Algèbre 3

Semestre d'hiver 2012/2013

Université du Luxembourg

Gabor Wiese
gabor.wiese@uni.lu

Version du 19 décembre 2012

Préface

L'objet principal du cours sera l'étude des extensions algébriques des corps commutatifs. En particulier, la théorie de Galois sera développée et appliquée. Elle permet entre autres de démontrer que l'équation générale de degré au moins 5 ne peut pas être résolue en radicaux et de résoudre (parfois de manière négative) plusieurs problèmes classiques (provenant des anciens Grecs) de construction à la règle et au compas comme la trisection d'un angle et la quadrature du cercle.

Au début du cours nous allons finir le traitement de la réduction de Jordan d'une matrice commencé avant l'été.

Littérature

Voici quelques références sur la théorie de Galois en français :

- Jean-Pierre Escoffier : *Théorie de Galois*
- Jean-Claude Carrega : *Théorie des corps, la règle et le compas*
- Antoine Chambert-Loir : *Algèbre corporelle*
- Yvan Gozard : *Théorie de Galois*
- Patrice Tauvel : *Corps commutatifs et théorie de Galois*
- Josette Calais : *Extension de corps, théorie de Galois*
- Evariste Galois : le texte original !

Voici quelques d'autres références :

- Siegfried Bosch : *Algebra* (en allemand), Springer-Verlag. Ce livre est très complet et bien lisible.
- Ian Stewart : *Galois Theory*. Ce livre est bien lisible. Le traitement de la théorie de Galois dans le cours sera un peu plus général puisque Stewart se restreint dans les premiers chapîtres aux sous-corps des nombres complexes.
- Serge Lang : *Algebra* (en anglais), Springer-Verlag. C'est comme une encyclopédie de l'algèbre ; on y trouve beaucoup de sujets rassemblés, écrits de façon concise.

1 Réduction de Jordan

Nous commençons ce cours par la réduction de Jordan que nous avons bien préparée le semestre précédent, mais, pas encore finie. Rappelons d'abord les définitions et résultats principaux déjà mis en place avant l'été. Dans toute cette section, soit K un corps commutatif.

Le théorème suivant est souvent appellé *théorème fondamental sur les matrices*, ce qui montre son rôle fondamental : il dit que – après un choix de bases (pas oublier ! !) – chaque application linéaire peut être décrite de façon unique par une matrice, et que, réciproquement, chaque matrice – encore pour un choix de bases fixé – définit une application linéaire.

Un mot sur les notations : contrairement à l'usage au semestre précédent, je noterai les bases maintenant avec des parenthèses, $S = (v_1, \dots, v_n)$, et non avec des accolades car la forme des matrices dépend de l'ordre des vecteur. Mais, maintenant il faut se méfier de ne pas confondre S avec un vecteur (qui est aussi noté avec des parenthèses). Si nous avons deux sous-espace W_1 et W_2 d'un espace vectoriel V avec des bases $S_1 = (v_1, \dots, v_n)$ et $S_2 = (w_1, \dots, w_m)$, on notera $(v_1, \dots, v_n, w_1, \dots, w_m)$ quand-même par $S_1 \cup S_2$.

Théorème 1.1. *Soient V, W deux K-espaces vectoriels de dimensions finies n et m. Rappellons que nous notons $\mathrm{Hom}_K(V, W)$ l'ensemble de toutes les applications $\varphi : V \to W$ qui sont K-linéaires. Soient $S = (v_1, \dots, v_n)$ une K-base de V et $T = (w_1, \dots, w_m)$ une K-base de W. Pour $\varphi \in \mathrm{Hom}_K(V, W)$ et $1 \leq i \leq n$, le vecteur $\varphi(v_i)$ appartient à W, alors, on peut l'exprimer en tant que combinaison K-linéaire des vecteurs dans la base T ainsi :*

$$\varphi(v_i) = \sum_{j=1}^{m} a_{j,i} w_j.$$

Nous « rassemblons » les coefficients $a_{j,i}$ dans une matrice :

$$M_{T,S}(\varphi) := \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} \in \mathrm{Mat}_{m \times n}(K).$$

L'utilité de cette matrice est la suivante : Soit $v \in V$ un vecteur qui s'écrit en coordonnées pour la base S comme $v = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$. Alors, le produit matriciel

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

est égale au vecteur $\varphi(v)$ écrit en coordonnées pour la base T. C'est à dire que nous avons exprimé l'image $\varphi(v)$ en coordonnées. Alors, la matrice $M_{T,S}(\varphi)$ décrit l'application linéaire φ en coordonnées.

L'assertion principale du théorème c'est : L'application

$$\mathrm{Hom}_K(V,W) \to \mathrm{Mat}_{m\times n}(K), \quad \varphi \mapsto M_{T,S}(\varphi)$$

est une bijection. Elle est même un isomorphisme de K-algèbres.

Démonstration. La preuve n'est qu'un calcul assez simple et a été donnée avant l'été. Elle fait partie de celles que chaqu'un(e) devrait pouvoir reproduire. Alors, c'est le cas ? □

Dans le reste de cette section nous nous intéressons au cas spécial $W = V$. Une application K-linéaire $\varphi : V \to V$ est aussi appellée *endomorphisme* et nous écrivons

$$\mathrm{End}_K(V) := \mathrm{Hom}_K(V,V).$$

A partir d'ici, fixons un K-espace vectoriel V de dimension finie n.

Définition 1.2. *Soit $\varphi \in \mathrm{End}_K(V)$.*
- *$a \in K$ est appellé* valeur propre *de φ s'il existe $0 \neq v \in V$ t.q. $\varphi(v) = av$ (ou équivalent : $\ker(\varphi - a\cdot \mathrm{id}_V) \neq 0$).*
- *On pose $E_\varphi(a) := \ker(\varphi - a\cdot \mathrm{id}_V)$. Si a est une valeur propre de φ, on appelle $E_\varphi(a)$* l'espace propre pour a.
- *Chaque $0 \neq v \in E_\varphi(a)$ est appellé* vecteur propre pour la valeur propre a.
- *On pose $\mathrm{Spec}(\varphi) = \{a \in K \mid a$* est valeur propre de $\varphi\}$.
- *On appelle φ* diagonalisable *si $V = \bigoplus_{a\in\mathrm{Spec}(\varphi)} E_\varphi(a)$.*

Vous avez déjà vu beaucoup d'exemples, en algèbre linéaire et en algèbre 2 avant l'été. Rappellons quand-même une formulation équivalente de la diagonalisabilité (qui explique le nom).

Proposition 1.3. *Soit $\varphi \in \mathrm{End}_K(V)$ et $\mathrm{Spec}(\varphi) = \{a_1,\dots,a_r\}$. Les assertions suivantes sont équivalentes :*

(i) φ est diagonalisable.

(ii) Il existe une base S de V t.q.

$$M_{S,S}(\varphi) = \begin{pmatrix} a_1 & & & & & & & & & \\ & \ddots & & & & & & & & \\ & & a_1 & & & & & & & \\ & & & a_2 & & & & & & \\ & & & & \ddots & & & & & \\ & & & & & a_2 & & & & \\ & & & & & & \ddots & & & \\ & & & & & & & \ddots & & \\ & & & & & & & & a_r & \\ & & & & & & & & & \ddots \\ & & & & & & & & & & a_r \end{pmatrix}.$$

Pour $1 \le i \le r$, la valeur a_i apparaît $\dim_K E_\varphi(a_i)$ fois sur la diagonale.

Démonstration. « (i) $\Rightarrow$ (ii) » : Pour chaque $1 \leq i \leq r$ nous choisissons (par exemple, en la calculant) une base S_i de $E_\varphi(a_i)$ et posons $S = S_1 \cup S_2 \cup \cdots \cup S_r$. Puisque φ est diagonalisable, V est la somme directe des $E_\varphi(a_i)$; ceci ne dit rien d'autre que S est une base de V. La forme diagonale de la matrice provient immédiatement du théorème fondamental sur les matrices 1.1.

« (ii) $\Rightarrow$ (i) » : Ecrivons $S = (v_1, \ldots, v_n)$ et e_i pour le nombre de fois que a_i apparaît sur la diagonale. Alors, $E_\varphi(a_1)$ est le sous-espace de V engendré par les premiers e_1 vecteurs de S ; ensuite, $E_\varphi(a_2)$ est le sous-espace de V engendré par les prochains e_2 vecteurs de S, etc. Ceci montre que V est bien la somme directe des $E_\varphi(a_i)$ pour $1 \leq i \leq r$. □

Définition 1.4. – *Soit $M \in \mathrm{Mat}_{n\times n}(K)$ une matrice. Le* polynôme caractéristique de M *est défini comme*

$$\mathrm{car}_M(X) := \det\left(X \cdot \mathrm{id}_n - M\right) \in K[X].$$

– *Soit $\varphi \in \mathrm{End}_K(V)$. Le* polynôme caractéristique de φ *est défini comme*

$$\mathrm{car}_\phi(X) := \mathrm{car}_{M_{S,S}(\varphi)}(X).$$

Avant l'été nous nous sommes convaincues que car_φ ne dépend pas du choix de la base S. Nous avons aussi vu plusieurs exemples que nous n'allons pas répeter ici.

Proposition 1.5. $\mathrm{Spec}(\varphi) = \{a \in K \mid \mathrm{car}_\varphi(a) = 0\} = \{a \in K \mid \ (X-a) \mid \mathrm{car}_\varphi(X)\}$.

Démonstration. C'est facile, n'est-ce pas ? □

A part le polynôme caractéristique nous avons également introduit le polynôme minimal dont on rappelle aussi la définition. On se souvient qu'on a démontré que $K[X]$ est un anneau euclidien (pour la division euclidienne de polynômes, c'est à dire « avec reste »), alors, comme on l'a démontré également, $K[X]$ est un anneau principal : chaque idéal est principal, c'est à dire, peut être engendré par un seul élément. Nous allons utiliser ce fait maintenant.

Définition-Lemme 1.6. *(a) Soit $M \in \mathrm{Mat}_{n\times n}(K)$ une matrice. Si $f(X) = \sum_{i=0}^d a_i X^i \in K[X]$ est un polynôme, alors nous posons $f(M) := \sum_{i=0}^d a_i M^i$, ce qui est encore une matrice dans $Mat_{n\times n}(K)$.*

(b) L'application « evaluation »

$$\mathrm{ev}_M : K[X] \to \mathrm{Mat}_{n\times n}(K), \quad f(X) \mapsto f(M)$$

est un homomorphisme d'anneaux (même de K-algèbres).

(c) Le noyau $\ker(ev_M)$ est un idéal principal non-nul de l'anneau principal $K[X]$, alors, il existe un unique polynôme normalisé $m_M(X) \in K[X]$ qui engendre $\ker(ev_M)$. On appelle $m_M(X)$ le polynôme minimal de M.

(d) $m_M(X)$ est le polynôme normalisé de degré minimal qui annule M (c'est à dire : $m_M(M) = 0_n$ où 0_n est la matrice zéro dans $\mathrm{Mat}_{n\times n}(K)$ (qu'on denotéra aussi 0 pour simplicité)).

(e) Soit $\varphi \in \mathrm{End}_K(V)$. Nous posons

$$m_\varphi(X) := m_{M_{S,S}(\varphi)}(X)$$

et l'appellons polynôme minimal de φ. *Ce polynôme ne dépend pas du choix de la base S.*

Démonstration. (a) est clair.

(b) C'est un calcul facile.

(c) Remarquons que $K[X]$ est de dimension infinie alors que la dimension de $\mathrm{Mat}_{n\times n}(K)$ est finie, ce qui montre que ev_M ne peut pas être injective. Alors, son noyau est non-nul et engendré par un polynôme qui est unique à multiplication par $K^\times$ près, ce qui nous permet de le normaliser.

(d) est clair.

(e) L'indépendence du choix de la base provient du fait que la conjugaison avec la matrice de changement de base décrit un isomorphisme de $\mathrm{Mat}_{n\times n}(K)$. □

Le polynôme caracteristique $\mathrm{car}_M(X)$ et le polynôme minimal $m_M(X)$ sont liés par le théorème de Cayley-Hamilton.

Théorème 1.7 (Cayley-Hamilton)**.** *Soit $M \in \mathrm{Mat}_{n\times n}(K)$. Alors,*

$$\mathrm{car}_M(M) = 0_n \in \mathrm{Mat}_{n\times n}(K).$$

En particulier, $m_M(X)$ est un diviseur de $\mathrm{car}_M(X)$.

Démonstration. L'astuce est d'utiliser les matrices adjointes. Nous avons

$$(X\cdot \mathrm{id}_n - M)^{\mathrm{adj}} \cdot (X\cdot \mathrm{id}_n - M) = \det(X\cdot \mathrm{id}_n - M)\cdot \mathrm{id}_n \overset{\text{déf}}{=} \mathrm{car}_M(X)\cdot \mathrm{id}_n. \tag{1.1}$$

Notez que la matrice $X\cdot \mathrm{id}_n - M$ est à coefficients dans l'anneau des polynômes $K[X]$. Mais, il est facile de vérifier que la propriété principale des matrices adjointes que nous venons d'utiliser est valable pour chaque anneau commutative et pas seulement pour $\mathbb{R}$, le cas pour lequel vous avez vu la preuve en algèbre linéaire.

La définition de la matrice adjointe montre que la plus grande puissance de X qui peut apparaître dans un coefficient de la matrice $(X\cdot \mathrm{id}_n - M)^{\mathrm{adj}}$ est $n-1$. Nous pouvons alors écrire cette matrice en tant que polynôme de degré $n-1$ à coefficients dans $\mathrm{Mat}_{n\times n}(K)$:

$$(X\cdot \mathrm{id}_n - M)^{\mathrm{adj}} = \sum_{i=0}^{n-1} B_i X^i \quad \text{avec} \quad B_i \in \mathrm{Mat}_{n\times n}(K).$$

Nous écrivons $\mathrm{car}_M(X) = \sum_{i=0}^{n} a_i X^i$ et reprenons l'équation (1.1) :

$$\begin{aligned}\mathrm{car}_M(X)\cdot \mathrm{id}_n &= \sum_{i=0}^{n} a_i \cdot \mathrm{id}_n \cdot X^i = \big(\sum_{i=0}^{n-1} B_i X^i\big)(X\cdot \mathrm{id}_n - M)\\ &= \sum_{i=0}^{n-1}(B_i X^{i+1} - B_i M X^i) = -B_0 M + \sum_{i=1}^{n-1}(B_{i-1} - B_i M)X^i + B_{n-1}X^n.\end{aligned}$$

Nous comparons les coefficients (encore des matrices !) pour obtenir

$$a_0\cdot \mathrm{id}_n = -B_0 M, \quad a_i\cdot \mathrm{id}_n = B_{i-1} - B_i M \text{ pour } 1\le i\le n-1 \quad \text{et} \quad B_{n-1} = 0.$$

On peut maintenant conclure la preuve de $\mathrm{car}_M(M) = 0_n$ par un calcul simple :

$$\mathrm{car}_M(M) \cdot \mathrm{id}_n = \sum_{i=0}^{n} a_i \cdot M^i = -B_0 M + \sum_{i=1}^{n-1} (B_{i-1} - B_i M) M^i$$
$$= -B_0 M + B_0 M - B_1 M^2 + B_1 M^2 - B_2 M^3 + B_2 M^3 - \cdots - B_{n-2} M^{n-1} + B_{n-2} M^{n-1} = 0_n.$$

La propriété $\mathrm{car}_M(M) = 0_n$ montre que $\mathrm{car}_M(X)$ est dans le noyau de ev_M de 1.6, alors $m_M(X)$ divise $\mathrm{car}_M(X)$, car $m_M(X)$ est un générateur de l'idéal principal $\ker(\mathrm{ev}_M)$. □

Le théorème de Cayley-Hamilton reste évidemment vrai si l'on remplace la matrice M par un endomorphisme $\varphi \in \mathrm{End}_K(V)$.

Exemple 1.8. *Sur la feuille d'exercice no. 1 vous trouvez une façon de calculer les polynômes minimaux en général, et surtout une façon pour souvent éviter beaucoup de calcul. Le théorème 1.10 et la proposition 1.13 se montreront très utiles.*

Voici des exemples clés pour comprendre la différence entre polynôme minimal et polynôme caractéristique :

- *Les trois matrices suivantes ont le même polynôme caractéristique, $(X-1)^2$:*

$$M_1 := \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \quad M_2 := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \quad M_3 := \left(\begin{smallmatrix} 1 & 691 \\ 0 & 1 \end{smallmatrix}\right).$$

  Le polynôme minimal de M_1 est $X-1$. Puisque $M_2 - 1 \cdot \mathrm{id}_2 = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \neq 0_2$ et $M_3 - 1\mathrm{id}_2 = \left(\begin{smallmatrix} 0 & 691 \\ 0 & 0 \end{smallmatrix}\right) \neq 0_2$, le polynôme minimal est $(X-1)^2$ dans ces deux cas. Notez que nous avons utilisé le fait que les seuls diviseurs normalisés non-constants de $(X-1)^2$ sont $X-1$ et $(X-1)^2$, alors, le polynôme minimal doit être un parmi ces deux.
- *Les mêmes arguments donnent les polynômes minimaux des matrices suivantes (mais, notez qu'il y a une possibilité de plus) :*

$$M_4 := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, M_5 := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, M_6 := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Le lemme suivant est notre premier pas vers la décomposition spectrale et la forme de Jordan.

Lemme 1.9. *Soit $\varphi \in \mathrm{End}_K(V)$.*

(a) Soit $f \in K[X]$ et $W := \ker(f(\varphi))$. Alors, W est un sous-espace de V stable par φ, c'est à dire : pour tout $w \in W$ on a $\varphi(w) \in W$. Ceci nous permet de restreindre φ à W ; on notéra l'application restreinte par $\varphi|_W : W \to W$.

