Cours d'algèbre

Christian Blanchet

http://people.math.jussieu.fr/~blanchet/enseignement

M1, Paris-Diderot (Paris 7), 2011-2012

Le cours comporte deux parties. La première partie (1-5) est consacrée à la théorie de Galois et ses applications. On intègre les compléments utiles sur les anneaux, anneaux de polynômes et groupes. La seconde partie (6-9) aborde la théorie des modules : notions de bases, résultats de structure des modules de type fini sur les anneaux principaux avec les applications correspondantes, calcul des idéaux dans les anneaux de polynômes. On traite les représentations des groupes finis et des algèbres comme exemples de modules.

1. Anneaux commutatifs, anneaux de polynômes : rappels et compléments.
2. Extensions de corps : généralités ; algébricité ; corps de décomposition, clôture algébrique ; corps finis, corps cyclotomiques.
3. Groupes : action de groupe, théorèmes de Sylow, groupes résolubles.
4. Théorie de Galois : groupe de Galois ; extensions normales, extensions séparables, correspondance de Galois.
5. Applications de la théorie de Galois : résolubilité par radicaux, constructibilité.
6. Introduction à la théorie des modules : généralités, exemples, éléments de torsion, modules libres, produit tensoriel.
7. Modules sur les anneaux principaux : théorèmes de structure ; groupes abéliens de type fini, réseaux ; réduction des endomorphismes des espaces vectoriels de dimension finie.
8. Modules et anneaux noethériens ; cas des polynômes ; bases de Gröbner.
9. Représentations linéaires d'un groupe et d'une algèbre. Irréductibilité. En dimension finie : exemples de décomposition d'une représentation linéaire en somme directe de sous-représentations, lemme de Schur. Cas des groupes finis : théorie des caractères.

RÉFÉRENCES :

– Polycopié d'Alain Bruguières.
– Dummit D.S., Foote R.M., *Abstract Algebra*, (3ed., Wiley 2004) (ch.7-14,18-19).
– Goblot Rémi, *Algèbre commutative*, Masson.
– Chambert-Loir Antoine, *Algèbre commutative*, notes de cours.
– Chambert-Loir Antoine, *Algèbre corporelle*, Editions polytechniques.
– Gozard, *Théorie de Galois*, Ellipses.
– Tauvel, *Corps commutatifs et théorie de Galois*, Eyrolles.
– Escofier, *Théorie de Galois*, Dunod.

Chapitre 1

Anneaux commutatifs, anneaux de polynômes : rappels et compléments

1.1 Définitions et exemples de base

Définition 1.1.1. Un anneau (resp. anneau commutatif) est un groupe abélien $(A, +)$ muni d'une seconde opération $m : A \times A \to A$, notée multiplicativement (i.e. le plus souvent sans symbole : $m(a, b) = ab$ ou avec un point si besoin),

qui est associative (resp. associative et commutative),
admet un élément neutre (appelé unité et souvent noté 1),
et est distributive à gauche et à droite par rapport à l'addition.

Remarque 1.1.2. Dans ce chapitre on ne s'intéresse qu'aux anneaux commutatifs.

Remarques 1.1.3.

1. Pour $x \in A$: $0.x = x.0 = 0$, et $(-1).x = -x = x.(-1)$.
2. Pour $x \in A$, $y \in A$, on a : $(-x)y = x(-y) = -(xy)$ et $(-x)(-y) = xy$.
3. Sauf pour l'anneau réduit au seul élément 0 (anneau nul), l'élément unité est non nul.

Définition 1.1.4. a) Un élément d'un anneau A est dit inversible si et seulement s'il est symétrisable pour la seconde opération.
b) Un élément non nul x d'un anneau A est un diviseur de zéro si et seulement si son produit avec un autre élément non nul vaut zéro :

$$\exists y \neq 0,\ xy = 0 \text{ ou } yx = 0\ .$$

On note $A^\times$ l'ensemble des éléments inversibles de A.

Proposition 1.1.5. *Si A est un anneau non nul, l'ensemble $A^\times$ des éléments inversibles est un groupe multiplicatif.*

Définition 1.1.6. a) Un corps est un anneau non nul ($1 \neq 0$) dans lequel tout élément non nul est inversible, i. e. $A^\times = A - \{0\}$.
b) Un anneau intègre est un anneau non nul sans diviseur de zéro ; un anneau commutatif intègre est aussi appelé *domaine d'intégrité*.

Exercice 1.1.7. Montrer qu'un anneau fini intègre est un corps.

Exemples 1.1.8.

1. L'anneau des entiers : $\mathbb{Z}$; les décimaux : $\mathbb{D}$.
2. Le corps des rationnels : $\mathbb{Q}$; les réels : $\mathbb{R}$; les complexes : $\mathbb{C}$.
3. Les anneaux de congruences : $\mathbb{Z}/n\mathbb{Z}$, $n \geq 2$; les corps $\mathbb{Z}/p\mathbb{Z}$ pour p premier.
4. Les anneaux de fonctions : si A est un anneau et X un ensemble, les applications de X vers A forment un anneau noté $\mathcal{A}(X, A)$.

Définition 1.1.9. Un sous-anneau d'un anneau A est une partie B de A qui est un anneau avec les opérations induites de A, et la même unité que A.

Proposition 1.1.10. *Une partie B d'un anneau A est un sous-anneau si et seulement si :*

B est un sous-groupe additif,
B est stable par multiplication, et
B contient l'unité de A.

Exemples 1.1.11.

1. L'ensemble des entiers de Gauss
$$\mathbb{Z}[i] = \{a + ib;\ a \in \mathbb{Z}, b \in \mathbb{Z}\}$$
forme un sous-anneau de $\mathbb{C}$.
2. Les fonctions complexes continues sur un intervalle I : $\mathcal{C}(I, \mathbb{C})$ forment un sous-anneau de $\mathcal{A}(I, \mathbb{C})$.

Exercice 1.1.12. Déterminer les éléments inversibles de $\mathbb{Z}[i]$.

Définition 1.1.13. Soit A et B deux anneaux. Une application $f : A \to B$ est un morphisme d'anneau si et seulement si f respecte les opérations et l'élément unité. Un isomorphisme d'anneau est un morphisme bijectif.

Définition 1.1.14. Soit A un anneau commutatif. Une algèbre sur A est un anneau B muni d'un morphisme d'anneau

$$\eta : A \to B \ .$$

Définition 1.1.15. Soient B_1 et B_2 deux algèbres sur l'anneau commutatif A, avec morphismes de structure $\eta_i : A \to B_i$. Un morphisme d'algèbre de B_1 vers B_2 est un morphisme d'anneau $f : B_1 \to B_2$ tel que :

$$\eta_2 = f \circ \eta_1 \ .$$

1.2 Anneaux de polynômes

Soit A un anneau commutatif et X une *indéterminée* (un symbole). On note $A[X]$ l'ensemble des suites d'éléments de A avec un nombre fini de termes non nul, notées comme combinaisons linéaires des X^n, $n \geq 0$: les éléments de $A[X]$ s'écrivent sous la forme :

$$P = \sum_n a_n X^n = \sum_{n=0}^{N} a_n X^n \ .$$

$A[X]$ est muni des opérations :

$$(\sum_n a_n X^n) + (\sum_n b_n X^n) = \sum_n (a_n + b_n) X^n \ .$$

$$(\sum_n a_n X^n) \times (\sum_m b_m X^m) = \sum_p c_p X^p \ , c_p = \sum_k a_k b_{p-k} \ .$$

Proposition 1.2.1. *$A[X]$ est une algèbre sur A.*

Remarque 1.2.2. L'application qui définit la structure d'algèbre est injective, d'image les polynômes constants ; A est identifié au sous-anneau de $A[X]$ formé par les polynômes *constants*.

Proposition 1.2.3 (Propriété universelle)**.** *Soit B une algèbre sur l'anneau commutatif A, et b un élément de B, alors il existe un unique morphisme d'algèbre $E_b : A[X] \to B$ tel que $E_b(X) = b$.*

Remarque 1.2.4. E_b est appelé morphisme d'évaluation et $E_b(P)$ est noté $P(b)$.

Définition 1.2.5. Le degré d'un polynôme non nul $P = \sum_n a_n X^n$ est le plus grand n pour lequel $a_n \neq 0$ (convention : $\deg(0) = -\infty$).

Proposition 1.2.6. *Si A est un anneau commutatif intègre, alors :*
a) $\deg(PQ) = \deg(P) + \deg(Q)$,
b) les inversibles de $A[X]$ sont les inversibles de A, et
c) $A[X]$ est un anneau intègre.

1.3 Anneaux quotients

Définition 1.3.1. Un idéal d'un anneau commutatif A est un sous-groupe additif I de A, tel que : $IA \subset I$.

Remarque 1.3.2. Dans le cas non commutatif, il y a une notion d'idéal à droite et d'idéal à gauche ; on précise parfois idéal bilatère.

Exemples 1.3.3. Dans $\mathbb{Z}$ tous les sous-groupes additifs sont de la forme $n\mathbb{Z}$; ce sont tous des idéaux.

Proposition 1.3.4. *Soit $f : A \to B$ un morphisme d'anneau. Le noyau de f est un idéal de A et l'image de f est un sous-anneau de B.*

Proposition 1.3.5. *Soit I un idéal d'un anneau A, alors la multiplication de A induit sur le groupe additif quotient une structure d'anneau.*

Proposition 1.3.6 (Factorisation d'un morphisme d'anneau)**.** *Soit $f : A \to B$ un morphisme d'anneau, I un idéal de A et $p : A \to A/I$ la projection* canonique*. Le morphisme f factorise par le quotient A/I (i.e. il existe un morphisme d'anneau $g : A/I \to B$ tel que $f = g \circ p$) si et seulement si $I \subset \mathrm{Ker}(f)$. Le morphisme g a même image que f et est injectif si et seulement si $I = \mathrm{Ker}(f)$.*

Corollaire 1.3.7 (Premier théorème d'isomorphisme des anneaux)**.** *Soit $f : A \to B$ un morphisme d'anneau, alors le quotient $A/\mathrm{Ker}(f)$ est isomorphe à l'image de f.*

Exercice 1.3.8 (Second théorème d'isomorphisme des anneaux). Soient B un sous-anneau de A, et I un idéal de A.

1. Démontrer que $B + I$ est un sous anneau de A.
2. Démontrer que $B \cap I$ est un idéal de B et que : $(B+I)/I$ est isomorphe à $B/(B \cap I)$.

Exercice 1.3.9 (Troisième théorème d'isomorphisme des anneaux). Soient $I \subset J$ deux idéaux de l'anneau A. Démontrer que J/I est un idéal de A/I, et que $A/J)$ est isomorphe à $(A/I)/(J/I)$.

1.4 Propriétés des idéaux

1.4.1 Constructions d'idéaux

Proposition 1.4.1. *L'intersection d'une famille non vide d'idéaux est un idéal.*

Corollaire 1.4.2. *Soit E une partie d'un anneau A, alors il existe un plus petit idéal qui contient E. On l'appelle l'idéal engendré par E, et on le note (E), ou $(E)_A$ s'il y a ambiguïté.*

Proposition 1.4.3 (Somme et produit)**.** *a) L'idéal engendré par $I \cup J$ est :*

$$I + J = \{i + j,\ i \in I\ j \in J\}\ .$$

On appelle cet idéal la somme de I et J.
b) L'idéal engendré par l'ensemble des produits ij, $i \in I$ $j \in J$ est :

$$\{\sum_k\ i_k j_k,\ \forall k\ i_k \in I\ j_k \in J\}\ .$$

Cet idéal est appelé le produit de I et J et noté (IJ).

Exercice 1.4.4. Soit A un anneau **commutatif**.

1. Démontrer que l'idéal engendré par $a \in A$ est Aa.
2. Démontrer que l'idéal engendré par $\{a_1, \ldots, a_n\} \subset A$ est $Aa_1 + \cdots + Aa_n$.

Définition 1.4.5. Un idéal principal est un idéal engendré par un élément. Un idéal de génération finie est un idéal engendré par une partie finie.

Proposition 1.4.6. *Tous les idéaux de $\mathbb{Z}$ sont principaux.*

Exercice 1.4.7. Quel est l'idéal engendré par un élément inversible ?

Exercice 1.4.8.
1. Quels sont les idéaux d'un corps ?
2. Montrer que si A est un corps, tout morphisme d'anneau $f : A \to B$ est injectif.
3. Montrer qu'un anneau commutatif qui a deux idéaux est un corps.

