exercice . i) Montrer qu'un A-module M est plat si et seulement si pour toute injection A-linéaire $f : M_1\to M_2$ $f\otimes_A id_M$ est injective.

ii) Montrer que tout A-module libre est plat.

Théorème III.2. *Soient M et N deux modules sur un anneau commutatif unifère A. Alors*

i) Si M et N sont plats, alors $M\otimes_A N$ est plat.

ii) Si A est un anneau principal, M est plat si et seulement si M est sans torsion.

Démonstration du théorème. i) Le premier point est une conséquence immédiate de l'associativité du produit tensoriel.

ii) Soit M un A-module plat. Montrons qu'il est sans torsion. Prouvons dans un premier temps le résultat suivant : si A est un anneau commutatif unifère et si M est un A-module plat, alors M est sans torsion.
En effet, en notant $K := Fr(A)$, on vérifie, comme dans les Td[2] que M_t l'ensemble des éléments de torsion de M vérifie

$$M_t = \ker(\varphi), \varphi : m \in M \mapsto 1 \otimes m \in K \otimes_A M$$

En passant à l'isomorphisme canonique $A \otimes_A M \cong M$, φ correspond à $\psi : a \otimes m \in A \otimes_A M \mapsto \frac{a}{1} \otimes m \in K \otimes_A M$ i.e $\psi = j \otimes id_m$ avec j l'injection canonique de A dans K. Par platitude de M, comme j est injective, on en déduit que $j \otimes id_M$ est injective, et donc que φ est injective. Ainsi, $M_t = \{0\}$. En particulier, sur un anneau principal, tout module plat est sans torsion.
Réciproquement, soit M un A-module sans torsion. Comme dans le Td2, poru vérifier que M est plat, il suffit de vérifier que pour tout idéal I de type fini de A, l'application A-linéaire "naturelle" $M \otimes_A I \to M$ est injective.
Mais la multiplication par $a \in A$ définit :

- Une injection A-linéaire $\mu_a : A \to A$.
- Un isomorphisme de A-modules $A \to I$.

□

III-B- 3. Adjonction de foncteurs

Donnons d'abord une caractérisation pratique des suites exactes :

Proposition III.1. *Une suite d'applications A-linéaires $M_1 \overset{f_1}{\to} M \overset{g}{\to} M_2 \to 0$ est exacte si et seulement si la suite $0 \to Hom_A(M_2; N) \overset{-\circ g}{\to} Hom_A(M; N) \overset{-\circ f}{\to} Hom_A(M_1; N)$ est exacte.*

Démonstration de la proposition. □

2. Td2 pour être exact

IV. Algèbres tensorielles, symétriques et extérieures

IV-A. Algèbre tensorielle d'un module

Définition IV.1. *Une A-algèbre graduée par $\mathbb{N}$ est une A-algèbre B munie d'une décomposition sous la forme $B = \oplus_{i=0}^{\infty} B_n$ vérifiant les conditions suivantes :*

- $B_0 = \rho(A)$
- *Pour tout couple d'entiers naturels (n, m), $B_n \cdot B_m \subseteq B_{n+m}$*

Les éléments de B_n sont appelés éléments homogènes de degré n.

Définition IV.2. *Soit M un A-module. On définit par récurrence sur $n \in \mathbb{N}$ le A-module $T^n M$ par*

- $T^0 M = A$
- *Si $n \geq 1$, $T^n M := T^{n-1} \otimes_A M$*

On appelle <u>algèbre tensorielle de M sur A</u> la A-algèbre définie par

$$TM := \oplus_{i=0}^{\infty} T^i M$$

muni de la multiplication définie par sa restrictions aux sous-modules $T^n M$ et $T^m M$ comme

$$\underset{\in T^n M}{x} \cdot \underset{\in T^m M}{y} := \underset{\in T^{n+m} M}{x \otimes y}$$

En fait, $T^n M$ est l'objet correspondant à la propriété universelle suivante :

Toute application n-linéaire $M \to N$ se factorise de manière unique par une application $\varphi \in Hom_A(T^n M; N)$.

Justifions que la multiplication ainsi définie vérifie les bonnes propriétés, c'est-à-dire qu'elle est A-bilinéaire. Pour cela, considérons l'application $(x, y) \in T^n M \times T^m M \to x \otimes y \in T^{n+m} M$. Elle est bilinéaire et se factorise, par propriété universelle en une application A-linéaire sur $T^n M \otimes_A T^m M$. On prendra bien garde que l'algèbre TM n'est, en général, pas commutative : il n'y aucune raison que $x \otimes y = y \otimes x$ de manière générale.

Exercice . $T^1 M$ engendre TM en tant qu'algèbre. C'est une propriété fondamentale de l'agèbre tensorielle.

Solution . Une récurrence immédiate montre que $T^1 M$ engendre, en tant que A-algèbre, toutes les composantes homogènes de l'algèbre TM, d'où le résultat.

Exercice . L'algèbre tensorielle TM satisfait la propriété universelle suivante :

Pour toute A-algèbre graduée B, pour tout $\tilde{\varphi} \in Hom_A(M; B)$, $\tilde{\varphi}$ se factorise de manière unique en morphisme d'algèbres graduées $\varphi : TM \to B$.

Solution . Il suffit en effet de définir φ sur les éléments de $T^1 M$.

Ainsi, la construction de l'agèbre tensorielle provient d'un foncteur T de la catégorie des A-modules dans les A-algèbres graduées :

IV-B. Algèbre symétrique d'un module

Définition IV.3. *<u>L'algèbre symétrique d'un A-module M</u> est le quotient abélien maximal de TM. On le note $Sym_A(M)$. Il est muni d'un structure d'algèbre graduée.*

En fait, on a une construction explicite de $Sym_A(M)$: si on pose I l'idéal du A-module TM engendré par les relations $\{x_1 \otimes x_n - x_{\sigma(1)} \otimes x_{\sigma(n)}, \sigma \in S_n, n \in \mathbb{N}\}$, qui est un idéal bilatère. Alors $Sym_A(M) = TM/I$.
On verra en TD que les composantes homogènes de degré n de $Sym_A(M)$, appelées n-ième puissances symétriques de M s'obtienne par quotient de $T^n M$ par un idéal de la forme de I. Par construction, $Sym^0 M = A$ et $Sym^1 M = M$.

Exercice . Soit $f : M \to B$ une application A-linéaire entre un A-module et une algèbre graduée vérifiant $f(x)f(y) = f(y)f(x)$. Alors f se factorise de manière unique à travers $Sym_A(M)$.

On en déduit donc l'existence d'un foncteur Sym et d'une infinité de foncteurs Sym^n.
Donnons enfin un exemple d'algèbre symétrique : un calcul immédiat montre, TA étant commutatif, $TA \cong symA \cong \oplus A \cong A[X]$.

Théorème IV.1. *Soient M et N deux A-modules. Alors*
- $T^n(M \otimes_A N) \cong T^n M \otimes_A T^n M$
- $Sym_A(M) \otimes_A Sym_A(N) \cong Sym(M \oplus N)$ *pour leurs structures d'algèbres sur A graduées.*

Démonstration du théorème. Le premier point est immédiat. En ce qui concerne le second, les applications A-linéaires canonique $f : M \to M \oplus N$ et $g : N \to M \oplus N$ donnent lieu, par fonctorialité de Sym à deux morphismes de A-algèbres graduées : $\mu : Sym_A(M) \to Sym_A(M \oplus N)$ et $\nu : N \to Sym_A(M \oplus N)$. Par propriété universelle du produit tensoriel, on en déduit donc une application $\mu \otimes \nu : Sym_A(M) \otimes_A Sym_A(N) \to Sym_A(M \oplus N)$ dont on vérifie que c'est un morphisme d'algèbres graduées.
Pour montrer qu'il s'agit bien d'un isomorphisme, on va construire explicitement l'application réciproque. Comme dans les sections précédentes, il suffit de construire une application $f : M(\cong Sym^1_A(M)) \to Sym_A(M) \otimes Sym_A(N)$et $g : N(\cong Sym^1_A(N)) \to Sym_A(M) \otimes Sym_A(N)$

Appliquons cela au A-module A^r ou à tout A-module libre de rang $r \geq 1$. Ainsi, la A-algèbre graduée $Sym_A(A^r)$ est isomorphe à $A[X_1, \ldots, X_r]$: en effet, par commutativité de A, on sait que $TA = \oplus_{n \in \mathbb{N}} A$ est isomorphe à $Sym_A(A)$ et donc $Sym_A(A) = A[X]$. Le résultat précédent permet alors d'écrire $Sym_A(A^r) \cong A[X] \otimes_A \ldots \otimes_A A[X]$.

Exercice . Soit M un A-module libre de rang r. Montrer que $Sym^d_A(M)$ est libre de base $\{e_{i_1} \otimes \ldots e_{i_d}, i_1, \ldots, i_d \in \mathbb{N}_d, i_1 \leq \cdots \leq i_d\}$.

IV-C. Algèbres et puissances extérieures

Définition IV.4. *On appelle <u>n-ième puissance extérieure d'un A-module M</u> le A-module quotient*

$$\Lambda^n M := T^n M / J_n$$

où J_n est le sous A-module de $T^n M$ engendré par les relations :$\{m_1 \otimes \ldots \otimes m_n, \exists i \neq j | m_i = m_j\}$. <u>L'algèbre extéieure du module M</u> est alors définie par

$$\Lambda M := \oplus_{n=0}^{+\infty} \Lambda^n M$$

Définition IV.5. *Si $(m_1, \ldots, m_n) \in M^n$, on note $m_1 \wedge \ldots m_n$ l'image de $m_1 \otimes \ldots \otimes m_n$ dans ΛM.*

ATTENTION : ΛM n'est pas commutatif !!! En effet, $x \wedge y = -y \wedge x$.

Lemme IV.1. *Pour toute application A-linéaire $f : M \to N$, il existe une unique application $f^\wedge : \Lambda M \to \Lambda N$ telle que pour tout $(m_1, \ldots, m_n) \in M^n$ on a $f^\wedge(m_1 \wedge \ldots m_n) = f(m_1) \wedge \ldots f(m_n)$.*

Proposition IV.1 : *Propriété universelle de l'algèbre extérieure. Pour toute application A-n- linéaire alternée $f : M^n \to N$, il existe une unique application linéaire $\varphi : \Lambda^n M \to N$ telle que*

$$\forall (m_1, \dots, m_n) \in M^n, \varphi(m_1 \wedge \dots m_n) = f(m_1, \wedge \dots f(m_n)$$

Cette proposition est immédiate : il suffit simplement de remarquer que, sur chaque composante homogène, l'application f passe au quotient.

IV-D. Déterminants d'applications A-linéaires

Soit M un A-module libre de rang $n \leq 1$. Soient N un A-module et $f \in Hom_A(M; N)$. Ainsi, pour tout entier $r \geq r$, on dispose d'une application A-linéaire $\Lambda^r f : \Lambda^r M \to \Lambda^r N$ telle que pour tout $(m_1, \dots, m_R) \in M^r, \Lambda^r f(m_1 \wedge \dots m_r) = f(m_1) \wedge \dots \wedge f(m_r)$. Mais on sait que $\Lambda^n M$ est libre de base $\{e_1 \wedge e_n\}$. Ainsi, $\Lambda^n f$ est un multiple de $e_1 \wedge \dots \wedge e_n$.

Définition IV.6. *On appelle <u>déterminant de f</u> l'unique scalaire λ tel que*

$$f = \lambda \cdot e_1 \wedge \dots \wedge e_n$$

Ainsi, pour tout $(m_1, \dots, m_n) \in M^n$, on a l'égalité

$$f(m_1) \wedge \dots \wedge f(m_n) = \Lambda^n f(m_1 \wedge \dots \wedge e_n) = det(f) m_1 \wedge \dots \wedge m_n$$

Théorème IV.2. *Soit M un A-module libre de rang n. Alors pour tout $f \in Hom_A(M : M)$, f est inversible si et seulement si $det(f)$ est inversible, si et seulement si f est surjective.*

V. De la localisation aux anneaux de valuation discrète

V-A. Rappels sur la localisation

V-A- 1. Localisation des anneaux

A désigne toujours un anneau commutatif.

Définition V.1. *Soit $S \subset A$. On dit que S est une partie multiplicative de A si*

i) $1_A \in S$

ii) Pour tout $(s,t) \in S^2, s \cdot t \in S$

Exemple . Si A est intègre, l'ensemble de ses éléments non nuls est une partie multiplicative de A.

Définition V.2. *Soit $S \subset A$ une partie multiplicative de A. Le localisé de A en S est l'ensemble des classes d'équivalence de $A \times S$ pour la relation d'équivalence $\sim$ définie par*

$$(a,s) \sim (b,t) \Leftrightarrow \exists u \in S |\ u(at - bs) = 0 \tag{3}$$

En d'autres termes, on demande que $at - bs$ soit un élément de A-torsion, mais que le coefficient de torsion puisse être choisi dans S. On note cet ensemble $S^{-1}A$.

Si $(a,s) \in A \times S$, on désigne sa classe déquivalence sous la relation $\sim$ par $[a,s]$ ou par $\frac{a}{s}$. Remarquons que si $0 \in S$, le localisé de S en A est réduit à un unique élément.

I.1.1 Structure d'anneau commutatif sur $S^{-1}A$ On définit une structure d'anneau commutatif sur $S^{-1}A$ en posant :

- $0_{S^{-1}A} := [(0,1)]$
- $1_{S^{-1}A} := [(1,1)]$
- Si $[(a,s)], [(b,t)] \in S^{-1}A$, on pose $[(a,s)] + [(b,t)] := [(at + bs, ts)]$
- Si $[(a,s)], [(b,t)] \in S^{-1}A$ pose $[(a,s)] \cdot [(b,t)] := [(ab, ts)]$

On vérifie que ces définitions ne dépendent pas des représentants choisis. Il s 'agit d'un simple jeu d'écriture.
On dispose d'une applciation naturelle $\rho : A \to S^{-1}A$ envoyant a sur $[(a,1)]$. Il est immédiat que, pour la structure ci-dessus, ρ est un morphisme d'anneaux commutatifs.

Exemple . Supposons A intègre. Considérons $A_0 := A \backslash \{0\}$. Le localisé de A en A_0 est naturellement isomorphe à $Frac(A) := k$, ce qui est immédiat vu la construction explicite du corps des fractions.