(b) Soient $f, g \in K[X]$ deux polynômes premiers entre eux, c'est à dire : $\mathrm{pgcd}(f(X), g(X)) = 1$. Alors,

$$\underbrace{\ker(f(\varphi) \cdot g(\varphi))}_{=:W} = \underbrace{\ker(f(\varphi))}_{=:W_1} \oplus \underbrace{\ker(g(\varphi))}_{=:W_2}.$$

Avant la preuve, un petit mot sur la notation : $f(\varphi)$ est une application K-linéaire $V \to V$, alors on peut l'appliquer à un vecteur $v \in V$. Notre notation pour ceci c'est : $f(\varphi)(v)$ ou bien $f(\varphi)v$. Notez les rôles distincts des deux paires de paranthèses dans la première expression. On pourrait aussi l'écrire $(f(\varphi))(v)$, mais, je trouve cette écriture un peu lourde.

Démonstration. (a) Nous savons que le noyau de chaque application K-linéaire est un sous-espace. Ecrivons $f(X) = \sum_{i=0}^{d} a_i X^i$. Soit alors $w \in W$, i.e. $f(\varphi)w = \sum_{i=0}^{d} a_i \varphi^i(w) = 0$. Nous calculons

$$f(\varphi)(\varphi(w)) = \sum_{i=0}^{d} a_i \varphi^i(\varphi(w)) = \sum_{i=0}^{d} a_i \varphi^{i+1}(w) = \varphi\big(\sum_{i=0}^{d} a_i \varphi^i(w)\big) = \varphi(0) = 0.$$

(b) Il est clair que $W_1 \subseteq W$ et $W_2 \subseteq W$, alors $W_1 + W_2 \subseteq W$. Nous devons démontrer
- $W_1 \cap W_2 = 0$ (le K-espace vectoriel zéro) et
- $W_1 + W_2 = W$.

Puisque $K[X]$ est un anneau euclidien, nous pouvons utiliser l'algorithme d'Euclide (de Bézout) pour obtenir deux autres polynômes $a, b \in K[X]$ tels que $1 = a(X)f(X) + b(X)g(X)$. Soit d'abord $w \in W_1 \cap W_2$. Alors

$$w = \mathrm{id}_V(w) = a(\varphi)f(\varphi)w + b(\varphi)g(\varphi)w = 0 + 0 = 0,$$

ce qui montre le premier point. Pour le deuxième soit $w \in W$. L'équation qu'on vient d'utiliser s'écrit comme

$$w = w_2 + w_1 \text{ avec } w_2 := a(\varphi)f(\varphi)w \text{ et } w_1 := b(\varphi)g(\varphi)w.$$

Mais, on a

$$f(\varphi)(w_1) = b(\varphi)f(\varphi)g(\varphi)w = b(\varphi)0 = 0 \Rightarrow w_1 \in W_1$$

et

$$g(\varphi)(w_2) = a(\varphi)f(\varphi)g(\varphi)w = a(\varphi)0 = 0 \Rightarrow w_2 \in W_2,$$

achevant la démonstration. □

Théorème 1.10 (Décomposition spectrale)**.** *Soit $\varphi \in \mathrm{End}_K(V)$ avec polynôme minimal $m_\varphi(X) = f_1^{e_1}(X) \cdot f_2^{e_2}(X) \cdot \ldots \cdot f_r^{e_r}(X)$ où les polynômes $f_i(X)$ sont irréductibles (ce sont alors des éléments premiers dans l'anneau principal $K[X]$) et premiers entre eux, c'est à dire $\mathrm{pgcd}(f_i, f_j) = 1$ pour tout $1 \leq i < j \leq n$ (si l'on normalise les f_i, alors la condition ne revient qu'à dire que les polynômes sont distincts). Posons $W_i := \ker(f_i(\varphi))$. Alors, les assertions suivantes sont vraies.*

(a) $V = \bigoplus_{i=1}^{r} W_i$.

(b) Si l'on choisit une base S_i du sous-espace W_i pour $1 \leq i \leq r$, alors $S = S_1 \cup S_2 \cup \cdots \cup S_r$ est une base de W pour laquelle on a :

$$M_{S,S}(\varphi) = \begin{pmatrix} \boxed{M_1} & \boxed{0} & \boxed{0} & \ldots & \boxed{0} \\ \boxed{0} & \boxed{M_2} & \boxed{0} & \ldots & \boxed{0} \\ \vdots & & \ddots & \ddots & \vdots \\ \boxed{0} & \ldots & \boxed{0} & \boxed{M_{r-1}} & \boxed{0} \\ \boxed{0} & \ldots & \boxed{0} & \boxed{0} & \boxed{M_r} \end{pmatrix}$$

avec $M_i := M_{S_i,S_i}(\varphi|_{W_i})$ pour $1 \leq i \leq r$.

Démonstration. (a) suit du lemma 1.9 (b) par récurrence.

(b) est clair : Ecrivez la matrice selon les règles et vous allez obtenir cette forme. Notez que les blocs en dehors de la diagonale sont zéros parce que $\varphi(W_i) \subseteq W_i$. □

Le cas le plus important pour nous est celui où $f_i(X) = X - a_i$ avec $a_i \neq a_j$ pour $i \neq j$ (ce qui implique que les f_i sont irréductibles et distincts). La décomposition spectrale n'est en fait qu'un pas (décisif !) vers la réduction de Jordan. Nous voyons dans la prochaine propostion aussi son utilité pour la diagonalisation. Pour l'instant nous illustrons l'effet de la décomposition spectrale à l'aide d'un exemple. Avant cela, il peut être utile de se rappeller comment appliquer les résultats pour les applications linéaire φ aux matrices.

Remarque 1.11. *Soit $M \in \mathrm{Mat}_{n\times n}(K)$. On peut appliquer la décomposition spectrale à la matrice M comme suit. Pour la base canonique $B := (\begin{pmatrix}1\\0\\0\\\vdots\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\\vdots\\0\\0\end{pmatrix}, \ldots, \begin{pmatrix}0\\0\\0\\\vdots\\0\\1\end{pmatrix})$ la matrice M décrit une application K-linéaire φ et l'on a $M = M_{B,B}(\varphi)$ (voir le théorème 1.1).*

La décomposition spectrale nous donne une base S. Soit $C := M_{B,S}(\mathrm{id})$ la matrice de changement de bases entre la base S et la base canonique. Alors, nous avons

$$M_{S,S}(\varphi) = C^{-1}MC$$

(comme nous l'avons vu avant l'été). Pour être encore un peu plus concret, rappellons comment écrire la matrice C. Si $S = (v_1, \ldots, v_n)$ et les vecteurs v_i sont donnés en coordonnées pour la base standarde, alors la i-ième colonne de C est juste le vecteur v_i.

Alors, la décomposition spectrale peut être utilisée pour calculer une matrice semblable (par définition, deux matrices A, B sont semblables *si l'une est une conjugée de l'autre : il existe une matrice inversible C telle que $B = C^{-1}AC$) à M de la jolie forme du théorème.*

Exemple 1.12. *Soit $M := \begin{pmatrix}1 & 2 & 3\\0 & 1 & 4\\0 & 0 & 5\end{pmatrix}$ à coefficients dans $\mathbb{Q}$. Le polynôme caractéristique est $(X-1)^2(X-5)$. Il est clair que $\ker(M - 5\cdot \mathrm{id}_3)$ est de dimension 1 ; c'est à dire que 5 est une valeur propre de multiplicité 1 (par définition : son espace propre est de dimension 1). Sans calcul il est clair que $\dim\ker((M-\mathrm{id}_3)^2) = 3 - 1 = 2$.*

Le théorème 1.10 implique l'existence d'une matrice C telle que

$$C^{-1}\cdot M \cdot C = \begin{pmatrix}1 & x & 0\\0 & 1 & 0\\0 & 0 & 5\end{pmatrix}$$

pour un $x \in \mathbb{Q}$ qui reste à être déterminé.

En fait, on voit facilement que $x \neq 0$, car dans ce cas le polynôme minimal serait $(X-1)(X-5)$ ce qui est faux (voir aussi la Proposition 1.13). Le théorème sur la réduction de Jordan 1.17 nous dira que nous pouvons choisir C telle que même $x = 1$.

Le polynôme minimal nous permet de donner encore une autre caractérisation de la diagonalisabilité :

Proposition 1.13. *(a)* $\mathrm{Spec}(\varphi) = \{a \in K \mid \ (X-a) \mid m_\varphi(X)\} = \{a \in K \mid m_\varphi(a) = 0\}$.

(b) Soit $\varphi \in \mathrm{End}_K(V)$. Alors, les assertions suivantes sont équivalentes :

(i) φ est diagonalisable.

(ii) $m_\varphi(X) = \prod_{a\in\mathrm{Spec}(\varphi)}(X-a)$.

Démonstration. (a) La deuxième égalité est claire : en utilisant la division euclidienne on voit qu'un $a \in K$ est un zéro d'un polynôme $f \in K[X]$ si et seulement si $X-a$ divise $f(X)$. Pour voir la première égalité supposons d'abord $(X-a) \nmid m_\varphi(X)$. De cela nous déduisons que $(X-a)$ et $m_\varphi(X)$ sont premiers entre eux, ce qui nous permet (par l'algorithme d'Euclide/Bézout) de trouver $b, c \in K[X]$ tels que $1 = b(X)(X-a) + c(X)m_\varphi(X)$. Soit maintenant $v \in V$ t.q. $\varphi(v) = av$. Nous avons

$$v = \mathrm{id}_V v = b(\varphi)(\varphi(v) - av) + c(\varphi)m_\varphi(\varphi)v = 0 + 0 = 0,$$

alors $a \notin \mathrm{Spec}(\varphi)$.

Supposons maintenant $(X-a) \mid m_\varphi(X)$ ce qui nous permet d'écrire $m_\varphi(X) = (X-a)g(X)$ pour un $g \in K[X]$. Puisque le degré de g est strictement plus petit que celui de $m_\varphi(X)$, il doit y avoir un $v \in V$ tel que $w := g(\varphi)v \neq 0$ (sinon, le polynôme minimal $m_\varphi(X)$ serait un diviseur de $g(X)$ ce qui est absurde). Nous avons alors

$$(\varphi - a)w = m_\varphi(\varphi)v = 0,$$

alors $a \in \mathrm{Spec}(\varphi)$.

(b) On écrit $\mathrm{Spec}(\varphi) = \{a_1, \ldots, a_r\}$.

« (i) $\Rightarrow$ (ii) » : On choisit une base S telle que $M := M_{S,S}(\varphi)$ est diagonale (voir la proposition 1.3). Un calcul très simple montre que $\prod_{i=1}^r (M - a_i) = 0_n$. Alors, $m_\varphi(X)$ est un diviseur de $\prod_{i=1}^r (X - a_i)$. Mais, (a) montre que pour chaque i on a $(X-a_i) \mid m_\varphi(X)$. Donc, $m_\varphi(X) = \prod_{i=1}^r (X-a_i)$ (les deux polynômes sont normalisés).

« (ii) $\Rightarrow$ (i) » : On applique la décomposition specrale 1.10 et il suffit de noter que les matrices M_i sont diagonales car $W_i = E_\varphi(a_i)$ est l'espace propre pour la valeur propre a_i. □

Il est utile de remarquer que les propositions 1.5 et 1.13 (a) disent que $\mathrm{car}_\varphi(X)$ et $m_\varphi(X)$ ont les mêmes facteurs de degré 1.

Exemple 1.14. *Considérons la matrice* $M := \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 4 \end{pmatrix}$ *à coefficients dans $\mathbb{Q}$. Son polynôme minimal est $(X-1)(X-4)$, alors, elle est diagonalisable.*

(Pour obtenir le polynôme minimal il suffit de voir que l'espace propre pour la valeur propre 1 est de dimension 2.)

Nous avons vu dans la proposition 1.3 que les matrices diagonalisables sont semblables à des matrices diagonales. L'utilité d'une matrice diagonale pour des calculs est évidente. Malheureusement, les matrices ne sont pas toutes diagonalisables. Notre but maintenant est de choisir une base S de V de façon que $M_{S,S}(\varphi)$ ait une forme « simple, jolie et élégante » et le plus proche possible de la forme diagonale.

Nous avons aussi vu que la décomposition spectrale 1.10 nous donne une forme diagonale « en blocs ». Notre but pour la réduction de Jordan sera de rendre les matrices dans les blocs le plus simple possible.

Nous présentons la *réduction de Jordan* (la *forme normale de Jordan*) d'un point de vue algorithmique. Les preuves peuvent être abrégées un peu si on travaille sans coordonnées, mais, dans ce cas, le calcul de la réduction n'est pas clair.

Lemme 1.15. *Soient $a \in K$, $e \in \mathbb{N}_{>0}$ et $v \in V$ tels que*

$$(\varphi - a \cdot \mathrm{id})^e(v) = 0 \quad \text{et} \quad (\varphi - a \cdot \mathrm{id})^{e-1}(v) \neq 0.$$

Nous posons :

$$\begin{aligned} v_e &:= v, \\ v_{e-1} &:= (\varphi - a \cdot \mathrm{id})(v), \\ &\dots \\ v_2 &:= (\varphi - a \cdot \mathrm{id})^{e-2}(v), \\ v_1 &:= (\varphi - a \cdot \mathrm{id})^{e-1}(v). \end{aligned}$$

et $\langle v \rangle_\varphi := \langle v_1, \dots, v_e \rangle$, le sous-espace de V engendré par les $v_1, \dots, v_e$.

(a) Les $v_1, \dots, v_e$ sont K-linéairement indépendants et, en conséquence, forment une base S de $\langle v \rangle_\varphi$.

(b) Nous avons :

$$\begin{aligned} \varphi(v_1) &= a v_1, \\ \varphi(v_2) &= v_1 + a v_2, \\ \varphi(v_3) &= v_2 + a v_3, \\ &\dots, \\ \varphi(v_e) &= v_{e-1} + a v_e. \end{aligned}$$

(c) $\varphi(\langle v \rangle_\varphi) \subseteq \langle v \rangle_\varphi$.

(d) $M_{S,S}(\varphi|_{\langle v \rangle_\varphi}) = \begin{pmatrix} a & 1 & 0 & 0 & \dots & 0 \\ 0 & a & 1 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 1 & 0 \\ 0 & 0 & \dots & 0 & a & 1 \\ 0 & 0 & \dots & 0 & 0 & a \end{pmatrix}$.

Démonstration. (a) Notez que la plus grande puissance de φ qui apparaît dans la définition d'un des v_i est égale à $e-1$. Une combinaison linéaire non-triviale de la forme $0 = \sum_{i=1}^{e} \alpha_i v_i$ se réécrit alors sous la forme $g(\varphi)(v) = 0$ avec un polynôme $0 \neq g(X) \in K[X]$ de degré au plus $e-1$. Comme le polynôme minimal de φ est de degré e, nous obtenons une contradiction.

(b) C'est un calcul très facile :

$$\begin{aligned}(\varphi - a\cdot\mathrm{id})v_1 = (\varphi - a\cdot\mathrm{id})^e v = 0 \qquad & \Rightarrow \varphi(v_1) = av_1.\\ (\varphi - a\cdot\mathrm{id})v_2 = v_1 \qquad & \Rightarrow \varphi(v_2) = v_1 + av_2.\\ \cdots & \\ (\varphi - a\cdot\mathrm{id})v_{e-1} = v_e \qquad & \Rightarrow \varphi(v_e) = v_{e-1} + av_e.\end{aligned}$$

(c) et (d) sont évidents à cause de (b). □

Nous voulons décomposer V en blocs de la forme du lemme précédent. Ceci se fait par le prochain lemme. Il est assez technique et un peu formel, mais, il fait précisement ce qui nous faut : Supposons que nous avons déjà trouvé des sous-espaces $W_1, \ldots, W_r \leq V$ tels que $W_1 \oplus \cdots \oplus W_r \lneq V$ et des bases S_i de W_i telles que les matrices $M_{S_i,S_i}(\varphi|_{W_i})$ soit de la forme « jolie » du lemme 1.15 (dans le prochain lemme on aura $W_i = \langle x_i\rangle_\varphi$). Le but du prochain lemme est de construire un sous-espace W_{r+1} (c'est $\langle\tilde{y}\rangle_\varphi$) tel que les mêmes propriétés restent vraies pour les $r+1$ sous-espaces. Ce processus pourra être continué pour nous mener à la réduction de Jordan. La construction de $\tilde{y}$ est très explicite et assez facile à vérifier, mais, un peu technique.

Lemme 1.16. *Soient $a \in K$, $e_i \in \mathbb{N}_{>0}$ et $x_1, \ldots, x_r \in V$ tels que pour tout $1 \leq i \leq r$*

$$(\varphi - a\cdot\mathrm{id})^{e_i}(x_i) = 0 \text{ et } (\varphi - a\cdot\mathrm{id})^{e_i-1}(x_i) \neq 0.$$

Nous savons par le lemme 1.15 que, pour tout $1 \leq i \leq r$, le sous-espace $\langle x_i\rangle_\varphi$ possède la base

$$S_i = (\varphi - a\cdot\mathrm{id})^{e_i-1}(x_i),\ \ (\varphi - a\cdot\mathrm{id})^{e_i-2}(x_i),\ \ \ldots, (\varphi - a\cdot\mathrm{id})(x_i),\ \ x_i.$$

Nous supposons en plus que $X := \sum_{i=1}^r \langle x_i\rangle_\varphi$ est égale à $\bigoplus_{i=1}^r \langle x_i\rangle_\varphi$. En conséquence, $S := S_1 \cup S_2 \cup \cdots \cup S_r$ est une K-base de X. Soit $y \in V \setminus X$ tel que $(\varphi - a\cdot\mathrm{id})^{e_i} y = 0$ pour tout $1 \leq i \leq r$.