1.4.2 Idéaux maximaux

Définition 1.4.9. Un idéal I d'un anneau commutatif A est maximal si et seulement si A/I est un corps.

Le vocabulaire est justifié par la proposition suivante :

Proposition 1.4.10. *Dans un anneau commutatif non nul A, un idéal I est maximal si et seulement si c'est un élément maximal pour l'inclusion parmi les idéaux distincts de A.*

Théorème 1.4.11. *Tout anneau commutatif non nul contient au moins un idéal maximal.*

Corollaire 1.4.12. *Dans un anneau commutatif A, tout idéal distinct de A est contenu dans un idéal maximal.*

Remarque 1.4.13. La preuve générale du théorème précédent utilise le lemme de Zorn. Dans beaucoup d'anneaux le résultat est élémentaire et indépendant du lemme de Zorn.

fin du cours 14/09

1.4.3 Idéaux premiers

Définition 1.4.14. Un idéal I d'un anneau commutatif est premier si et seulement si A/I est un anneau intègre.

Remarque 1.4.15. Un anneau intègre est par définition non nul, l'anneau lui-même n'est donc pas un idéal premier.

Remarque 1.4.16. On peut reformuler la définition : L'idéal I de l'anneau A est premier si et seulement si $I \neq A$ et

$$\forall a,\ \forall b\ ab \in I \Rightarrow a \in I \text{ ou } b \in I\ .$$

Remarque 1.4.17. Dans un anneau commutatif tout idéal maximal est premier.

Dans $\mathbb{Z}$ l'idéal nul est premier mais n'est pas maximal. Les autres idéaux premiers sont les $p\mathbb{Z}$ avec p premiers. Ils sont maximaux.

1.5 Divisibilité dans les anneaux commutatifs intègres

Soit A un anneau commutatif intègre. On note avec une barre verticale la relation de divisibilité.

Remarque 1.5.1. Il y a équivalence entre :

(i) $x|y$ et $y|x$,
(ii) $\exists u \in A^\times \quad y = ux$,
(iii) $(x) = (y)$.

Proposition 1.5.2. *a) Sur A la relation $x \sim y \Leftrightarrow \exists u \in A^\times \quad y = ux$ est une relation d'équivalence.*
Les classes d'équivalence sont appelées classes d'éléments associés.

c) La relation divise induit une relation d'ordre sur les classes d'éléments associés.

La relation d'ordre précédente permet de définir les notions de PGCD et de PPCM. L'existence n'est pas garantie, mais il y a toujours unicité comme classe d'éléments associés. Donnons une formulation précise naïve.

Définition 1.5.3. Soit A un anneau commutatif intègre, et F un ensemble d'éléments de A.
a) d est (un) PGCD de F si et seulement si :

$$\forall x \in F \quad d|x \text{ , et}$$

$$\forall \delta \in A - \{0\} \ (\forall x \in F \quad \delta|x) \Rightarrow \delta|d \ .$$

b) m est (un) PPCM de F si et seulement si :

$$\forall x \in F \quad x|m \text{ , et}$$

$$\forall \mu \in A - \{0\} \ (\forall x \in F \quad x|\mu) \Rightarrow m|\mu \ .$$

Définition 1.5.4. $p \in A$ est irréductible si seulement si p a deux classes de diviseurs : $A^\times$ et $pA^\times$.

On va relier cette notion à celle d'idéal.

Proposition 1.5.5. *Si l'idéal pA est premier (on dit que p est premier), alors p est irréductible.*

1.6 Anneaux principaux

Définition 1.6.1. Un anneau principal est un anneau commutatif intègre dans lequel tout idéal est principal (engendré par un seul élément).

Définition 1.6.2. Un anneau A est euclidien si et seulement s'il existe une application $d : A - \{0\} \longrightarrow \mathbb{N}$ satisfaisant la condition suivante :
pour tout couple (a, b), avec $b \neq 0$, il existe un couple (q, r) tel que :

$$a = bq + r \text{ et } (r = 0 \text{ ou } d(r) < d(b)) \ .$$

Remarque 1.6.3. L'application d est appelée un stathme (ou une norme).

Proposition 1.6.4. *Tout anneau euclidien est principal.*

Exemples 1.6.5. L'anneau $\mathbb{Z}$, les anneaux $\mathbb{K}[X]$ avec $\mathbb{K}$ un corps sont des anneaux euclidiens.

Théorème 1.6.6. *Soient a et b deux éléments d'un anneau principal A.*

a) d est PGCD de a et b si et seulement si $(d) = (a) + (b)$.
b) m est PPCM de a et b si et seulement si $(m) = (a) \cap (b)$.

Plus généralement :

Théorème 1.6.7. *Soit F une partie non vide d'un anneau principal A.*

a) d est PGCD de F si et seulement si d est générateur de l'idéal engendré par F.
b) m est PPCM de F si et seulement si $(m) = \bigcap_{a \in E} aA$.

Corollaire 1.6.8. *Dans un anneau principal toute partie non vide de A a un PGCD et un PPCM.*

Théorème 1.6.9 (Bezout)**.** *Dans un anneau principal A, deux éléments ont 1 comme PGCD (sont premiers entre eux) si et seulement s'il existe un couple (u, v) tel que :*

$$ua + vb = 1 \ .$$

Théorème 1.6.10. *Soit p un élément non nul d'un anneau principal. Les énoncés suivants sont équivalents :*

a) p est irréductible ;
b) l'idéal (p) est premier (p est premier) ;
c) l'idéal (p) est maximal.

Corollaire 1.6.11. *Dans un anneau principal, tout idéal premier non nul est maximal.*

Proposition 1.6.12 (Lemme de Gauss)**.** *Dans un anneau principal A, si $a|bc$ et a est premier avec b, alors $a|c$.*

Corollaire 1.6.13 (Lemme d'Euclide)**.** *Dans un anneau principal A, si un élément premier divise un produit, alors il divise l'un des facteurs.*

Proposition 1.6.14. *Dans un anneau principal, toute suite croissante d'idéaux est stationnaire.*

Théorème 1.6.15. *Dans un anneau principal, il existe une décomposition en facteurs irréductibles, unique aux inversibles près et à l'ordre près des facteurs (essentiellement unique).*

1.7 Anneaux factoriels

Définition 1.7.1. Un anneau commutatif intègre est factoriel si et seulement si tout élément non nul et non inversible se décompose de manière essentiellement unique comme produits d'éléments irréductibles.

Théorème 1.7.2. *Un anneau A est factoriel si et seulement si :*

a) Toute suite croissante d'idéaux principaux est stationnaire, et
b) tout élément irréductible de A est premier.

Proposition 1.7.3. *Dans un anneau factoriel toute famille finie a un PGCD et un PPCM.*

Proposition 1.7.4 (Lemme de Gauss)**.** *Dans un anneau factoriel A, si $a|bc$ et a est premier avec b (i.e. 1 est PGCD de a et b), alors $a|c$.*

1.8 Corps des fractions

Dans cette section on considère des anneaux commutatifs intègres.

Définition 1.8.1. Une partie multiplicative d'un anneau commutatif intègre A est une partie S de $A - \{0\}$ contenant l'unité et multiplicativement stable.

Etant donné une partie multiplicative S d'un anneau (commutatif intègre) A. On définit $S^{-1}A$ comme le quotient de $S \times A$ par la relation :

$$(s, a) \sim (s', a') \Leftrightarrow sa' = as' \ .$$

On note $\frac{a}{s}$ la classe de (s, a) dans l'ensemble quotient $S^{-1}A$.

Théorème 1.8.2. *Les opérations :*

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + sa'}{ss'} \ ,$$

$$\frac{a}{s} \times \frac{a'}{s'} = \frac{aa'}{ss'} \ ,$$

sont bien définies et munissent $S^{-1}A$ d'une structure d'anneau qui contient $\frac{A}{1} \approx A$ comme sous-anneau.

Théorème 1.8.3 (Propriété universelle)**.** *Pour tout morphisme d'anneau $f : A \to B$ qui envoie les éléments de S sur des inversibles, il existe une unique extension $F : S^{-1}A \to B$. Le noyau de F est l'idéal $S^{-1}\mathrm{Ker(f)}$; en particulier si f est injective alors F est aussi injective.*

Exemples 1.8.4.
1. Si on prend $S = A - \{0\}$, on obtient le corps des fractions de A : $\mathcal{Q}(A)$.
2. Pour $A = \mathbb{Z}$, $S = \{10^n,\ n \in \mathbb{N}\}$, on construit les décimaux.
3. Pour $A = \mathbb{K}[X]$, avec $\mathbb{K}$ un anneau commutatif, et $S = \{X^n,\ n \in \mathbb{N}\}$, on obtient l'anneau des polynômes de Laurent noté $\mathbb{K}[X, X^{-1}]$.
4. Pour $A = \mathbb{K}[X]$, avec $\mathbb{K}$ un corps commutatif, le corps des fractions obtenu est le corps des fractions rationnelles, noté $\mathbb{K}(X)$.

1.9 Critères d'irréductibilité

On étudie dans cette section l'irréductibilité des polynômes à coefficients dans un **anneau factoriel**. On utilisera la notation $\doteq$ pour une égalité modulo un inversible de l'anneau.

Définition 1.9.1. Soit A un anneau factoriel.
a) Le contenu $c(P)$ d'un polynôme $P \in A[X]$ est le PGCD de ses coefficients.
b) Un polynôme $P \in A[X]$ est primitif si et seulement si son contenu vaut 1 : $c(P) \doteq 1$.

Remarque 1.9.2. On suppose que l'anneau A est factoriel.
1. Un polynôme irréductible non constant de $A[X]$ est nécessairement primitif.
2. Si $P \in A[X]$ est primitif et irréductible dans $\mathcal{Q}(A)[X]$, alors il est irréductible dans $A[X]$. Nous allons étudier la réciproque.

16/09/2011

Lemme 1.9.3. *Soit f un élément irréductible dans l'anneau factoriel A. La surjection canonique $\pi : A \to A/fA$ s'étend en un morphisme d'anneau :*

$$\begin{array}{rccc} \Pi : & A[X] & \to & A/fA\,[X] \\ & P = \sum_k a_k X^k & \mapsto & \sum_k \overline{a}_k X^k \end{array} ,$$

et induit un isomorphisme : $A[X]/fA[X] \approx A/fA\,[X]$.

Corollaire 1.9.4. *Si f est un élément premier dans A, alors f est premier dans $A[X]$.*

Proposition 1.9.5. *Le produit de deux polynômes primitifs à coefficients dans un anneau factoriel est un polynôme primitif.*

Corollaire 1.9.6. *Pour P et Q dans $A[X]$, avec A factoriel, on a $c(PQ) \doteq c(P)c(Q)$.*

Corollaire 1.9.7. *Soit A un anneau factoriel. Si $P \in A[X]$ est divisible dans $\mathcal{Q}(A)[X]$ par un polynôme primitif $Q \in A[X]$, alors P est divisible par Q dans $A[X]$.*

Proposition 1.9.8. *Un polynôme $P \in A[X]$ non constant et primitif est irréductible dans $A[X]$ si et seulement s'il l'est dans $\mathcal{Q}(A)[X]$.*

Les polynômes constants irréductibles dans $A[X]$ sont les irréductibles de A. Les polynômes non constants irréductibles dans $A[X]$ sont les polynômes non constants primitifs de $A[X]$ qui sont irréductibles dans $\mathcal{Q}(A)[X]$.

Théorème 1.9.9 (Factorialité des anneaux de polynômes)**.** *Si A est un anneau factoriel, alors l'anneau $A[X]$ est factoriel.*

Proposition 1.9.10 (Réduction des coefficients)**.** *Soit f est un élément premier de l'anneau factoriel A, et soit $P \in A[X]$ un polynôme primitif non constant. Si la réduction de P modulo f est irréductible, alors P est irréductible dans $A[X]$, donc dans $\mathcal{Q}(A)[X]$.*

Proposition 1.9.11 (Critère d'Eisenstein)**.** *Soient A un anneau factoriel, f un élément irréductible de A, et*

$$P = \sum_{k=0}^{n} a_k X^k$$

un polynôme non constant primitif dans $A[X]$.
Si : $f \not| a_n$, $\forall i < n$ $f | a_i$, et $f^2 \not| a_0$, alors P est irréductible dans $A[X]$.