I.1.2 Propriété universelle du localisé

Proposition V.1. *Soit $S \subset A$ une partie multiplicative. Alors pour tout anneau B, pour tout morphisme d'anneaux $f : A \to B$ tel que $f(S) \subset B^*$, il existe un unique morphisme d'anneaux $\overline{f} : S^{-1}A \to B$ tel que, pour tout $(a,s) \in A \times S$, $\overline{f}([(a,s)]) = f(a)f(s)^{-1}$.*

Démonstration de la proposition. L'unicité est immédiate : la condition que l'on impose prescrit chacune des valeurs. Il faut donc montrer que l'on peut trouver un morphisme d'anneaux de cette forme.
Posons donc $\overline{f} : [(a,s)] \mapsto f(a)f(s)^{-1}$. Il suffit de vérifier que cette application est bien définie. Il est immédiat qu'il s'agit d'un morphisme d'anneaux.
Supposons donc $\frac{a}{s} = \frac{b}{t}$. Soit $u \in S$ tel que $u(at - bs) = 0$. Ainsi, $f(u)f(at - bs) = 0$. Comme $f(u) \in f(S) \subset B^*, f(at - bs) = 0$ d'où, f étant un morphisme d'anneaux, $f(a)f(s)^{-1} = f(b)f(t)^{-1}$. Ceci conlut la démonstration.

□

I.1.3 Idéaux du localisé Rappelons que l'image directe d'un idéal par un morphisme d'anneaux $f : A \to$ est un idéal du sous-anneau $f(A)$, mais pas nécessairement de B. En revanche, l'image réciproque d'un idéal par un morphisme d'anneaux est toujours un idéal de A.

Proposition V.2. *Soit S une partie multiplicative de A et ρ le morphisme canonique de A dans $S^{-1}A$. Alors :*

- *Pour tout idéal I de A, $S^{-1}I := \{[(i,s)], (i,s) \in I \times S\}$ est un idéal de $S^{-1}A$.*
- *L'application qui à un idéal I de A fait correspondre $S^{-1}I$ induit une bijection entre les idéaux premiers de $S^{-1}A$ et les idéaux de A ne rencontrant pas S. Elle préserve les inclusions et envoit idéaux maximaux de $S^{-1}A$ et idéaux maximaux de A.**dans le cas d'un localise premier, les ideaux maximaux sont tous envoyes sir** $\mathfrak{p}A_p$*

Avant de passer à la démonstration, rappelons deux formules : En notant, pour $A' \subset S^{-1}A$ $\Im(A')$ l'idéal engendré par A', on a

- Si I est un idéal de A, $S^{-1}I = \Im(\rho(I))$
- Si J est un idéal de $S^{-1}A$, $J = S^{-1}(\rho^{-1}(J))$

Démonstration de la proposition. • Le premier point est immédiat.

- **finir de taper cela**

□

V-A- 2. Lien avec les anneaux locaux

Définition V.3. *Soit A un anneau commutatif unifère. On dit que A est un <u>anneau local</u> s'il possède un unique idéal maximal. La notation $(A, \mathfrak{m})$ signifie que l'on considère un anneau local d'idéal maximal $\mathfrak{m}$. Le corps $A/\mathfrak{m}$ est appelé <u>corps résiduel de A</u>.*

I.2.1 Caractérisation des anneaux locaux

Proposition V.3. *Les assertions suivantes sont équivalentes :*

i) A est un anneau local.

ii) Le complémentaire des inversibles de A est un idéal de A.

iii) Pour tout $x \in A$, x ou$1 - x$ est inversible.

iv) La somme de deux éléments non inversibles est non inversible.

Démonstration de la proposition. Dans toute la suite, on note $A' := A \backslash A^*$.

- <u>i)⇒ii)</u> : Tout idéal maximal de A est inclus dans A'. Notons $\mathfrak{m}$ l'unique idéal maximal de A. Si $\mathfrak{m} \subsetneq A'$, alors il existe $y \in A' \backslash \mathfrak{m}$. Par le lemme de Krull, $\mathfrak{m}$ est contenu dans un idéal maximal autre que $\mathfrak{m}$, ce qui est absurde.
- <u>ii)⇒iii)</u> : Par l'absurde, soit $x \in A$ tel que x et $1 - x$ soient non inversibles. Comme A' est un idéal de A, il est stable par addition, et donc $1 = x + (1 - x) \in A'$, ce qui est absurde.
- <u>iii)⇒iv)</u> : Par l'absurde, soient x et y deux éléments non inversible de A tels que $x+y$ soit inversible, d'inverse z. Alors $xz + yz = 1$ et donc xz et $1 - xz$ sont non inversibles, ce qui est absurde.
- <u>iv)⇒iii)</u> : c'est immédiat en raisonnant par l'absurde.
- <u>iii)⇒ii)</u> : Il suffit de montrer que A' est stable par addition, les autres propriétés étant évidentes. Mais si $x, y \in A'$ vérifient $x + y \in A^*$ alors, si z en est un inverse, zx n'est pas inversible, de même que $1 - zx$, ce qui est absurde.
- <u>ii)⇒i)</u> : Comme dit plus haut, tout idéal maximal de A est inclus dans A'. Si ce dernier est lui-même un idéal, il s'agit du seul idéal maximal de A, et A est donc un anneau local.

□

I.2.2 Localisation par rapport à un idéal premier Étudions le cas fondamental de la localisation par rapport ùn idéal premier.

Définition V.4. *Soit $\mathfrak{p}$ un idéal premier de A. $A\backslash\mathfrak{p} := S_{\mathfrak{p}}$ est une partie multiplicative de A. Le localisé de A par rapport à $\mathfrak{p}$ est le localisé de A en $S_{\mathfrak{p}}$. On le note $A_{\mathfrak{p}}$.*

Théorème V.1. *Soit $\mathfrak{p}$ un idéal premier de A. Alors $A_{\mathfrak{p}}$ est un anneau local d'idéal maximal $\mathfrak{p}A_{\mathfrak{p}} := \Im(\rho(\mathfrak{p}))$. Son corps résiduel est isomorphe à $Fr(A/\mathfrak{p})$.*

Démonstration du théorème. Soit $\mathfrak{m}$ un idéal maximal de $A_{\mathfrak{p}}$. Par la proposition V.2, $\mathfrak{m}$ s'identifie, comme idéal premier, à un idéal de $A\backslash\mathfrak{p}$ et, comme il s'agit d'un idéal maximal, il s'identifie donc à $\mathfrak{p}$ (sinon, on pourrait trouver un idéal plus gros).
Étudions à présent le corps résiduel de $A_{\mathfrak{p}}$. On le note $k_{\mathfrak{p}}$. On dispose du diagramme suivant, où j et π désigne les surjections naturelles de, respectivement, A sur $A/\mathfrak{p}$ et de $A_{\mathfrak{p}}$ sur $A_{\mathfrak{p}}/(\mathfrak{p}A_{\mathfrak{p}})$, et i l'injection naturelle $A/\mathfrak{p} \hookrightarrow Frac(A/\mathfrak{p})$:

$$\begin{tikzcd}
A \arrow[r, two heads, "\rho"] \arrow[d, two heads, "j"] & A_{\mathfrak{p}} \arrow[d, two heads, "\pi"] \\
A/\mathfrak{p} \arrow[d, hook, "i"] & k_{\mathfrak{p}} = A_{\mathfrak{p}}/(\mathfrak{p}A_{\mathfrak{p}}) \\
Frac(A/\mathfrak{p}) &
\end{tikzcd}$$

On veut obtenir le diagramme suivant, où φ serait un isomorphisme de corps :

$$\begin{tikzcd}
A \arrow[r, two heads, "\rho"] \arrow[d, two heads, "j"] & A_{\mathfrak{p}} \arrow[d, two heads, "\pi"] \\
A/\mathfrak{p} \arrow[r, dotted, "\psi"] \arrow[d, hook, "i"] & k_{\mathfrak{p}} = A_{\mathfrak{p}}/(\mathfrak{p}A_{\mathfrak{p}}) \\
Frac(A/\mathfrak{p}) \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

Pour cela, on rajoute la flèche en pointillés, ce qui permet de conclure : détaillons un peu cela.
Par construction, $\mathfrak{p} \subset ker(\pi \circ \rho)$. On peut donc factoriser $\pi \circ \rho$ à travers $A/\mathfrak{p}$ en une application ψ. Maintenant, par propriété universelle du corps des fractions (notons qu'il est légitime de considérer cet objet, l'anneau $A/\mathfrak{p}$ étant premier par primalité de $\mathfrak{p}$), on peut étendre ψ en un morphisme de corps $\varphi : Frac(A/\mathfrak{p}) \to k_{\mathfrak{p}}$. Comme φ n'est pas identiquement nul, par construction, il est injectif. Pour conclure, il reste à établir la surjectivité de l'application φ.
Mais cela n'est guère compliqué. En effet, il suffit de remarquer que, par construction, ψ est surjective.

□

Exemple . Prenons $A = \mathbb{Z}$ et p un entier premier. L'anneau $\mathbb{Z}_{(p)}$ est un anneau local, d'idéal maximal engendré par p et de corps résiduel isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Attention toutefois, le corps résiduel ne caractérise pas le localisé : en effet, on remarque que le localisé de $\mathbb{Z}$ en $\{p^n, n \in \mathbb{N}\}$ est également $\mathbb{Z}_p$.

revoir les equivalences premier maximal dans les principaux

V-B. Localisation des modules

Définition V.5. *Soit M un A-module et S une partie multiplicative de A. Le localisé de M en S est l'ensemble $S \times M$ quotienté par la relation*

$$(s, m) \sim (s', m') \Leftrightarrow \exists u \in S, u(s'm - sm') = 0 \tag{4}$$

On le note $S^{-1}M$.

De même que précedemment, on notera indifféremment $\frac{m}{s}$ ou $[(m,s)]$ la classe de (m,s) sous la relation d'équivalence $\sim$. De même que dans la première sous-partie, on peut munir $S^{-1}M$ d'une structure de $S^{-1}A$ module (et ainsi, par restriction des scalaires, de A-module) tel que le morphisme canonique $\rho_M : M \to S^{-1}M$ soit une application $\underline{\underline{A}}$-linéaire.

Théorème V.2. *Il existe un isomorphisme canonique de $S^{-1}A$ modules*

$$S^{-1}M \cong S^{-1}A \otimes_A M$$

pour la structure naturelle de $S^{-1}A$ module sur $S^{-1}A \otimes_A M$ définie par extension des sclaires.

Démonstration du théorème. Posons, pour toute paire $([(a,s)],m) \in S^{-1}A \times M$

$$\varphi([(a,s)],m) := \frac{1}{s}\rho_M(am) = \frac{a}{s}\rho_M(m)$$

C'est un simple exercice d'écriture de vérifier que φ est bien définie et A-bilinéaire. φ induit donc une application $\overline{\varphi} : S^{-1}A \otimes_A M \to S^{-1}M$ vérifiant

$$\forall([(a,s)],m) \in S^{-1}A \times M, \overline{\varphi}([(a,s)] \otimes m) = \frac{a}{s}\rho_M(m)$$

Remarquons à présent que , si $(\frac{a}{s}, m, \frac{b}{t}) \in S^{-1}A \times M \times S^{-1}A$, on a les égalités suivantes :

$$\begin{aligned}\overline{\varphi}(\frac{b}{t}(\frac{a}{s} \otimes m)) &= \frac{ab}{st}\rho_M(m) \\ &= \frac{b}{t}\overline{\varphi}(\frac{a}{s} \otimes m)\end{aligned}$$

Les tenseurs simples engendrent le $S^{-1}A$-module $S^{-1}A \otimes_A M$, d'où l'on déduit que $\overline{\varphi}$ est $S^{-1}A$ linéaire. Construisons explicitement un inverse de $\overline{\varphi}$. Pour cela, on pose, pour $\frac{m}{s} \in S^{-1}M$

$$\psi(\frac{m}{s}) := \frac{1}{s} \otimes m \in S^{-1}A \otimes_A M$$

Elle et bien définie et $S^{-1}A$-linéaire. Il est alors clair que φ et ψ sont deux applications linéaires inverses l'une de l'autre.

□

II.0.3 Propriété universelle du localisé Soit A un anneau, S une partie multiplicative de A, M et N deux A-module. Si pour tout $s \in S$ l'application $\mu_S : n \in N \mapsto sn \in N$ est un isomorphisme de A-modules, pour toute application $f \in Hom_A(M;N)$, il exite un unique $\overline{\varphi} \in Hom_A(S^{-1}M;N)$ tel que pour tout $m \in M$, $\overline{\varphi}(\frac{m}{a}) = f(m)$.
Considérons en effet $\overline{\varphi} : \frac{m}{s} \mapsto \mu_s^{-1}(f(m))$. Cette application A-linéaire convient. Vérifions que c'est la seule : soit ψ une autre application A-linéaire de $S^{-1}M$ dans N telle que

$$\forall m \in M, \psi(\frac{m}{1}) = f(m)$$

Alors, pour tout $(\frac{m}{s}) \in S^{-1}M$ $\psi(\frac{m}{s}s) = f(m)$, d'où $\psi(\frac{m}{s}) = \mu_s^{-1}f(m)$.

V-B- 1. Propriétés locales

Définition V.6. *Soit M un A-module. Une propriété (P) est dite <u>propriété locale</u> si les assertions suivantes sont équivalentes :*

1. *M vérifie (P).*
2. *$M_{\mathfrak{p}}(:= A_{\mathfrak{p}} \otimes_A M)$ vérifier (P) pour tout idéal premier $\mathfrak{p}$ de A.*

Proposition V.4. *La propriété "être nul" est une propriété locale.*

Démonstration de la proposition. Il est clair que si $M = \{0\}$, tous ses localisés sont également nuls.
Réciproquement, supposons que pour tout idéal premier $\mathfrak{p}$ de A, $M_{\mathfrak{p}} = \{0\}$. Soit $m \in M$. Ainsi, pour tout idéal premier $\mathfrak{p}$ de A il existe $s_{\mathfrak{p}} \in A \backslash \mathfrak{p}$ tel que $s_{\mathfrak{p}} m = 0$.
Soit $I := \{a \in A, am = 0\}$. I est un idéal qui n'est inclus dans aucun idéal maximal, d'où l'on conclut que $I = A$. Ainsi, $m = 0$, ce qui achève la démonstration.