(a) φ induit un endomorphisme de $\langle y\rangle_\varphi/(X \cap \langle y\rangle_\varphi)$. Son polynôme minimal est de la forme $(X-a)^k$ avec $k \leq e_i$ pour tout $1 \leq i \leq r$, et k est le plus petit entier positif tel que $(\varphi - a\cdot\mathrm{id})^k(y) \in X$.

(b) Soit k comme dans (a). En représentant $(\varphi - a\cdot\mathrm{id})^k(y)$ dans la base S, on obtient des uniques $\alpha_{i,j} \in K$ tels que

$$(\varphi - a\cdot\mathrm{id})^k(y) = \sum_{i=1}^{r}\sum_{j=k}^{e_i-1} \alpha_{i,j}(\varphi - a\cdot\mathrm{id})^j(x_i).$$

(c) Soient k comme dans (a) et $\alpha_{i,j}$ comme dans (b). On pose

$$\tilde{y} := y - \sum_{i=1}^{r}\sum_{j=k}^{e_i-1} \alpha_{i,j}(\varphi - a\cdot\mathrm{id})^{j-k}(x_i).$$

Alors,
- *$(\varphi - a\cdot\mathrm{id})^k(\tilde{y}) = 0$ et $(\varphi - a\cdot\mathrm{id})^{k-1}(\tilde{y}) \neq 0$,*
- *$\langle\tilde{y}\rangle_\varphi \cap X = 0$ et, en conséquence,*
- *$\langle x_1\rangle_\varphi \oplus \langle x_2\rangle_\varphi \oplus \cdots \oplus \langle x_r\rangle_\varphi \oplus \langle\tilde{y}\rangle_\varphi$ est un K-sous-espace de V.*

Démonstration. (a) Il est clair que φ induit un endomorphisme. Comme $(\varphi - a \cdot \mathrm{id})^{e_i}(y) = 0$, le polynôme minimal recherché doit être un diviseur de $(X-a)^{e_i}$, d'où l'assertion.

(b) En écrivant $(\varphi - a \cdot \mathrm{id})^k(y)$ dans la base S, on obtient

$$(\varphi - a \cdot \mathrm{id})^k(y) = \sum_{i=1}^{r} \sum_{j=1}^{e_i-1} \alpha_{i,j} (\varphi - a \cdot \mathrm{id})^j(x_i).$$

Il faut donc montrer $\alpha_{i,j} = 0$ pour tout $0 \leq j \leq k-1$. On agit des deux côtés par $(\varphi - a \cdot \mathrm{id})^{d-k}$ où d est le minimum des e_i et on obtient

$$0 = \sum_{i=1}^{r} \sum_{j=1}^{e_i-1-(d-k)} \alpha_{i,j} (\varphi - a \cdot \mathrm{id})^{d-k+j}(x_i).$$

Puisque tous les coefficients du vecteur zéro dans chaque base sont égaux à zéro, il en suit que $\alpha_{i,j} = 0$ si $j \leq e_i - 1 - (d-k) = k - 1 + (e_i - d)$. Puisque $d \leq e_i$, on a, en particulier, $\alpha_{i,j} = 0$ si $j \leq k-1$, comme requis.

(c) L'égalité de (b) se réécrit comme

$$(\varphi - a \cdot \mathrm{id})^k(y) = (\varphi - a \cdot \mathrm{id})^k \big(\sum_{i=1}^{r} \sum_{j=k}^{e_i-1} \alpha_{i,j} (\varphi - a \cdot \mathrm{id})^{j-k}(x_i) \big) = (\varphi - a \cdot \mathrm{id})^k (y - \tilde{y}),$$

d'où

$$(\varphi - a \cdot \mathrm{id})^k(\tilde{y}) = 0. \tag{1.2}$$

Soit $f(X) \in K[X]$ tel que $f(\varphi)(\tilde{y}) \in X$. Il en suit que $f(\varphi)(y) \in X$ car la différence $\tilde{y} - y$ est dans X. Par (a), $(X-a)^k$ divise $f(X)$. Alors, par l'équation (1.2) on a $f(\varphi)(\tilde{y}) = 0$, donc $\langle \tilde{y} \rangle_\varphi \cap X = 0$.

Pour finir, supposons que $(\varphi - a \cdot \mathrm{id})^{k-1}(\tilde{y}) = 0$. Par le même argument on en déduit que $(\varphi - a \cdot \mathrm{id})^{k-1}(y) \in X$ ce qui contredit le choix de k fait dans (a) ; alors, $(\varphi - a \cdot \mathrm{id})^{k-1}(\tilde{y}) \neq 0$. □

Théorème 1.17 (Réduction de Jordan)**.** *Supposons que le polynôme minimal de φ est égal à*

$$m_\varphi(X) = \prod_{i=1}^{r} (X - a_i)^{e_i}$$

avec différents $a_i \in K$ et $e_i > 0$ (ceci est toujours le cas lorsque K est algébriquement clos, par exemple $K = \mathbb{C}$).

En calculant $V_i := \ker\big((\varphi - a_i \cdot \mathrm{id})^{e_i}\big)$, on obtient la décomposition spectrale *(voir la proposition 7.5), c'est à dire :*

$$V = \bigoplus_{i=1}^{r} V_i \quad \text{et} \quad \varphi(V_i) \subseteq V_i \text{ pour tout } 1 \leq i \leq r.$$

Pour chaque $1 \leq i \leq r$, on peut construire (voir la preuve) des $x_{i,1}, \ldots, x_{i,s_i} \in V_i$ tels que

$$V_i = \langle x_{i,1} \rangle_\varphi \oplus \cdots \oplus \langle x_{i,s_i} \rangle_\varphi \quad \text{et} \quad \varphi(\langle x_{i,j} \rangle_\varphi) \subseteq \langle x_{i,j} \rangle_\varphi.$$

Soit $e_{i,j}$ l'entier positif minimal tel que $(\varphi - a_i \cdot \mathrm{id})^{e_{i,j}}(x_{i,j}) = 0$ pour tout $1 \leq i \leq r$ et $1 \leq j \leq s_i$.

Pour tout espace $\langle x_{i,j} \rangle_\varphi$ on chosit la base $S_{i,j}$ comme dans le lemme 1.15. On pose

$$S := S_{1,1} \cup S_{1,2} \cup \cdots \cup S_{1,s_1} \cup S_{2,1} \cup S_{2,2} \cup \cdots \cup S_{2,s_2} \cup \ldots\ldots\ldots \cup S_{r,s_r}.$$

Alors, S est une K-base de V telle que

$$M_{S,S}(\varphi) = \begin{pmatrix} \boxed{M_1} & \boxed{0} & \boxed{0} & \ldots & \boxed{0} \\ \boxed{0} & \boxed{M_2} & \boxed{0} & \ldots & \boxed{0} \\ \vdots & & \ddots & \ddots & \vdots \\ \boxed{0} & \ldots & \boxed{0} & \boxed{M_{r-1}} & \boxed{0} \\ \boxed{0} & \ldots & \boxed{0} & \boxed{0} & \boxed{M_r} \end{pmatrix}$$

(matrice diagonale de blocs), où, pour tout $1 \leq i \leq r$,

$$M_i = \begin{pmatrix} \boxed{N_{i,1}} & \boxed{0} & \boxed{0} & \ldots & \boxed{0} \\ \boxed{0} & \boxed{N_{i,2}} & \boxed{0} & \ldots & \boxed{0} \\ \vdots & & \ddots & \ddots & \vdots \\ \boxed{0} & \ldots & \boxed{0} & \boxed{N_{i,s_i-1}} & \boxed{0} \\ \boxed{0} & \ldots & \boxed{0} & \boxed{0} & \boxed{N_{i,s_i}} \end{pmatrix}$$

(matrice diagonale de blocs), où, pour tout $1 \leq j \leq s_i$,

$$N_{i,j} = \begin{pmatrix} a_i & 1 & 0 & 0 & \ldots & 0 \\ 0 & a_i & 1 & 0 & \ldots & 0 \\ 0 & 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 1 & 0 \\ 0 & 0 & \ldots & 0 & a_i & 1 \\ 0 & 0 & \ldots & 0 & 0 & a_i \end{pmatrix},$$

qui est d'ordre $e_{i,j}$. On appelle les $N_{i,j}$ les blocs de Jordan *(pour la valeur propre a_i).*

Démonstration. Il suffit de décrire la construction des $x_{i,j}$. Pour simplifier les notations, posons $W := V_i$, $a := a_i$, $e := e_i$ et $k_1 := e$.

- On choisit $x_1 \in \ker\left((\varphi - a \cdot \mathrm{id})^{k_1}\right) \setminus \ker\left((\varphi - a \cdot \mathrm{id})^{k_1-1}\right)$.
  Nous savons qu'un tel x_1 existe, car dans le cas contraire, la puissance de $X - a$ dans le polynôme minimal serait au plus $k_1 - 1 = e - 1$. Pour calculer un tel x_1, on peut calculer le noyau de $(\varphi - a \cdot \mathrm{id})^{k_1-1}$ et choisir un élément de V qui n'est pas dans ce noyau.
- Si $\langle x_1 \rangle_\varphi$ est déjà égal à W, on arrête.
  Sinon, on calcule le minimum k_2 tel que $(\varphi - a \cdot \mathrm{id})^{k_2}$ annule $W/\langle x_1 \rangle_\varphi$. Notez $k_1 \geq k_2$.
  On choisit $y \in W$ tel que $(\varphi - a \cdot \mathrm{id})^{k_2-1}(y) \notin \langle x_1 \rangle_\varphi$.
  Nous pouvons appliquer la formule du lemme 1.16 pour obtenir $\tilde{y}$.
  On pose $x_2 := \tilde{y}$ et on obtient $\langle x_1 \rangle_\varphi \oplus \langle x_2 \rangle_\varphi \leq W$ et $(\varphi - a \cdot \mathrm{id})^{k_2-1}(x_2) \neq 0$.

– Si $\langle x_1\rangle_\varphi \oplus \langle x_2\rangle_\varphi$ est déjà égal à W, on arrête.
Sinon, on calcule le minimum k_3 tel que $(\varphi - a\cdot\mathrm{id})^{k_3}$ annule $W/(\langle x_1\rangle_\varphi \oplus \langle x_2\rangle_\varphi)$. Notez $k_1 \geq k_2 \geq k_3$.
On choisit $y \in W$ tel que $(\varphi - a\cdot\mathrm{id})^{k_3-1}(y) \notin \langle x_1\rangle_\varphi \oplus \langle x_2\rangle_\varphi$.
Nous pouvons appliquer la formule du lemme 1.16 pour obtenir $\tilde{y}$.
On pose $x_3 := \tilde{y}$ et on obtient $\langle x_1\rangle_\varphi \oplus \langle x_2\rangle_\varphi \oplus \langle x_3\rangle_\varphi \leq W$ et $(\varphi - a\cdot\mathrm{id})^{k_3-1}(x_3) \neq 0$.
– On continue ainsi jusqu'à ce que $W = \langle x_1\rangle_\varphi \oplus \langle x_2\rangle_\varphi \oplus \cdots \oplus \langle x_s\rangle_\varphi$.

□

Remarque 1.18. *Explicitement, la base S est la suivante :*

$$\begin{array}{ccccc}
(\varphi - a_1\cdot\mathrm{id})^{e_{1,1}-1}(x_{1,1}), & (\varphi - a_1\cdot\mathrm{id})^{e_{1,1}-2}(x_{1,1}), & \dots & (\varphi - a_1\cdot\mathrm{id})(x_{1,1}), & x_{1,1},\\
(\varphi - a_1\cdot\mathrm{id})^{e_{1,2}-1}(x_{1,2}), & (\varphi - a_1\cdot\mathrm{id})^{e_{1,2}-2}(x_{1,2}), & \dots & (\varphi - a_1\cdot\mathrm{id})(x_{1,2}), & x_{1,2},\\
\vdots & \vdots & \vdots & \vdots & \vdots\\
(\varphi - a_1\cdot\mathrm{id})^{e_{1,s_1}-1}(x_{1,s_1}), & (\varphi - a_1\cdot\mathrm{id})^{e_{1,s_1}-2}(x_{1,s_1}), & \dots & (\varphi - a_1\cdot\mathrm{id})(x_{1,s_1}), & x_{1,s_1},\\
(\varphi - a_2\cdot\mathrm{id})^{e_{2,1}-1}(x_{2,1}), & (\varphi - a_2\cdot\mathrm{id})^{e_{2,1}-2}(x_{2,1}), & \dots & (\varphi - a_2\cdot\mathrm{id})(x_{2,1}), & x_{2,1},\\
(\varphi - a_2\cdot\mathrm{id})^{e_{2,2}-1}(x_{2,2}), & (\varphi - a_2\cdot\mathrm{id})^{e_{2,2}-2}(x_{2,2}), & \dots & (\varphi - a_2\cdot\mathrm{id})(x_{2,2}), & x_{2,2},\\
\vdots & \vdots & \vdots & \vdots & \vdots\\
(\varphi - a_2\cdot\mathrm{id})^{e_{2,s_2}-1}(x_{2,s_2}), & (\varphi - a_2\cdot\mathrm{id})^{e_{2,s_2}-2}(x_{2,s_2}), & \dots & (\varphi - a_2\cdot\mathrm{id})(x_{2,s_2}), & x_{2,s_2},\\
(\varphi - a_3\cdot\mathrm{id})^{e_{3,1}-1}(x_{3,1}), & (\varphi - a_3\cdot\mathrm{id})^{e_{3,1}-2}(x_{3,1}), & \dots & (\varphi - a_3\cdot\mathrm{id})(x_{3,1}), & x_{3,1},\\
\vdots & \vdots & \vdots & \vdots & \vdots\\
\vdots & \vdots & \vdots & \vdots & \vdots\\
(\varphi - a_r\cdot\mathrm{id})^{e_{r,s_r}-1}(x_{r,s_r}), & (\varphi - a_r\cdot\mathrm{id})^{e_{r,s_r}-2}(x_{r,s_r}), & \dots & (\varphi - a_r\cdot\mathrm{id})(x_{r,s_r}), & x_{r,s_r}
\end{array}.$$

Notez que la réduction de Jordan n'est pas unique en générale (on peut, par exemple, permuter les blocs). Alors, pour être précis on devrait parler plutôt d'une réduction de Jordan, ce que nous allons faire parfois. Si S est une base telle que $M_{S,S}(\varphi)$ ait la forme du théorème, on dira que $M_{S,S}(\varphi)$ est *la/une réduction de Jordan* ou bien qu'elle a *la/une forme de Jordan*.

Pour appliquer le théorème 1.17 aux matrices voyez (encore une fois) la remarque 1.11.

Exemple 1.19. *(a) Les matrices M_1, M_2, M_4, M_5, M_6 de l'exemple 1.8 ont déjà la forme de Jordan. La réduction de Jordan de M_3 est M_2.*

(b) La/une réduction de Jordan de la matrice de l'exmple 1.12 est $M := \begin{pmatrix} 1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 5 \end{pmatrix}$.

(c) Considérons la matrice $M := \begin{pmatrix} 1 & 1 & 0\\ -1 & 3 & 0\\ -1 & 1 & 2 \end{pmatrix}$ *à coefficients dans $\mathbb{Q}$.*

Un calcul montre que $\mathrm{car}_M(X) = (X-2)^3$. *Alors, $r = 1$ dans les notation du théorème 1.17 et, alors, la réduction de Jordan doit être parmi les trois matrices suivantes :*

$$\begin{pmatrix} 2 & 0 & 0\\ 0 & 2 & 0\\ 0 & 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 & 0\\ 0 & 2 & 0\\ 0 & 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 & 0\\ 0 & 2 & 1\\ 0 & 0 & 2 \end{pmatrix}.$$

On calcule facilement que $m_M(X) = (X-1)^2$*. De ce fait nous pouvons déjà déduire que la réduction de Jordan est* $\begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$.

La question devient plus désagréable si on nous démande de calculer une matrice C *telle que* $C^{-1}MC = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$*. Mais, cela n'est pas aussi difficile que ça. Nous suivons l'algorithme donné dans la preuve du théorème 1.17.*

- *On a* $M - 2\mathrm{id}_3 = \begin{pmatrix} -1 & 1 & 0 \\ -1 & 1 & 0 \\ -1 & 1 & 0 \end{pmatrix}$.
- *Alors,* $\ker(M - 2\mathrm{id}_3) = \langle \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \rangle$.
- *Nous savons que* $m_M(X) = (X-2)^2$ *(ce qu'on révérifie facilement :* $M^2 = 0_3$*). Selon l'algorithme, nous choisissons*

$$x_1 \in \ker((M - 2\mathrm{id}_3)^2) \setminus \ker(M - 2\mathrm{id}_3) = \mathbb{Q}^3 \setminus \langle \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \rangle,$$

  par exemple $x_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.
- *Nous commençons à écrire notre base* S*. Le premier vecteur le la base est, selon l'algorithme,*

$$v_1 := (M - 2\mathrm{id}_3)x_1 = \begin{pmatrix} -1 & 1 & 0 \\ -1 & 1 & 0 \\ -1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}$$

  et le deuxième est juste $v_2 := x_1$.
- *Comme* $\mathbb{Q}^3/\langle x_1 \rangle_\varphi = \mathbb{Q}^3/\langle v_1, v_2 \rangle$ *est de dimension* $3 - 2 = 1$*, alors nous recherchons maintenant un* $y \in \mathbb{Q}^3$ *tel que* $(M - 2\mathrm{id}_3)^0 y = y \notin \langle x_1 \rangle_\varphi = \langle v_1, v_2 \rangle$.