Exercice 1.9.12. Montrer que si A est un anneau intègre, les diviseurs d'un monôme de $A[X]$ sont des monômes.

Chapitre 2

Extensions de corps : généralités

Tous les corps considérés dans ce cours sont commutatifs.

2.1 Théorie de base

Rappel : La caractéristique d'un corps est soit zéro, soit un nombre premier.

Définition 2.1.1. Si K et L sont des corps, on appelle morphisme de corps tout morphisme d'anneau $f : K \to L$. Un tel morphisme est injectif et aussi appelé extension de K. Le degré de l'extension, noté $[L : K]$ est la dimension de L comme espace vectoriel sur K.

Proposition 2.1.2. *a) Si K est un corps de caractéristique nulle, alors il existe une unique extension $f : \mathbb{Q} \to K$.*
b) Si K est un corps de caractéristique $p > 0$, alors il existe une unique extension $f : \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \to K$.

Définition 2.1.3. L'image de l'homorphisme précédent s'appelle le sous-corps premier de $\mathbb{K}$: c'est le plus petit sous-corps de $\mathbb{K}$.

Proposition 2.1.4 (Tour d'extensions)**.** *Soit $f : K \to L$, $g : L \to E$ une* tour d'extension*, alors le degré $[E : K]$ est fini si et seulement si $[E : L]$ et $[L : K]$ le sont, et :*

$$[E : K] = [E : L][L : K] \ .$$

2.2 Construction d'extensions

2.2.1 Corps de rupture d'un polynôme irréductible

Soit $P \in K[X]$ un polynôme irréductible, alors $K[X]/(P)$ est un corps.

Proposition 2.2.1. *L'extension $K \to K[X]/(P)$, avec $P \in K[X]$ polynôme irréductible, est une extension de degré* $\deg(P)$.

2.2.2 Adjonction d'éléments

Soit $f : K \to L$ une extension de corps, et $\alpha \in L$. On note $K(\alpha)$ le plus petit sous-corps de L qui contient $f(K)$ et α ; on l'appelle extension de K engendrée par α. On définit de même l'extension $K \to K(A)$ engendrée par une partie $A \subset L$.

Définition 2.2.2. Une extension est de type finie si et seulement si elle est engendrée par une partie finie. Une extension est simple si et seulement si elle est engendrée par un élément (appelé élément primitif).

2.3 Algébricité

Proposition 2.3.1. *Soit $f : K \to L = K(\alpha)$ une extension simple, alors il y a équivalence entre :*
a) l'extension est de degré finie ;
b) l'anneau $K[\alpha]$ est égal au corps $K(\alpha)$;
c) l'idéal annulateur de α : $I_\alpha = \{P \in K[X],\ P(\alpha) = 0\}$ est non trivial.

23/09/2011

Remarques 2.3.2. 1. Lorsque l'idéal annulateur de α est non trivial, il est engendré par un polynôme irréductible unitaire P_α appelé le polynôme minimal de α et $K[X]/(P_\alpha)$ est isomorphe à $K(\alpha)$.
2. Si α et β ont le même polynôme minimal, alors les extensions $K \to K(\alpha)$ et $K \to K(\beta)$ sont isomorphes.

Définition 2.3.3. a) Avec les hypothèses précédentes, l'élément α est algébrique sur K si et seulement s'il satisfait les conditions équivalentes de la proposition ; dans le cas contraire, α est dit transcendant.
b) Une extension $f : K \to L$ est algébrique si et seulement si tous les éléments de L sont algébriques sur K.

Théorème 2.3.4. *Les éléments de L algébriques sur K forment un sous-corps de L.*

2.4 Corps de décomposition

Définition 2.4.1. Soit $Q \in K[X]$ un polynôme unitaire, et $f : K \to L$ une extension. On dit que L est un corps de décomposition de Q si et seulement si :
a) $f(Q)$ est scindé dans L et
b) l'extension L est engendrée par les racines de Q.

Théorème 2.4.2. *Soit $Q \in K[X]$ un polynôme unitaire, alors il existe une extension qui est un corps de décomposition de K, et deux telles extensions sont isomorphes.*

2.5 Corps cyclotomiques

On note $\zeta_n = e^{\frac{i2\pi}{n}} \in \mathbb{C}$.

Proposition 2.5.1. *Le corps $\mathbb{Q}(\zeta_n)$ est le corps de décomposition du polynôme $X^n - 1$.*

Définition 2.5.2. Le corps $\mathbb{Q}(\zeta_n)$ est appelé corps cyclotomique des racines n-ièmes de l'unité.

Polynômes cyclotomiques

Définition 2.5.3. On appelle racine primitive n-ième de l'unité tout générateur du groupe $U_n \subset \mathbb{C}$ des racines n-ièmes de 1. Ce sont les éléments d'ordre n de $\mathbb{C}^*$.

Définition 2.5.4. Le polynôme cyclotomique $\Phi_n \in \mathbb{C}[X]$ est le polynôme unitaire dont les racines sont les racines primitives n-ièmes de 1 :

$$\Phi_n = \prod_{\substack{0 \leq k < n \\ PGCD(k,n)=1}} (X - \zeta_n^k) \ .$$

Théorème 2.5.5. *Le polynôme cyclotomique Φ_n est à coefficients entiers et il est irréductible sur $\mathbb{Q}$.*

Corollaire 2.5.6. *Le degré de l'extension $\mathbb{Q} \to \mathbb{Q}(\zeta)$ est l'indicateur d'Euler $\phi(n) = \text{card}((\mathbb{Z}/n\mathbb{Z})^\times) = \deg(\Phi_n)$.*

2.6 Corps finis

Soit $\mathbb{F}$ un corps fini de caractéristique p, et de cardinal q, alors $\mathbb{F}$ est une extension de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. On a $q = p^m$, où $m = [\mathbb{F} : \mathbb{F}_p]$.

Théorème 2.6.1. *Soit $q = p^m$, $m \geq 1$. Un corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^q - X$ est un corps fini à q éléments, et tout corps commutatif à q éléments lui est isomorphe.*

Remarques 2.6.2. 1. L'isomorphisme précédent n'est pas canonique.
2. L'hypothèse de commutativité n'est pas nécessaire : Tout corps fini est commutatif (théorème de Wedderburn).

28/09/2011

Exercice 2.6.3. a) Montrer que tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.
b) Montrer que toute extension entre corps finis est simple : il existe un élément primitif.

Exercice 2.6.4. a) Montrer que s'il existe une extension $F \to F'$ entre deux corps finis de caractéristique p, de cardinaux respectifs $q = p^d$ et $q' = p^n$, alors d divise n.
c) Soit $\mathbb{F}_q$ est un corps de caractéristique p à $q = p^n$ éléments. Montrer que si d divise n, alors $\mathbb{F}_q$ contient un unique sous-corps à p^d éléments.

Polynômes irréductibles sur $\mathbb{F}_p$

Proposition 2.6.5. *Tout polynôme irréductible de degré d à coefficients dans le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ divise $X^{p^d} - X$.*

Proposition 2.6.6. *Pour p premier et $d > 0$, soit $n_p(d)$ le nombre de polynômes irréductibles unitaires de degré d sur $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, alors :*

$$p^n = \sum_{d|n} d\, n_p(d) \ .$$

2.7 Corps algébriquement clôs, clôture algébrique

Définition 2.7.1. a) Un corps commutatif L est algébriquement clos si et seulement si tout polynôme à coefficients dans L a au moins une racine dans L.
b) Un clôture algébrique d'un corps commutatif K est une extension algébrique qui est algébriquement close.

Etant donné une extension $K \to L$, la fermeture algébrique de K dans L est l'ensemble $K_{\mathrm{alg},L}$ des éléments de L algébriques sur K. C'est un sous-corps de L.

Proposition 2.7.2. *Si L est algébriquement clos, alors la fermeture algébrique de K dans L est une clôture algébrique de K.*

Corollaire 2.7.3. *Le corps des nombres algébriques $\overline{\mathbb{Q}} = \mathbb{Q}_{\mathrm{alg},L}$ est une clôture algébrique de $\mathbb{Q}$.*

Clôture algébrique de $\mathbb{F}_p$

Pour p premier on pose $K_1 = \mathbb{F}_p$, et pour $n \geq 2$ on définit l'extension $K_{n-1} \to K_n$ comme corps de décomposition de $X^{p^{n!}} - X$; K_n est un corps à $p^{n!}$ éléments.

Proposition 2.7.4. *En identifiant K_{n-1} à son image dans K_n, la réunion $\overline{\mathbb{F}}_p = \cup_n K_n$ est une clôture algébrique de $\mathbb{F}_p$.*

Existence d'une clôture algébrique

Théorème 2.7.5. *Soient $f : K \to L$ une extension algébrique, et $g : K \to E$ une extension de K algébriquement close.*
a) Il existe une extension $h : L \to E$ qui prolonge f.
b) Si l'extension g est algébrique, alors h est un isomorphisme.

Théorème 2.7.6. *Tout corps commutatif K admet une clôture algébrique, et deux telles clôtures sont (non canoniquement) isomorphes (comme K-algèbre).*

Chapitre 3

Séparabilité

3.1 Polynômes et extensions séparables

Définition 3.1.1. a) Soit K un corps commutatif. Un polynôme irréductible $P \in K[X]$ est séparable sur K si et seulement s'il n'a pas de racine multiple dans son corps de décomposition.
b) Un polynôme $P \in K[X]$ est séparable sur K si et seulement si ses facteurs irréductibles sont séparables. Dans le cas contraire, on dit que P est inséparable.

Proposition 3.1.2. *a) Si K est de caractéristique nulle, un polynôme irréductible de $K[X]$ est toujours séparable.*
b) Si K est de caractéristique $p > 0$, un polynôme irréductible de $K[X]$ est inséparable si et seulement s'il appartient à $K[X^p]$.

Exercice 3.1.3. Soit K un corps de caractéristique non nulle p.

1. Montrer que si b n'a pas de racine p-ième dans K, alors $X^p - b$ est irréductible sur K.
2. Montrer que si b n'a pas de racine p-ième dans K, alors pour tout $k > 0$ $X^{p^k} - b$ est irréductible sur K.
3. Montrer que le polynôme $X^p - y$ est inséparable sur le corps de fractions rationnelles $K = \mathbb{F}_p(y)$.

Définition 3.1.4. Soit $f : K \to L$ une extension algébrique (tout élément de L est algébrique sur K).
a) Un élément $\alpha \in L$ est séparable si et seulement si son polynôme minimal est séparable.
b) L'extension est séparable si et seulement si tous les éléments de L sont séparables.

Proposition 3.1.5. *Soit $k \to K \to L$ une tour d'extensions. Si $k \to L$ est séparable, alors $k \to K$ et $K \to L$ sont séparables.*

30/09/2011

3.2 Corps parfaits

Définition 3.2.1. Un corps K est parfait si et seulement si toute extension algébrique est séparable.

Remarque 3.2.2. Tout corps de caractéristique zéro est parfait.

On rappelle que sur un corps K de caractéristique $p > 0$, l'application :

$$\begin{array}{ccc} K & \to & K \\ x & \mapsto & x^p \end{array}$$

est un homomorphisme, appelé homomorphisme de Frobenius. Comme homomorphisme de corps, il est toujours injectif. Pour un corps fini, cet homomorphisme est surjectif.

Théorème 3.2.3. *Un corps de caractéristique non nulle est parfait si et seulement si son homomorphisme de Frobenius est surjectif.*

Exercice 3.2.4. Soit K un corps de caractéristique non nulle p.

1. Montrer que si b n'a pas de racine p-ième dans K, alors $X^p - b$ est irréductible sur K.
2. Montrer que si b n'a pas de racine p-ième dans K, alors pour tout $k > 0$ $X^{p^k} - b$ est irréductible sur K.

3.3 Séparabilité et morphismes

Etant donné deux extensions $f : k \to K$ et $g : k \to L$, on s'intéresse au cardinal de l'ensemble $Hom_{k-\text{alg}}(K, L)$ des morphismes de k-algèbre de K dans L. On utilisera la notation plus précise $Hom_{(k,f)-\text{alg}}(K, L)$ en cas d'ambiguïté.

Proposition 3.3.1. *Soient $f : k \to K$ et $g : k \to L$ deux extensions de k. Si K est une extension simple : $K = k(\alpha)$, alors l'application $[h \mapsto h(\alpha)]$ définit une bijection entre $Hom_{k-\text{alg}}(K, L)$ et l'ensemble des racines du polynôme minimal P_α dans L.*
En particulier : $\sharp Hom_{k-\text{alg}}(K, L) \leq [K : k]$.