□

Théorème V.3. *La platitude est une propriété locale.*

V-C. Anneaux de valuation discrète

V-C- 1. Valuations sur un corps

Définition V.7. *Soit k un corps. Une valeur absolue sur k est une application $|\cdot| : k \to \mathbb{R}^+$ telle que*

- $|x| = 0$ *si et seulement si* $x = 0$.
- *Pour tout* $(\lambda, x) \in k^2$, $|\lambda x| = |\lambda| \cdot |x|$.
- *Pour tout* $(x, y) \in k^2$, $|x + y| \leq |x| + |y|$.

La distance sur k définie par $d'x, y) := |x - y|$ est appelée distance associée à la valeur absolue. Deux valeurs abslues sur k sont dites équivalentes si les distances associées induisent des topologies équivalentes.

Définition V.8. *Notons $\overline{\mathbb{R}} := \mathbb{R} \cup \{+\infty\}$ pour sa structure de monoide totalement ordonné naturelle. Une valuation réelle sur k est une application $v : k \to \overline{\mathbb{R}}$ telle que*

- $v(x) = \infty$ *si et seulement si* $x = 0$.
- *Pour tout* $(x, y) \in k^2, v(xy) = v(x) + v(y)$.
- *Pour tout* $(x, y) \in k^2, v(x + y) \geq \inf(v(x), v(y))$.

Remarque. Une valuation réelle est essentiellement caractérisée par un morphisme

$$\begin{array}{rl} f: & (k^*, x) \longrightarrow (\mathbb{R}, +) \\ & x \mapsto v(x) \end{array}$$

En particulier, $v(k^*)$ est un sous-groupe de $\mathbb{R}$. Il est donc discret ou dense. On dit qu'une valuation réelle v sur un corps k est dite discrète si le sous-groupe qu'elle engendre de manière naturelle est discret. Elle est dite |underlinenormalisée si $v(k^*) = \mathbb{Z}$. Remarquons qu'une valuation discrète admet toujours une valuation discrète équivalente normalisée.

Exemple . Un exemple fondamental est la valuation p-adique. Soit p un entier naturel premier. On pose $v_p(0) = +infty$ et, pour tout $a \in \mathbb{Z}$, $v_p(a)$ la valuation p-adique usuelle. On l'étend à $\mathbb{Z} \times \mathbb{Z} \backslash \{0\}$ en posant $v_p(\frac{a}{b}) := v_p(a) - v_p(b)$.

V-C- 2. Anneaux de valuation

Définition V.9. *Soit A un anneau intègre, de corps des fractions k. On dit que A est un anneau de valuation discrète s'il existe une valuation discrète sur k telle que $A = \{x \in k, v(x) \geq 0\}$.*

On note généralement, pour k un corps et v une valuation réelle sur k, $\mathcal{O}_k(v) := \{x \in k, v(x) \geq 0\}$ l'anneau de la valuation.

Proposition V.5. *Supposons que $A = \mathcal{O}_k(v)$ pour une certaine valuation v sur son corps des fractions. Les inversibles de $\mathcal{O}_k(v)$ sont exactement les éléments de valuation nulle. A est un anneau local d'idéal maximal $\{x \in A, v(x) > 0\}$.*

Proposition V.6. *Soit A un anneau de valuation discrète pour (k, v). Alors*

i) A est un anneau local d'iéal maximal $\{x \in A, v(x) \geq 1\}$.

ii) Les idéaux de A sont les $\{x \in A, v(x) \geq n\} =: \mathfrak{m}_n$ et $\bigcap_{n\in\mathbb{N}} \mathfrak{m}_n = \{0\}$.

Théorème V.4. *Soit A un anneau commutatif intègre. A est un anneau de valuation discrète si et seulement si A est un anneau local principal admettant un unique idéal premier non nul.*

Définition V.10. *Soit A un anneau de valuation discrète. On appelle uniformisante de A tout générateur de l'unique idéal premier non nul de A.*

V-C- 3. Deux exemples fondamentaux d'anneaux de valutation discrète

III.3.1 Localisation des anneaux principaux Soit A un anneau principal et $\mathfrak{p}$ un idéal premier de A. On sait que l'on peut voir $A_\mathfrak{p}$ comme un sous-anneau de $Fr(A)$.
Par principalité de A, il existe $\omega \in A$ irréductible tel que $\mathfrak{p} = \omega A$. Par ailleurs, A est factoriel. Ainsi, tout élément non nul de $k = Fr(A)$ s'écrit de manière unique sous la forme $\omega^n u$, où $n \in \mathbb{Z}$ et où $u = \frac{a}{b}$ ne peut pas se factoriser par une puissance, positive ou négative, de ω. On note $n = n(x)$.
Considérons alors l'application

$$v_\omega \begin{cases} k \to \mathbb{Z} \\ x \mapsto n(x) \cdot \chi_{x\neq 0} + \infty \cdot \chi_{x=0} \end{cases}$$

Il est immédiat qu'il s'agit d'une valuation discrète sur k. Calculons son anneau de valuation $\mathcal{O}_k(v_\omega)$. Clairement, comme on localise par rapport à l'idéal premier, tout élément de $A_\mathfrak{p}$, vu comme sous-anneau de $Fr(A)$ est de valuation positive ou nulle. Réciproquement, si l'on considère $\frac{a}{b}$ un élément de valuation positive, on en déduit qu'il est égal à un $\frac{a'}{b'}$ où $v_\omega(a') \geq 0$ et $v_\omega(b') = 0$. On en déduit donc le résultat suivant :

Si A est un anneau principal, si $\mathfrak{p}$ est un idéal premier de A, $A_\mathfrak{p}$ est un anneau de valuation discrète.

III.3.2 L'anneau des entiers p-adiques Soit p un entier naturel premier. On a déjà défini la valuation p-adique, qui définit une valuation discrète sur $\mathbb{Q}$, et induit ainsi une norme **ultramétrique**, la norme p-adique, notée $|\cdot|_p$. Remarquons que $|x|_p = p^{-v_p(x)}$. Le complété de $\mathbb{Q}$ pour cette norme est appelé corps des p-adiques et est noté $\mathbb{Q}_p$.
Montrons que $v_p, |\cdot|_p$ se prolonge sur $\mathbb{Q}_p$ de sorte que $v_p(\mathbb{Q}_p^*) = v_p(\mathbb{Q}^*) = \mathbb{Z}$. (c td5). En particulier, l'anneau de la valuation v_p sur $\mathbb{Q}_p$ est appelé anneau des entiers p-adiques, est noté $\mathbb{Z}_p$, et c'est un anenau de valuation discrète vérifiant $v_p(\mathbb{Z}_p\backslash\{O\}) = v_p(\mathbb{Z}\backslash\{0\}) = \mathbb{N}$. L'idéal maximal de $\mathbb{Z}_{p\mathbb{Z}}$ et $p\mathbb{Z}_{p\mathbb{Z}}$ et son corps résiduel est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

III.3.3 Germe des fonctions holomorphes en un point

III.3.4 L'anneau des séries formelles $k[[T]]$

V-D. Anneaux de Dedekind

V-D- 1. Définition et caractérisation des anneaux de Dedekind

Définition V.11. *Un anneau de Dedekind est un anneau commutatif, noethérien, intégralement clos, dont tout idéal premier non nul est maximal et qui n'est pas un corps.*

Ainsi, par l'exercice 14 du td4, tout anneau de valuation discrète est un anneau de Dedekind. Par ailleurs, les anneaux principaux sont de Dedekind, puisqu'ils sont intégralement clôs.
ATTENTION : en général, un anneau de Dedekind n'est pas factoriel.

Proposition V.7. *Soit A un anneau de Dedekind et S une partie multiplicative de A ne contenant pas 0. Alors $S^{-1}A$ et soit un corps, soit un anneau de Dedekind.*

Démonstration de la proposition. Supposons que $S^{-1}A$ n'est pas un corps, de sorte que $\{0\}$ n'est pas un idéal maximal de $S^{-1}A$. D'après le TD4, on sait que $S^{-1}A$ est intègre, intégralement clos. On sait que l'on peut faire correspondre les idéaux premiers de $S^{-1}A$ avec les idéaux premiers de A ne rencontrant pas S, par une bijection préservant l'inclusion. Soit donc $\mathfrak{p}$ un idéal premier non nul de $S^{-1}A$. Il correspond ainsi à un idéal premier non nul de A, qui est donc, par hypothèse, maximal. Il est donc maximal.

Théorème V.5. *Soit A un anneau intègre noethérien qui n'est pas un corps. Alors A est un anneau de Dedekind si et seulement si pour tout idéal $\mathfrak{p} \in Spec(A)\backslash\{0\}$, $A_{\mathfrak{p}}$ est un anneau de valuation discrète.*

Démonstration du théorème. Montrons l'implication directe. On sait que, si $\mathfrak{p}$ est un idéal premier donc maximal de A, $A_{\mathfrak{p}}$ est soit un anneau de Dedekind, soit un corps. Pour montrer qu'il s'agit d'un anneau de valuation discrète, il faut donc montrer qu'il admet un unique idéal premier non nul. Mais on a déjà établi ce fait dans la preuve de la proposition précédente.
Montrons l'implication réciproque : Comme A est intègre, , on sait par le td4 que $A = \bigcap_{\mathfrak{p}\in Spec(A)} A_{\mathfrak{p}}$. Mais la notion "être intégralement clos " est une propriété locale. On en déduit donc, cette propriété étant stable par passage à l'intersection, que A est intégralement clos : En effet, si $x \in k := Fr(A)$ est entier sur A, x est également entier sur chaque $A_{\mathfrak{p}}$, et appartient donc à chacun des $A_{\mathfrak{p}}$. Il nous reste donc à montrer que tout idéal premier non nul est maximal. Soit donc $\mathfrak{p} \in Spec(A)\backslash\{0\}$. Supposons qu'il existe un idéal maximal $\mathfrak{m}$ tel que $\mathfrak{p} \subset \mathfrak{m}$. On a ainsi $\mathfrak{p}A_{\mathfrak{m}} \subset \mathfrak{m}A_{\mathfrak{m}}$ et $\mathfrak{p}A_{\mathfrak{m}}$ est toujours un idéal premier non nul. Ainsi, $\mathfrak{p}A_{\mathfrak{m}} = \mathfrak{m}A_{\mathfrak{m}}$, d'où l'on tire $\mathfrak{p} = \mathfrak{m}$.

V-D- 2. Idéaux fractionnaires

Définition V.12. *Soit A un anneau intègre de corps des fractions k. Soit I un sous-A-module de k. On dit que Iest un idéal fractionnaire de A s'il existe $d \in A\backslash\{0\}$ tel que $d \cdot I \subset A$. On note $I(A)$ l'ensemble des idéaux fractionnaires de A. Un idéal fractionnaire I de A est dit idéal entier si $I \subset A$.*

Définition V.13. *Soit $J \in I(A)$. Définissons $J^{\perp}$ par*

$$J^{\perp} := \{x \in k, x \cdot J \subseteq A\}$$

Plus génralement, si J_1, J_2 ston deux idéaux fractionnaires de A, on définit le transporteur de J_1 dans J_2 par

$$(J_2 : J_1) := \{x \in k, x \cdot J_1 \subseteq J_2\}$$

Proposition V.8. *i) Pour tout idéal fractionnaire J de A, $J^\perp$ est un idéal fractionnaire non nul de A et $JJ^\perp$ est un idéal entier de A.*

ii) Plus généralement, si J_1 et J_2 sont deux idéaux fractionnaires de A, $(J_1 : J_2)$ est un idéal fractionnaire de A.

Démonstration de la proposition. i) Admettons *ii*). Alors $JJ^\perp$ est un idéal fractionnaire, et pour tout $x \in J^\perp$, $J \cdot x \subseteq A$ et donc $JJ^\perp \subseteq A$.

ii) On vérifie, trivialement, que $(J_2 : J_1)$ est un sous-A-module de k. Soit donc $d \in A\backslash\{0\}$ tel que $d \cdot J_2 \subseteq A$. Ainsi, pour tout $x \in (J_2 : J_1)$, $dx \in J_1^\perp$**finir la preuve**

On peut donc munir $I(A)$ d'une structure de monoide commutatif, via la multiplication traditionnelle des idéaux.

Définition V.14. *Un idéal fractionnaire J de A est dit <u>inversible</u> s'il existe un autre idéal fractionnaire I de A tel que $JI = A$.*

Proposition V.9. *Un idéal fractionnaire J de A est inversible si et seulement si $J \cdot J^\perp = A$.*

Démonstration de la proposition. Soit J un idéal fractionnaire inversible, d'inverse $\tilde{J}$. Nécessairement, $\tilde{J} \subseteq J^\perp$. Ainsi :

$$J\tilde{J} \subset JJ^\perp \subseteq A$$

et donc $J^\perp = \tilde{J}$.

Exercice . Soit A un anneau principal. Calculer $I(A)$ puis, pour $J \in I(A)$, calculer $J^\perp$.

Solution .

Théorème V.6. *Soit A un anneau de Dedekind. Alors tout idéal maximal de A est inversible dans $I(A)$.*

Démonstration du théorème. Soit $\mathfrak{m}$ un idéal maixmal de A. Par la proposition précédente, il suffit de montrer que $\mathfrak{m} \cdot \mathfrak{m}^\perp = A$. Comme $\mathfrak{m}$ est un idéal de A, on dispose de l'inclusion $A \subseteq \mathfrak{m}^\perp$. Par ailleurs, on a montré que $\mathfrak{m} \cdot \mathfrak{m}^\perp$ est un idéal entier de A. On en déduit donc la chaîne d'inclusions :

$$\mathfrak{m} \subseteq \mathfrak{m} \cdot \mathfrak{m}^\perp \subseteq A$$

Remarquons à présent que $\mathfrak{m} \subsetneq \mathfrak{m} \cdot \mathfrak{m}^\perp$. Avant de prouver cela, notons que cette observation permet de conclure : En effet, comme $\mathfrak{m}$ est un idéal maximal, cela force $\mathfrak{m} \cdot \mathfrak{m}^\perp = A$.
Pour prouver que $\mathfrak{m} \subsetneq \mathfrak{m} \cdot \mathfrak{m}^\perp$, raisonnons par l'absurde et supposons $\mathfrak{m} = \mathfrak{m} \cdot \mathfrak{m}^\perp$. Montrons que cela implique $\mathfrak{m}^\perp = A$, ce qui est impossible pour une raison que nous développerons plus bas.
Soit donc $x \in \mathfrak{m}^\perp$. Par définition, cela signifie que $x \cdot \mathfrak{m} \subseteq A$ et, par hypothèse, $x \cdot \mathfrak{m} \subseteq \mathfrak{m}$. A étant intégralement clos, il faut montrer que x est entier sur A ou, ce qui est équivalent, que le sous-A-module $A[x]$ est de type fini. Mais par une récurrence immédiate, $A[X] \subseteq \mathfrak{m}^\perp$. Comme $\mathfrak{m}^\perp$ est un idéal fractionnaire, il existe $d \in A$ tel que $d \cdot A[x] \subseteq A.A$ est noethérien, donc $dA[x]$ est de type fini, d'où l'on conclut que $A[x]$ est de type fini. Ainsi, $x \in A$.
Taper la preuve du td5 pour avoir $\mathfrak{m}^\perp \neq A$(en gros, il y a des éléments par lesquels on peut diviser).