  Il est utile de choisir $y = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ *car c'est un vecteur propre. Comme ça nous n'avons pas besoin de faire l'ajuster (c'est à dire calculer* $\tilde{y}$*) et nous pouvons directement prendre* $v_3 = y$*. Dans le cas de dimension* 3 *on peut toujours éviter le calcul de* $\tilde{y}$*.*
- *Il suffit d'écrire les vecteurs* v_1, v_2, v_3 *dans les colonnes d'une matrice :*

$$C := \begin{pmatrix} -1 & 1 & 0 \\ -1 & 0 & 0 \\ -1 & 0 & 1 \end{pmatrix}.$$

Le théorème 1.17 nous dit que

$$C^{-1}MC = \begin{pmatrix} 0 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ -1 & 3 & 0 \\ -1 & 1 & 2 \end{pmatrix} \begin{pmatrix} -1 & 1 & 0 \\ -1 & 0 & 0 \\ -1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix},$$

ce qu'on peut vérifier pour se convaincre des calculs.

Remarque 1.20. *Dans les exemples et sur la feuille d'exercices no. 1 vous avez vu/voyez que la connaissance du polynôme minimal nous donne déjà beaucoup de renseignements sur la réduction de Jordan.*

Plus précisement : Si a est une valeur propre de φ et $(X-a)^e$ est la plus grande puissance de $X-a$ qui divise le polynôme minimal $m_\varphi(X)$, alors la taille du plus grand bloc de Jordan avec a sur la diagonale est e.

En général, on n'obtient pas toute la réduction de Jordan de cette manière ; si, par exemple, $(X-a)^{e+2}$ et la plus grande puissance de $X-a$ qui divise $\mathrm{car}_\varphi(X)$, alors, on a deux possibilités : (1) il y a deux blocs de Jordan pour la valeur propre a de taille e et 2 ; ou (2) il y a trois blocs de Jordan pour a de taille e, 1 et 1.

2 Théorème de Gauß et critère d'irréductibilité de polynômes

Le premier but de cette section est de montrer l'assertion suivante démontrée par Gauß : Si A est un anneau factoriel, alors l'anneau des polynômes $A[X]$ est aussi factoriel. Nous nous intéressons surtout au cas $A = \mathbb{Z}$, mais, nous allons donner la démonstration en général (car c'est la même).

Commençons par rappeler des notions sur les anneaux factoriels. Soit A un anneau intègre.

- Nous notons par $A^\times$ le groupe des éléments inversibles de A (avec la multiplication comme loi de groupe).
- On appelle $x \in A \setminus (A^\times \cup \{0\})$ *irréductible* s'il ne s'écrit pas comme produit $x = yz$ avec $y, z \notin A^\times$.
  Rappelons que les unités de $A[X]$ et celles de A sont les mêmes.
- On appelle $x \in A \setminus (A^\times \cup \{0\})$ *premier* si $x \mid yz$ avec $y, z \in A$ implique $x \mid y$ ou $x \mid z$. Rappelons aussi que x est premier si et seulement si l'idéal principal $(x) \lhd A$ est un idéal premier (ce qui équivaut à ce que l'anneau quotient $A/(x)$ soit un anneau intègre, par la proposition 5.1 du semestre dernier ; nous allons utiliser ce fait dans la démonstration de la proposition 2.7 plus bas).
- Deux éléments $a, b \in A$ sont appellés *associés* s'il existe $u \in A^\times$ tel que $ua = b$ (ce qui équivaut à l'égalité d'idéaux principaux $(a) = (b)$). Être associé est une relation d'équivalence. Nous avons vu que tout élément premier est irréductible ; nous avons aussi vu que l'assertion réciproque n'est pas valable en général.
- Nous avons défini les anneaux factoriels comme les anneaux intègres tels que (1) tout élément irréductible $x \in A \setminus (A^\times \cup \{0\})$ est premier, et (2) il n'y a pas de chaîne de diviseurs de longeur infinie.
- Un des résultats principaux du semestre dernier est le suivant :

$$A \text{ est un anneau euclidien } \Rightarrow A \text{ est un anneau principal } \Rightarrow A \text{ est un anneau factoriel.}$$

- Les principaux exemples que nous avons étudiés sont l'anneau des entiers $\mathbb{Z}$ et l'anneau des polynômes à coefficients rationnels $\mathbb{Q}[X]$.
- Les unités de $\mathbb{Z}$ ne sont que $\{1, -1\}$. Alors, $a, b \in \mathbb{Z}$ sont associés si et seulement si $a = b$ ou $a = -b$. Les éléments premiers de $\mathbb{Z}$ sont tous de la forme $\pm p$ où p est un « nombre premier habituel », c'est-à-dire $2, 3, 5, 7, 11, \ldots$ (par définition, $p \geq 2$ est divisible que par ± 1 et $\pm p$; en fait, on peut reformuler cette définition comme : positif et irréductible).
  Si on nous demande un ensemble $\mathbb{P}$ de représentants des éléments premiers à association près de $\mathbb{Z}$, nous pouvons juste prendre les nombres premiers habituels.
- Les unités de $\mathbb{Q}[X]$ sont les polynômes constants et non nuls. Alors, deux polynômes $f, g \in \mathbb{Q}[X]$ sont associés si et seulement s'il existe $u \in \mathbb{Q}^\times$ tel que $uf(x) = g(x)$. (Rappelons : $\mathbb{Q}^\times$ est le groupe des unités de $\mathbb{Q}$ pour la multiplication ; puisqu'on peut diviser par chaque élément de $\mathbb{Q}$ sauf 0, nous avons $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$).
  Les éléments premiers de $\mathbb{Q}[X]$ sont alors les polynômes irréductibles. Si on nous demande un ensemble $\mathbb{P}$ de représentants des éléments premiers à association près de $\mathbb{Q}[X]$, nous pouvons juste prendre les polynômes irréductibles et unitaires.
- Soit K un corps. Tout ce que nous avons dit sur $\mathbb{Q}[X]$ reste valable pour $K[X]$.
- L'anneau de polynômes $\mathbb{Z}[X]$ a une structure plus compliquée que $\mathbb{Q}[X]$ (ce qui peut étonner à première vue car c'est un sous-anneau). Par exemple, $\mathbb{Z}[X]$ a plus d'éléments premiers.
  Pour être plus concret, considérons le polynôme constant $2 \in \mathbb{Z}[X]$. C'est clairement un élément irréductible de $\mathbb{Z}[X]$ (essayez de l'écrire comme un produit de deux polynômes $2 = f(X)g(X)$ avec $f, g \in \mathbb{Z}[X]$; vous trouverez tout de suite $f(X) = \pm 1$ ou $g(X) = \pm 1$). Puisque nous n'avons pas encore démontré que $\mathbb{Z}[X]$ est un anneau factoriel nous ne savons pas encore que $2 \in \mathbb{Z}[X]$ est un élément premier. C'est un de nos buts. Voici, l'idée : si 2 divise $f(X)g(X)$, alors il faut qu'on montre que soit les coefficients de $f(X)$ ou de $g(X)$ sont pairs. Pour ceci, nous allons étudier la divisibilité des coefficients dans un produit de polynômes ; pour faire ainsi, nous allons introduire la valuation d'un polynôme et étudier comment elle se comporte dans des produits (voir la proposition 2.7).
  Mais, soulignons que 2 et 1 ne sont pas associés dans $\mathbb{Z}[X]$, car les unités de cet anneau sont $\{1, -1\}$ (mais, les deux éléments sont associés dans $\mathbb{Q}[X]$) ; alors, en particulier, l'idéal principal $2\mathbb{Z}[X] = \{2f(x) \mid f \in \mathbb{Z}[X]\}$, l'ensemble de tous les polynômes t.q. tous les coefficients sont pairs, est strictement inclus dans $\mathbb{Z}[X]$ (l'idéal $2\mathbb{Q}[X]$ de $\mathbb{Q}[X]$ est évidemment égal à $\mathbb{Q}[X]$, car on peut diviser par 2).
  Un autre type d'exemples d'éléments irréductibles dans $\mathbb{Z}[X]$ est le suivant : soit $f(X) \in \mathbb{Z}[X]$ un polynôme unitaire (plus bas, on va considérer la notion de « polynôme primitif » qui est un peu plus générale) qui est irréductible dans l'anneau $\mathbb{Q}[X]$. Nous allons voir qu'un tel polynôme est aussi un élément irréductible dans $\mathbb{Z}[X]$.
  Mais, notez qu'une condition comme « unitaire » ou « primitif » est nécessaire : le polynôme $2X + 2$ est irréductible dans $\mathbb{Q}[X]$, mais, il ne l'est pas dans $\mathbb{Z}[X]$: $2X + 2 = 2 \cdot (X + 1)$ (rappelons encore une fois que 2 n'est pas une unité de $\mathbb{Z}[X]$).

Voici le théorème fondamental sur les anneaux factoriels (théorème 4.8 du semestre dernier).

Théorème 2.1. *Soit A un anneau factoriel et soit $\mathbb{P}$ un ensemble de représentants des éléments premiers à association près.*

Alors, pour chaque $x \in A \setminus \{0\}$ il existe des uniques $r \in \mathbb{N}$, $u \in A^\times$ et des éléments premiers uniques (à l'ordre près) $p_1, \ldots, p_r$ tels que

$$x = u \cdot \prod_{i=1}^{r} p_i.$$

Définition 2.2. *Nous pouvons réécrire l'assertion du théorème 2.1 comme suit :*

Chaque $x \in A \setminus \{0\}$ s'écrit de façon unique comme produit

$$x = u \cdot \prod_{p \in \mathbb{P}} p^{v_p(x)}$$

avec $u \in A^\times$, $v_p(x) \in \mathbb{N}_{\geq 0}$ et $v_p(x) = 0$ pour tous les $p \in \mathbb{P}$ sauf un nombre fini.

On pose $v_p(0) = \infty$.

*On appelle la fonction $v_p : A \to \mathbb{N} \cup \{\infty\}$ la p-*valuation *(ce qui explique le choix de la lettre v).*

Voici un exemple concret : Dans $A = \mathbb{Z}$ nous écrivons le nombre 84 comme $84 = 2^2 \cdot 3 \cdot 7$, c'est-à-dire $v_2(84) = 2$, $v_3(84) = 1$, $v_7(84) = 1$ et $v_p(84) = 0$ pour tout nombre premier $p \notin \{2, 3, 7\}$.

Rappelons maintenant le corps des fractions. C'est en fait très facile. Le corps des fractions de $\mathbb{Z}$ n'est autre que $\mathbb{Q}$. On ne reproduit pas ici la construction (mais, allez voir la proposition 5.7 du semestre dernier) ; on note seulement que les éléments de $K := \mathrm{Frac}(A)$ s'écrivent comme $\frac{x}{y}$ avec $y \in A \setminus \{0\}$.

Nous allons maintenant étendre la définition 2.2 au corps des fractions $K := \mathrm{Frac}\, A$.

Définition-Lemme 2.3. *Chaque $z \in K \setminus \{0\}$ s'écrit de façon unique comme produit*

$$z = u \cdot \prod_{p \in \mathbb{P}} p^{v_p(z)}$$

avec $u \in A^\times$, $v_p(z) \in \mathbb{Z}$ et $v_p(z) \neq 0$ seulement pour un nombre fini de $p \in \mathbb{P}$.

Illustrons d'abord la définition par un exemple concret :

$$\frac{-84}{30} = \frac{-2^2 \cdot 3^1 \cdot 7^1}{2^1 \cdot 3^1 \cdot 5^1} = -1 \cdot 2^1 \cdot 5^{-1} \cdot 7^1.$$

Notez que la fraction choisie s'écrit aussi comme $\frac{-14}{5}$ et comme $\frac{-14000}{5000}$, mais, on trouvera toujours la formule ci-dessus (c'est l'indépendance mentionnée à la fin de la preuve suivante).

Démonstration. On a $z = \frac{x}{y}$ et on utilise $x = u_1 \cdot \prod_{p \in \mathbb{P}} p^{v_p(x)}$ et $y = u_2 \cdot \prod_{p \in \mathbb{P}} p^{v_p(y)}$, dont on conclut

$$z = \frac{x}{y} = \frac{u_1}{u_2} \cdot \prod_{p \in \mathbb{P}} \frac{p^{v_p(x)}}{p^{v_p(y)}} = \frac{u_1}{u_2} \cdot \prod_{p \in \mathbb{P}} p^{v_p(x) - v_p(y)}$$

en utilisant les règles pour calculer avec les exposants. On pose évidemment $v_p(z) := v_p(x) - v_p(y)$.

Notez qu'il faut encore vérifier que la définition ne dépend pas du choix de x et y. On vous laisse ceci comme exercice. □

Lemme 2.4. *(a) Pour tous $x, y \in K$ on a $v_p(xy) = v_p(x) + v_p(y)$. Pour que cette égalité ait un sens si $x = 0$ ou $y = 0$ nous admettons les égalités $a + \infty = \infty$ et $\infty + \infty = \infty$.*

(b) On a : $x \in A \Leftrightarrow v_p(x) \geq 0 \; \forall \, p \in \mathbb{P}$.

(c) Soit $x \in A$. *On a :* $v_p(x) = 0$ *pour tout* $p \in \mathbb{P} \Leftrightarrow x \in A^\times$.

Démonstration. Exercice. □

Après ces préliminaires, nous considérons maintenant le cas des polynômes et définissons une valuation pour les polynômes.

Définition 2.5. *Soit* $f(x) = a_r X^r + a_{r-1} X^{r-1} + \cdots + a_1 X + a_0 \in K[X]$. *Pour* $p \in \mathbb{P}$ *on pose*

$$v_p(f) := \min_{i=0,\ldots,r} v_p(a_i)$$

et on l'appelle la p-valuation de f.

Le polynôme f *est appellé* primitif *si* $v_p(f) = 0$ *pour tout* $p \in \mathbb{P}$.

Voici, des exemples concrets : $f(X) = X^2 + 2X + 4 \in \mathbb{Z}[X]$ est primitif. Ainsi, tous les polynômes $f(X) \in A[X]$ unitaires sont primitifs. Le polynôme $f(X) = 10X^2 + 2X + 4 \in \mathbb{Z}[X]$ satisfait à $v_2(f) = 1$ et $v_p(f) = 0$ pour tout $2 \neq p \in \mathbb{P}$.

Lemme 2.6. *Soit* $0 \neq f \in K[X]$. *Alors :*

(a) On a que $v_p(f) \neq 0$ *seulement pour un nombre fini de* $p \in \mathbb{P}$.

(b) $v_p(f) \geq 0 \; \forall \, p \in \mathbb{P} \Leftrightarrow f \in A[X]$.

(c) Si $0 \neq f(X) = \sum_{i=0}^{r} a_i X^i \in A[X]$, *alors* $v_p(f) = v_p(\mathrm{pgcd}(a_0, a_1, \ldots, a_r))$.

(d) Il existe $a \in K \setminus \{0\}$ *tel que* $af \in A[X]$ *est un polynôme primitif.*

(e) Pour tout $a \in K \setminus \{0\}$ *on a* $v_p(af) = v_p(a) + v_p(f)$.

Démonstration. Exercice. □

Proposition 2.7 (Lemme de Gauß)**.** *Soient* $p \in \mathbb{P}$ *et* $f, g \in K[X]$. *Alors, on a*

$$v_p(fg) = v_p(f) + v_p(g).$$

Démonstration. (1) Nous commençons par le cas spécial $f, g \in A[X]$ et $v_p(f) = 0$ et $v_p(g) = 0$ (et nous allons réduire l'étude générale à ce cas). L'argument est abstrait, mais, très simple :

Considérons l'homomorphisme d'anneaux « réduction mod p » :

$$\pi : A[X] \to A/(p)[X], \quad \sum_{i=0}^{r} a_i X^i \mapsto \sum_{i=0}^{r} \overline{a_i} X^i,$$

où $\overline{a_i}$ est la classe de a_i dans $A/(p)$. C'est-à-dire que nous réduisons les coefficients des polynômes modulo p. (Par exemple, si $A = \mathbb{Z}$ et $p = 2$, alors, le polynôme $X^3 + 7X^2 + 4X + 9$ est envoyé sur $X^3 + X^2 + 1 \in \mathbb{F}_2[X]$.)

Les conditions $f \in A[X]$ et $v_p(f) = 0$ impliquent que $\pi(f) \neq 0 \in A/(p)[X]$ puisqu'il doit y avoir un coefficient de f qui ne se réduit pas en $\overline{0}$. Nous avons la même conclusion pour g, c'est-à-dire $\pi(g) \neq 0$.

Maintenant, utilisons le fait que p est un élément premier. Alors, (p) est un idéal premier de A, et en conséquence, $A/(p)$ est un anneau intègre. Alors, $0 \neq \pi(f)\pi(g)$.

Puisque π est un homomorphisme d'anneaux nous trouvons $0 \neq \pi(fg)$. Ceci implique que le polynôme $f(X)g(X)$ doit avoir un coefficient avec p-valuation 0, alors, on a démontré $v_p(fg) = 0$. On réécrit cette égalité comme la tautologie $v_p(fg) = 0 = 0 + 0 = v_p(f) + v_p(g)$.

(2) Supposons maintenant seulement $f, g \in A[X]$. Nous allons réduire au cas $v_p(f) = 0 = v_p(g)$.