Théorème 3.3.2. *Soit $f : k \to K$ une extension de degré fini.*
a) Pour tout extension $g : k \to L$, $\sharp Hom_{k-\mathrm{alg}}(K, L) \leq [K : k]$.
b) Si l'extension $f : k \to K$ est séparable et si $g : k \to L$ est une extension algébriquement close, alors $\sharp Hom_k(K, L) = [K : k]$.
c) S'il existe une extension $g : k \to L$ telle que : $\sharp Hom_{k-\mathrm{alg}}(K, L) = [K : k]$, alors l'extension $f : k \to K$ est séparable.

Lemme 3.3.3 (Transitivité)**.** *Soient $f : k \to K$ et $g : K \to L$ des extensions de degré fini. Si f et g sont séparables, alors l'extension $g \circ f : k \to L$ est séparable.*

Exercice 3.3.4. Démontrer l'énoncé précédent sans l'hypothèse de degré fini.

Théorème 3.3.5. *Une extension de degré fini $k \to K$ est séparable si et seulement si elle est engendrée par des éléments séparables.*

3.4 Elément primitif

Théorème 3.4.1. *Toute extension $f : k \to K$ qui est séparable de degré fini est simple (i.e. admet un élément primitif).*

Exercice 3.4.2. Montrer que si le corps de base k est infini, un k-espace vectoriel E n'est pas réunion finie de sous-espaces propres.

05/10/2011

Chapitre 4

Théorie de Galois

Notation : une extension $f : K \to L$ sera notée simplement $(L{:}K)$ s'il n'y a pas d'ambiguïté ; en cas de besoin on pourra préciser : $(L : K, f)$.

4.1 Extensions normales

Définition 4.1.1. Une extension $(L : K)$ est normale si et seulement si tout polynôme irréductible de $K[X]$ qui admet une racine dans L est scindé dans L.

Théorème 4.1.2. *Soit $(L : K)$ une extension. Il y a équivalence entre :*
a) l'extension est normale et de degré fini ;
b) L est corps de décomposition d'un polynôme unitaire de $K[X]$.

Définition 4.1.3. Une clôture normale d'une extension de degré fini : $(L : K)$ est une extension normale minimale $L' : L)$:
a) l'extension $(L' : K)$ est normale, et
b) si on a une tour d'extension $(L' : E : L : K)$ telle que $(E : K)$ est normale, alors : $E = L'$.

Théorème 4.1.4. *Toute extension de degré fini admet une clôture normale, et deux telles clôtures sont isomorphes.*

4.2 Extension galoisienne

Définition 4.2.1. Une extension de corps est galoisienne si et seulement si elle est normale et séparable.

Nous allons étudier les extensions galoisiennes de degré fini via leurs automorphismes.

Définition 4.2.2. a) Un automorphisme du corps K est un homomorphisme bijectif de K dans lui-même.
b) Un automorphisme d'une extension $(L : K)$ est un automorphisme de L qui est un morphisme de K-algèbre.

Proposition 4.2.3. *Les automorphismes d'un corps K forment un groupe :* $\mathrm{Aut}(K)$. *Les automorphismes d'une extension $(L : K)$ forment un groupe :* $\mathrm{Gal}(L : K)$.

Définition 4.2.4. Le groupe $\mathrm{Gal}(L : K)$ est appelé groupe de Galois de l'extension $(L : K)$.

Remarque 4.2.5. Lorsque K est le sous-corps premier de L, $\mathrm{Gal}(L : K) = \mathrm{Aut}(L)$.

Théorème 4.2.6. *Soit $L : K$ une extension de degré fini, alors il y a équivalence entre :*
a) l'extension est galoisienne,
b) $|\mathrm{Gal}(L : K)| = [L : K]$,
c) L est corps de décomposition d'un polynôme séparable sur K.

Soit H un groupe fini d'automorphismes du corps L, alors l'ensemble L^H des éléments fixés par tous les éléments de H est un sous-corps de L : le corps fixe de H. Si le groupe H est contenu dans le groupe de Galois $\mathrm{Gal}(L : K)$, alors L^H est une extension de K.

Théorème 4.2.7. *Soit H un groupe fini d'automorphismes du corps L et L^H le corps fixe associé. Alors l'extension $(L : L^H)$ est galoisienne, de groupe de Galois H.*

Démonstration. Nous allons démontrer dans le lemme qui suit que le degré $n = [L : L^H]$ est fini et majoré par le cardinal m du groupe H. On a alors :

$$H \subset \mathrm{Gal}(L : L^H) = \mathrm{Hom}_{L^H-\mathrm{alg}}(L, L) \ .$$

Le nombre de L^H-morphismes est majoré par le degré : $m \leq n$. □

Lemme 4.2.8. *Sous les hypothèses du théorème précédent,*

$$n = [L : L^H] \leq m = |H| \ .$$

Démonstration. Notons $H = \{\sigma_1 = Id_L, \sigma_2, \ldots, \sigma_m\}$, et supposons que $m < n$. Fixons une partie libre de L sur L^H de cardinal $m+1 : x_1, \ldots, x_{m+1}$. La matrice formée par les $\sigma_i(x_j)$, $1 \leq i \leq m$, $1 \leq j \leq m+1$, a m lignes et $m+1$ colonnes : ses colonnes sont dépendantes. On renumérote éventuellement,

pour que les r premières colonnes forment une partie liée minimale (rang $r-1$). On a une relation de dépendance avec tous les coefficients $y_j \in L$ non nuls :

$$\forall i \ \sum_{j=1}^{r} \sigma_i(x_j) y_j = 0 \ .$$

On peut trouver une telle relation avec $y_1 = 1$, ce que nous supposons désormais.

$$\forall \tau \in H \ \forall i \ \sum_{j=1}^{r} \tau(\sigma_i(x_j) y_j) = 0 \ .$$

En posant $\tau\sigma_i = \sigma_k$:

$$\forall \tau \in H \ \forall k \ \sum_{j=1}^{r} \sigma_k(x_j) \tau(y_j) = 0 \ .$$

Pour chaque τ on obtient une nouvelle relation. En utilisant que le rang est égal à $r-1$, et que $\tau(y_1) = y_1 = 1$, on obtient pout tout j, $\tau(y_j) = y_j$. Chaque y_j est fixé par tous les élements de H : $y_j \in L^H$. Reprenons la relation de dépendance qui est maintenant à coefficients dans L^H :

$$\forall i \ \sum_{j=1}^{r} \sigma_i(x_j) y_j = 0 \ .$$

Avec $i = 1$, on obtient une relation de dépendance entre les x_j, ce qui donne une contradiction. On conclut : $[L : L^H] \leq m$. □

07/10/2011

Corollaire 4.2.9. *Une extension de degré fini $(L : K, f)$ est galoisienne si et seulement si $f(K) = L^{\mathrm{Gal}(L,K)}$.*

4.3 Correspondance de Galois

Théorème 4.3.1 (Galois)**.** *Soit $(L : K, f)$ une extension de degré fini galoisienne, alors :*
i) l' application : $H \mapsto L^H$, établit une bijection entre les sous-groupes H de $\mathrm{Gal}(L : K)$, et les corps E intermédiaires : $f(K) \subset E \subset L$; la bijection réciproque étant $E \mapsto \mathrm{Gal}(L : E)$.
ii) L'extension $(L^H : K)$ est galoisienne si et seulement si H est un sous-groupe distingué de $\mathrm{Gal}(L : K)$. Dans ce cas le groupe de Galois, $\mathrm{Gal}(E : K)$ est isomorphe au quotient : $\mathrm{Gal}(L : K)/H$.

La preuve du ii) dans le théorème de Galois utilise le lemme suivant :

Lemme 4.3.2. *Soient $(L : K)$ une extension galoisienne, et $E \subset L$ le sous-corps (*corps intermédiaire*) associé au sous-groupe $H \subset \mathrm{Gal}(L : K)$, alors pour tout $\sigma \in \mathrm{Gal}(L : K)$, on a $\mathrm{Gal}(L : \sigma(E)) = \sigma H \sigma^{-1}$, et la restriction définit un morphisme surjectif $N(H) \to \mathrm{Gal}(E, K)$ de noyau $\mathrm{Gal}(L : E)$. ($N(H)$ est le normalisateur de H, i.e ; le stabilisateur pour l'action de conjugaison sur les sous-groupes).*

Exercice 4.3.3. Etudier les extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ et $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, j)$ ($j = e^{i\frac{2\pi}{3}}$). Sont-elles galoisiennes ? Calculer le groupe de Galois. Déterminer les corps intermédiaires.

4.4 Un exemple élémentaire

Soit $L \subset \mathbb{C}$ le corps de décomposition (sur $\mathbb{Q}$) de $X^4 - 2$. C'est une extension galoisienne, comme corps de décomposition d'un polynôme séparable (en caractéristique zéro tout polynôme est séparable). Les racines de $X^4 - 2$ sont $\pm\sqrt[4]{2}$, $\pm i\sqrt[4]{2}$. Le polynôme $X^4 - 2$ étant irréductible sur $\mathbb{Q}$ (justifier), l'extension $(\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q})$ est de degré 4. L'extension $(L : \mathbb{Q}(\sqrt[4]{2}))$ est de degré 2 : elle est engendrée par i qui n'est pas dans $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$. On a donc : $[L : \mathbb{Q}] = 8$. Le groupe de Galois $G = \mathrm{Gal}(L : \mathbb{Q})$ est de cardinal 8. Pour $\rho \in G$, $\rho(i) = \pm i$ et $\rho(\sqrt[4]{2}) \in \{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$. L'application

$$\begin{array}{rccc} r : & G & \to & \{\pm i\} \times \{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\} \\ & \rho & \mapsto & (\rho(i), \rho(\sqrt[4]{2})) \end{array}$$

est injective, car i et $\sqrt[4]{2}$ engendrent l'extension. C'est une application entre ensembles finis de mêmes cardinaux : elle est bijective. Les éléments $\tau = r^{-1}(-i, \sqrt[4]{2})$, $\sigma = r^{-1}(i, i\sqrt[4]{2})$ engendrent le groupe G, avec les relations :

$$\tau^2 = \sigma^4 = id \ , \ \sigma\tau = \tau\sigma^{-1} \ .$$

On reconnaît le groupe diédral D_4 (groupe des isométries du carré). Il y a 5 éléments d'ordre 2 et un élément d'ordre 4 qui engendrent des sous-groupes cycliques, et il y a deux sous-groupes de cardinal 4 non cycliques. Voir les corps correspondants dans la figure 4.1. 12/10/2011

4.5 Corps cyclotomiques

Définition 4.5.1. On appelle corps cyclotomique une extension $(\mathbb{Q}(\zeta_n) : \mathbb{Q})$, où ζ_n est une racine primitive n-ième de l'unité.

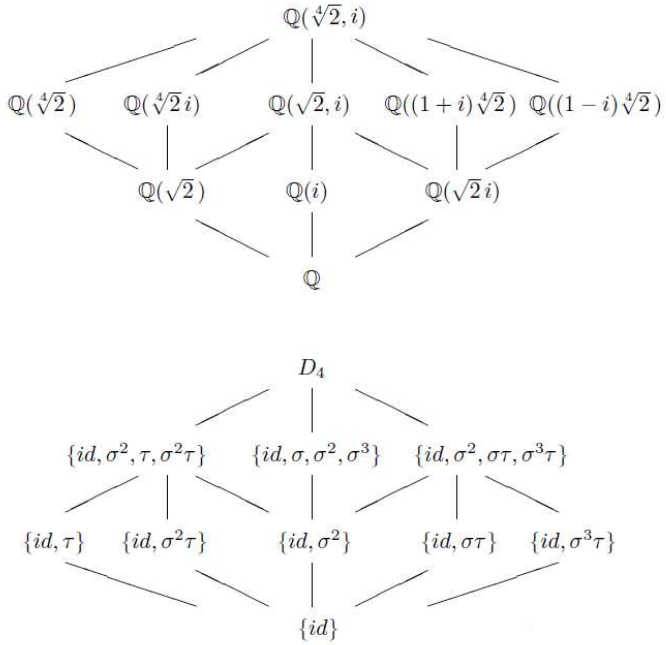


FIGURE 4.1 – Correspondance de Galois pour $X^4 - 2$

Proposition 4.5.2. *L'extension cyclotomique* $(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ *est galoisienne, de groupe de Galois isomorphe à* $(\mathbb{Z}/n\mathbb{Z})^\times$.