Théorème V.7. *Soit A un anneau de Dedekind. Tout élément J de $I(A)$ s'écrit de manière unique sous la forme*

$$J = \prod_{\mathfrak{p} \in Spec(A)\backslash\{0\}} \mathfrak{p}^{v_{\mathfrak{p}}(J)}$$

où les $v_{\mathfrak{p}}(I)$ sont des éléments de $\mathbb{Z}$ presque tous nuls.

Ce théorème permet de définir une notion de valuation $\mathfrak{p}$-adique d'un idéal, pour $\mathfrak{p}$ parcourant l'ensemble $Spec(A)\backslash\{0\}$:

Proposition V.10. *L'application* $[J \in I(A) \mapsto v_{\mathfrak{p}}(J)]$ *est une valuation discrète (le cours doit être faux à ce moment là*

Deuxième partie

Théorie de Galois

VI. Extensions de corps

VI-A. Définitions générales

Définition VI.1. *Soit k un corps. Une extension de corps est la donnée d'un corps l et d'un morphisme de corps injectif $i : k \to l$. On considéra implicitement que i est l'inclusion, et on notera l'extension l/k.*

Exercice . Montrer que tout corps de caractéristique nulle (resp $p > 0$) est une extension de $\mathbb{Q}$ (resp. $\mathbb{Z}/p\mathbb{Z}$).

On a par exemple le diagramme d'extensions suivant :

$$\begin{tikzcd}
 & \mathbb{C}(X) \\
\mathbb{C} \arrow[ur, dash] \arrow[d, dash] & \mathbb{R}(X) \arrow[u, dash] \\
\mathbb{R} \arrow[ur, dash] &
\end{tikzcd}$$

On parle aussi de "treillis d'extensions".

Définition VI.2. *Soit l/k une extension de corps. l est naturellement muni d'une structure d'espace vectoriel sur k. Sa dimension, éventuellement infinie, est notée $[l : k]$ et est appelée degré de l'extension.*

Ainsi, $\mathbb{C}$ est une extension quadratique (i.e de degré 2) de $\mathbb{R}$.

Proposition VI.1. *On a multiplicativité des degrés : si l/k est une sous-extension de corps et si m/k est une extension intermédiaire, alors*

$$[l : k] = [l : m] \cdot [m : k]$$

On dit que l'extension est finie si $[l : m] < +\infty$.

Définition VI.3. *Soient l_1/k et l_2/k deux extensions de corps de morphismes respectifs i_1 et i_2. Un k-morphisme de l_1 dans l_2 est un morphisme de corps $\varphi : l_1 \to l_2$ "fixant " k, au sens où il fait commuter le diagramme suivant :*

$$\begin{tikzcd}
k \arrow[r, "i_2"] \arrow[d, "i_1"] & l_1 \\
l_1 \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

Il est en particulier k-linéaire pour la structure de k-espace vectoriel. On note $Hom_k(l_1; l_2)$ l'ensemble des k-morphismes et $Aut_k(l_1)$ l'ensemble des k-automorphismes de l_1.

VI-B. Extensions engendrées, extensions composées

Dans toute la suite, k désigne un corps.

Définition VI.4. *Soit l/k une extension de corps et $A \subseteq l$. On note $k[A]$ la sous-k-algèbre de l engendrée par k et par les éléments de A. On pose $k(A) := Fr(k[A])$; c'est le plus petit sous-corps de l contenant k et les éléments de A.*

Ainsi, pour toute indeterminée T, $k(\{T\}) = k(T)$. Dans le cas où $A = \{a\}$, on abrège la notation $k[\{a\}]$ en $k[a]$, et de même $k(a) := k(\{a\})$. Par ailleurs, si A et B sont deux parties de l, alors $K(A \cup B) = k(A)(B)$. En particulier, si $A = \{\alpha_1, \dots, \alpha_n\}$, on dispose de la tour d'extension naturelle suivante :

$$\begin{tikzcd}
k(A) = k(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) \arrow[d, dash] \\
k(\alpha_1, \dots, \alpha_{n-1}) \arrow[d, dotted] \\
k(\alpha_1, \alpha_2) \arrow[d, dash] \\
k(\alpha_1)
\end{tikzcd}$$

Définition VI.5. *Un extension de corps l/k est dite* <u>*de type fini*</u> *s'il existe une partie finie A de l telle que $l = k(A)$. Elle est dite* <u>*monogène*</u> *s'il existe $\alpha \in l$ tel que $l = k(\alpha)$.*

Il est immédiat que toute extension finie est de type fini : en effet, toute base de l comme k-espace vectoriel engendre l comme espace vectoriel, donc a fortiori comme k-algèbre.
ATTENTION : une extension de type fini n'est pas nécessairement finie, et une extension de type finie n'est pas nécessairement monogène.
Parlons à présent de la notion d'extension composée : Considérons le diagramme suivant :

$$\begin{tikzcd}
 & l \\
l_1 \arrow[ur, dash] \arrow[d, dash] & l_2 \arrow[u, dash] \\
k \arrow[ur, dash] &
\end{tikzcd}$$

Définition VI.6. *Soient l/k une extension de corps et l_1/k, l_2/k deux sous-extension. L'*<u>*extension composée*</u> *de l_1 et l_2 dans l est le plus petit sous-corps de l contenant l_1 et l_2, c'est-à-dire $k(l_1 \cup l_2)$. On la note $l_1 l_2$.*

En d'autres termes, on construit le diagramme suivant :

$$\begin{tikzcd}
 & l \arrow[d, dash] \\
 & l_1 l_2 \arrow[dl, dash] \arrow[d, dash] \\
l_1 \arrow[d, dash] & l_2 \arrow[dl, dash] \\
k &
\end{tikzcd}$$

Proposition VI.2. *Avec les mêmes notations que précedemment, les assertions suivantes sont équivalentes :*

i) Toute base de l_1 comme k-ev est libre sur l_2.

ii) Toute base de l_2 comme k-ev est libre sur l_1.

On dit alors que l_1 et l_2 sont linéairement indépendantes.

Démonstration de la proposition. On remarque que les deux premières assertions sont équivalentes à "pour toute k-base $(e_i)_i$ de l_1, pour toute k-base de l_2, $(e_i f_j)$ est libre sur k."

□

Corollaire VI.1. *Soient l_1/k et l_2/k deux sous-extensions de l/k. Supposons qu'elles sont finies. Alors*

$$[l_1 l_2 : k] \leq [l_1 : k] \cdot [l_2 : k]$$

avec égalité si l_1 et l_2 sont linéairement indépendantes.

VI-C. Extensions algébriques, degré de transcendance

VI-C- 1. Éléments algébriques et transcendants

Soit l/k une extension de corps et $\alpha \in l$. Pour toute extension de corps m/k, se donner un k-morphisme $\varphi : k(\alpha) \to m$ revient simplement à se donner un élément de m, à savoir $\varphi(\alpha)$.

Définition VI.7. *Si $\alpha \in l$, on dit que α est algébrique sur k si le morphisme canonique de k-algèbres $\varphi_\alpha : k[X] \to k[\alpha]$ envoyant X sur α n'est pas injectif. Sinon, α est dit transcendant.*

Proposition VI.3. *Soit l/k une extension de corps et $\alpha \in l$. Les assertions suivantes sont équivalentes :*

i) α est algébrique sur k.

ii) $k[\alpha]$ est un corps.

iii) $[k(\alpha) : k] < +\infty$.

Définition VI.8. *Soit l/k une extension de corps et $\alpha \in l$ un élément algébrique sur k. Le générateur unitaire de $ker(\varphi_\alpha)$ est appelé polynôme minimal de α sur k, et on le note $\mu_{\alpha,k} \in k[X]$.*

Il est immédiat que $\mu_{\alpha,k}$ est irréductible sur k. Par ailleurs, si α est algébrique sur k et si $d = deg(\mu_{\alpha,k})$, $[k[\alpha] : k] = d : \{1, \alpha, \ldots, a^{d-1}\}$ est une k-base de $k[\alpha]$.

VI-C- 2. Extensions algébriques, extensions transcendantes

Définition VI.9. *Une extension de corps l/k est dite algébrique si tout élément de l est algébrique sur k.*

Remarquons que toute extension finie est algébrique et que pour tout $\alpha \in l$, $deg(\mu_{\alpha,k})|[l : k]$. Il existe également des extensions non algébriques : on peut par exemple penser à $\mathbb{Q}(X)/\mathbb{Q}$: en effet, X est transcendant sur $\mathbb{Q}$.

Proposition VI.4. *Soit l/k une extension de corps. Pour toute famille $(\alpha_1, \ldots, \alpha_n)$ d'éléments de l, les assertions suivantes sont équivalentes :*

i) Il n'existe pas de polynôme non nul $P \in k[X_1, \ldots, X_n]$ tel que $P(\alpha_1, \ldots, \alpha_n) = 0$.

ii) Le morphisme de k-algèbres $\varphi : k[X_1, \ldots, X_n] \to l$ déifni par $\varphi(X_i) = \alpha_i$ est injectif.

iii) Il existe un k-morphisme $\varphi : k(X_1, \ldots, X_n) \to l$ de corps envoyant X_i sur α_i.

Quand ces conditions sont vérifiées, on dit que les éléments sont algébriquement indépendants sur k.

Définition VI.10. *Soit l/k une extension de corps. Une partie finie $(\alpha_1, \ldots, \alpha_n)$ est une base de transcendance de l sur k si les deux conditions suivantes sont vérifiées :*

- *$(\alpha_1, \ldots, \alpha_n)$ forme une famille algébriquement indépendante sur k.*
- *L'extension $l/k(\alpha_1, \ldots, \alpha_n)$ est algébrique.*

Théorème VI.1. *Soient A_1 et A_2 deux parties finies de l telles que A_1 soit formée d'éléments algébriquement indépendants sur k et que l'extensions $l/k(A_2)$ soit algébrique. Alors l/k a une base de transcendance B vérifiant*

$$A_1 \subseteq B \subseteq A_2$$

Demonstration à taper.
En particulier, toute extension de type fini admet une base de transcendance.

Théorème VI.2. *Soit l/k une extension de corps. Soient $(x_1, \ldots, x_m)$ et $(y_1, \ldots, y_m)$ deux bases de transcendance de cette extension. Alors pour tout $i \in \mathbb{N}_n$, il existe $j \in \mathbb{N}_m$ tel que $(x_1, \ldots, x_{i-1}, y_j, x_{i+1}, \ldots, , x_n)$ soit une base de transcendance. En particulier, deux bases de transcendance ont même cardinal. Ce cardinal commun est appelé degré de transcendance de l'extension. On le note $deg_{tr}(l/k)$.*

Théorème VI.3. *Soient l/k et m/l deux extensions de corps de type fini. Alors*

$$deg_{tr}(m/k) = deg_{tr}(m/l) + deg_{tr}(l/k)$$

Théorème VI.4. *Soir C un corps algébriquement clos. Soit $\varphi : k \to C$ un morphisme de corps et l/k un extension algébrique de k. Il existe un morphisme de corps $\varphi' : l \to C$ prolongeant ce morphisme, et il existe au plus $[l : k]$ tels prolongements.*

VI-D. Exercices corrigés

On s'autorise, quand les éléments sont algébriques, à confondre $k(a)$ et $k[a]$ dans les rédactions, ces deux ensembles étant égaux.

VI-D- 1. Corps de décomposition, corps de rupture

Exercice .

Solution . 1. On raisonne par récurrence sur le degré de P, noté n. Si $n = 1$, alors $L = k$ est un corps de décomposition pour P. De même, si P est produit de facteurs de degré 1, $L = k$ est un corps de décomposition de P. Sinon, P admetun facteur irréductible, disons Q, de degré compris entre 2 et n. Soit k' un corps de rupture pour Q et x une racine de Q dans k'. On peut donc écrire $P = (X - x)P'$ dans $k'[X]$, et $degP' < degP$. Soit L un corps de décomposition de

P' sur k'. Mais L est alors également un corps de décomposition de P sur k.
On montre par récurrence que $[L : k] \leq n!$. Pour $n = 1$, c'est évident. Sinon, comme ci-dessus, on remarque que P admet un facteur irréductible Q, de degré q. On écrit $P = QR, degR \geq 1$. Considérons l_1 un corps de décomposition de Q sur k. Par hypothèse de récurrence, $[l_1 : k] \leq (q)!$. Soit l_3 un corps de décomposition de R sur l_1 (qui est aussi un corps de décomposition pour P). Alors $[l_3 : l_1| \leq (n-q)!$. Ainsi,

$$[l_3 : k] = [l_3 : l_1] \cdot [l_1 : k] \leq (n-q)!q! \leq (n-q)!q!C_n^q = n!$$

2. On le montre ici encore par récurrence. Si $n = 1$, c'est évident, car $[k : k] = 1$. Sinon, on remarque que dans le raisonnement de la question précédente, en reprenant les mêmes notations, on sait, par récurrence, que $[l_1 : k]|q!$ et que $[l_3 : l_1]|(n-q)!$, donc $[l_3 : k]|q!(n-q)!$. A fortiori, comme $q!(n-q)!|n!$, $[l_3 : k]|n!$.
3. Supposons P irréductible. Soit a une racine de P dans son corps de décomposition l. Alors, par le théorème de la base téléscopique, $[l : k] = [l : k(a)] \cdot [k(a) : k]$. Comme P est irréductible, le polynôme minimal de a est P lui-même, et donc $[k(a) : k] = n$, d'où l'on conclut que $n|[l : k]$.
4. Les racines de $P := X^4 - 7$ dans $\mathbb{C}$ sont ${}^4\sqrt{7}, -{}^4\sqrt{7}, {}^4\sqrt{7} \cdot i$ et ${}^4\sqrt{7} \cdot (-i)$. Donc le corps de décomposition de P sur $\mathbb{Q}$ est $l = \mathbb{Q}(i, {}^4\sqrt{7})$.