C'est facile car nous avons le lemme 2.6 (c). Soit d_f le pgcd des coefficients de f et d_g le pgcd des coefficients de g. Nous pouvons diviser f par d_f et g par d_g pour obtenir des polynômes $\tilde{f}$ et $\tilde{g}$ qui satisfont $v_p(\tilde{f}) = 0 = v_p(\tilde{g})$. On a

$$\begin{aligned} v_p(f) + v_p(g) = v_p(d_f\tilde{f}) + v_p(d_g\tilde{g}) &= v_p(d_f) + v_p(d_g) + v_p(\tilde{f}) + v_p(\tilde{g}) \\ &\overset{(1)}{=} v_p(d_f) + v_p(d_g) + v_p(\tilde{f}\tilde{g}) = v_p(d_f d_g \tilde{f}\tilde{g}) = v_p(fg). \end{aligned}$$

(3) On finit la preuve maintenant pour $f, g \in K[X]$ en réduisant au cas (2). On choisit $a, b \in A \setminus \{0\}$ tels que $af, bg \in A[X]$ et on obtient :

$$\begin{aligned} v_p(f) + v_p(g) &= v_p(af) + v_p(bg) - v_p(a) - v_p(b) \\ &\overset{(2)}{=} v_p(afbg) - v_p(a) - v_p(b) = v_p(fg) + v_p(a) + v_p(b) - v_p(a) - v_p(b) = v_p(fg). \end{aligned}$$

□

Corollaire 2.8. *Soit $f, g \in K[X]$ unitaires. Si $fg \in A[X]$, alors $f, g \in A[X]$.*

Démonstration. Puisque f, g sont unitaires, alors, fg l'est aussi. Soit $p \in \mathbb{P}$. En conséquence, on a

$$0 = v_p(fg) \overset{\text{Prop. 2.7}}{=} v_p(f) + v_p(g).$$

Le fait que f, g sont unitaires implique aussi $v_p(f), v_p(g) \leq 0$; donc, $v_p(f) = v_p(g) = 0$ pour tout $p \in \mathbb{P}$. Alors $f, g \in A[X]$. □

En mots, le corollaire dit que si le produit de deux polynômes unitaires n'a pas de dénominateur, alors, chacun des deux polynômes n'a pas de dénominateur. Ceci n'est pas si évident que ça !

Nous pouvons maintenant démontrer le théorème principal de cette section.

Théorème 2.9 (Gauß)**.** *(a) Soit A un anneau factoriel et K son corps de fractions. Soit $f \in A[X]$. Les deux assertions suivantes sont équivalentes :*

(i) f est premier dans $A[X]$.

(ii) f est d'une des deux formes suivantes :

(I) $f \in A$ (polynôme constant) et f est premier dans A.

(II) f est primitif et f est premier dans $K[X]$.

(b) Si A est un anneau factoriel, alors l'anneau des polynômes $A[X]$ est aussi un anneau factoriel.

Démonstration. (a) « $\Leftarrow$ » : Nous montrons d'abord que tout f de type (I) est en effet un élément premier de $A[X]$. Alors, maintenant f est un élément premier de A. Nous utilisons l'application π « réduction mod f » de la preuve de la proposition 2.7 qui est clairement surjective. Alors le théorème d'isomorphisme implique que $A[X]/\ker(\pi)$ est isomorphe à l'anneau intègre $A/(f)[X]$, donc $\ker(\pi)$ est un idéal premier de $A[X]$. Un polynôme $g \in A[X]$ est dans le noyau de π si et seulement si tous ses coefficients sont divisibles par f. C'est-à-dire, $\ker(\pi) = (f) = f \cdot A[X] \lhd A[X]$. Donc, f est un élément premier de $A[X]$.

Montrons maintenant que tout f de type (II) est aussi un élément premier de $A[X]$. Soit, $f \in A[X]$ primitif et élément premier de $K[X]$. On va vérifier la définition ; soient $g, h \in A[X]$ tels que $f \mid gh$. Lisons cette divisibilité dans $K[X]$; ceci implique que $f \mid g$ ou $f \mid h$ dans $K[X]$; disons, $f \mid g$ sans perte de généralité. On écrit cette divisibilité comme $g = fk$ avec $k \in K[X]$. On utilise la proposition 2.7 : $0 \leq v_p(g) = v_p(f) + v_p(k) = v_p(k)$ (puisque f est primitif : $v_p(f) = 0$), donc $k \in A[X]$, alors la divisibilité $f \mid gh$ est vraie dans $A[X]$. En conséquence, f est premier dans $A[X]$.

« $\Rightarrow$ » : Nous démontrons d'abord : Tout $f \in A[X]$ est un produit fini d'éléments premiers de type (I) ou (II).

Choisissons $a \in K \setminus \{0\}$ tel que $g := \frac{1}{a} f \in A[X]$ est primitif. On a $0 \leq v_p(a) = v_p(f)$, donc $a \in A \setminus \{0\}$. Puisque A est un anneau factoriel, nous écrivons $a = \prod_{i=1}^{r} p_i$ avec $p_1, \ldots, p_r$ des éléments premiers de A, c'est-à-dire, des éléments premiers de $A[X]$ de type (I). Puisque $K[X]$ est un anneau factoriel, nous pouvons écrire $g = \prod_{i=1}^{s} h_i$ avec $h_1, \ldots, h_r \in K[X]$ des polynômes irréductibles. Soit $a_i \in K^\times$ t.q. $\tilde{h}_i := a_i h_i \in A[X]$ est primitif pour tout $1 \leq i \leq s$. Notez que les $\tilde{h}_i$ sont des éléments premiers de $A[X]$ de type (II). Posons $u = a_1 \cdot \ldots \cdot a_s \in K^\times$. Encore par la proposition 2.7 on a : $0 = v_p(g) = -v_p(u)$. Donc, $u \in A^\times$ et on obtient l'assertion désirée :

$$f = ag = u \cdot a_1 \cdot \ldots \cdot a_r \cdot \tilde{h}_1 \cdot \ldots \cdot \tilde{h}_s.$$

Soit $f \in A[X]$ un élément irréductible. Par ce que nous venons de voir, f s'écrit comme un produit fini d'éléments premiers de type (I) ou (II). L'irréductibilité de f implique que ce produit n'a qu'un seul facteur qui est soit de type (I), soit de type (II). Puisque tout élément premier est irréductible, ceci achève la démonstration de (a).

(b) Nous avons vu dans le paragraphe précédent que tout élément irreductible est premier. Nous avons aussi démontré que tout $f \in A[X]$ s'écrit comme produit fini d'éléments premiers : $f = \prod_{i=1}^{r} f_i$. Si $g \in A[X]$ divise f, alors $f = f_1 \cdot \ldots \cdot f_r = gh$ pour un $h \in A[X]$. Tout f_i divise soit g, soit h (par la propriété que f_i est un élément premier). Il en suit que g est le produit d'un sous-ensemble des f_i fois une unité de A. Alors, g n'a qu'un nombre fini de diviseurs à association près. En conséquence il n'y a pas de chaîne de diviseurs de longeur infinie dans $A[X]$. Nous avons alors démontré que $A[X]$ est un anneau factoriel. □

Traitons le cas spécial qui nous intéressera le plus dans le corollaire suivant :

Corollaire 2.10. *Soit A un anneau factoriel et $f \in A[X]$ un polynôme primitif non constant. Alors, les assertions suivantes sont équivalentes :*

(i) f est irréductible dans $A[X]$.

(ii) f est premier dans $A[X]$.

(iii) f *est premier dans* $K[X]$.

(iv) f *est irréductible dans* $K[X]$.

Démonstration. Les équivalences « (i) $\Leftrightarrow$ (ii) » et « (iii) $\Leftrightarrow$ (iv) » proviennent du fait que $A[X]$ et $K[X]$ sont des anneaux factoriels. L'équivalence « (ii) $\Leftrightarrow$ (iii) » est une conséquence directe du théorème 2.9 (f doit être de type (II), car f est non constant). □

Le corollaire nous dit alors qu'un polynôme unitaire $f \in \mathbb{Z}[X]$ est irréductible si et seulement s'il est irréductible en tant que polynôme de $\mathbb{Q}[X]$. Le corollaire suivant est obtenue par une simple récurrence.

Corollaire 2.11. *Soit A un anneau factoriel et $n \in \mathbb{N}$. Alors, l'anneau $A[X_1, \ldots, X_n]$ est un anneau factoriel.*

Exemple 2.12. *L'anneau $\mathbb{Q}[X, Y]$ est factoriel, mais, pas principal. Par exemple, l'idéal (X, Y) ne peut pas être engendré par un seul polynôme. Ceci donne un exemple d'un anneau factoriel non principal.*

Nous allons maintenant prouver deux critères d'irréductibilité pour les polynômes : le critère de réduction et le critère d'Eisenstein.

Proposition 2.13 (Critère de réduction)**.** *Soit A un anneau factoriel et $f(X) = \sum_{i=0}^{d} a_i X^i \in A[X]$ un polynôme primitif non constant. Pour un élément premier $p \in A$ nous considérons l'application « réduction mod p » comme dans la preuve de la proposition 2.7 :*

$$\pi : A[X] \to A/(p)[X], \quad \sum_{i=0}^{r} a_i X^i \mapsto \sum_{i=0}^{r} \overline{a_i} X^i,$$

Si p ne divise pas a_d et $\pi(f)$ est irréductible dans $A/(p)[X]$, alors, f est irréductible dans $A[X]$.

Démonstration. Supposons le cas contraire : $f = gh$ avec $g, h \in A[X]$ non constants. Alors, on a $\pi(f) = \pi(gh) = \pi(g)\pi(h)$. Puisque $\pi(f)$ est irréductible, il en suit que $\pi(g)$ ou $\pi(h)$ est constant.

Utilisons maintenant que $p \nmid a_d$. Ecrivons $g(X) = \sum_{i=1}^{r} b_i X^i$ et $h(X) = \sum_{i=1}^{s} c_i X^i$ avec $b_r \neq 0 \neq c_s$. Puisque $a_d = b_r c_s$, on obtient que $p \nmid b_r$ et $p \nmid c_s$. Alors, le degré de $\pi(g)$ est égal au degré de g, et le degré de $\pi(h)$ est égal au degré de h. On obtient alors que soit g est constant, soit h l'est. Cette contradiction finit la preuve. □

Exemple 2.14. – *Considérons $f_1(X) = X^2 + X + 1 \in \mathbb{Z}[X]$, $f_2(X) = X^2 + 15X - 53 \in \mathbb{Z}[X]$, $f_3(X) = X^2 + 14X - 55 \in \mathbb{Z}[X]$ et $f_4(X) = X^2 + 15X - 54 \in \mathbb{Z}[X]$.*
Ces polynômes sont unitaires, donc primitifs. Notez que le polynôme $X^2 + X + 1 \in \mathbb{F}_2[X]$ est irréductible (pour les polynômes de degré au plus 3 il suffit de vérifier qu'il n'y a pas de zéro). Le critère de réduction modulo 2 montre alors que f_1 et f_2 sont irréductibles comme éléments de $\mathbb{Z}[X]$ (et aussi de $\mathbb{Q}[X]$). Cette argumentation ne s'applique pas à f_3. La réduction de f_3 modulo 3 est $X^2 + 2X + 2 \in \mathbb{F}_3[X]$ qui est irréductible ; alors, nous obtenons la même conclusion. Pour f_4 on ne peut ni utiliser la réduction modulo 2, ni modulo 3. En fait, aucun critère peut marcher puisqu'on a $X^2 + 15X - 54 = (X + 18)(X - 3)$.

– *Soit $A = \mathbb{Q}[T]$ et considérons un polynôme de la forme $f(T,X) = \sum_{i=0}^{d} a_i(T)X^i \in A[X]$. Notez que T est un élément premier de $\mathbb{Q}[T]$: si $T \mid g(T)h(T)$ avec $g, h \in \mathbb{Q}[T]$, alors soit $T \mid h(T)$ ou $T \mid g(T)$.*
La réduction d'un polynôme $a(T) \in A[T]$ modulo T revient à l'évaluer en zéro $a(0)$: si $a(T) = b_0 + b_1T + \cdots + b_eT^e$, alors la classe de $a(T)$ et la classe de $b_0 = a(0)$ modulo T sont les mêmes car $a(T) - b_0 = T \cdot (b_1 + b_2T + \ldots b_eT^{e-1}) \in (T)$.
Alors, si $f(T,X)$ est unitaire en la variable X et $f(0,X)$ est irréductible, alors $f(T,X)$ est irréductible dans $A[X] = \mathbb{Q}[T,X]$.
– *Le polynôme $X^2 + X + 2TX + 5T^2X + T^3 + 1 \in \mathbb{Q}[T,X]$ est irréductible, puisqu'il est unitaire (pour la variable X) et $f(0,X) = X^2 + X + 1$ est irréductible.*

Proposition 2.15 (Critère d'Eisenstein)**.** *Soit A un anneau factoriel et $f(X) = \sum_{i=0}^{d} a_iX^i \in A[X]$ un polynôme primitif non constant. Soit $p \in A$ un élément premier tel que*

$$p \nmid a_d, \quad p \mid a_i \text{ pour tout } 0 \leq i \leq d-1 \quad \text{et } p^2 \nmid a_0.$$

Alors, f est irréductible dans $A[X]$ (donc aussi irréductible dans $K[X]$).

Démonstration. Supposons le contraire et écrivons $f = gh$ avec $g(X) = \sum_{i=0}^{r} b_iX^i \in A[X]$, $h(X) = \sum_{i=0}^{s} c_iX^i \in A[X]$ non constants et $b_r \neq 0 \neq c_s$. A cause de $a_d = b_rc_s$, la condition $p \nmid a_d$ implique $p \nmid b_r$ et $p \nmid c_s$. A cause de $a_0 = b_0c_0$, les conditions $p \mid a_0$ et $p^2 \nmid a_0$ impliquent sans perte de généralité que $p \mid b_0$ et $p \nmid c_0$.

Soit t le plus petit entier entre 1 et r tel que $p \nmid b_t$. Alors $1 \leq t \leq r < d$, puisque $p \mid b_0$ et $p \nmid b_r$. Nous posons $c_i = 0$ pour $i > s$ et on a :

$$\underbrace{a_t}_{\text{divisible par } p} = \underbrace{b_0c_t + b_1c_{t-1} + \cdots + b_{t-1}c_1}_{\text{divisible par } p} + \underbrace{b_tc_0}_{\text{pas divisible par } p}.$$

Cette contradiction finit la preuve. □

Exemple 2.16.
– *Considérons $f_1(X) = X^2 + 2X + 2 \in \mathbb{Z}[X]$ et $f_2(X) = X^7 + 72X^2 + 111X - 30 \in \mathbb{Z}[X]$. Ces polynômes sont unitaires, donc primitifs. Le critère d'Eisenstein avec $p = 2$ montre que f_1 est irréductible dans $\mathbb{Z}[X]$. L'irréductibilité de f_2 se montre par le critère d'Eisenstein avec $p = 3$.*
– *Soit p un nombre premier et $A = \mathbb{F}_p[T]$. Soit $f(T,X) = X^p - T \in A[X] = \mathbb{F}_p[T,X]$. Comme dans l'exemple 2.14 on voit que T est un élément premier de A. Le polynôme $f(T,X)$ satisfait aux conditions du critère d'Eisenstein en tant que polynôme dans la variable X pour l'élément premier T. Alors, $f(T,X)$ est irréductible.*
Plus tard, ce polynôme nous servira comme exemple d'un polynôme irréductible, mais inséparable.
– *Soit p un nombre premier. Considérons le polynôme $X^p - 1 \in \mathbb{Q}[X]$. Il n'est pas irréductible puisque nous avons :*

$$X^p - 1 = (X-1)\underbrace{(X^{p-1} + X^{p-2} + \cdots + X + 1)}_{=:\Phi_p(X)} \in \mathbb{Z}[X].$$

*On appelle $\Phi_p(X)$ le p-*ième polynôme cyclotomique (en allemand : Kreisteilungspolynom). *Il jouera un rôle plus tard dans le cours. Voici, la preuve que $\Phi_p(X)$ est irréductible :*
Il suffit de montrer que $\Phi_p(X+1)$ est irréductible (car, si $\Phi_p(X+1) = f(X)g(X)$, alors, $\Phi_p(X) = f(X-1)g(X-1)$). On a

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{(X+1)-1} = \frac{(X+1)^p - 1}{X} = \frac{\sum_{i=1}^{p} \binom{p}{i} X^i}{X} = X^p + \sum_{i=1}^{p-1} \binom{p}{i} X^{i-1},$$

qui est alors un polynôme d'Eisenstein pour l'élément premier p car $p \mid \binom{p}{i}$ pour tout $1 \leq i \leq p-1$ et $p^2 \nmid \binom{p}{1} = p$. Donc, $\Phi_p(X)$ est irréductible dans $\mathbb{Z}[X]$ (et alors aussi dans $\mathbb{Q}[X]$).

3 Caractéristique

Définition-Lemme 3.1. *Soit A un anneau intègre. Le noyau de l'unique homomorphisme d'anneaux $\varphi_A : \mathbb{Z} \to A$ est un idéal premier (p) de $\mathbb{Z}$ pour $p = 0$ ou un nombre premier. On appelle p* la caractéristique de A, *noté* $\mathrm{car}(A) = p$.

Démonstration. Comme φ_A est un homomorphisme d'anneaux, on a $\varphi_A(1) = 1$, donc $\varphi_A(n) = \underbrace{1+1+\cdots+1}_{n \text{ fois}}$ si $n \geq 0$, et $\varphi_A(n) = \underbrace{-1-1-\cdots-1}_{|n| \text{ fois}}$ si $n < 0$. Puisque A est un anneau intègre, l'image de φ_A, qui est un sous-anneau de A, est aussi un anneau intègre. Le théorème d'isomorphisme nous dit $A/\ker(\varphi_A) \cong \mathrm{im}(\varphi_A)$, donc par la caractérisation des idéaux premiers, $\ker(\varphi_A)$ est un idéal premier. Nous savons que les idéaux premiers de $\mathbb{Z}$ sont soit (0), soit les idéaux engendrés par les nombres premiers, donc le résultat. □

Exemple 3.2.
- $\mathrm{car}(\mathbb{C}) = \mathrm{car}(\mathbb{Z}) = \mathrm{car}(\mathbb{Q}) = \mathrm{car}(\mathbb{R}) = 0$.
- *Rappelons que $\mathbb{F}_p := \mathbb{Z}/(p)$ pour un nombre premier p est un corps de cardinal p. On a* $\mathrm{car}(\mathbb{F}_p) = p$.