Démonstration. Le corps cyclotomique $\mathbb{Q}(\zeta_n)$ est le corps de décomposition sur $\mathbb{Q}$ du polynôme $X^n - 1$: c'est une extension galoisienne. Le polynôme minimal de ζ_n est le polynôme cyclotomique Φ_n dont les racines sont les ζ_n^k, $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. Notons $\tau_k \in \mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ l'automorphisme correspondant à ζ_n^k. On a : $\tau_k \tau'_k = \tau_{kk'}$. Les groupes $\mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ et $(\mathbb{Z}/n\mathbb{Z})^\times$ sont isomorphes. □

Remarque 4.5.3. La structure du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ découle du théorème chinois et des résultats suivants (voir par exemple le cours d'arithmétique de Bernhard Keller, section 19, `http://www.math.jussieu.fr/~keller/mt282/arith.pdf` :

1. Pour p premier impair et $\alpha > 0$, $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.
2. Pour $\alpha \geq 3$, $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est isomorphe au produit de $\mathbb{Z}/2$ par un groupe cyclique.

On peut en déduire les sous-groupes et donc les sous-corps de $\mathbb{Q}(\zeta_n)$.

Exercice 4.5.4. Etudier les sous-corps de $\mathbb{Q}(\zeta_{12})$.

4.6 Corps finis

Proposition 4.6.1. *Soit $\mathbb{F}_q$, $q = p^m$, un corps à q-éléments. L'extension $(\mathbb{F}_q : \mathbb{F}_p)$ est galoisienne. Le groupe de Galois est cyclique, engendré par l'automorphisme de Frobenius.*

Démonstration. Pour un corps fini, le morphisme de Frobenius $F : x \mapsto x^p$ est un automorphisme : $F \in \mathrm{Gal}(\mathbb{F}_q : \mathbb{F}_p)$. On va montrer qu'il est d'ordre $m = [\mathbb{F}_q : \mathbb{F}_p]$. Cela justifie que l'extension est galoisienne : $\mathrm{Gal}(\mathbb{F}_q : \mathbb{F}_p) = [\mathbb{F}_q : \mathbb{F}_p]$, et que F engendre le groupe de Galois.
Le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique de cardinal $q - 1$. Notons α un générateur : α engendre l'extension. On a $\frac{F^\nu(\alpha)}{\alpha} = \alpha^{p^\nu - 1}$, d'où :

$$F^m = Id \text{ et } F^\nu \neq Id \text{ pour } 0 < \nu < m \ .$$

□

Remarque 4.6.2. La correspondance de Galois redonne que les sous-corps de F_q sont en bijection avec les diviseurs de m.

4.7 Groupe de Galois d'un polynôme

Définition 4.7.1. Le groupe de Galois d'un polynôme est celui d'une extension qui réalise un corps de décomposition : pour $P \in K[X]$, $\mathrm{Gal}(P) = \mathrm{Gal}(L : K)$, où L est corps de décomposition de P.

Remarque 4.7.2. L'extension qui réalise un corps de décomposition d'un polynôme P est galoisienne si et seulement si le polynôme est séparable.

Proposition 4.7.3. *Le groupe de Galois de P agit sur les racines de P, et cette action est fidèle : on obtient un isomorphisme entre* $\mathrm{Gal}(P)$ *et un sous-groupe du groupe des permutations des racines de P.*

14/10/2011

Exercice 4.7.4. Soit G le groupe de Galois du polynôme, à coefficients rationnels, $P = X^4 - 2X^2 - 2$.

1. Montrer que P est irréductible.
2. Soient $\alpha_1 = \sqrt{1 + \sqrt{3}}$, $\alpha_2 = i\sqrt{-1 + \sqrt{3}}$ et $L = \mathbb{Q}(\alpha_1, \alpha_2)$. Montrer que l'extension $(L : \mathbb{Q})$ est galoisienne.
3. Pour $i \in \{1, 2\}$, soit $K_i = \mathbb{Q}(\alpha_i)$, $K = K_1 \cap K_2$.
   (a) Montrer que K_1 n'est pas égal à K_2.
   (b) Déterminer le degré $[K : \mathbb{Q}]$.

(c) Donner un élément primitif de l'extension $(K : \mathbb{Q})$.

4. (a) Montrer que l'extension $(L : K)$ est galoisienne.

   (b) Déterminer la structure du groupe de Galois $\mathrm{Gal}(L : K)$.

   (c) Déterminer les sous-corps de L qui contiennent K.

5. (a) Quel est le degré de l'extension $(L : \mathbb{Q})$.

   (b) Montrer que chaque élément dans $\mathrm{Gal}(P)$ induit une bijection de l'ensemble $\{\alpha_1, \alpha_2, \alpha_3 = -\alpha_1, \alpha_4 = -\alpha_2\}$.

   (c) Montrer qu'il existe des éléments de $\mathrm{Gal}(P)$ qui envoient α_1 sur α_4. Combien ?

   (d) Expliciter un isomorpghisme entre $\mathrm{Gal}(P)$ et un sous-groupe du groupe des permutations $\mathcal{S}_4$.

   (e) Quelle est la structure de $\mathrm{Gal}(P)$?

   (f) Combien L contient-il de sous-corps qui sont des extensions de $\mathbb{Q}$ de degré 4 ? Lesquelles sont galoisiennes sur $\mathbb{Q}$?

Chapitre 5

Compléments : groupes, polynômes

5.1 Produits semi-directs

Soient G' et G deux groupes notés multiplicativement, et $\gamma : G \to \mathrm{Aut}(G')$ un morphisme de groupe. L'image par γ de $x \in G$ est notée γ_x.
On définit sur le produit cartésien $G \times G'$ une opération :

$$(x', x)(y', y) = (x'\gamma_x(y'), xy) \ .$$

Proposition 5.1.1. *L'opération précédente définit une structure de groupe.*

Définition 5.1.2. On appelle produit semi-direct de G' et G au dessus de γ le groupe précédent. On le note $G' \times_\gamma G$.

Remarque 5.1.3. Lorsque γ est constante : $\forall x \in G, \gamma_x = Id_{G'}$, on retrouve le produit direct.

Exemple 5.1.4. Soient $G' =< a >$, $G =< b >$ des groupes cycliques d'ordres respectifs $n \geq 2$ et 2, et $\gamma : G \to \mathrm{Aut}(G')$ défini par $\gamma_b(a^k) = a^{-k}$.
Le produit semi-direct $G' \times_\gamma G$ est appelé *groupe diédral* à $2n$ éléments, et noté D_n. Il est engendré par $\alpha = (a, b^0)$ et $\beta = (a^0, b)$ qui satisfont les relations (ici $e = (a^0, b^0)$ est le neutre) : $\alpha^n = e = \beta^2$, $\beta\alpha = \alpha^{-1}\beta$. Notons que les éléments $\alpha^k\beta$ qui ne sont pas dans le groupe cyclique $< \alpha >$ sont d'ordre 2 et pour $n > 2$ engendrent un sous-groupe qui n'est pas distingué. 19/10/2011

Théorème 5.1.5 (Décomposition en produit semi-direct)**.** *Soient H et K des sous-groupes d'un groupe G noté mutiplicativement. Si H est un sous-groupe distingué et $H \cap K = \{e\}$, alors HK est un sous-groupe de G isomorphe au produit semi direct $H \times_\gamma K$, où $\gamma_k(h) = khk^{-1}$.*

Remarque 5.1.6. Dans le cas de groupes finis, le cardinal de HK est le produit des cardinaux de H et de K, il est facile de voir si HK est égal à G !

5.2 Groupes libres et présentations

Etant donné deux symboles a et b, on considère l'ensemble des mots (suites finies) en a, b, $\overline{a}$ et $\overline{b}$ (le mot vide est admis). Un mot est réduit si et seulement s'il ne contient aucune occurrence d'un symbole suivi de son *inverse* : $a\overline{a}$, $\overline{a}a$, $b\overline{b}$ ou $\overline{b}b$,
Le groupe libre à deux éléments $L(a,b)$ est l'ensemble des mots réduits en a, b, $\overline{a}$ et $\overline{b}$ (y compris le mot vide), muni de l'opération obtenue avec la concaténation suivie de la réduction : on itère l'enlèvement de l'occurence d'un symbole suivi de son inverse, tant qu'on en trouve.

Proposition 5.2.1. *a) $L(a,b)$ est un groupe.*
b) Pour tout groupe G, et tout $x \in G$, and $y \in G$, il existe un unique morphisme de groupe $\phi : L(a,b) \to G$ tel que $\phi(a) = x$, $\phi(b) = y$.

On défini de même plus généralement le groupe libre à n générateurs : $L(a_1, \ldots, a_n)$, voire le groupe libre $L(E)$ avec un ensemble quelconque de générateurs.
Etant donné un ensemble $R \subset L(E)$, on note :

$$\langle E; R \rangle \ ,$$

le quotient du groupe libre $L(E)$ par le sous-groupe normal engendré par R.

Définition 5.2.2. Une présentation d'un groupe G est un ensemble E de générateurs et un ensemble $R \subset L(E)$ qui engendre, comme sous-groupe normal, le noyau du morphisme $L(E) \to G$ qui étend l'inclusion des générateurs :

$$\langle E; R \rangle \simeq G \ .$$

5.3 Action de groupe

Définition 5.3.1. Une action d'un groupe G sur un ensemble X est un morphisme du groupe G dans les bijections de X, $\gamma : G \to \mathcal{B}(X)$.

On note habituellement $g.x$ pour $\gamma_g(x)$. On peut aussi définir une action comme l'opération externe : $(g,x) \mapsto g.x$, avec $e.x = x$ et $g.(g'.x) = (gg').x$ pour tout x,g, g'.

Exemple 5.3.2. Un sous-groupe H d'un groupe G opère sur G par translation à gauche.

5.3.1 Orbites et stabilisateur

Une action d'un groupe G sur un ensemble X définit une partition de G en orbites $Gx = \{g.x,\ g \in G\}$. Le stabilisateur d'un élément x est le sous-groupe $\mathrm{Stab}(x) = \{g,\ g.x = x\}$.
Dans le cas de l'action par translation à gauche de l'exemple précédent les orbites sont les classes à gauche Hx et le stabilisateur est trivial.

Lemme 5.3.3. *Etant donnée une action du groupe G sur X, le cardinal de l'orbite de $x \in X$ est égal à l'indice du stabilisateur $[G : \mathrm{Stab}(x)]$.*

Théorème 5.3.4 (Formule des classes)**.** *Etant donnée une action du groupe G sur un ensemble fini X, on a :*

$$\mathrm{card}(X) = \sum_{x \in R} \sharp Gx = \sum_{x \in R} [G : \mathrm{Stab}(x)] \ ,$$

où $R \subset X$ est un ensemble représentatif des classes.

Action de conjugaison

Un groupe G agit sur lui-même par conjugaison : $(g, h) \mapsto ghg^{-1}$. Le stabilisateur de h, noté C_h, s'appelle alors le centralisateur de h.
Un groupe G agit sur ses sous-groupes par conjugaison : $(g, H) \mapsto gHg^{-1}$. Le stabilisateur de H ; noté N_H s'appelle alors le normalisateur de H.

Proposition 5.3.5. *Dans un groupe G de cardinal p^α avec p premier, le centre est non trivial.*

24/10/2011

5.4 Groupes résolubles

Définition 5.4.1. Un groupe G est résoluble si et seulement s'il existe une suite :

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_m = G \ ,$$

avec, pour tout $i < m$, G_i sous-groupe distingué de G_{i+1}, et G_{i+1}/G_i abélien.

Théorème 5.4.2. *Tout groupe G de cardinal p^α avec p premier est résoluble.*

5.5 Théorèmes de Sylow

Définition 5.5.1. Dans un groupe G de cardinal mp^α, p premier qui ne divise pas m, on appelle p-sous-groupe de Sylow (ou simplement p-Sylow) tout sous-groupe de cardinal p^α.