VI-D- 2.

Exercice .

Solution . 1. Soit μ le polynôme minimal de a sur k. Il est de degré n. Soit ν le polynôme minimal de a sur $k[b]$. C'est un facteur de μ dans $k[b][X]$, et il est donc de degré $d \leq n$. Par ailleurs, en appliquant le théorème de la base téléscopique, on obtient $[k(a, b) : k] = dm \leq nm$, mais également que $[k(a, b) : k] = [k(a, b) : k[a]] \cdot n$, donc est un multiple de n. Comme $n \wedge m = 1$, n :'ecessairement, $n = d$, donc $\nu = \mu$, et donc μ est irréductible dans $k[b][X]$.

2. Montrons que $k[a] \cap k[b] = k$. Mais, par le théorème de la base téléscopique, $[k(a) \cap k(b) : k] \cdot [k(a) : k(a) \cap k(b)] = [k(a) : k] = n$ et on obtient par un raisonnement analogue le fait que $[k(a) \cap k(b) : k]$ divise m et n. Comme $m \wedge n = 1$, $[k(a) \cap k(b) : k] = 1$, et, finalement,

$$k(a) \cap k(b) = k$$

VII. Extensions séparables et corps parfaits

VII-A. Polynômes séparables : rappels et compléments

Dans toute la suite, on se fixe k un corps et Ω une clôture algébrique de k.

Définition VII.1. *Soit $P \in k[X]$ non constant. On dit que P est séparable (sur k) s'il admet $deg(P)$ racines distinctes dans Ω. Sinon, il est dit inséparable.*

Par exemple, $X^3 - 7$ est séparable sur $\mathbb{Q}$. Par contre, si $k = \mathbb{F}_p(T)$, $P := X^p - T$ est inséparable. Il est évident que tout facteur d'un polynôme séparablee est séparable, ce qui justifie le fait que l'on n'étudie que la séparabilité des polynômes irréductibles.

Proposition VII.1. *Soit $P \in k[X]$ non constant. Les assertions suivantes sont équivalentes :*

i) P est inséparable.

ii) $P' \wedge P = 1$.

La preuve de cette proposition est immédiate. Ainsi, la notion de séparabilité ni de k ni de la clôture algébrique choisie.

Proposition VII.2. *Soit $P \in k[X]$ non constant et irréductible sur k. Les assertions suivantes sont équivalentes :*

i) P est inséparable.

ii) $P' = 0$.

iii) k est de caractéristique $p > 0$ et il existe $Q \in k[X]$ tel que $P = Q(X^p)$.

Démonstration de la proposition. Montrons l'équivalence des deux premières propositions en montrant l'équivalence des contraposées : Supposons que P est séparable.

□

VII-B. Éléments séparables

Définition VII.2. *Soit l/k une extension de corps. Un élément α de l est dit séparable sur k si α est algébrique sur k et si son polynôme minimal sur k est séparable. L'extension est dite séparable si c'est une extension algébrique dont tout élément est séparable*

Ainsi, en caractéristique nulle, toute extension algébrique est séparable par la proposition précédente. On a un lien très fort entre les prolongements de morphismes et la notion d'extension séparable : Si l/k est une extension de corps finie monogène, on peut trouver $P \in k[X]$ irréductible tel que $l = k[X]/(P)$. La preuve du théorème de prolongements de morphisme assure que si Ω est une clôture algébrique de k alors

$$|Hom_k(l;\Omega)| = |\{\text{racines distinctes de } P \text{ dans } \Omega\}|$$

On a en particulier l'équivalence : le polynôme P est séparable ssi

$$|Hom_k(l;\Omega)| = [l : k]$$

Théorème VII.1. *Soit l/k une extension finie. Les assertions suivantes sont équivalentes :*

i) L'extension est séparable.

ii) Tout morphisme de corps $\varphi \in Hom(k;\Omega)$, avec Ω une clôture algébrique de k, admet exactement $[l : k]$ prolongements à l.

iii) Il existe un élément $\alpha \in l$ séparable sur k tel que $l = k(\alpha)$.

Démonstration du théorème. Pour montrer $i)\Rightarrow ii)$, on va avoir besoin d'un résultat : en notant, pour l/k une extension algébrique, $[l : m]_s = |Hom_k(l;\Omega)|$, alors, si m/l et l/k sont des extensions algébriques, on a l'égalité suivante :

$$[m : k]_s = [m : l]_s[l : k]_s$$

C'est une simple application du théorème de prolongement des morphismes. En effet, en notant $(\varphi_i)_{i\in I}$ l'ensemble des éléments de $Hom_k(l;\Omega)$ on sait que chacun d'entre eux définit, indépendamment de l'indice i, $[m : l]_s$ éléments de $Hom_k(m;\Omega)$. On a donc au moins $[m : l]_s[l : k]_s$ éléments dans $Hom_k(m : \Omega)$. Inversement, étant donné un élément β de $Hom_k(m;\Omega)$, il se restreint à l en un k-morphisme de l dans Ω. C'est donc l'un des φ_i, d'où le résultat.
Revenons à la démonstration du théorème : comme l'extension l/k est finie, elle est en particulier de type fini. Considérons un système minimal de générateurs $\{x_1, \dots, x_n\}$ et définissons, pour $i \in \mathbb{N}_n$, l'extension intermédiaire l_i par

$$l_i := k[x_1, \dots, x_i]$$

Si on montre $ii)$ pour chacune des extensions intermédiaires, le petit résultat prouvé au début de la démonstration permettra de conclure. Mais il s'agit d'une banale récurrence, qui ne se sert que de l'équivalence entre la séparabilité d'un polynôme irréductible P et le fait qu'il existe $deg(P)$ k-morphismes distincts de $k[X]/(P)$ dans Ω et du théorème de la base téléscopique.
Pour montrer l'implication $ii)\Rightarrow iii)$ on remarque que l'on peut déjà éliminer le cas où l est un corps fini. En effet, dans ce cas-ci, il suffit de voir que le groupe multiplicatif d'un corps fini est cyclique. Dans la cas d'un corps infini, on note $\varphi_1, \dots, \varphi_n$ les éléments distincts de $Hom_k(l;\Omega)$ et on considère, pour $i \neq j$ le sous-espace vectoriel (relativement à la structure k-linéaire) $V_{i,j} := ker(\varphi_i - \varphi_j)$. Comme les φ_i sont distincts, les $V_{i,j}$ sont des sous-espaces vectoriels stricts de l et on ne peut donc pas avoir

$$l = \cup_{i,j} V_{i,j}$$

Il existe donc $\alpha \in l$ tel que pour tout $i \neq j$ $\varphi_i(\alpha) \neq \varphi_j(\alpha)$. Ainsi, la famille $(\varphi_{i|k(\alpha)})_{i=1,\dots,n}$ définit n k-morphismes distincts de $k(\alpha)$ dans Ω. Donc $|Hom_k(k(\alpha);\Omega)| = n \leq [k(\alpha);k]$ et donc $k(\alpha) = l$. En considérant le polynôme minimal de α sur k, on voit que α est séparable.
Montrons enfin $iii)\Rightarrow i)$: on se fixe un élément α donné par $iii)$ et il s'agit de montrer que pour tout $x \in l$, il y a exactement $deg(\mu_x)$ k-morphismes de $k[X]/(\mu_x)$ dans Ω où μ_x désigne le polynôme minimal de x sur k. Soit P le mpolynôme minimal de α sur k et soit $d := |Hom_k(k(x);\Omega)|$. On sait que $d \leq [k(x) : k]$ et que α est séparable sur $k(x)$, puisque tout facteur irréductible d'un polynôme séparable est encore séparable, en vertu de quoi

$$|Hom_{k(x)}(l;\Omega)| = [k(\alpha) : k(x)]$$

Toujours par le résultat préliminaire et par séparabilité de l'élément α,

$$[k(\alpha);k] = d|Hom_{k(x)}(l;\Omega)| \leq [k(x) : k][l : k(x)]$$

Par multiplicativité du degré, on en déduit que l'élément x est séparable.

□

Corollaire VII.1. *Dès que l/k est une extension algébrique, l'élément α est séparable si et seulement si l'extension $k(\alpha)/k$ est une extension séparable.*

Par ailleurs, la démonstration du théorème contient, en germe, la démonstration de la proposition suivante :

Proposition VII.3. *Si m/l et l/k sont deux extensions de corps, l'extension m/k est séparable si et seulement si les extensions m/l et l/k le sont toutes les deux. En particulier, si $A \subset l$ est une famille d'éléments séparables, l'extension $k(A)/k$ est séparable.*

Il est également clair que si l_1 et l_2 sont deux sous-corps de l contenant k séparables, l'extension composée l_1l_2/k est séparable.

VII-C. Corps parfaits

Définition VII.3. *Un corps k est dit parfait si toute extension algébrique de k est séparable.*

Ainsi, tout corps de caractéristique nulle est parfait. Le défaut de perfection vient du morphisme de Frobenius, comme l'explique la proposition suivante :

Proposition VII.4. *Soit p un entier premier, k un corps de caractéristique p et $f : k \to k$ le morphisme de Frobenius. k est parfait si et seulement si f est surjectif.*

Démonstration de la proposition. Montrons l'implication réciproque en travaillant par l'absurde : soit l/k une extension algébrique ; supposons la non séparable. On peut donc choisir $\alpha \in l$ tel que α ne soit pas séparable. Son polynôme minimal sur k, $\mu_{\alpha,k}$ n'est pas séparable. Ainsi, il existe $Q \in k[X]$ tel que $P = Q(X^p)$. Écrivons $Q = \sum_{i=0,\dots,d} a_i X^i$. Par surjectivité de f, pour tout $i \in \{0, \dots, d\}$ il existe $\alpha_i \in k$ tel que $\alpha_i^p = a_i$ et, comme f est un morphisme de corps, on a donc

$$\mu_{\alpha,k} = (\sum_{i=0}^{d} \alpha_i X^i)^p$$

ce qui est absurde. Donc $ii) \Rightarrow i)$.
Pour l'implication réciproque, supposons par l'absurde que f ne soit pas surjectif. Soit donc $a \in k \backslash f(k)$. Soit b une racine de $X^p - a$ dans une clôture algébrique de k. Alors $X^p - a = (X - b)^p$ donc tous les facteurs irréductibles de $P = X^p - a$ dans $k[X]$ sont de la forme $(X - b)^n$ ce qui est absurde : en effet, le terme de degré $n - 1$ a pour coefficient b. Ainsi, P est un polynôme irréductible sur k, et donc b n'est pas séparable.

□

Ainsi, puisque qu'un corps fini est de caractéristique positive et de cardinal une puissance de sa caractéristique, tout corps fini est parfait, le Frobenius étant injectif, donc surjectif.

VIII. Extensions galoisiennes

VIII-A. Extensions normales

Soit k un corps et Ω une clôture algébrique de k.

Définition VIII.1. *Soit l/k une extension algébrique. Elle est dite normale si pour tout $\alpha \in l$, le polynôme minimal de α sur k est scindé sur l (on ne demande pas qu'il soit scindé à racines simples).*
Étant donné $\alpha \in l$, les conjugués de α sont les racines de $\mu_{\alpha,k}$ dans Ω.

Exemple . Si $k = \mathbb{Q}$, si $d \in \mathbb{N}$ est sans facteur carré, pour tout $n \geq 2$ considérons $l := \mathbb{Q}(\sqrt[n]{d})$. L'extension l/k est-elle normale ? Si $n = 2$, oui. En revanche, si $n \geq 3$, l'extension n'est pas normale. En effet, $l \subseteq \mathbb{R}$ mais, si $n \geq 3$, une des racines primitives n-èmes de l'unité est contenue dans $\overline{\mathbb{Q}} \backslash \mathbb{R}$. Ici encore, on a une caractérisation de cette propriété en termes de k-morphismes :

Théorème VIII.1. *Soit l/k une extension algébrique. Les assertions suivantes sont équivalentes :*
i) L'extension est normale.
ii) Pour tout k-morphisme $\varphi : l \to \Omega$, $\varphi(l) \subseteq l$.
iii) Pour tout k-morphisme $\varphi : l \to \Omega$, $\varphi(l) = l$.

Démonstration du théorème. L'implication $i) \Rightarrow ii)$ est simple : soit φ un k-morphisme de l dans Ω. Si $x \in l$, comme φ est un morphisme de corps, $\varphi(x)$ est encore racine de $\mu_{x,k}$, le polynôme minimal de x sur k. Comme l'extension est supposée normale, l contient tous les conjugués de x, donc contient $\varphi(x)$, d'où $ii)$.
Montrons $ii) \Rightarrow iii)$. Soit $\varphi \in Hom_k(l; \Omega)$. On sait que $\varphi(l) \subseteq l$ et que φ est injective ; reste donc à montrer sa surjectivité. Soit $x \in l$. Montrons que x est atteint : soient $x_1, \ldots, x_d$ ses conjugués. Le k-espace vectoriel $m := k[x_1, \ldots, x_d]$ est de dimension finie et est stable par φ. Ainsi, $\varphi(m) = m$. Comme $\varphi(l) \subseteq l$, on en déduit

$$\varphi(m \cap l) \subseteq m \cap l$$

Par égalité des dimensions (on travaille en dimension finie), $\varphi(m \cap l) = m \cap l$. Comme $x \in m \cap l$, ceci permet de conlure.
Enfin, montrons l'implication $iii) \Rightarrow i)$. On va utiliser le théorème de prolongement de morphisme. Pour cela, on peut définir $\overline{\varphi} : k(x) \to \Omega$ fixant k et envoyant x sur y, où y est un conjugué de x (on travaille avec $x \in k$, sinon le résultat est évident...) L'extension $l/k(x)$ est algébrique et ce morphisme induit donc un k-morphisme $\varphi : l \to \Omega$. Par hypothèse, $\varphi(l) = l$, donc $y \in l$, et l'extension est donc normale.