Lemme 3.3. *(a) Soit $\varphi : A \to B$ un homomorphisme injectif d'anneaux intègres. Alors,* $\mathrm{car}(A) = \mathrm{car}(B)$.

(b) Soient K, L deux corps commutatifs de caractéristiques différentes. Il n'y a pas d'homomorphisme de corps $\varphi : K \to L$.

(c) Soit A un anneau intègre et $K := \mathrm{Frac}(A)$ son corps des fractions. Alors, $\mathrm{car}(A) = \mathrm{car}(K)$.

Démonstration. (a) La composée $\mathbb{Z} \xrightarrow{\varphi_A} A \xrightarrow{\varphi} B$ est égale à φ_B. Puisque φ est injective, on a $\ker(\varphi_A) = \ker(\varphi_B)$, donc $\mathrm{car}(A) = \mathrm{car}(B)$.
(b) Des homomorphismes entre corps sont injectifs car le noyau est un idéal premier, donc (0).
(c) Le plongement naturel $A \to K$ donné par $a \mapsto \frac{a}{1}$ est injectif, donc on peut utiliser (a). □

Lemme 3.4. *(a) Soit A un anneau intègre de caractéristique 0. Alors $\varphi_A : \mathbb{Z} \to A$ est injective.*

(b) Soit A un anneau intègre de caractéristique $p > 0$. Alors il existe un homomorphisme d'anneaux injectif $\overline{\varphi}_A : \mathbb{F}_p \to A$.

(c) Soit K un corps commutatif de caractéristique 0. Alors il existe un homomorphisme de corps $\varphi_K : \mathbb{Q} \to K$.

Le plus petit sous-corps d'un corps K s'appelle *corps premier de K* (en anglais : *prime field* ; en allemand : *Primkörper*). Le lemme dit alors que le corps premier d'un corps de caractéristique 0 est $\mathbb{Q}$ et que le corps premier d'un corps de caractéristique $p > 0$ est $\mathbb{F}_p$.

Démonstration. (a) φ_A est injective car son noyau est (0) par définition de la caractéristique.

(b) Le théorème d'isomorphisme nous dit que φ_A induit l'application récherchée.

(c) On pose $\varphi_K(\frac{r}{s}) := \frac{\varphi_K(r)}{\varphi_K(s)}$ (noter que cela est permis car $\varphi_K(s) \neq 0$ pour $s \neq 0$ comme φ_K est injective). □

Définition-Lemme 3.5. *(a) Soit A un anneau intègre de caractéristique $p > 0$. On définit l'application*

$$\mathrm{Frob} : A \to A, \quad x \mapsto x^p,$$

dite « homomorphisme de Frobenius ». C'est un homomorphisme d'anneaux.

(b) Si K est un corps fini de caractéristique $p > 0$, alors Frob est un automorphisme de K (par définition, un automorphisme de K est un isomorphisme de K dans lui-même).

Démonstration. (a) La seule chose qui doit être démontrée est la multiplicativité :

$$\mathrm{Frob}(a+b) = (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p.$$

On utilise que $p \mid \binom{p}{i}$ pour tout $1 \leq i \leq p-1$.

(b) Les homomorphismes de corps sont injectifs. Puisque le nombre d'éléments de K est fini, Frob est bijectif. □

Proposition 3.6. *Soit K un corps de caractéristique $p > 0$. Alors, l'image de $\overline{\varphi}_K : \mathbb{F}_p \to K$ est égale à l'ensemble $\{x \in K \mid \mathrm{Frob}(x) = x^p = x\}$.*

Démonstration. La preuve est très facile si nous nous rappelons de deux choses :

- Le « petit théorème de Fermat » : $a^p = a$ pour tout $a \in \mathbb{F}_p$. La preuve est aussi facile : le groupe multiplicatif $\mathbb{F}_p^\times$ a $p-1$ éléments. Si on éléve un élément d'un groupe à la puissance l'ordre du groupe, alors, on obtient l'élément neutre du groupe. Dans notre cas cela veut dire : si $a \in \mathbb{F}_p \setminus \{0\}$, alors, $a^{p-1} = 1$, donc, $a^p = a$. Cette égalité est trivialement satisfaite pour $a = 0$ aussi.
- Un polynôme de degré d à coefficients dans un anneau intègre a au maximum d zéros. Donc, le polynôme $X^p - X \in K[X]$ a au plus p zéros. Nous en connaissons déjà p : les éléments $\varphi(x)$ pour $x \in \mathbb{F}_p$.

Si on interprète l'ensemble $\{x \in K \mid \mathrm{Frob}(x) = x^p = x\}$ comme l'ensemble des zéros dans K de $X^p - X \in K[X]$, la preuve est complète. □

4 Extensions algébriques

Tout corps est supposé commutatif pour la suite du cours.

Définition-Lemme 4.1. *(a) Soit L un corps et $K \subseteq L$ un sous-corps. Dans ce cas on dit que L est* une extension du corps K *(ou bien que L/K est une* extension de corps*).*

(b) La multiplication sur L peut être vue comme une multiplication scalaire

$$K \times L \to L, \quad (x, y) \mapsto xy$$

qui muni L d'une structure de K-espace vectoriel.

(c) Le degré *de l'extension de corps L/K est défini comme*

$$[L : K] := \dim_K(L) \in \mathbb{N} \cup \{\infty\}.$$

Si $[L : K] < \infty$ on parle d'une extension finie de corps *(attention : ne pas confondre avec extension de corps finis !).*

Démonstration. Il n'y a que (b) à montrer. C'est trivial car les axiomes pour l'espace vectoriel font partie des axiomes pour un corps. □

Proposition 4.2 (Multiplicativité du degré)**.** *Soient $K \subseteq L \subseteq M$ des extensions de corps. Alors,*

$$[M : K] = [L : K] \cdot [M : L].$$

Démonstration.
– $\underline{M/L \text{ et } L/K \text{ sont finies :}}$ En tant que K-espaces vectoriels on a $L \cong K^{[L:K]}$ (car tout K-espace vectoriel de dimension d est isomorphe à K^d). De la même façon on a $M \cong L^{[M:L]}$. Donc

$$K^{[M:K]} \cong M \cong (K^{[L:K]})^{[M:L]} = K^{[L:K]\cdot[M:L]}.$$

– $\underline{M/L \text{ infinie :}}$ Il existe un ensemble infini d'éléments $m_1, m_2, \ldots \in M$ qui sont L-linéairement indépendants, donc aussi K-linéairement indépendants. Donc $[M : K] = \infty$.
– $\underline{L/K \text{ infinie :}}$ Comme $M \supseteq L$ on a $\dim_K(M) \geq \dim_K(L) = \infty$.

□

Le prochain corollaire montre déjà que la multiplicativité du degré est très utile.

Corollaire 4.3. *Soient $K \subseteq L \subseteq M$ des extensions de corps. Si $[M : K]$ est un nombre premier, alors $L = K$ ou $L = M$.*

Démonstration. Les degrés $[M : L]$ et $[L : K]$ sont des diviseurs du nombre premier $p = [M : K]$, donc, 1 ou p. □

Définition-Lemme 4.4. *Soient L/K une extension de corps et $a \in L$. Alors, l'application* évaluation

$$\mathrm{ev}_a : K[X] \to L, \quad \sum_{i=0}^{d} c_i X^i \mapsto \sum_{i=0}^{d} c_i a^i$$

est un homomorphisme d'anneaux. Pour être plus compact, on écrira aussi $K[X] \ni f(X) \mapsto f(a) \in L$.

*On note l'image de ev_a par $K[a]$ et on l'appelle la K-*algèbre engendrée par a.

Rappelez-vous qu'une K-algèbre A est un anneau qui est aussi un K-espace vectoriel « de façon compatible » ; par définition cela veut dire que l'application $K \to A$ donnée par $x \mapsto x.1$ (où $x.1$ est la multiplication scalaire du K-espace vectoriel A) est un homomorphisme d'anneaux. Il est donc évident que $K[a]$ est en effet une K-algèbre.

Démonstration. Exercice. □

Remarque 4.5. *Parfois on regardera aussi la variante évidente du lemme 4.4 pour un ensemble (fini ou infini) d'éléments :*

Soient $a_i \in L$ pour $i \in I$ (n'importe quel ensemble). Alors, l'application évaluation

$$\mathrm{ev}_{(a_i)_{i\in I}} : K[X_i \mid i \in I] \to L, \quad f((X_i)_{i\in I}) \mapsto f((a_i)_{i\in I})$$

est un homomorphisme d'anneaux.

On note l'image de $\mathrm{ev}_{(a_i)_{i\in I}}$ par $K[(a_i)_{i\in I}]$ et on l'appelle la K-algèbre engendrée par les a_i pour $i \in I$. *Si $I = \{1, 2, 3, \ldots, n\}$ est un ensemble fini, alors on écrit aussi $K[a_1, \ldots, a_n]$.*

Notez que $K[a]$ et $K[(a_i)_{i\in I}]$ sont des sous-anneaux de L (même de K-sous-algèbres), car l'image d'un homomorphisme d'anneaux est toujours un sous-anneau. Très explicitement les éléments de $K[a]$ sont tous de la forme $\sum_{i=0}^{d} r_i a^i$ pour $d \in \mathbb{N}$ et $r_0, \ldots, r_d \in K$. Cette forme rend évident le fait que les sommes, les différences et les produits de tels éléments sont aussi de cette forme ; ceci donne une autre preuve que $K[a]$ est un sous-anneau de L.

Exemple 4.6. *(a) $\mathbb{Q}[2] \subset \mathbb{R}$ est égal à $\mathbb{Q}$.*

(b) L'anneau $\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$ est égal à $\{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$ parce que

$$\sum_{i=0}^{n} r_i \sqrt{2}^i = \sum_{i=0 \text{ pair}}^{n} r_i 2^{i/2} + \Big(\sum_{i=1 \text{ impair}}^{n} r_i 2^{(i-1)/2}\Big)\sqrt{2}.$$

On voit que $\mathbb{Q}[\sqrt{2}]$ est un corps. L'inverse de $a + b\sqrt{2} \neq 0$ est $\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$. Notez que le dénominateur n'est jamais 0, car, s'il l'était, alors $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$. [Pour voir que $\sqrt{2} \neq 2$ il est possible d'utiliser le critère d'Eisenstein.]

En peu plus loin, on donnéra un argument direct qui implique ce fait parce que $\sqrt{2}$ est algébrique *(définition en bas).*

(c) Soit $i = \sqrt{-1} \in \mathbb{C}$. Alors, $\mathbb{R}[i] \subseteq \mathbb{C}$ est égal à $\mathbb{C}$ et $\mathbb{Q}[i] \subsetneq \mathbb{C}$ est un sous-corps (écrivez une formule pour l'inverse !).

(d) Soient $n, m \in \mathbb{N}$, $n \neq 0$. On trouve que $\mathbb{Q}[\sqrt[n]{m}]$ est un corps.

Ceci se démontre encore facilement « à la main », mais sera aussi une conséquence directe des résultats en bas.

(e) Soit $n \in \mathbb{N}$, $n > 0$. Posons $\zeta_n := e^{2\pi i/n} \in \mathbb{C}$. On appelle ζ_n une racine n-ième primitive d'unité *car $(\zeta_n)^n = 1$ est $(\zeta_n)^m \neq 1$ pour $0 < m < n$. On trouve que $\mathbb{Q}[\zeta_n]$ est un corps. Ce corps s'appelle* n-ième corps cyclotomique *(en anglais :* cyclotomic field*; en allemand :* Kreisteilungskörper*).*

Ceci se démontre encore facilement « à la main », mais sera aussi une conséquence directe des résultats en bas.

(f) Soit π le nombre réel appelé π, donc, le nombre réel qui est égal au quotient de la circonférence d'un cercle par son diamétre ou deux fois la valeur du zéro minimal positif de la fonction $\cos$*. Un théorème célèbre de Lindemann (qui n'est pas très difficile, mais, on ne le démontrera pas ; une preuve se trouve par exemple dans le livre de Stewart sur la théorie de Galois) implique que le sous-anneau $\mathbb{Q}[\pi] \subsetneq \mathbb{R}$ n'est pas un sous-corps.*

On donne maintenant la définition du sous-*corps* engendré par un élément. En général, cela n'est pas la même chose que la sous-*algèbre* engendrée par le même élément (sauf si l'élément est algébrique, comme on le verra) à cause de l'existence possible d'éléments non-inversibles.

Notez que l'intersection d'un ensemble de sous-corps d'un corps L est un corps lui-même. (Evidemment, l'assertion similaire pour les réunions n'est pas vraie.)

Définition 4.7. *Soient L/K une extension de corps et $a \in L$. On défini $K(a)$ comme l'intersection de tous les sous-corps de L qui contiennent K et a, et on l'appelle* le sous-corps de L engendré par a sur K *ou bien* l'extension simple de K par a.

C'est le plus petit sous-corps de L qui contient K et a.

Remarque 4.8. *(a) Parfois on utilisera la définition précédente pour plus qu'un élément :*

Si $a_i \in L$ pour $i \in I$ on défini $K(a_i \mid i \in I)$ comme l'intersection de tous les sous-corps de L qui contiennent K et les a_i pour $i \in I$. Il est appelé le sous-corps de L engendré par les a_i pour $i \in I$ sur K.

(b) La relation entre $K[a]$ est $K(a)$ s'exprime élégamment comme suit $\mathrm{Frac}(K[a]) = K(a)$.

Raison : Il est clair que $K[a] \subseteq K(a)$. Comme $K(a)$ est un corps, nous avons l'inclusion $\mathrm{Frac}(K[a]) \subseteq K(a)$. L'autre inclusion provient directement de la définition de $K(a)$: c'est l'intersection de tout les sous-corps de L qui contiennent K et a, et $\mathrm{Frac}(K[a])$ en est un.

On jette un deuxième regard sur l'exemple précédent.

Exemple 4.9. *(a)* $\mathbb{Q}[2] = \mathbb{Q}(2) = \mathbb{Q} \subset \mathbb{R}$.

(b) $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$.

(c) Soit $i = \sqrt{-1} \in \mathbb{C}$. Alors, $\mathbb{R}[i] = \mathbb{R}(i) \subseteq \mathbb{C}$ est égal à $\mathbb{C}$ et $\mathbb{Q}[i] = \mathbb{Q}(i) \subsetneq \mathbb{C}$.

(d) Soient $n, m \in \mathbb{N}$, $n \neq 0$. On a $\mathbb{Q}[\sqrt[n]{m}] = \mathbb{Q}(\sqrt[n]{m})$.

(e) Soit $n \in \mathbb{N}$, $n > 0$. Posons $\zeta_n := e^{2\pi i/n} \in \mathbb{C}$. On a $\mathbb{Q}[\zeta_n] = \mathbb{Q}(\zeta_n)$.

(f) $\mathbb{Q}[\pi] \subsetneq \mathbb{Q}(\pi) \subsetneq \mathbb{R}$. Remarquons que $\mathbb{Q}(\pi)$ est dénombrable, mais $\mathbb{R}$ ne l'est pas.

On traitera maintenant la question si la dimension de $K[a]$ en tant que K-espace vectoriel est finie ou infinie. L'idée simple mais importante est de considérer les deux alternatives :

(1) Les éléments $1 = a^0, a, a^2, a^3, a^4, \ldots$ sont K-linéairement indépendants.

(2) Les éléments $1 = a^0, a, a^2, a^3, a^4, \ldots$ sont K-linéairement dépendants.

En cas (1) $K[a]$ est un espace vectoriel de dimension infinie.

En cas (2) il existe une combinaison linéaire

$$0 = \sum_{i=0}^{n} r_i a^i$$

avec $n \in \mathbb{N}$, $r_i \in K$ pour $0 \leq i \leq n$ et $r_n \neq 0$. En divisant par r_n, nous pouvons supposer que cette combinaison linéaire est de la forme

$$0 = a^n + \sum_{i=0}^{n-1} r_i a^i.$$

On peut interpreter cette égalité comme suit : Le polynôme unitaire $f(X) := X^n + r_{n-1}X^{n-1} + \cdots + r_1 X + r_0 \in K[X]$ a a come zéro : $f(a) = 0$. Dans la proposition suivante nous allons voir que $K[a]$ est de dimension finie en tant que K-espace vectoriel et que même $K[a]$ est un corps lui-même, donc $K[a] = K(a)$ et $K(a)/K$ est une extension finie de corps.

Définition 4.10. *Soit L/K une extension de corps.*

Un élément $a \in L$ est appelé algébrique sur K *s'il existe un polynôme non-zéro $f \in K[X]$ tel que $f(a) = 0$ (c'est à dire que a est un zéro (ou racine) de f).*

Un élément $a \in L$ qui n'est pas algébrique sur K est appelé transcendant sur K.

Il est important de noter que l'algébricité est une notion *relative*. Un élément est algébrique *sur* un corps (et non algébrique tout seul).

Proposition 4.11. *Soient L/K une extension de corps et $a \in L$.*

(a) L'évaluation $\mathrm{ev}_a : K[X] \to L$ donnée par $f \mapsto f(a)$ (voir le lemme 4.4) est injective si et seulement si a est transcendant sur K.