Théorème 5.5.2. *Soit G un groupe de cardinal mp^α, p premier qui ne divise pas m, alors le nombre n_p de p-sous-groupes de Sylow est congru à 1 modulo p.*

Théorème 5.5.3. *Soit G un groupe de cardinal mp^α, p premier qui ne divise pas m, alors tous les p-sous-groupes de Sylow sont conjugués et leur nombre n_p divise m.*

5.6 Polynômes à n variables

Soit A un anneau commutatif et $X_1, \ldots, X_n$ des *indéterminées*. On note $A[X_1, \ldots, X_n]$ l'ensemble des familles d'éléments de A indexées par $\mathbb{N}^n$, avec un nombre fini de termes non nuls, notées comme combinaisons linéaires des $X_1^{k_1} \ldots X_n^{k_n}$, $k_j \geq 0$: les éléments de $A[X_1, \ldots, X_n]$ s'écrivent sous la forme :

$$P = \sum_{k_1,\ldots,k_n} a_{k_1,\ldots,k_n} X_1^{k_1} \ldots X_n^{k_n} = \sum_{\underline{k}} a_{\underline{k}} X_1^{k_1} \ldots X_n^{k_n} \ .$$

$A[X_1, \ldots, X_n]$ est muni des opérations :

$$(\sum_{\underline{k}} a_{\underline{k}} X_1^{k_1} \ldots X_n^{k_n}) + (\sum_{\underline{k}} b_{\underline{k}} X_1^{k_1} \ldots X_n^{k_n}) = \sum_{\underline{k}} (a_{\underline{k}} + b_{\underline{k}}) X_1^{k_1} \ldots X_n^{k_n}.$$

$$(\sum_{\underline{k}} a_{\underline{k}} X_1^{k_1} \ldots X_n^{k_n})(\sum_{\underline{l}} b_{\underline{l}} X_1^{l_1} \ldots X_n^{l_n}) = \sum_{\underline{\nu}} c_{\underline{\nu}} X_1^{\nu_1} \ldots X_n^{\nu_n} \ ,$$

$$\text{avec } c_{\underline{\nu}} = \sum_{\underline{k}+\underline{l}=\underline{\nu}} a_{\underline{k}} b_{\underline{l}} \ ,$$

et de l'application de structure :

$$\begin{array}{rccc} \eta : & A & \to & A[X_1, \ldots, X_n] \\ & a & \mapsto & aX^0 = a \end{array}$$

Proposition 5.6.1. *$A[X_1, \ldots, X_n]$ est une algèbre sur A.*

Remarque 5.6.2. L'application qui définit la structure d'algèbre est injective, d'image les polynômes constants ; A est identifié au sous-anneau de $A[X_1, \ldots, X_n]$ formé par les polynômes *constants*.

Proposition 5.6.3 (Propriété universelle)**.** *Soit B une algèbre sur l'anneau commutatif A, et $b_1, \ldots, b_n$ des éléments de B, alors il existe un unique morphisme d'algèbre $E_{(b_1,\ldots,b_n)} : A[X_1, \ldots, X_n] \to B$ qui envoie chaque X_i sur b_i.*

Proposition 5.6.4. *Les anneaux $A[X_1, \ldots, X_{n-1}, X_n]$ et $A[X_1, \ldots, X_{n-1}][X_n]$ sont isomorphes.*

Corollaire 5.6.5. *Si l'anneau A est factoriel, alors $A[X_1, \ldots, X_n]$ est factoriel.*

Définition 5.6.6. Le multidegré d'un monôme $a_{k_1,\ldots,k_n} X_1^{k_1} \ldots X_n^{k_n}$ est la suite des exposants $(k_1, \ldots, k_n)$; son degré total ou simplement son degré est la somme des exposants : $|\underline{k}| = \sum_i k_i$.
Le degré d'un polynôme non nul est le maximum des degrés (totaux) de ses monômes.

5.7 Polynômes symétriques

Le groupe symétrique $\mathcal{S}_n$ agit à gauche sur $A[X_1, \ldots, X_n]$ par permutation des variables : pour $\sigma \in \mathcal{S}_n$,

$$\sigma.P(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) \ .$$

Définition 5.7.1. Les polynômes invariants sous l'action du groupe symétrique forme un sous-anneau de $A[X_1, \ldots, X_n]$: le sous-anneau des polynômes symétriques, noté $A[X_1, \ldots, X_n]^{sym}$.

Polynômes symétriques élémentaires

Définition 5.7.2. Pour $1 \leq k \leq n$ le polynôme symétrique élémentaire $\sigma_k \in A[X_1, \ldots, X_n]^{sym}$ est le coefficient de degré $n - k$ du polynôme :

$$\prod_i (T + X_i) \in A[X_1, \ldots, X_n][T] \ .$$

Remarques 5.7.3. 1. On a : $\sigma_k = \sum_{i_1 < i_2 < \cdots < i_k} X_{i_1} \ldots X_{i_k}$.

2. Relations entre coefficients et racines :

$$\prod_{i=1}^{n} (X - \alpha_i) = X^n + \sum_{k=1}^{n} (-1)^k \sigma_k(a_1, \ldots, a_n) X^{n-k} \ .$$

Théorème 5.7.4. *Tout polynôme symétrique s'écrit de manière unique comme un polynôme dans les polynômes symétriques élémentaires : le morphisme d'algèbre de $A[Y_1, \ldots, Y_n]$ dans $A[X_1, \ldots, X_n]^{sym}$ qui envoit Y_k sur σ_k est un isorphisme d'algèbre.*

5.8 Résultant et discriminant

Définition 5.8.1. Soient K un corps, $P \in K[X]$ un polynôme unitaire et pour $Q \in K[X]$, ψ_Q la multiplication par Q modulo P :

$$\begin{array}{rccc} \psi_Q : & \mathbb{K}[X]/(P) & \to & \mathbb{K}[X]/(P) \\ & \overline{U} & \mapsto & \overline{UQ} \end{array}$$

On définit le résultant :

$$\mathrm{Res}(Q,P) = \det(\psi_Q) \ .$$

Théorème 5.8.2. *Le résultant* $\mathrm{Res}(Q,P)$ *est non nul si et seulement si* P *et* Q *sont premiers entres eux.*

Remarque 5.8.3. Le résultant ne change pas par extension du corps des coefficients.

Proposition 5.8.4. *a)* $\mathrm{Res}(Q_1Q_2,P) = \mathrm{Res}(Q_1,P)\mathrm{Res}(Q_2,P)$.
b) $\mathrm{Res}((Q,X-\alpha)^k) = Q(\alpha)^k$.
c) $\mathrm{Res}(Q,P_1P_2) = \mathrm{Res}(Q,P_1)\mathrm{Res}(Q,P_2)$.
d) Si P *est scindé :* $P = \prod_{i=1}^{n}(X-\alpha_i)$, *alors :*

$$\mathrm{Res}(Q,P) = \prod_{i=1}^{n} Q(\alpha_i).$$

Discriminant

Soit $P = a_0 + \cdots + a_{n-1}X^{n-1} + X^n$ un polynôme unitaire de degré n à coefficients dans un corps K.

Définition 5.8.5. Le discriminant de P est :

$$\mathrm{Disc}(P) = (-1)^{\frac{n(n-1)}{2}}\mathrm{Res}(P',P) \ .$$

Théorème 5.8.6. *Si le polynôme unitaire* P *est scindé :* $P = \prod_{i=1}^{n}(X-x_i)$, *alors :*

$$\mathrm{Disc}(P) = \prod_{i<j}(x_j-x_i)^2 \ .$$

Corollaire 5.8.7. *Le polynôme unitaire* P *a une racine double si et seulement si son discriminant est nul.*

Chapitre 6

Applications de la théorie de Galois

6.1 Groupe de Galois d'un polynôme générique

Soit K un corps. On appelle polynôme générique sur K le polynôme

$$P = X^n - y_1 X^{n-1} + \cdots + (-1)^n y_n \in K(y_1, \ldots, y_n)[X] \ ,$$

Théorème 6.1.1. *Le polynôme générique sur K est séparable et son groupe de Galois est isomorphe au groupe symétrique $\mathcal{S}_n$.*

Démonstration. On étudie l'extension $(K(X_1, \ldots, X_n) : K(X_1, \ldots, X_n)^{sym})$. Toute permutation des variables s'étend en un automorphisme du corps $K(X_1, \ldots, X_n)$ qui est l'identité sur $K(X_1, \ldots, X_n)^{sym}$. Les corps $K(y_1, \ldots, y_n)$ et $K(X_1, \ldots, X_n)^{sym}$ sont isomorphes. On obtient que $K(X_1, \ldots, X_n)$ est corps de décomposition du polynôme séparable P, et l'action $\mathrm{Gal}(P) \to \mathcal{B}(\{X_1, \ldots, X_n\}) \simeq \mathcal{S}_n$ est un isomorphisme. □

Remarque 6.1.2. Si on a une extension $(K : k)$, on obtient le même résultat pour un polynôme $P \in K[X]$ dont les coefficients sont *algébriquement indépendants* sur k.

6.2 Groupe de Galois d'un polynôme et discriminant

Le groupe des permutations des racines d'un polynôme P, isomorphe au groupe symétrique $\mathcal{S}_n$, contient le sous-groupe des permutations paires (iso-

morphe au groupe alterné $\mathcal{A}_n$).

Remarque 6.2.1. Le discriminant de $P \in K[X]$ est invariant sous l'action du groupe de Galois de P ; il appartient au corps K et plus précisément au corps engendré par les coefficients de P.

Proposition 6.2.2. *Le groupe de Galois d'un polynôme séparable $P \in K[X]$ est contenu dans le sous-groupe des permutations paires si et seulement si le discriminant de P est un carré dans K.*

Démonstration. Le discriminant de $P = \prod_{i=1}^{n}(X - x_i)$ est $D = d^2$, avec $d = \prod_{1 \leq i < j \leq n}(x_j - x_i)$. C'est un carré dans le corps K si et seulement si d est fixe par tous les élements du groupe de Galois. Pour une permutation σ des racines de P, $\sigma.d = \epsilon_\sigma d$, où ϵ_σ est la signature : le discriminant de P est un carré dans K si et seulement si tout élément du groupe de Galois induit une permutation paire. □

6.3 Théorème de d'Alembert-Gauss par la théorie de Galois

On se propose de démontrer que $\mathbb{C}$ est algébriquement clos. On obtient, sans utiliser le théorème de d'Alembert-Gauss les lemmes suivants (démontrer) :

Lemme 6.3.1. *Le corps $\mathbb{C}$ n'a pas d'extension de degré 2.*

Lemme 6.3.2. *Le corps $\mathbb{R}$ n'a pas d'extension non triviale de degré impair.*

Théorème 6.3.3 (d'Alembert-Gauss)**.** *Le corps $\mathbb{C}$ est algébriquement clos.*

Démonstration. Soit P un polynôme à coefficients complexes, et K son corps de décomposition : c'est une extension galoisienne de $\mathbb{C}$ et aussi de $\mathbb{R}$. On écrit le degré de l'extension $(K : \mathbb{C})$ sous la forme $[K : \mathbb{C}] = 2^\alpha m$, avec m impair. On a alors $[K : \mathbb{R}] = 2^{\alpha+1} m$. Par le théorème de Sylow, le groupe de Galois $\mathrm{Gal}(K : \mathbb{R})$ de cardinal $2^{\alpha+1}m$ a un sous-groupe $H \subset \mathrm{Gal}(K : \mathbb{R})$ de cardinal $2^{\alpha+1}$. Le corps fixe K^H est une extension de $\mathbb{R}$ de degré m impair : elle est triviale, $m = 1$. Il reste un groupe de Galois $G = \mathrm{Gal}(K : \mathbb{C})$ de cardinal 2^α. L'exercice ci-dessous montre que si G, de cardinal 2^α est non trivial, alors il a un sous-groupe d'indice 2. Le corps fixe pour ce sous-groupe ferait une extension de $\mathbb{C}$ de degré 2, ce qui est exclu par le lemme précédent. Finalement $K = \mathbb{C}$. □

Exercice 6.3.4. Montrer que tout groupe de cardinal p^α avec p premier et $\alpha > 0$ a un sous-groupe distingué d'indice p.

6.4 Résolubilité par radicaux

Définition 6.4.1. Une extension $(L : K)$ est cyclique (resp. abélienne) si et seulement si elle est galoisienne et son groupe de Galois est cyclique (resp. commutatif).