□

En particulier, on a le corollaire suivant :

Corollaire VIII.1. *Soit l/k une extension algébrique. Soit $A \subseteq l$ telle que $l = k(A)$. Alors l/k est normale si et seulement si pour tout $a \in A, \mu_{a,k}$ son polynôme minimal sur k est scindé sur l.*

Pour montrer l'implication réciproque, il suffit de remarquer que si chacun des éléments de A est séparable, alors pour tout k-morphisme $\varphi : l \to \Omega$, $\varphi(A) \subseteq A$.

Proposition VIII.1. *Soit l/k une extension finie. Cette extension est normale si et seulement si il existe $P \in k[X]$ tel que $D_k(P) = l$ où $D_k(\cdot)$ désigne le corps de décomposition sur k.*

Démonstration de la proposition. Pour l'implication directe : puisque l/k est finie, elle est a fortiori de type finie. Soit $(\alpha_1, \ldots, \alpha_d)$ un système générateur minimal. Pour $i \in \mathbb{N}_d$, on note μ_i le polynôme minimal de α_i sur k. Chacun des μ_i est scindé sur l, donc $\mu := \prod_i \mu_i$ l'est également, et l est engendré par les racines de μ. Ainsi, $l = D_k(\mu)$.
L'implication réciproque découle immédiatement du corollaire.

□

Proposition VIII.2. *Soit l/k une extension et l/m une extension intermédiaire. Si l/k est normale, alors l/m est normale.*

La réciproque est fausse : il suffit de considérer le cas $l = \mathbb{Q}(\sqrt[4]{2}), m = \mathbb{Q}(\sqrt{2})$ et $k = \mathbb{Q}$. En revanche, si l_1/k et l_2/k sont deux extensions intermédiaires normales, alors $l_1 \cap l_2$ et $l_1 l_2/k$ sont deux extensions normales.

VIII-B. Extensions galoisiennes

Définition VIII.2. *Soit l/k une extension algébrique. Elle est dite galoisienne si elle est normale et séparable.*

Ainsi, une extension galoisienne finie l/k correpond en fait à l'extension $D_k(P)/k$ où P est un polynôme séparable sur k. On peut également reformuler cela en termes d'éléments primitifs.**à vérifier**.

Théorème VIII.2. *Soit l/k une extension finie. Notons $Aut_k(l)$ l'ensemble des k-automorphismes de corps de l. Alors*

$$|Aut_k(l)| \leq [l : k]$$

avec égalité si et seulement si k est galoisienne.

Démonstration du théorème. Montrons l'implication réciproque : Supposons que l'extension l/k soit galoisienne. Comme l'extension est finie, l'inégalité

$$|Hom_k(l; \Omega)| \leq [l : k]$$

est acquise. Par séparabilité,

$$|Hom_k(l; \Omega)| = [l : k]$$

Par normalité,

$$Hom_k(l; \Omega) = Aut_k(l)$$

do'ù le résultat voulu.
Montrons l'implication directe : supposons donc

$$|Aut_k(l)| = [l : k]$$

Comme l'extension est finie, l'inégalité

$$|Hom_k(l; \Omega)| \leq [l : k] = |Aut_k(l)|$$

est acquise. Ainsi,

$$|Hom_k(l)| = [l : k]$$

donc l'extension est séparable. De même,

$$Aut_k(l) = Hom_k(l; \Omega)$$

donc l'extension est normale. L'extension est donc galoisienne.

□

On peut alors introduire la notion fondamentale de cette partie, la notion de groupe de Galois :

Définition VIII.3. *Soit l/k une extension galoisienne. On appelle groupe de Galois de l'extension l/k l'ensemble des k-automorphismes de l. On le note $Gal(l/k)$.*

On dispose d'une action naturelle $Gal(l/k) \curvearrowright l$. Moralement, ce groupe échange les racines d'un polynôme :

Proposition VIII.3. *Soit l/k une extension galoisienne et $(x, y) \in l^2$. Les assertions suivantes sont équivalentes :*

i) x et y sont dans la même orbite sous l'action du groupe de Galois de l'extension.

ii) x et y ont même polynôme minimal sur k.

Démonstration de la proposition. $i) \Rightarrow ii)$ est immédiat : Il suffit de remarquer que pour tout polynôme $P \in k[X], P(\sigma(x)) = \sigma(P(x))$ si $\sigma \in Gal(l/k)$.
L'implication réciproque se fait par prolongement de morphisme : $k[x]$ et $k[y]$ sont deux corps de rupture pour le polynôme irréductible $\mu_{x,k}$, et ils sont donc isomorphes via $f : x \to y$ et qui est égal à l'identité sur k (on suppose $x \notin k$, sinon le résultat est évident). Ce morphisme se prolonge donc en un élément du groupe de Galois, σ, qui envoit x sur y.

□

On obtient donc le corollaire suivant :

Corollaire VIII.2. *Pour toute extension galoisienne l/k, $l^{Gal(l/k)} = k$.*

Théorème VIII.3. *Soit p un entier premier et $n \in \mathbb{N}^*$. Soit $q := p^f, f \in \mathbb{N}^*$. L'extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ est galoisienne, de groupe de Galois cyclique d'ordre n engendré par le morphisme de Frobenius.*

Démonstration du théorème. Il s'agit d'une extension finie d'un corps fini ; elle est donc séparable, par perfection des corps finis. Pour montrer qu'elle est normale, on va utiliser le théorème de l'élément primitif : il existe $\alpha \in \mathbb{F}_{q^n}$ tel que $\mathbb{F}_{q^n} = \mathbb{F}_q[\alpha]$. Soit P le polynôme minimal de α sur $\mathbb{F}_p$. Il faut montrer que ce polynôme est scindé sur $\mathbb{F}_{q^n}$, ce qui montrera que l'extension est normale.
Notons φ le morphisme de Frobenius : supposons montré que φ est d'ordre n. Alors $(\varphi^i(\alpha))_{i \in \mathbb{N}^n}$ fournit n racines distinctes de P : en effet, si $\varphi^j(\alpha) = \alpha, 1 \leq j < n$, on aboutit à une absurdité, puisque α est d'ordre $q^n - 1$. Ceci conclut la preuve, une fois remarqué que $\varphi^n = id$.

□

Corollaire VIII.3. *Soit P un polynôme irréductible sur $\mathbb{F}_q[X]$ non constant. Alors P est scindé à racines simples dans $\mathbb{F}_{q^{deg(P)}}$ et, si α est une racine de P, l'ensemble des racines de P est l'ensemble des $\varphi^i(\alpha)$.*

Ce corollaire est simple à démontrer : On sait que si P admet une racine dans $\mathbb{F}_{q^d}$, les autres racines de P dans $\mathbb{F}_{q^d}$ forment l'orbite de la première sous l'action de groupe de Galois de l'extension. Comme P est séparable par perfection des corps finis, ses racines sont distinctes, et comme l'extension est galoisienne toutes ses racines sont dans $\mathbb{F}_{q^d}$. Toutes les racines sont dans l'orbite de la première sous l'action de Galois, et cette orbite est de cardinal inférieur à $deg(P)$. Il est donc égal à $deg(P)$.

VIII-C. Groupe de Galois d'un polynôme

Définition VIII.4. *Soit P un polynôme séparable de $k[X]$. Son groupe de Galois est le groupe*

$$Gal_k(P) := Gal(D_k(P)/k)$$

Ce groupe de Galois ne dépend pas du corps de décomposition choisi.

Lemme VIII.1. *Soit $P \in k[X]$ séparable.Soit l un corps de décomposition de P sur k. Soit $Z(P)$ l'ensemble des racines de P dans l. Alors*

$$Gal(l/k) \cdot Z(P) \subseteq Z(P)$$

On a donc une action de groupe $Gal(l/k) \curvearrowright Z(P)$, c'est-à-dire un morphisme de groupes $\varphi : Gal(l/k) \to S_{|Z(P)|}$. Ce morphisme est injectif, indépendamment de la numérotation des racines, mais n'est en général pas surjectif.

IX. Correspondance de Galois

IX-A. Le lemme d'Artin et la correspondance de Galois

IX-A- 1. Le lemme d'Artin

THÉORÈME IX.1. *Soit l un corps et G un sous-groupe fini du groupe des automorphismes de corps de l. Alors l^G est un sous-corps de l, et l'extension l/l^G est galoisienne de groupe de Galois G.*

DÉMONSTRATION DU THÉORÈME. Le premier point est immédiat. Pour montrer le deuxième point, il suffit de montrer que l'extension est galoisienne de degré $n := |G|$: en posant $k := l^G$, on aura alors $Aut_k(l) \leq n$ et $G \subseteq Gal(l/k)$. Il suffit donc de majorer $[l : k]$ par n. On travaille par l'absurde : soit une famille $(x_0, \ldots, x_n)$ linéairement indépendante sur k. On note $\{\sigma_1, \ldots, \sigma_n\}$ les éléments de G. On considère ensuite le système suivant :

$$\left\{ \sum_{j=0}^{n} y_j \sigma_i(x_j) \right\}_{i \in \mathbb{N}_n}$$

Il y a n équations et $n+1$ inconnues, il admet donc une solution non triviale $\xi = (\xi_0, \ldots, \xi_n\}$.Quitte à tout renuméroter, on peut supposer qu'il existe un entier $r \in [|0; n|]$ tel que pour tout $i \in [|0; r|]$ $\xi_i \neq 0$ et que pour tout $i > r, \xi_i = 0$. On peut en outre supposer r minimal pour cette propriété. En divisant le système par ξ_r, on voit que l'on peut également supposer $\xi_r = 1$. Le système s'écrit alors

$$\forall i \in \mathbb{N}_n, \sigma_i(x_r) + \sum_{j=0}^{n-1} \sigma_i(x_j)\xi_j = 0$$

On applique à cette équation un élément σ_j quelconque de G. On en déduit

$$\forall i \in \mathbb{N}_n, \forall \sigma \in G, \sigma_i(x_j) + \sum_{j=0}^{r-1} \sigma(\xi_j)\sigma_i(x_j) = \sigma_i(x_r) + \sum_{j=0}^{n-1} \sigma_i(x_j)\xi_j = 0$$

Ainsi,

$$\sum_{j=0}^{r-1} (\sigma(\xi_j) - \xi_j)\sigma_i(x_j) = 0$$

donc soit r n'est pas minimal soit pour tout $j \in [|0; r-1|]$ $\xi_j \in k$, ce qui est absurde par hypothèse. Ceci termine la démonstration.

□

IX-A- 2. La correspondance de Galois pour les extensions finies

THÉORÈME IX.2. *Soit l/k une extension galoisienne finie, $Gal(l/k) = G$. Soit H un sous-groupe de G. Alors :*

- *l/l^H est une extension galoisienne de groupe de Galois H.*
- *L'application φ envoyant un sous-groupe H de H sur l^H est une bijection décroissante de l'ensemble des sous-groupes de G dans l'ensembles des extensions intermédiaires de l/k.*
- *Étant donné un sous-groupe H de G, l'extension l^H/k est galoisienne si et seulement si H est distingué dans G. Elle est alors de groupe de Galois $\frac{G}{H}$.*

DÉMONSTRATION DU THÉORÈME. • Le premier point est immédiat.

- La décroissance de φ est évidente. Pour l'injectivité, il faut remarquerque si H_1 et H_2 sont deux sous-groupes de G alors
$$H_1 = Gal(l/l^{H_1}) = Gal(l/l^{H_2}) = H_2$$
Montrons la surjectivité. Dès que l'on se fixe une extension intermédiaire m de l/k, l'extension l/m est galoisienne finie, de groupe de Galois contenu dans G et donc $m = \varphi(Gal(l/m))$.
- Soit H un sous-groupe distingué de G. Montrons que l^H/k est galoisienne. Il suffit de montrer qu'il s'agit d'une extension normale, puisque l'on sait déjà qu'elle est séparable. Par normalité de l'extension l/k et par extension des morphismes, il s'agit donc de montrer que pour tout $\sigma \in Gal(l/k), \sigma(l^H) \subseteq l^H$. Mais on remarque que
$$\sigma(l^H) \subseteq l^{\sigma H \sigma^{-1}} = l^H$$
Réciproquement si l^H/k est galoisienne, on peut considérer l'application $f = Gal(l/k) \to Gal(l^H/k)$ définie par $f(\sigma) = \sigma_{|l^H}$. Il s'agit dun morphisme de groupes. Calculons son noyau :
$$\begin{aligned} ker(f) &= \{\sigma \in Gal(l/k), \sigma_{|l^H} = id_{l^H}\} \\ &= \{\sigma \in Gal(l/k), \forall x \in l^H, \sigma(x) = x\} \\ &= Gal(l/L^H) \\ &= H \end{aligned}$$
Donc H est bien distingué, et on a l'égalité annoncée.

□

On peut enfin justifier l'étrange notation $[l : k]$: dès que l'on a une extension galoisienne l/k, pour tout sous-groupe distingué H de G, on a légalité
$$[l^H : k] = [G : H]$$
où le membre de gauche est l'indice de H dans G, et on a la suite exacte :
$$1 \to \underset{\cong H}{Gal(l/l^H)} \to Gal(l/k) \to Gal(l^H/k) \to 1$$
On explicitera, à titre d'exercice, la correspondance de Galois dans le cas des corps finis.

IX-B. Extensions cyclotomiques

IX-B- 1. Présentation des extensions cyclotomiques

Soit k un corps et m un entier non divisible par $car(k)$.

Définition IX.1. *Une extension de corps l/k est dite cyclotomique s'il existe $\xi \in l$ racine de l'unité tel que $l = k[\xi]$.*

Si l/k est cyclotomique de générateur ξ, ξ est une racine de l'unité d'ordre non divisible par $car(k)$. Toute extension de corps fini est cyclotomique. Attention, il n'y a ni unicité du ξ, ni même unicité de son ordre.

Proposition IX.1. *Soit l/k une extension de corps ; supposons la finie. Les assertions suivantes sont équivalentes :*

i) l/k est cyclotomique engendrée par une racine primitive n-ème de l'unité.

ii) l est le corps de décomposition sur k du polynôme $X^n - 1$.