(b) Si a est algébrique sur K, alors il existe un unique polynôme unitaire $\mathrm{mipo}_a(X) \in K[X]$ tel que $(\mathrm{mipo}_a) = \ker(\mathrm{ev}_a)$ (c'est à dire : l'idéal principal (mipo_a) est le noyau de l'évaluation).

Le polynôm mipo_a est appelé le polynôme minimal de a sur K.

(c) Si a est algébrique sur K, le polynôme minimal $\mathrm{mipo}_a \in K[X]$ de a sur K est irréductible (en tant qu'élément de $K[X]$). Il peut être caractérisé comme le polynôme unitaire dans $K[X]$ de degré minimal dont a est un zéro.

(d) Soit a algébrique sur K. Alors l'application induite

$$\mathrm{ev}_a : K[X]/(\mathrm{mipo}_a) \to L, \quad f + (\mathrm{mipo}_a) \mapsto f(a)$$

est un homomorphisme injectif de corps et elle identifie $K[X]/(\mathrm{mipo}_a)$ avec $K[a]$ et $K(a)$.

(e) Soit a algébrique sur K. Alors, $K(a)$ est une extension finie de K et son degré $[K(a) : K]$ est égal au degré du polynôme minimal mipo_a de a sur K. Une K-base de $K(a)$ est donnée par $1, a, a^2, \ldots, a^{d-1}$, où $d = [K(a) : K]$.

Démonstration. (a) Si a est algébrique sur K, alors il existe un polynôme non-zéro $f \in K[X]$ tel que $f(a) = 0$. Alors f est dans le noyau de l'évaluation, donc, ev_a n'est pas injective. Réciproquement, si ev_a n'est pas injective, alors il existe un polynôme non-zéro f dans le noyau de ev_a. Ceci ne dit autre que $f(a) = 0$; donc a est algébrique.

(b) Nous savons que $K[X]$ est un anneau principal. Donc le noyau de ev_a est un idéal principal, donc engendré par un élément f. Puisque ev_a n'est pas injective (car a est algébrique), f est non-zéro. Le générateur d'un idéal principal est unique à une unité de l'anneau près. Donc, f est unique

à multiplication par une unité de K près (car les unités de $K[X]$ sont les mêmes que celles de K). Si f est de la forme $r_dX^d + r_{d-1}X^{d-1} + \cdots + r_0 \in K[X]$ avec $r_d \neq 0$, alors $\mathrm{mipo}_a := \frac{1}{r_d}f = X^d + \frac{r_{d-1}}{r_d}X^{d-1} + \cdots + \frac{r_0}{r_d}$ est l'unique polynôme unitaire recherché.

(c) Soit $f \in K[X]$ un polynôme non-zéro tel que $f(a) = 0$. Alors $f \in \ker(\mathrm{ev}_a) = (\mathrm{mipo}_a)$, donc $\mathrm{mipo}_a \mid f$. En conséquence le degré de mipo_a est plus petit ou égal au degré de f.

Si mipo_a était réductible, on aurait $\mathrm{mipo}_a = fg$ avec $f, g \in K[X]$ tous les deux de degré strictement plus petit que le degré de mipo_a. Mais, $0 = \mathrm{mipo}_a(a) = f(a)g(a)$ donnerait $f(a) = 0$ ou $g(a) = 0$. Les deux contradiraient la minimalité du degré de mipo_a.

(d) Puisque mipo_a est irréductible, $K[X]/(\mathrm{mipo}_a)$ est un corps. L'application induite (et son injectivité – qui est claire de toute façon car $K[X]/(\mathrm{mipo}_a)$ est un corps) provient du théorème d'isomorphisme. Comme $K[a]$ est un corps, il est égal à $K(a)$.

(e) Ecrivons le polynôme minimal de a sur K comme $\mathrm{mipo}_a(X) = X^d + c_{d-1}X^{d-1} + \cdots + c_0$. On veut démontrer que $1, a, a^2, a^3, \ldots, a^{d-1}$ est une K-base pour $K[a]$.

D'abord il est clair que ces éléments sont K-linéairement indépendants, car s'ils ne l'étaient pas, alors il y'aurait $r_0, \ldots, r_{d-1} \in K$ pas tous zéro tels que $0 = \sum_{i=0}^{d-1} r_i a^i$, donc le polynôme minimal de a aurait degré strictement plus petit que d, une contradiction.

Donc il faut montrer que $1, a, a^2, a^3, \ldots, a^{d-1}$ engendrent $K[a]$ en tant que K-espace vectoriel. Il suffit de représenter a^n, pour tout n, comme combinaison K-linéaire de $1, a, a^2, a^3, \ldots, a^{d-1}$. Pour le faire on utilise le polynôme minimal qui donne

$$a^d = -\big(c_{d-1}a^{d-1} + \cdots + c_0\big).$$

Supposons que la plus grande puissance de a qui apparaît est a^m pour $m \geq d$. Dans ce cas, nous multiplions l'équation par a^{m-d} et obtenons :

$$a^m = -\big(c_{d-1}a^{m-1} + \cdots + c_0a^{m-d}\big).$$

Donc on peut exprimer a^m comme une combinaison linéaire de puissances moins élévées de a. Ayant fait cela, il reste au pire des puissances a^{m-1}, et on applique le même processus autant de fois jusqu'à ce que seulement des puissances a^n pour $n \leq d-1$ restent. □

Exemple 4.12. *(a) Soit K un corps. Tout $a \in K$ est algébrique sur K. En effet, a est un zéro du polynôme $X - a \in K[X]$ qui est clairement le polynôme minimal de a sur K.*

(b) $\sqrt{2}$ est algébrique sur $\mathbb{Q}$. En effet, $\sqrt{2}$ est un zéro du polynôme $X^2 - 2 \in \mathbb{Q}[X]$ qui est le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$. Notez que le polynôme $X - \sqrt{2}$ ne peut pas être utilisé ici, car ses coefficients ne sont pas dans $\mathbb{Q}$!

(c) Soit p un nombre premier et $n \in \mathbb{N}$, $n > 1$. Alors, $X^n - p$ est le polynôme minimal de $\sqrt[n]{p}$ sur $\mathbb{Q}$.

(d) Soit p un nombre premier. Alors, $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Q}[X]$ est le polynôme minimal de $\zeta_p = e^{2\pi i/p}$ sur $\mathbb{Q}$.

(e) π est transcendant sur $\mathbb{Q}$. Ceci est le théorème de Lindemann déjà mentionné. Plus loin, on obtiendra de ce théorème par la théorie de Galois que la quadrature du cercle à la règle et au compas est impossible. Ceci veut dire qu'il est impossible de construire un carré du même aire qu'un cercle donné en utilisant seulement une règle (sans échelle) et un compas.

(f) π *est algébrique sur* $\mathbb{R}$ *(cas spécial de (a)).*

(g) $i = \sqrt{-1}$ *est algébrique sur* $\mathbb{Q}$*. On a* $\mathrm{mipo}_i(X) = X^2 + 1 \in \mathbb{Q}[X]$.

Exemple 4.13. *Considérons l'exemple* $\mathbb{Q}(\zeta_3)$ *pour* $\zeta_3 = e^{2\pi i/3}$*. Le polynôme minimal de* ζ_3 *sur* $\mathbb{Q}$ *est* $X^2 + X + 1$*, donc* $\mathbb{Q}(\zeta_3)$ *est l'image de* $\mathbb{Q}[X]/(X^2 + X + 1)$ *dans* $\mathbb{C}$*. La* $\mathbb{Q}$*-base la plus facile c'est* $1, \zeta_3$*. Donc on exprime tout élément de* $\mathbb{Q}(\zeta_3)$ *comme* $a + b\zeta_3$ *pour* $a, b \in \mathbb{Q}$*.*

Soient $\alpha = a_0 + a_1\zeta_3$ *et* $\beta = b_0 + b_1\zeta_3$ *deux tels éléments. Alors*

$$\alpha + \beta = (a_0 + b_0) + (a_1 + b_1)\zeta_3$$

et

$$\begin{aligned}\alpha \cdot \beta = (a_0 + a_1\zeta_3)(b_0 + b_1\zeta_3) &= a_0b_0 + \zeta_3(a_0b_1 + a_1b_0) + a_1b_1(\zeta_3)^2 \\ &= (a_0b_0 - a_1b_1) + (a_0b_1 + a_1b_0 - a_1b_1)\zeta_3,\end{aligned}$$

car $\zeta_3^2 = -\zeta_3 - 1$ *à cause de son polynôme minimal.*

Définition 4.14. *Soit* K *un corps et* $f \in K[X]$ *un polynôme irréductible non-zéro. Une extension* L *de* K *est appelée* corps de rupture *du polynôme* f *sur* K *s'il existe* $a \in L$ *tel que* $f(a) = 0$ *et* $L = K(a)$.

Exemple 4.15. *Soit* L/K *une extension de corps et* $a \in L$ *algébrique. Alors,* $K(a)$ *est un corps de rupture du polynôme minimal de* a *sur* K.

Proposition 4.16. *Soit* K *un corps et* $f \in K[X]$ *un polynôme irréductible non-zéro. Il existe un corps de rupture de* f *sur* K.

Démonstration. Ecrivons $f(X) = \sum_{i=0}^{d} a_i X^i \in K[X]$. On pose $L := K[X]/(f(X))$ (c'est bien un corps car f est irréductible) et $\alpha := X + (f)$, donc la classe de X dans L. L'application naturelle $K \to L$ donnée par $b \mapsto b + (f(X))$ est un homomorphisme de corps. Donc on peut voir K de façon naturelle comme sous-corps de L.

Nous démontrons que α est un zéro de f dans L :

$$f(X + (f(X))) = \sum_{i=0}^{d} a_i(X + (f(X)))^i = \sum_{i=0}^{d} a_i X^i + (f(X)) = f(X) + (f(X)) = 0 + (f(X)).$$

Donc on a $f(\alpha) = 0$ dans L.

Nous obtenons que L est un corps de rupture de f sur K. □

Définition 4.17. *Soit* L/K *une extension de corps.*

On appelle L/K algébrique *(ou alternativement on dit que* L *est une* extension algébrique *de* K*) si tout* $a \in L$ *est algébrique sur* K.

Si L/K *n'est pas algébrique, alors elle est dite* transcendante.

Proposition 4.18. *Toute extension finie de corps* L/K *est algébrique. Elle peut être engendrée par un nombre fini d'éléments algébriques sur* K.

Démonstration. Soit $a \in L$. Comme $K[a]$ est un sous-espace de L, il est de K-dimension finie. Donc, a est algébrique sur K.

Démontrons maintenant que L/K peut être engendrée par un nombre fini d'éléments de L (qui sont automatiquement algébriques). Soit $a_1 \in L \setminus K$. On a $K \subsetneq K(a_1) \subseteq L$, donc $[L : K] > [L : K(a_1)]$. Si $K(a_1) \neq L$, alors on prend $a_2 \in L \setminus K(a_1)$. On a $K(a_1) \subsetneq K(a_1, a_2) \subseteq L$, donc $[L : K(a_1)] > [L : K(a_1, a_2)]$. On continue ainsi. Comme le degré est un entier positif, ce processus s'arrêtera et alors on aura $K(a_1, a_2, \ldots, a_n) = L$. □

Proposition 4.19. *Soient L/K une extension de corps et $a_1, \ldots, a_n \in L$. Les deux assertions suivantes sont équivalentes :*

(i) Tous les a_i pour $i = 1, \ldots, n$ sont algébriques sur K.

(ii) L'extension $K(a_1, a_2, \ldots, a_n)/K$ est finie.

Démonstration. Exercice. □

Proposition 4.20. *Soient $M/L/K$ des extensions de corps.*

(a) Supposons que L/K est algébrique et $a \in M$ est algébrique sur L. Alors a est algébrique sur K.

(b) (Transitivité de l'algébricité) M/K est algébrique si et seulement si M/L et L/K sont algébriques.

Démonstration. (a) Soit $\mathrm{mipo}_a = \sum_{i=0}^{d} c_i X^i \in L[X]$ le polynôme minimal de a sur L. Ses coefficients $c_i \in L$ sont algébriques sur K. Donc l'extension $N := K(c_0, c_1, \ldots, c_{d-1})$ de K est finie par la proposition 4.19. Car N contient les coefficients d'un polynôme qui annulle a, l'extension $N(a)$ est algébrique sur N, donc le degré $[N(a) : N]$ est fini. Par la multiplicativité du degré, l'extension $N(a)/K$ est aussi fini, donc algébrique. En particulier, a est algébrique sur K.

(b) Une direction est triviale, l'autre est une conséquence de (a). □

On termine cette partie par une définition très importante, mais, qui ne jouera pas de grand rôle dans ce cours.

Définition 4.21. *Soit L/K une extension de corps et $a_1, \ldots, a_n \in L$. On dit que les éléments $a_1, \ldots, a_n$ sont* algébriquement dépandants sur K *si l'évaluation $\mathrm{ev}_{a_1,\ldots,a_n}$ n'est pas injective.*

Dans le cas contraire on parle d'éléments algébriquement indépandants sur K.

Exemple 4.22.
- *(π, π^2) sont algébriquement dépendants sur $\mathbb{Q}$ (considérer : $X_1^2 - X_2$).*
- *Il n'est pas connu si (e, π) (avec e la base de l'exponentielle naturelle) sont algébriquement indépendants sur $\mathbb{Q}$.*

5 Constructions à la règle et au compas

Nous regardons des constructions en géométrie plane initiées par les grecs anciens. Pour ces constructions nous nous permettons seulement l'utilisation d'une règle (non graduée) et d'un compas.

Dans ce qui suit nous allons regarder $\mathbb{C}$ en même temps comme corps algébriquement clos qui contient $\mathbb{Q}$ et comme le plan réel.

Soit $P_0 \subset \mathbb{C}$ un sous-ensemble. Nous considérons les deux opérations suivantes :

Règle Soit $r_1, r_2 \in P_0$ deux points distincts. Tracer la droite passant par r_1 et r_2.

Compas Soit $r_1, r_2, r_3 \in P_0$. Tracer le cercle de centre r_1 et de rayon la distance entre r_2 et r_3.

Définition 5.1. *Soit $P_0 \subseteq \mathbb{C}$ un sous-ensemble. On dit qu'un point $z \in \mathbb{C}$ peut être* contruit à la règle et au compas en un seul pas à partir de P_0 *si*

- *z est le point d'intersection de deux droites distinctes construites selon l'opération* **règle***, ou*
- *z est un point d'intersection d'une droite construite selon l'opération* **règle** *et d'un cercle construit selon l'opération* **compas***, ou*
- *z est un point d'intersection de deux cercles construits selon l'opération* **compas***.*

Pour $n \in \mathbb{N}_{\geq 1}$ soit P_n le sous-ensemble de $\mathbb{C}$ de tous les points qui peuvent être construits à la règle et au compas en un seul pas à partir de P_{n-1}. On pose $\mathcal{X}(P_0) := \bigcup_{n\geq 0} P_n$, c'est le sous-ensemble de $\mathbb{C}$ de tous les points qui peuvent être construits à la règle et au compas en un nombre fini de pas à partir de P_0.

Proposition 5.2. *Les constructions suivantes peuvent être fait à la règle et au compas, c'est-à-dire avec les opérations* **règle** *et* **compas** *:*

(a) Tracer la droite perpendiculaire à une droite donnée passant par un point donné.

(b) Tracer la droite passant par un point donné et parallèle à une droite donnée.

(c) Tracer la médiatrice d'un segment donné.

(d) Additionner deux angles.

(e) Réflexion d'un point par rapport à une droite donnée.

(f) Construction du triangle équilatéral à partir d'un segment donné.

(g) Tracer la bisectrice d'un angle.

Démonstration. Elémentaire. □

Corollaire 5.3. *Soit $P_0 \subseteq \mathbb{C}$ tel que $0, 1 \in P_0$ et $z, z_1, z_2 \in \mathcal{X}(P_0)$. Alors :*

(a) $z_1 + z_2 \in \mathcal{X}(P_0)$ *;*

(b) $-z \in \mathcal{X}(P_0)$ *;*

(c) $|z| \in \mathcal{X}(P_0)$ *;*

(d) $e^{\pi i/3} \in \mathcal{X}(P_0)$ *;*

(e) $|z_1| \cdot |z_2| \in \mathcal{X}(P_0)$ *;*

(f) $\frac{1}{|z|} \in \mathcal{X}(P_0)$ *(pour $z \neq 0$) ;*

(g) $z_1 \cdot z_2 \in \mathcal{X}(P_0)$ *;*

(h) $\frac{1}{z} \in \mathcal{X}(P_0)$ *(pour $z \neq 0$) ;*

(i) $\pm\sqrt{z} \in \mathcal{X}(P_0)$.

En particulier, $\mathcal{X}(P_0)$ est un corps tel que pour tout $z \in \mathcal{X}(P_0)$ on a $\sqrt{z} \in \mathcal{X}(P_0)$.

Démonstration. Exercice avec indications au tableau. Pour (e) et (f) utiliser le théorème de Thalès (allemand : Strahlensatz) et pour (i) utiliser le théorème de Thalès sur le cercle (allemand : Satz von Thales). □

Notation 5.4. *Soit $M \subseteq \mathbb{C}$. On note $\overline{M} := \{\overline{z} \mid z \in M\}$. Ici $\overline{z}$ est le conjugé complexe de $z \in \mathbb{C}$.*

Proposition 5.5. *Soit $P_0 \subseteq \mathbb{C}$ un sous-corps tel que $\overline{P_0} = P_0$ et $i \in P_0$. Si $z \in P_1$, alors $[P_0(z) : P_0] \leq 2$.*

Démonstration. Notons d'abors que si $z = x + iy \in P_0$ (avec $x, y \in \mathbb{R}$), alors $\overline{z} = x - iy \in P_0$ par hypothèse et donc $x = \frac{1}{2}(z + \overline{z}) \in P_0$ et $y = \frac{1}{2i}(z - \overline{z}) \in P_0$. Pour cela nous avons utilisé $i \in P_0$. Donc, les « coordonnées » de tous $z \in P_0$ (c'est-à-dire, la partie réelle et la partie imaginaire) appartiennent à P_0. Le même argument est évidemment valable pour P_1.