Proposition 6.4.2. *Soit K un corps, de caractéristique nulle ou première avec n, qui contient les racines n-ièmes de l'unité. Pour $a \in K$ l'extension $K(b)$ où b est racine n-ième de a (dans le corps de décomposition de $X^n - a$) est cyclique de degré d diviseur de n.*

Proposition 6.4.3. *Soit $(L : K)$ une extension cyclique de degré n sur un corps, de caractéristique nulle ou première avec n, qui contient les racines n-ièmes de l'unité, alors $L = K(b)$ avec b de polynôme minimal $X^n - a$.*

Définition 6.4.4. a) Une extension radicale d'un corps K est un corps obtenu par une suite d'extensions, chacune étant engendrée par une racine :

$$K = K_0 \subset K_1 \subset \dots K_m = L \ ,$$

avec $K_i = K_{i-1}(b_i)$, $b_i^{n_i} = a_i$, $a_i \in K_{i-1}$.
b) Un polynôme à coefficients dans un corps de caractéristique nulle est résoluble par radicaux si et seulement s'il existe une extension radicale qui contient toutes ses racines.

Théorème 6.4.5. *Un polynôme P à coefficients dans un corps de caractéristique nulle est résoluble par radicaux si et seulement si son groupe de Galois G est résoluble, c'est à dire qu'il existe une suite :*

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_m = G \ ,$$

avec, pour tout $i < m$, G_i sous-groupe distingué de G_{i+1}, et G_{i+1}/G_i abélien.

Démonstration. Soit P un polynôme à coefficients dans K.
Supposons que P est résoluble par radicaux : le corps de décomposition L de P sur K est contenu dans une extension K_m telle que :

$$K = K_0 \subset K_1 \subset \cdots \subset K_m \ ,$$

avec $K_i = K_{i-1}(b_i)$, $b_i^{n_i} = a_i \in K_{i-1}$. Pour $n = PPCM(n_1, \dots, n_m)$, notons $K' = K(\zeta_n)$ l'extension cyclotomique de K obtenu en adjoignant la racine n-ième de l'unité ζ_n et $K'_i = K_i(\zeta_n) = K'_{i-1}(b_i)$. L'extensions $(K' : K)$ est abélienne. Comme n_i divise n, K'_i contient les racines n_i-ièmes de l'unité, et les extensions $(K'_i : K'_{i-1})$ sont cycliques pour $1 \leq i \leq m$.

On obtient une tour d'extension galoisiennes :

$$K'_{-1} = K \subset K'_0 = K' \subset K'_1 \subset \cdots \subset K'_m \ .$$

La correspondance de Galois nous donne une suite de groupes :

$$G'_{-1} \supset G'_0 \supset \cdots \supset G'_m = \{id\} \ .$$

avec pour tout $0 \leq i \leq m$, G'_i distingué dans G'_{i-1} et G'_{i-1}/G'_i abélien. Le groupe $G'_{-1} = \mathrm{Gal}(K'_m, K)$ est donc résoluble. On a une tour d'extensions galoisiennes :

$$K \subset L \subset K'_m.$$

Le groupe de Galois $\mathrm{Gal}(L, K) = \mathrm{Gal}(K'_m, K)/\mathrm{Gal}(K'_m, L)$ est quotient d'un groupe résoluble. C'est un groupe résoluble.
Supposons que le groupe de Galois du polynôme P, $\mathrm{Gal}(P) = \mathrm{Gal}(L, K)$ est résoluble (L est corps de décomposition de P) :

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_m = G \ ,$$

avec, pour tout $i < m$, G_i sous-groupe distingué de G_{i+1}, et G_{i+1}/G_i cyclique (voir l'exercice 6.4.7). On considère les corps fixes $K_i = L^{G_{m-i}}$. On obtient une tour d'extensions :

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = L \ .$$

Les extensions $(L : K_i)$ sont galoisiennes, et $\mathrm{Gal}(L, K_i) = G_{m-i}$ est un sous-groupe distingué de $\mathrm{Gal}(L, K_{i-1}) = G_{m-i+1}$. Les extensions $(K_i : K_{i-1})$ sont donc galoisiennes de groupe de Galois cyclique G_{m-i+1}/G_{m-i}. Elles sont donc primitives : $K_i = K_{i-1}(x_i)$. On adjoint à chaque corps K_i une racine de l'unité ζ_n d'ordre $n = [L : K]$: $K'_i = K_i(\zeta_n) = K_i(\zeta_n, x_i) = K'_i(x_i)$. L'extension $(K_i : K_{i-1})$ est galoisienne, donc le groupe de Galois $\mathrm{Gal}(K_i, K_{i-1})$ est en bijection avec les racines du polynôme minimal de x_i sur K_{i-1}, qui sont toutes dans K_i. Le groupe de Galois $\mathrm{Gal}(K'_i, K'_{i-1})$ est isomorphe au sous-groupe de $\mathrm{Gal}(K_i, K_{i-1})$ correspondant aux racines du polynôme minimal de x_i sur K_{i-1} qui sont aussi racines du polynôme minimal de x_i sur K'_{i-1}. C'est un sous-groupe d'un groupe cyclique, donc un groupe cyclique. Le degré n_i de l'extension (K'_i, K'_{i-1}) divise n, donc les racines n_i-ièmes de l'unité sont dans K'_i. L'extension $(K'_i : K'_{i-1})$ est donc de la forme $K'_{i-1}(b_i)$, $b_i^{n_i}$. On obtient que L est inclus dans une extension radicale. □

Exercice 6.4.6. Montrer qu'un groupe fini G est résoluble si et seulement s'il existe une suite :

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_m = G \ ,$$

avec, pour tout $i < m$, G_i sous-groupe distingué de G_{i+1}, et G_{i+1}/G_i cyclique

Exercice 6.4.7. Montrer qu'un quotient d'un groupe résoluble est résoluble.

Théorème 6.4.8. *Pour $n \geq 5$, le polynôme générique de degré n n'est pas résoluble par radicaux.*

C'est une conséquence du fait que pour $n \geq 5$ le groupe alterné $\mathcal{A}_n$ est simple (pas de sous-groupe distingué autre que le trivial et lui-même).

Exercice 6.4.9. Décrire les classes de conjugaison dans $\mathcal{A}_5$, et déduire une preuve de la simplicité de $\mathcal{A}_5$.

6.5 Polynômes de petit degré

Chapitre 7

Introduction à la théorie des modules

7.1 Définitions de base

Soit A un anneau.

Définition 7.1.1. Un module (à gauche) sur A est un groupe abélien M muni d'une opération externe :

$$\begin{array}{rcl} A \times M & \to & M \\ (a, v) & \mapsto & a.v \end{array}$$

qui vérifie :

la double distributivité : $\forall (a,b) \in A^2 \ \forall v \in M \ (a+b).v = a.v + b.v$ et $\forall a \in A \ \forall (v,w) \in M^2 \ a.(v+w) = a.v + a.w$;

l'associativité mixte : $\forall (a,b) \in A^2 \ \forall v \in M \ a.(b.v) = (ab).v$;

l'action du neutre : $\forall v \in M \ 1.v = v$.

Un module sur un corps est un espace vectoriel.

Exemples 7.1.2.
1. Un anneau A est un module sur lui-même ; une algèbre sur A est aussi un module.
2. Un groupe abélien est un module sur $\mathbb{Z}$.

Définition 7.1.3. Un sous-module d'un A-module M est un sous-groupe abélien qui est stable pour l'opération externe.

Remarque 7.1.4. Les sous-modules de l'anneau A, vu comme module à gauche sur lui-même sont les idéaux à gauche.

L'intersection d'une famille de sous-modules est un sous-module, et on a donc une notion de sous-module engendré par une partie non vide $F \subset M$: le plus petit sous-module qui contient F.

Proposition 7.1.5. *Le sous-module engendré par $F \subset M$ est l'ensemble $\mathcal{C}(F)$ des combinaisons linéaires des éléments de F.*

Définition 7.1.6. La somme (interne) d'une famille de sous-modules de M est le sous-module engendré par la réunion. On la note : $\sum_{i \in I} M_i$.

Définition 7.1.7. Une application $f : M \to N$ entre les A-modules M et N est A-linéaire si et seulement si elle respecte les combinaisons linéaires :

$$\forall (a, b) \in A^2 \ \forall (v, w) \in M^2 \ f(a.v + b.w) = a.f(v) + b.f(w) \ .$$

Les applications A-linéaires de M vers N forment un module noté $\mathrm{Hom}_A(M, N)$. Les applications A-linéaires de M dans M (endomorphismes) forment une algèbre sur A, noté $\mathrm{End}_A(M)$. L'application réciproque d'un endomorphisme bijectif est linéaire : les endomorphismes bijectifs du A-module M forment un groupe noté $\mathrm{GL}_A(M)$.

Proposition 7.1.8. *Image et noyau d'une application linéaire sont des sous-modules.*

Changement d'anneau

Si B est une A-algèbre, tout B-module est aussi un A-module.

7.2 Module quotient

Proposition 7.2.1. *Soit N un sous-module d'un A-module M, alors l'opération externe induit sur le groupe abélien quotient M/N une structure de A-module.*

Proposition 7.2.2 (Factorisation d'un morphisme d'anneau)**.** *Soit $f : M \to M'$ une application linéaire, N un sous-module de M, $p : M \to M/N$ la projection* canonique. *L'application linéaire f factorise par le quotient M/N si et seulement si $N \subset \mathrm{Ker}(f)$. Le morphisme g a même image que f et est injectif si et seulement si $N = \mathrm{Ker}(f)$.*

Corollaire 7.2.3 (Premier théorème d'isomorphisme)**.** *Soit $f : M \to N$ une application linéaire, alors le quotient $M/\mathrm{Ker}(f)$ est isomorphe à l'image de f.*

Exercice 7.2.4 (Second théorème d'isomorphisme). Soient N et P deux sous-module de M. Démontrer que : $(N+P)/P$ est isomorphe à $N/N \cap P$.

Exercice 7.2.5 (Troisième théorème d'isomorphisme). Soient $P \subset N$ deux sous-modules de M. Démontrer que l'inclusion de N dans M induit une identification de N/P avec un sous-module de M/P, et que : M/N est isomorphe à $(M/P)/(N/P)$.

7.3 Modules libres et sommes directes

On note A^I la A-algèbre des applications de l'ensemble I dans A. On utilisera habituellement la notation $a = (a_i)_{i\in I}$ et le vocabulaire *famille*.
Les familles à support fini forment un sous-module noté $A^{(I)}$ (en fait un idéal de A^I) . Les élément de $A^{(I)}$ s'écrivent de manière unique comme combinaison linéaire des e_i qui prennent la valeur 1 en i et 0 ailleurs (base canonique).

Proposition 7.3.1 (Propriété universelle)**.** *Le A-module $A^{(I)}$ muni de la* base canonique $(e_i)_{i\in I}$ *vérifie la propriété universelle suivante : Pour tout A-module M, et toute famille $(b_i)_{i\in I}$ d'éléments de M, il existe une unique application linéaire $f : A^{(I)} \to M$ qui envoie chaque e_i sur b_i.*

Définition 7.3.2. Le A-module M est libre de base $(b_i)_{i\in I}$ si et seulement si l'application linéaire définie dans la proposition précédente est un isomorphisme.

Soit $(M_i)_{i\in I}$ une famille de module.

Définition 7.3.3. Le produit $\prod_{i\in I} M_i$ muni des opérations :

$$(x_i) + (y_i) = (x_i + y_i) \ , \ a.(x_i) = (a.x_i) \ ,$$

est un A-module.

Définition 7.3.4. La somme directe $\bigoplus_{i\in I} M_i$ est le sous-module du produit constitué des familles (x_i) qui n'ont qu'un nombre fini de termes non nuls (presque nulles).

7.4 Eléments de torsion

Définition 7.4.1. a) Un élément v d'un A-module M est de torsion si et seulement s'il existe $a \in A - \{0\}$ tel que $a.v = 0$.
b) Un module est de torsion si et seulement si tous ses éléments sont de torsion.

Exemples 7.4.2. 1. Dans un groupe abélien les éléments de torsion sont ceux d'ordre fini.
2. Le $\mathbb{Z}$-module $\mathbb{Q}/\mathbb{Z}$ est de torsion.

Proposition 7.4.3. *Soit M un module sur un anneau commutatif A. L'ensemble de ses éléments de torsion forme un sous-module (de torsion)* $\mathrm{Tors}(M)$.

Chapitre 8

Modules sur les anneaux principaux

8.1 Sous-modules d'un module libre

Théorème 8.1.1. *Tout sous-module d'un module libre sur un anneau principal est libre.*

8.2 Modules de type fini

Définition 8.2.1. Un module est de type fini si et seulement s'il admet une partie génératrice finie.