En particulier, toute extension cyclotomique est galoisienne.

Proposition IX.2. *Sous les hypothèses de la proposition précédente, $Gal(l/k)$ s'identifie canoniquement à un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$. Par suite, le degré de l'extension divise $\varphi(n)$, φ désignant ici l'indicatrice d'Euler.*

Démonstration de la proposition. Soit ξ une racine primitive n-ème de l'unité dans l. Pour tout élément du groupe de Galois $Gal(l/k)$, disons σ, $\sigma(\xi^k) = \sigma(\xi)^k$, donc $\sigma(\xi)$ est une racine primitive n-ème de l'unité. Par suite, il existe un unique $n_\sigma \in \mathbb{Z}/n\mathbb{Z}$ tel que $\sigma(\xi) = \xi^{n_\sigma}$. Soit $f : Gal(l/k) \to (\mathbb{Z}/n\mathbb{Z})*$ défini par $f(\sigma) = n_\sigma$. Il s'agit d'un morphisme de groupe injectif qui ne dépend pas de ξ. ATTENTION, f n'est en général pas surjective.

□

Voici enfin un théorème étudié dans le DM2.

Théorème IX.3. *Soit k un corps et $n \geq 1$ non divisible par $car(k)$. Soit l/k une extension cyclotomique, $l = k[\xi]$ où ξ est une racine primitive n-ème de l'unité. Alors $Gal(l/k) \cong (\mathbb{Z}/n\mathbb{Z})^*$ si et seulement si le n-ème polynôme cyclotomique est irréductible sur k.*

IX-C. Hilbert '90 et extensions cyclotomiques

Définition IX.2. *Soit l/k une extension galoisienne finie. On définit deux applications comme suit :*

- *<u>La norme relative</u> $N_{l/k}$ par*
$$N_{l/k}(x) := \prod_{\sigma \in Gal(l/k)} \sigma(x)$$
- *<u>La trace relative</u> $T_{l/k}$ par*
$$T_{l/k}(x) := \sum_{\sigma \in Gal(l/k)} \sigma(x)$$

$T_{l/k}$ est un morphisme de groupes additifs, et $N_{l/k}$ est un morphisme de groupes multiplicatifs.

Théorème IX.4. {*Lemme d'indépendance des caractères de Dedekind*} *Soit k un corps et G un gorupe. L'ensemble des homomorphismes de groupes $Hom(G; k^*)$ est une partie libre sur k de $\mathcal{F}(G; k^*)$.*

Théorème IX.5. { *Hilbert '90*}. *Soit l/k une extension galoisienne finie telle que le groupe $Gal(l/k)$ soit cyclique. Soit σ un générateur de $Gal(l/k)$. Pour tout $x \in l$, les assertions suivantes sont équivalentes :*

i) $x \in ker(N_{l/k})$ i.e $N_{l/k}(x) = 1$.

ii) Il existe $y \in l^*$ tel que $x = \frac{\sigma(y)}{y}$.

Soit k un corps, $n \geq 1$ un entier et supposons $\mu_n(k) = n$ i.e que k contienne une racine primitive n-ème de l'unité notée ξ (donc n n'est pas divisible par $car(k)$). Alors si $x \in k^*$,en posant $l := D_k(X^n - a)$, l'extension l/k est cyclique, et $Gal(l/k)$ s'identifie canoniquement à un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$, comme on le verra en Td.
Par ailleurs, si l/k est galoisienne finie et vérifie que $Gal(l/k)$ est cylique d'ordre $n \geq 1$, il existe $a \in k^*$ tel que $l = D_k(X^n - a)$.

X. Calcul de groupes de Galois en caractéristique nulle et résolubilité par radicaux

X-A. Groupes de Galois des polynômes entiers

Soit p un entier premier. Si $P \in \mathbb{Z}[X]$, désignons par $\pi(P)$ le polynôme de $\mathbb{F}_p[X]$ obtenu par réduction modulo p des coefficients de P. La connaissance de $Gal_{\mathbb{F}_p}(\pi(P))$ peut-elle nous donner des informations sur $Gal_{\mathbb{Z}}(P)$?

X-A- 1. Norme d'un entier algébrique

Rappelons tout d'abord que si $a \in \mathbb{C}$ est entier sur $\mathbb{Z}$, son polynôme minimal sur $\mathbb{Q}$ est en fait à coefficients dans $\mathbb{Z}[X]$, comme on peut le voir par division euclidienne.
Par ailleurs, $N_{\overline{\mathbb{Q}}/\mathbb{Q}}(a) = N_{l/\mathbb{Q}}(a) \in \mathbb{Z}$ où $l = D_{\mathbb{Q}}(\mu_{a,\mathbb{Q}})$, et, si a est rationnel, a est entier.
Soit $P \in \mathbb{Q}[x]$ un polynôme unitaire séparable de degré n est k un corps de décomposition de P. Soient $x_1, \ldots, x_n$ l'ensemble des racines de P dans k, et soit $A := \mathbb{Z}[x_1, \ldots, x_n]$. Soit p un entier premier. Posons $\overline{A_p} := A/pA$ (l'anneau quotient, pas une extension d'anneaux...). Vérifions déjà que $\overline{A_p}$ n'est pas l'anneau nul :

Proposition X.1. *$\overline{A_p}$ n'est pas l'anneau nul.*

Démonstration de la proposition. Supposons par l'absurde que $\overline{A_p}$ soit l'anneau nul. Ainsi, il existe $a \in A\backslash\{0\}$ tel que $1 = pa$. On a donc, via $K = Fr(A) = \mathbb{Q}(x_1, \ldots, x_n)$, $1 = N_{K/\mathbb{Q}}(1) = N_{K/\mathbb{Q}}(p)N_{K/\mathbb{Q}}(a)$. Mais $N_{K/\mathbb{Q}}(p) = p^{[K:\mathbb{Q}]}$ et $N_{k/\mathbb{Q}}(a) \in \mathbb{N}$, ce qui est absurde.

□

Par construction, $\overline{A_p}$ est un anneau de caractéristique p. Il est naturellement muni d'une structure de $\mathbb{F}_p$ espace vectoriel et le fait que A soit un $\mathbb{Z}$-module de type fini (puisqu'engendré par des éléments entiers) implique que $\overline{A_p}$ est un $\mathbb{F}_p$-espace vectoriel de dimension finie.
Soit $\overline{\mathfrak{p}}$ un idéal maximal de $\overline{A_p}$. Soit $\mathfrak{p}$ le noyau du morphisme d'anneaux naturels

$$h : A \twoheadrightarrow \overline{A_p} \twoheadrightarrow \overline{A_p}/\overline{\mathfrak{p}} =: k_{\mathfrak{p}}$$

On peut montrer que si $\overline{\mathfrak{q}}$ est un autre idéal maximal de $\mathbb{F}_p$, alors $k_{\mathfrak{p}} = k_{\mathfrak{q}}$. Le corps résiduel ne dépend donc que de l'entier premier p choisi, ce qui mène à noter k_p au lieu de $k_{\mathfrak{p}}$. Ainsi, $A/\mathfrak{p} \cong k_{\mathfrak{p}}$ et donc $\mathfrak{p}$ est un idéal maximal de A contenant pA. Comme k_p est un $\mathbb{F}_p$ espace vectoriel de dimension finie et qu'il s'agit d'un corps, k_p est un corps fini.
Finalement, remarquons que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. En effet, $p\mathbb{Z} \subseteq \mathfrak{p}$ et $\mathfrak{p} \cap (\mathbb{Z}/p\mathbb{Z})$ est le noyau du morphisme de corps (donc injectif) $g : \mathbb{Z}/p\mathbb{Z} \to A/\mathfrak{p}$. k_p est engendré par les $x_i \ mod\ \mathfrak{p}$ donc k_p est un corps de décomposition de $\pi(P)$ sur $\mathbb{F}_p$. Comme l'extension $k_p/\mathbb{F}_p$ est une extension finie d'un corps fini, elle est galoisienne, et on peut considérer son groupe de Galois $Gal(k_p/\mathbb{F}_p)$. On a également une action naturelle

$$Gal_k(P) \curvearrowright A = \mathbb{Z}[x_1, \ldots, x_n]$$

et on dispose du diagramme commutatif suivant :

$$\begin{array}{ccccc} Gal_k(P)\curvearrowright & A & \twoheadrightarrow & \overline{A_p} & \\ & \downarrow & & \downarrow & \\ & A/\mathfrak{p} & \xrightarrow{\sim} & k_p & \curvearrowleft Gal(k_p/\mathbb{F}_p) \end{array}$$

On aurait envie de factoriser l'action $\mathbb{Z}$-linéaire $Gal_k(P) \curvearrowright A$ en une action $\mathbb{F}_p$-linéaire. $Gal_k(P) \curvearrowright k_p$. Pour faire cela, il faut respecter les théorèmes d'isomorphismes et imposer la condition suivante :

$$\forall \sigma \in Gal_k(P), \sigma(\mathfrak{p}) \subseteq \mathfrak{p} \tag{5}$$

Cette condition s'avère bien trop restrictive, et justifie que l'on s'intéresse aux éléments du groupe de Galois stabilisant globalement $\mathfrak{p}$.

Définition X.1. {*Groupe de décomposition*} *Le groupe de décomposition de* $\mathfrak{p}$ *est le sous-groupe de* $Gal_k(P)$ *stabilisant gloabalement* $\mathfrak{p}$*, c'est-à-dire l'ensemble des* $\sigma \in Gal_k(P)$ *tels que* $\sigma(\mathfrak{p}) \subseteq \mathfrak{p}$*. On le note* $D_{\mathfrak{p}}$*.*

Par construction, l'action $Gal_k(P) \curvearrowright A$ induit une action $\mathbb{F}_p$-linéaire $D_{\mathfrak{p}} \curvearrowright k_p$ et donc un morphisme de groupes

$$e_{\mathfrak{p}} : D_{\mathfrak{p}} \to Gal(k_p/\mathbb{F}_p)$$

Les actions se font par morphismes d'anneaux.

Lemme X.1. *L'application* $e_{\mathfrak{p}}$ *est surjective.*

Démonstration du lemme. Par le théorème de l'élément primitif (ou par cyclicité du groupe multiplicatif des corps finis), on peut choisir $x \in k_p$ tel que $k_p = \mathbb{F}_p[x]$.
Soit ensuite $g \in Gal_k(P)$. Supposons $g \notin D_{\mathfrak{p}}$. Ainsi, $g^{-1}(\mathfrak{p}) \neq \mathfrak{p}$. Soient $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ les éléments distincts de l'ensemble $\{\sigma^{-1}(\mathfrak{p}), \sigma \notin D_{\mathfrak{p}}\}$. Comme on a l'isomorphisme

$$A/\mathfrak{p} \underset{g}{\cong} A/g^{-1}(\mathfrak{p})$$

$g^{-1}(\mathfrak{p})$ est un idéal maximal de A.
L'ensemble $\{\mathfrak{p}, \mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ est formé d'idéaux deux à deux premiers entre eux. Par le lemme chinois, il existe $y \in k_p$ tel que $y = x \bmod \mathfrak{p}$ et tel que pour tout $i \in \mathbb{N}_t$ $y \in \mathfrak{p}_i$.
Enfin, considérons le polynôme

$$Q := \prod_{g \in Gal_k(P)} (X - g(y))$$

Ce polynôme Q est invariant sous l'action de $Gal_k(P)$. Il est donc à coefficients rationnels. Lélément $g(y)$ étant entier sur $\mathbb{Z}$ pour tout $g \in Gal_k(P)$, par les relations coefficients-racines, les coefficients de Q sont entiers sur $\mathbb{Z}$. Il s'agit donc d'entiers naturels, $\mathbb{Z}$ étant intégralement clos. On peut donc le regarder après réduction modulo $\mathfrak{p}$. Dans $k_p[X]$, Q s'écrit

$$\prod_{g \in D_{\mathfrak{p}}} (X - \overline{g(y)}) \prod_{g \notin D_{\mathfrak{p}}} X$$

Le polynôme minimal de x sur $\mathbb{F}_p$ est

$$\mu(X) = \prod_{g \in Gal(k_p/\mathbb{F}_p)} (X - g(x))$$

Comme

$$\prod_{g \in Gal_k(P)} (x - \overline{g(z)}) = 0$$

(en passant au quotient dans $Q(y) = 0$) on en déduit que μ divise

$$\prod_{g \in D_{\mathfrak{p}}} (X - \overline{g(x)})$$

Si $\sigma \in Gal(k_p/\mathbb{F}_p)$, il existe donc $g \in D_{\mathfrak{p}}$ tel que $\overline{g(x)} = e_{\mathfrak{p}}(g)(x) = \sigma(x)$. Comme σ est entièrement déterminé par $\sigma(x)$, ceci termine la démonstration.

□

Théorème X.1. *Supposons de plus* $\pi(P)$ *séparable sur* $\mathbb{F}_p$*. Alors* $e_{\mathfrak{p}}$ *est un isomorphisme de groupes compatible aux plongements dans* S_n *: si* $Gal(\pi(P))$ *contient une permutation,* $D_{\mathfrak{p}}$ *contient une permutation du même type.*

Démonstration du théorème. Il suffit d'observer le fait suivant : si $\pi(P)$ est à racines simples sur $\mathbb{F}_p$, alors on dispose d'une identification naturelle entre $S_{\{x_1,\dots,x_n\}}$ et $S_{\{x_1 \bmod \mathfrak{p},\dots,x_n \bmod \mathfrak{p}\}}$ via $[x_i \mapsto x_i \bmod \mathfrak{p}]$. La diagramme suivant commute donc :

$$\begin{tikzcd} D_{\mathfrak{p}} \arrow[r, "e_{\mathfrak{p}}"] \arrow[d, hook] \arrow[dr] & Gal(k_p/\mathbb{F}_p) \arrow[d, hook] \\ S_{\{x_1,\dots,x_n\}} = & S_{\{x_1 \bmod \mathfrak{p},\dots,x_n \bmod \mathfrak{p}\}} \end{tikzcd}$$

La flèche diagonale est donc injective, d'où le résultat.