Définition 8.2.2. Le rang d'un A-module de type fini est le maximum des cardinaux des parties libres.

Théorème 8.2.3. *Soit A un anneau commutatif non nul et M un A-module qui admet une base finie de cardinal n, alors toutes les bases ont le même cardinal et celui-ci est égal au rang de M.*

Corollaire 8.2.4. *Un sous-module d'un module de type fini sur un anneau principal est de type fini.*

8.3 Forme normale de Smith

Un module M de type fini sur un anneau principal A est isomorphe au quotient d'un module libre L de rang fini par un sous-module N. Ce sous-module N est libre de type fini. Si $B = (b_1, \ldots, b_m)$ est une base de L et si $F = (f_1, \ldots, f_n)$ est une partie génératrice de N, on dit que la matrice

$P = ([f_j]_B)$ est une matrice de présentation de M : $M \approx A^m/\mathrm{Im}(P) = \mathrm{coker(P)}$.
On obtient un module isomorphe en multipliant, à gauche et à droite, la matrice de présentation par une matrice inversible. La forme normale de Smith étend la réduction de Gauss au cas d'un anneau principal.

Définition 8.3.1. Une matrice $D = (d_{ij})_{i \leq m, j \leq n}$ est de forme normale de Smith si et seulement si :
$d_{ij} = 0$ pour $i \neq j$, et
pour $i < \min(m, n)$, d_{ii} divise $d_{i+1,i+1}$.

Définition 8.3.2. Une matrice est dite élémentaire lorsqu'elle est obtenue par des opérations élémentaires sur les lignes ou colonnes de la matrice identité. Les opérations élémentaires sur une matrice sont les suivantes :

permuter deux lignes (resp. deux colonnes),
ajouter un multiple d'une ligne à une autre ligne (respectivement colonne),
multiplier une ligne ou une colonne par un scalaire inversible.

Théorème 8.3.3. *a) Pour toute matrice P à m lignes et n colonnes, à coefficients dans un anneau principal A, il existe des matrices inversibles U et V telle que $UPV = D$ est une matrice de forme normale.*
b) Dans le cas euclidien il existe des produits de matrices élémentaires U et V tels que $UPV = D$ est une matrice de forme normale de Smith.
c) Les coefficients de D sont déterminés à multiplication par un inversible près.

Corollaire 8.3.4. *Si A est un anneau euclidien, alors le groupe $GL_n(A)$ est engendré par les matrices élémentaires.*

8.4 Résultats de structure

Théorème 8.4.1. *Si un module de type fini sur un anneau principal est sans torsion, alors il est libre.*

Théorème 8.4.2. *Soit M un module de type fini sur un anneau principal, alors M contient un sous-module libre L tel que :*

$$\begin{array}{rcl} L \oplus \mathrm{Tors}(M) & \to & M \\ (x, y) & \mapsto & x + y \end{array}$$

est un isomorphisme. (On dit que M est somme directe interne de L et $\mathrm{Tors}(M)$.)

Remarque 8.4.3. L n'est pas unique comme sous-module de M, mais son rang est fixé : c'est celui de M.

Théorème 8.4.4. *Soit M un module de torsion de type fini sur un anneau principal, alors il existe une suite d'éléments de A croissante pour la divisibilité : $a_1|a_2 \dots |a_n \neq 0$, unique modulo produit par des inversibles, telle que M est isomorphe à :*

$$\bigoplus_{i=1}^{n} A/(a_i) \ .$$

Remarque 8.4.5. Les $\mathbb{Z}$-modules de torsion de type fini sont les groupes abéliens finis.

8.5 Modules primaires

Définition 8.5.1. a) Soient M un module sur un anneau principal A, et p un élément irréductible de A. Un élément v de M est p-primaire si et seulement s'il est annulé par une puissance de p :

$$\exists \alpha \in \mathbb{N} \ p^{\alpha}.v = 0 \ .$$

b) Les éléments p-primaires de M forment un sous-module : le sous-module M_p des éléments p-primaires.
c) Les sous-modules M_p non triviaux sont les composantes primaires de M.

Remarque 8.5.2. Lorsque p et q sont associés, les sous-modules M_p et M_q sont les mêmes.

Proposition 8.5.3. *a) Un module de torsion de type fini a un nombre fini de composantes primaires (non triviales).*
b) Un module de torsion de type fini est somme directe de ses composantes primaires.

Remarque 8.5.4. Deux modules de torsion de type fini sont isomorphes si et seulement si leurs composantes primaires sont isomorphes.

Structure des modules primaires

Théorème 8.5.5. *Soit A un anneau principal et M un A-module de type fini p-primaire. Il existe une unique suite croissante d'entiers : $0 < \alpha_1 \leq \alpha_2 \cdots \leq \alpha_n$ telle que M est isomorphe à :*

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

8.6 Invariants de similitude d'un endomorphisme

Soient E un $\mathbb{K}$-espace vectoriel de dimension finie, et f un endomorphisme de E. Une structure de $\mathbb{K}[X]$-module est définie sur E, avec l'opération externe :

$$\begin{array}{rcl} \mathbb{K}[X] \times E & \to & E \\ (P, v) & \mapsto & P.v = P(f)(v) \end{array}$$

Le $\mathbb{K}[X]$-module E est de torsion, et sa classe d'isomorphisme est caractérisée par ses facteurs invariants : une suite de polynômes unitaires, décroissante pour la division : $(P_1, \ldots, P_m)$. Le polynôme P_1 est le polynôme minimal.

Remarque 8.6.1. Une présentation de E comme $\mathbb{K}[X]$-module est $XI - U$ où U est une matrice de f.

La matrice compagne d'un polynôme unitaire

$$P = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n$$

est :

$$C(P) = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & -a_2 \\ 0 & 0 & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 & -a_{n-2} \\ 0 & 0 & \ldots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

Théorème 8.6.2. *L'endomorphisme f admet la suite de facteurs invariants $(P_1, \ldots, P_m)$ si et seulement s'il existe une base de E dans laquelle la matrice est diagonale par blocs, avec les matrices compagnes des P_i comme blocs diagonaux.*

Corollaire 8.6.3. *Deux endomorphismes d'un espace vectoriel de dimension finie sont conjugués si et seulement s'ils ont les mêmes facteurs invariants.*

Exercice 8.6.4. Dans le cas où le polynôme minimal est produit de facteurs de degré 1 (scindé), retrouver la forme de Jordan classique.

8.7 Classification des sous-modules d'un module libre

Théorème 8.7.1 (Base adaptée)**.** *Soient M un module libre de rang n sur un anneau principal A, et N un sous-module de rang m.*

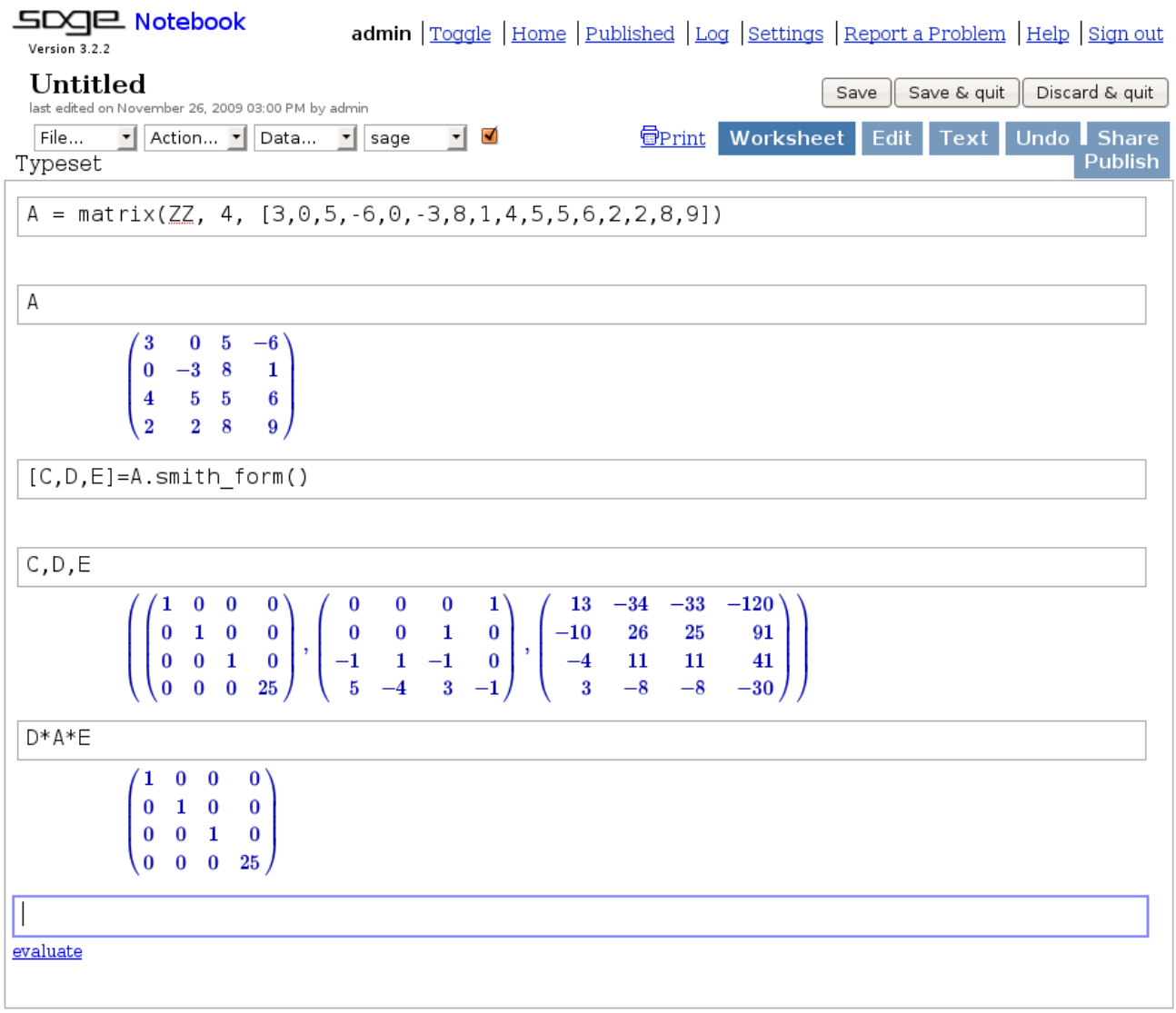
a) Il existe une suite $(a_1, \ldots, a_m)$ de A croissante pour la division, et une base $B = (b_1, \ldots, b_n)$ de M telles que : $(a_1 b_1, \ldots, a_m b_m)$ est une base de N.
b) La suite $(a_1, \ldots, a_m)$ est unique et caractérise la classe d'isomorphisme du sous-module N : deux sous-modules N et N' se correspondent par un isomorphisme de M si et seulement si leurs suites invariantes sont les mêmes.

8.8 Annexe : Modules de présentation finie

Définition 8.8.1. Soit A un anneau commutatif. Un A-module M est de présentation finie s'il est isomorphe au conoyau d'une application linéaire $P : A^n \to A^m$: $M \approx A^m/\mathrm{Im}(P)$. On dit que P est une (matrice de) présentation de M.

Remarque 8.8.2. Dans le cas noethérien tout module de type fini est de présentation finie.

Théorème 8.8.3. *Deux présentations d'un module de type fini sont reliées par une suite de transformations de l'un des types suivants :*
(i) Permutation des lignes ou des colonnes.
(ii) Transformation élémentaire sur les lignes : $L_i \leftarrow L_i + \alpha L_j$, ou sur les colonnes : $C_i \leftarrow C_i + \alpha C_j$.
(iii) Stabilisation $P \leftrightarrow \begin{pmatrix} P & 0 \\ 0 & 1 \end{pmatrix}$.
(iv) Ajout d'une ligne (resp. colonne nulle) ou l'inverse.


sage Notebook
Version 3.2.2
admin | Toggle | Home | Published | Log | Settings | Report a Problem | Help | Sign out
Untitled
last edited on November 26, 2009 03:00 PM by admin
Save
Save & quit
Discard & quit
File...
Action...
Data...
sage
Print
Worksheet
Edit
Text
Undo
Share
Publish
Typeset
A = matrix(ZZ, 4, [3,0,5,-6,0,-3,8,1,4,5,5,6,2,2,8,9])
A
[C,D,E]=A.smith_form()
C,D,E
D*A*E
evaluate