□

X-A- 2. Quelques exemples d'applications

Considérons le polynôme $P := X^4 + X + 1$. Soit P_2 le réduit de P dans $\mathbb{F}_2$. P_2 est irréductible sur $\mathbb{F}_2$. Il est donc séparable par perfection des corps parfaits. On peut donc considérer son groupe de Galois $Gal_k(P)_2$. $Gal_k(P)_2$ peut se voir comme un sous-groupe de S_4 puisqu'il agit transitivement sur $Z(P)$. Comme c'est un groupe cyclique d'ordre 4 (comme groupe de Galois d'une extension finie de corps finis), il contient un 4-cycle. Par critère d'irréductibilité modulaire [3], P est irréductible dans $\mathbb{Q}[X]$.Donc $Gal_k(P)$ est un sous-groupe de S_4 et contient un 4-cycle, donc $|Gal_k(P)|$ est un multiple de 4.
Soit P_3 le réduit de P dans $\mathbb{F}_3$. Dans $\mathbb{F}_3[X]$, P_3 se décompose en produit d'irréductibles de la manière suivante :

$$P_3(X) = (X-1) \qquad \underbrace{(X^3 + X^2 + X - 1)}_{=:Q_3(X)\text{irréductible car de degré 3 sans racines dans } \mathbb{F}_3}$$

Ainsi, $Gal(P_3) \cong Gal(Q_3)$ (immédiat) mais $Gal(Q_3) \cong Gal(\mathbb{F}_{27}/\mathbb{F}_3) \cong \mathbb{Z}/3\mathbb{Z}$. $Gal_k(P)$ a donc pour cardinal un multiple de 12. Donc $Gal_k(P)$ est S_4 ou A_4. Mais si $Gal_k(P) = A_4$, comme $Gal_k(P)$ contient un 3-cycle, on aboutit à une absurdité. Donc $Gal_k(P) = S_4$.

X-B. Résolubilité par radicaux

X-B- 1. Extensions radicales

Définition X.2. *Soit l/k une extension de corps. Elle est dite* <u>*radicale élémentaire*</u> *s'il existe $\alpha \in l$ un élément primitif de l'extension et un entier naturel non nul n tel que $\alpha^n \in k$.*
L'extension est dite <u>*radicale*</u> *s'il existe une suite finie d'extensions de corps*

$$k =: k_0 \subsetneq k_1 \subseteq \cdots \subseteq k_n := l$$

telle que pour tout $i \in [|0; n-1|]$ l'extension k_{i+1}/k_i soit radicale élémentaire, i.e il existe $\alpha_1, \dots, \alpha_n \in l$ et $j_1, \dots, j_n \in \mathbb{N}^*$ tels que $l = k(\alpha_1, \dots, \alpha_n)$ et tels que pour tout $i \in \{0, \dots n-1\}$ $\alpha_i^{j_i} \in k$.

Par exemple, toute extension cyclotomique est une extension radicale élémentaire.
Prenons quelques conventions : soit l/k une extension radicale et $k_0 \subsetneq k_1 \subseteq \cdots \subseteq k_n = l$ la suite d'extensions associée. On dit qu'il s'agit d'une <u>tour radicale</u>.
Pour tout $i \in [|0; n-1|]$, il existe $\alpha_i \in k_{i+1}$ et $j_i \in \mathbb{N}^*$ tels que $k_{i+1} = k_i(\alpha_i)$ et que $\alpha_i^{j_i} \in k_i$. On dit que la suite $(\alpha_1, \dots, \alpha_n)$ est une <u>suite radicale de l'extension</u>.
Étudions, comme d'habitude, la transitivité de cette notion :

Proposition X.2. *Soient l/k et m/l deux extensions de corps. Alors :*

1. *Si l/k est radicale et si m/l est radicale, m/k est radicale.*

3. Rappelons-le : Si p est un entier premier, si la réduction d'un polynôme $Q \in \mathbb{Z}[X]$ modulo p est irréductible sur $\mathbb{Z}/p\mathbb{Z}$, alors P est irréductible dans $\mathbb{Q}[X]$ et donc dans $\mathbb{Z}[X]$ s'il est primitif.

2. *Si m/k est radicale, alors m/l est radicale, mais l/k n'est en générale pas radicale.*

La preuve est laissée à titre d'exercice.

Proposition X.3. *Soit m/k une extension de corps et soient l_1/k et l_2/k deux extensions intermédiaires. Alors :*

1. *Si l_1/k et l_2/k sont radicales, l_1l_2/k est radicale.*
2. *Si m/k est radicale, il existe une extension de corps $\tilde{m}/m$ telle que l'extension $\tilde{m}/k$ soit une extension radicale normale.*

Démonstration de la proposition. 1. Soient $(\alpha_1, \dots, \alpha_r)$ et $(\beta_1, \dots, \beta_n)$ deux suites radicales respectivement associées à l_1/k et à l_2/k. Soient $k_0 \subseteq k_1 \cdots \subseteq k_r = l_1$ et $k'_0 \subseteq k'_1 \subseteq \cdots \subseteq k'_n = l_2$ les tours radicales associées. Posons alors, pour tout $i \in \mathbb{N}_n$, $k_{r+i} := k_r k'_i = k_{r+i-1}(\beta_i)$. Les extensions $(k_{j+1}/k_j)_{j\in\{0,\dots,n+r\}}$ sont bien radicales élémentaires et forment une tour radicale de l'extension l_1l_2/k, qui est donc une extension radicale.

2. Soit Ω une clôture algébrique de m. La clôture normale $\tilde{m}$ de m est une extension normale de k par construction et, comme
$$\tilde{m} = \prod_{\sigma\in Hom_k(m;\Omega)} \sigma(m)$$
l'extension $\tilde{m}/k$ est radicale.

□

Théorème X.2. *Soit k un corps contenant une racine primitive n-ème de l'unité ξ, $n \geq 2$. Alors :*

- *Si l/k est une extension radicaleélémentaire admettant $\{\alpha\}$ comme suite radicale, si $r \in \mathbb{N}^*$ est le plus petit entier non nul tel que $\alpha^r \in k$, l'extension l/k est galoisienne cyclique et $\alpha^{|Gal(l/k)|} \in k$.*
- *Si l/k est une extension galoisienne cyclique, alors l/k est une extension radicale élémentaire et admet une suite radicale $\{\alpha\}$ vérifiant $\alpha^n \in k$.*

On démontrera ce théorème dans le dernier Td.

X-B- 2. Résolubilité par radicaux

Définition X.3. *Soit k un corps et P un polynôme non constant à coefficients dans k. On dit que P est <u>résoluble par radicaux</u> s'il existe une extension radicale l/k de k dans laquelle P soit scindé.*

On suppose désormais que k est de caractéristique nulle.

Théorème X.3. {*Théorème de Galois*} *Pour tout $P \in k[X]$, les assertions suivantes sont équivalentes :*

i) P est résoluble par radicaux.

ii) $Gal_k(P)$ est un groupe résoluble.

Par exemple, $P = X^4 + X + 1$ est résoluble par radicaux sur $\mathbb{Q}$. En revanche, le polynôme $X^5 - 10X + 5$ n'est pas résoluble par radicaux.

X-B- 3. L'équation générique de degré n

On s'intéresse ici à des polynômes irréductibles de la forme $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_1 \in \mathbb{Q}[X]$. Peut-on résoudre "génériquement" l'équation $P(x) = 0$? On va considérer les coefficients $a_0, \ldots, a_{n-1}$ comme des indeterminées.

Définition X.4. *Soit $k := \mathbb{Q}(a_0, \ldots, a_{n-1})$. Le polynôme générique de degré n est le polynôme $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_1$ vu dans $k[X]$. On le note aussi Q.*

Proposition X.4. *Q est irréductible sur k et $Gal_k(Q) \cong S_n$.*

Démonstration de la proposition. Soit $l := \mathbb{Q}(X_1, \ldots, X_n)$. l est naturellement muni d'une action de S_n dont les points fixes sont les polynômes de $\mathbb{Q}(\Sigma_1, \ldots, \Sigma_n)$ où $\Sigma_1, \ldots, \Sigma_n$ sont les polynômes symétriques élémentaires. Par le théorème d'Artin, l/l^{S_n} est galoisienne de groupe de Galois S_n.
Par ailleurs, les relations coefficients-racines permettent d'identifier $\mathbb{Q}(\Sigma_1, \ldots, \Sigma_n)$ et $\mathbb{Q}(a_1, \ldots, a_n)$, via $D_k(Q)$ car Q est séparable.
Ainsi, $Gal_k(P) = Gal(D_k(P)/k) \cong Gal(l/l^{S_n}) \cong S_n$. Mais S_5 n'est pas résoluble, donc l'éqution générique de degré 5 n'est pas résoluble par radicaux.

□

On peut également montrer que, si l'on tire au hasard chacun des coefficients de P uniformément dans $[-N; N]$, en fixant toujours $deg(P) = n$, alors

$$\mathbb{P}[P \text{ est irréductible sur } \mathbb{Q} \text{ et de groupe de Galois } S_n] \underset{N \to +\infty}{\longrightarrow} 1$$

XI. Introduction à l'étude des corps de nombres

Dzns tout ce chapitre, k est un corps de nombres, c'est-à-dire une extension finie de $\mathbb{Q}$, et $\mathcal{O}_k$ désigne l'anneau des entiers de k (il est donc, par définition, intégralement clos).

XI-A. Théorème de la base entière et discriminant d'un corps

XI-A- 1. Discriminant d'une famille de vecteurs

Posons $\varphi : k \times K \to \mathbb{Q}$ défini par

$$\varphi(x, y) := Tr_{k/\mathbb{Q}}(xy)$$

Alors φ est une forme $\mathbb{Q}$-bilinéaire symétrique non dégénérée.

Définition XI.1. *Soit $n := [k : \mathbb{Q}]$. Pour tout $(\alpha_1, \ldots, \alpha_n) \in k^n$, on définit le discriminant de $(\alpha_1, \ldots, \alpha_n)$ relativement à $\mathbb{Q}$ par*

$$disc_{k/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) := det(\varphi(\alpha_i, \alpha_j))_{(i,j)\in\mathbb{N}_n^2}$$

Lemme XI.1. *Soit $n := [k : Q]$. Soit $(\alpha_1, \ldots, \alpha_n) \in k^n$. Alors :*

- *Cette famille est une $\mathbb{Q}$-base de k si et seulement si $disc_{k/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) \neq 0$.*
- *Soit $M = (m(i, j))_{(i,j)\in\mathbb{N}_n^2} \in M(n, k)$ et, pour tout $j \in \mathbb{N}_n, \mu_j := m(1, j)a1 + m(2, j)\alpha_2 + \cdots + m(n, j)\alpha_n$.Alors*
$$disc_{k/\mathbb{Q}}(\mu_1, \ldots, \mu_n) = det(M)^2 disc_{k/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$$
- *Supposons qu'il existe $\alpha \in k$ tel que pour tout $i \in \mathbb{N}_n$ $\alpha_i = \alpha^i$. Soit μ le polynôme minimal de α sur $\mathbb{Q}$. Alors*
$$disc_{k/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = disc(\mu, \mathbb{Q})$$
pour la notion traditionnelle de discriminant d'un polynôme.

XI-A- 2. Théorème de la base entière

Lemme XI.2. • *Pour tout $\sigma \in Hom_{\mathbb{Q}}(k; \mathbb{C})$, les éléments de $\sigma(\mathcal{O}_k)$ sont des complexes entiers sur $\mathbb{Z}$.*

- *Pour tout élément $x \in k$, il existe $m \in \mathbb{N}^*$ tel que $mx \in \mathcal{O}_k$.*

Théorème XI.1. *{De la base entière} L'anneau $\mathcal{O}_k$ est un $\mathbb{Z}$-module libre de rang $[k : /Q]$. En particulier, il existe $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_k$ tels que*

$$\mathcal{O}_k = \oplus_{i=1}^n \alpha_i \mathbb{Z}$$

Définition XI.2. *Une base entière sur k est une base formée d'éléments de $\mathcal{O}_k$.*

XI-B. Structure des corps de nombres

Théorème XI.2. *$\mathcal{O}_k$ est un anneau de Dedekind.*

Table des matières

I Avant-Propos . . . i
- I Conseils bibliographiques . . . i
- II Notations et conventions . . . i

I Algèbre Commutative **1**
- II Produit tensoriel . . . 2
  - I Motivation . . . 2
  - II Produit tensoriel de deux modules . . . 2
  - III Propriétés élémentaires du produit tensoriel . . . 3
  - IV Exemples de calculs de produits tensoriels . . . 5
  - V Changements de bases et produit tensoriel d'algèbres . . . 6
- III Propriétés fonctorielles du produit tensoriel . . . 7
  - I Catégories et foncteurs . . . 7
  - II Exactitude et platitude . . . 8
- IV Algèbres tensorielles, symétriques et extérieures . . . 12
  - I Algèbre tensorielle d'un module . . . 12
  - II Algèbre symétrique d'un module . . . 12
  - III Algèbres et puissances extérieures . . . 13
  - IV Déterminants d'applications A-linéaires . . . 14
- V De la localisation aux anneaux de valuation discrète . . . 15
  - I Rappels sur la localisation . . . 15
  - II Localisation des modules . . . 17
  - III Anneaux de valuation discrète . . . 19
  - IV Anneaux de Dedekind . . . 21

II Théorie de Galois **24**
- VI Extensions de corps . . . 25
  - I Définitions générales . . . 25
  - II Extensions engendrées, extensions composées . . . 25
  - III Extensions algébriques, degré de transcendance . . . 27
  - IV Exercices corrigés . . . 28
- VII Extensions séparables et corps parfaits . . . 30
  - I Polynômes séparables : rappels et compléments . . . 30
  - II Éléments séparables . . . 30
  - III Corps parfaits . . . 31
- VIII Extensions galoisiennes . . . 33
  - I Extensions normales . . . 33
  - II Extensions galoisiennes . . . 34
  - III Groupe de Galois d'un polynôme . . . 35
- IX Correspondance de Galois . . . 37
  - I Le lemme d'Artin et la correspondance de Galois . . . 37
  - II Extensions cyclotomiques . . . 38
  - III Hilbert '90 et extensions cyclotomiques . . . 39
- X Calcul de groupes de Galois en caractéristique nulle et résolubilité par radicaux . . . 40

I Groupes de Galois des polynômes entiers 40
II Résolubilité par radicaux 42
XI Introduction à l'étude des corps de nombres 45
I Théorème de la base entière et discriminant d'un corps 45
II Structure des corps de nombres 45