Les droites en question sont données par des équations linéaire à coefficients dans P_0, et les cercles par des équations de degré 2 également à coefficients dans P_0. Les coordonnées des points d'intersection sont donc des zéros d'équations linéaires. Donc, le degré de $[P_0(z) : P_0]$ est dans $\{1, 2, 4\}$ (par la multiplicativité des degrés). Un exercice montre que la valeur 4 n'apparaît pas. □

Lemme 5.6. *[Premier cas de la théorie de Kummer] Soit L/K une extensions de corps de degré 2. Alors il existe $a \in K$ tel que $L = K(\sqrt{a})$.*

Démonstration. Soit $b \in L \setminus K$ et $X^2 + rX + s \in K[X]$ le polynôme minimal de b sur K. Posons $a := b + \frac{r}{2}$. Alors :

$$a^2 = b^2 + br + \frac{r^2}{4} = \frac{r^2}{4} - s \in K.$$

Donc le polynôme minimal de a est $X^2 - \frac{r^2}{4} + s \in K[X]$. □

Théorème 5.7. *Soit $P_0 \subseteq \mathbb{C}$ avec $0, 1 \in P_0$. Posons $L_0 := \mathbb{Q}(P_0 \cup \overline{P_0})$. Soit $z \in \mathbb{C}$. Les deux assertions suivantes sont équivalentes :*

(a) $z \in \mathcal{X}(P_0)$.

(b) Il existe $n \in \mathbb{N}$ et pour tout $1 \leq i \leq n$ un corps L_i tel que

$$L_0 \subsetneq L_1 \subsetneq \cdots \subsetneq L_n$$

et $z \in L_n$ et pour tout $1 \leq i \leq n$ on a $[L_i : L_{i-1}] = 2$.

Démonstration. « (i) ⇒ (ii) » : Sans perte de généralité nous pouvons supposer $P_0 = \mathbb{Q}(P_0 \cup \overline{P_0}) = L_0$. Comme i peut être construit à partir de $0, 1$ et $[L(i) : L] \leq 2$, nous pouvons aussi supposer $i \in P_0$.

Si on construit un point z à partir d'un corps $L \subseteq \mathbb{C}$ avec $i \in L$ et $\overline{L} = L$, par la proposition 5.5 on a $[L(z) : L] \leq 2$ et $[L(\overline{z}) : L] \leq 2$. Si on pose $L' := L(z, \overline{z})$, alors on a une des trois possibilités :

$$L' = L, \quad [L' : L] = 2, \quad [L' : L(z)] = 2 \text{ et } [L(z) : L] = 2.$$

Donc, l'assertion est vraie si z peut être construit à partir de L_0 en un seul pas.

Si plusieurs constructions sont nécessaires pour arriver à z, on peut itérer ce processus.

« (ii) ⇒ (i) » : Nous avons $L_0 = \mathbb{Q}(P_0 \cup \overline{P_0})$. L'inclusion $L_0 \subseteq \mathcal{X}(P_0)$ est triviale. Le lemme 5.6 nous dit que pour tout $1 \leq i \leq n$ is existe $z_i \in L_{i-1}$ tel que $L_i = L_{i-1}(\sqrt{z_i})$. Par le corollaire 5.3 $\mathcal{X}(P_0)$ est un corps fermé sous les racines carrés, nous obtenons $L_n \subseteq \mathcal{X}(P_0)$, donc $z \in \mathcal{X}(P_0)$. □

Corollaire 5.8. *Soit $P_0 \subseteq \mathbb{C}$ avec $0, 1 \in P_0$.*

(a) L'extension de corps $\mathcal{X}(P_0)/\mathbb{Q}(P_0 \cup \overline{P_0})$ est algébrique.

(b) Pour tout $z \in \mathcal{X}(P_0)$ il existe $r \in \mathbb{N}$ tel que $[\mathbb{Q}(P_0 \cup \overline{P_0} \cup \{z\}) : \mathbb{Q}(P_0 \cup \overline{P_0})] = 2^r$.

Démonstration. C'est une conséquence directe du théorème 5.7 et la multiplicativité des degrés pour (b). □

Théorème 5.9 (Wantzel)**.** *Le cube ne peut pas être dupliqué à la règle et au compas ; c'est-à-dire, si $\overline{AB}$ est le coté d'un cube, il est impossible de construire à la règle et au compas un segment $\overline{CD}$ tel que le volume du cube avec le coté $\overline{CD}$ est le double du volume du cube avec le coté $\overline{AB}$.*

Démonstration. Sans perte de généralité nous pouvons prendre $A = 0$ et $B = 1$. Il s'agit donc de construire $\sqrt[3]{2}$. C'est impossible car $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ (pas de puissance de 2). □

Théorème 5.10 (Wantzel)**.** *Il est impossible de trisecter un angle donné à la règle et au compas.*

Démonstration. Par exemple on peut regarder l'angle $e^{2\pi i/3}$ (dans le triangle éqilatéral avec coté $\overline{01}$). Si on pouvait le trisecter, on aurait construit $e^{2\pi i/9}$. Mais son polynôme minimal est $X^6 - X^3 + 1 \in \mathbb{Z}[X]$, dont le degré $[\mathbb{Q}(e^{2\pi i/9}) : \mathbb{Q}] = 6$ n'est pas une puissance de 2. □

Théorème 5.11. *La quadrature du cercle est impossible ; c'est-à-dire, pour un cercle donné, il est impossible de construire un carré du même aire que le cercle à la règle et au compas.*

Démonstration. L'aire du cercle unitaire est π. Si la construction était possible, on aurait construit $\sqrt{\pi}$, et en particulier $\sqrt{\pi}$ serait algébrique sur $\mathbb{Q}$, ce qui n'est pas le cas, comme par le théorème de Lindemann π (et donc aussi $\sqrt{\pi}$) est transcendant sur $\mathbb{Q}$. □

Remarque 5.12. *Un théorème remarquable de Mohr et Mascheroni, démontré indépendamment par Georg Mohr en 1672 et par Lorenzo Mascheroni en 1797, affirme que si une construction géométrique est possible à la règle et au compas, alors elle est possible au compas seul (sauf le tracé effectif des droites).*

6 Corps de décomposition

Clôture algébrique

Définition-Lemme 6.1. *Soit L/K une extension de corps. On pose*

$$K_L := \{a \in L \mid a \text{ algébrique sur } K\}.$$

On appelle K_L la clôture algébrique de K dans L.

(a) K_L est un sous-corps de L.

(b) K_L/K est une extension algébrique.

Démonstration. (a) Soient $a, b \in K_L$. Il est difficile (mais, pas impossible) d'écrire les polynôme minimaux pour $a+b$, $a \cdot b$, $-a$ et $1/b$ (si $b \neq 0$) en partant des polynômes minimaux de a et b (en utilisant le « résultant » que nous n'allons pas traiter dans ce cours).

On va le faire autrement : $K(a,b)$ est fini et algébrique sur K (comme a, b sont algébriques sur K). Donc $a+b, a \cdot b, -a, 1/b \in K(a,b)$ sont algébriques sur K, donc $a+b, a \cdot b, -a, 1/b \in K_L$. Donc, K_L est un sous-corps de L.

(b) suit de la transitivité de l'algébricité. □

Exemple 6.2. $\overline{\mathbb{Q}} := \mathbb{Q}_{\mathbb{C}}$ *est la clôture algébrique de* $\mathbb{Q}$ *dans* $\mathbb{C}$*. Il satisfait les propriétés suivantes :*

- $\overline{\mathbb{Q}}/\mathbb{Q}$ *est algébrique.*
- $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$ *(par exemple,* $X^n - p \in \mathbb{Z}[X]$ *est irréductible pour tout* n *et tout nombre premier* p *par le critère d'Eisenstein ; donc* $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$*).*
- $\overline{\mathbb{Q}}$ *est dénombrable (car l'ensemble de polynômes dans* $\mathbb{Q}[X]$ *est dénombrable, donc l'ensemble de leurs zéros l'est aussi).*
- $\mathbb{C}$ *n'est pas dénombrable. Donc dans* $\mathbb{C}$ *il existe un ensemble non-dénombrable d'éléments qui sont transcendants sur* $\mathbb{Q}$*.*

Définition 6.3. *Soit* K *un corps. On appelle* K algébriquement clos *si tout* $f \in K[X]$ *de degré* ≥ 1 *possède un zéro dans* K*.*

Un corps $\overline{K}$ *est appelé* clôture algébrique de K *si* $\overline{K}$ *est algébriquement clos et* $\overline{K}/K$ *est une extension algébrique.*

Exemple 6.4. $\mathbb{C}$ *est algébriquement clos (c'est un résultat d'analyse complexe, par exemple).*

$\overline{\mathbb{Q}}$ *(du dernier exemple) est une clôture algébrique de* $\mathbb{Q}$*.*

Lemme 6.5. *Soit* K *un corps. Les assertions suivantes sont équivalentes :*

(i) K *est algébriquement clos.*

(ii) Tout $f \in K[X]$ *unitaire de degré* d *est de la forme*

$$f(X) = \prod_{i=1}^{d} (X - a_i)$$

avec $a_1, \ldots, a_d \in K$*.*

(iii) Si L/K *est une extension algébrique, alors* $L = K$*.*

Démonstration. « (i) ⇒ (ii) » C'est une application de la division euclidienne de polynômes.

« (ii) ⇒ (iii) » : Soit L/K algébrique, soit $a \in L$ et soit $f \in K[X]$ le polynôme minimal de a sur K. Tous les zéros de f sont dans K, donc $a \in K$. Donc $L = K$.

« (iii) ⇒ (i) » : Soit $f \in K[X]$ un polynôme non-constant. On peut supposer sans perte de généralité qu'il est irréductible. L'extension $L := K[X]/(f)$ sur K est algébrique, donc $L = K$, donc le degré de f est 1, donc f a un zéro dans K. □

Théorème 6.6. *Soit* K *un corps. Il existe une clôture algébrique de* K*.*

Démonstration. Exercice. □

Prolongation d'homomorphismes de corps

Définition 6.7. *Soient K'/K une extension de corps, L un corps et $\sigma : K \to L$ et $\tau : K' \to L$ des homomorphismes de corps.*

On dit que τ est une prolongation de σ *si $\tau|_K = \sigma$ (c'est-à-dire, $\tau(x) = \sigma(x)$ pour tout $x \in K$).*

Notation 6.8. *Soient K, L des corps et $\sigma : K \to L$ un homomorphisme de corps. Pour un polynôme $f(X) = \sum_{i=0}^{d} a_i X^i \in K[X]$ nous écrivons f^σ pour le polynôme $\sum_{i=0}^{d} \sigma(a_i) X^i \in L[X]$.*

Lemme 6.9. *Soient K, L des corps, $K' = K(a)$ une extension algébrique de K et $f := \mathrm{mipo}_a \in K[X]$. Soit $\sigma : K \to L$ un homomorphisme de corps. Alors :*

(a) Si $\sigma' : K' \to L$ est une prolongation de σ (c'est-à-dire, un homomorphisme de corps tel que $\sigma'|_K = \sigma$), alors $f^\sigma(\sigma'(a)) = 0$, donc $\sigma'(a)$ est un zéro de f^σ.

(b) Pour tout zéro $b \in L$ de f^σ il existe une unique prolongation $\sigma' : K' \to L$ telle que $\sigma'(a) = b$.

(c) Le nombre de prolongations de σ à K' est égal au nombre de zéro de f^σ, donc au plus égal à $\deg(f)$.

Démonstration. (a) Soit $f(X) = \sum_{i=0}^{d} c_i X^i$. On a

$$f^\sigma(\sigma'(a)) = \sum_{i=0}^{d} \sigma(c_i)\sigma'(a)^i = \sum_{i=0}^{d} \sigma'(c_i)\sigma'(a)^i = \sigma'\left(\sum_{i=0}^{d} c_i a^i\right) = \sigma'\left(f(a)\right) = \sigma'(0) = 0.$$

(b)

Unicité Comme K' a la K-base $1, a, a^2, \ldots, a^{d-1}$, tout homomorphisme de corps $K' \to L$ est uniquement déterminé par l'image de a.

Existence Considérons l'homomorphisme d'anneaux

$$\phi : K[X] \xrightarrow{f \mapsto f^\sigma} L[X] \xrightarrow{g \mapsto g(b)} L.$$

On a clairement $\phi|_K = \sigma$ (ici K est identifié avec les polynômes constants dans $K[X]$). On a aussi $f \in \ker(\phi)$ car $f^\sigma(b) = 0$. Comme f est irréductible, l'idéal $(f) \lhd K[X]$ est maximal, donc $(f) = \ker(\phi)$. Le théorème d'isomorphismes fournit un homomorphisme d'anneaux

$$\overline{\phi} : K[X]/(f(X)) \to L,$$

qui est automatiquement injectif (comme tous les homomorphismes de corps) et satisfait $\overline{\phi}(X + (f)) = b$ et $\overline{\phi}|_K = \sigma$.

Rappelons que $\overline{\mathrm{ev}_a} : K[X]/(f) \to K'$ est un isomorphisme de corps. Donc, $\sigma' := \overline{\phi} \circ \overline{\mathrm{ev}_a}^{-1}$ est la prolongation de σ recherchée.

(c) est une conséquence directe de (a) et (b). □

Exemple 6.10. – *On veut étendre l'identité $\mathbb{Q} \hookrightarrow \mathbb{C}$ à $K' := \mathbb{Q}(\sqrt{2})$. Un homomorphisme $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$ est uniquement déterminé par l'image de $\sqrt{2}$. Nous avons donc deux possibilités pour cette image, car elle doit être un zéro du polynôme $f^\sigma(X)$ pour $f(X) = X^2 - 2$. Mais $f^\sigma = f$, donc, soit l'image et $\sqrt{2}$, soit $-\sqrt{2}$.*

– *On veut étendre l'identité $\mathbb{Q} \hookrightarrow \mathbb{C}$ à $K' := \mathbb{Q}(\sqrt[3]{2})$. De la même manière nous trouvons que l'image de $\sqrt[3]{2}$ doit être une racine de $X^3 - 2$. Pour cette raison nous le factorisons dans $\mathbb{C}$:*

$$X^3 - 2 = (X - \sqrt[3]{2})(X - \zeta_3\sqrt[3]{2})(X - \zeta_3^2\sqrt[3]{2})$$

avec $\zeta_3 = e^{2\pi/3}$. Donc, nous avons trois prolongations possibles, à savoir, l'image de $\sqrt[3]{2}$ est soit $\sqrt[3]{2}$, soit $\zeta_3\sqrt[3]{2}$, soit $\zeta_3^2\sqrt[3]{2}$.

Proposition 6.11. *Soient K'/K une extension algébrique (qui peut être infinie), L un corps algébriquement clos et $\sigma : K \to L$ un homomorphisme de corps. Alors :*

(a) Il existe une prolongation $\sigma' : K' \to L$ de σ.

(b) Si K' est algébriquement clos et $L/\sigma(K)$ est algébrique, alors toute prolongation $\sigma' : K' \to L$ de σ est un isomorphisme de corps.

Démonstration. (a) Cet argument utilise le lemme de Zorn (voir Algèbre 2). Regardons l'ensemble

$$M := \{(F, \tau) \mid K'/F/K,\ \tau : F \to L \text{ prolongation de } \sigma\}.$$

– $M \neq \emptyset$ car $(K, \sigma) \in M$.
– M est (partiellement) ordonné pour la relation d'ordre définie par

$$(F_1, \tau_1) \leq (F_2, \tau_2) \ \Leftrightarrow\ F_1 \subseteq F_2 \text{ et } \tau_2|_{F_1} = \tau_1.$$

– Tout sous-ensemble $T \subseteq M$ qui est totalement ordonné (c'est-à-dire, pour tout $(F_1, \tau_1) \in T$, $(F_2, \tau_2) \in T$ on a $(F_1, \tau_1) \leq (F_2, \tau_2)$ ou $(F_2, \tau_2) \leq (F_1, \tau_1)$) a une majorante dans M, à savoir $(\tilde{f}, \tilde{\tau})$ avec $\tilde{F} = \bigcup_{(F,\tau)\in M} F$ et $\tilde{\tau} : F \to L$ défini par $\tilde{\tau}(x) := \tau(x)$ pour un (n'importe lequel) $(F, \tau) \in M$ tel que $x \in F$.

Nous avons vérifié les hypothèses du lemme de Zorn qui nous donne donc un élément maximal $(F, \tau) \in M$. Nous montrons $F = K'$. Si cela n'était pas le cas, alors on pourrait choisir $a \in K' \setminus F$. Comme K'/K est algébrique, a l'est aussi. Donc, par le lemme 6.9 on peut donc prolonger τ à $F(a)$, c'est une contradiction à la maximalité.

(b) On choisit une prolongation $\sigma' : K' \to L$ (possible par (a)). Comme σ' est injective (comme tout homomorphisme de corps), K' est isomorphe à $\sigma'(K')$. Donc, $\sigma'(K')$ est aussi algébriquement clos. Par hypothèse, $L/\sigma(K)$ est algébrique, donc $L/\sigma'(K')$ est aussi algébrique, et en conséquence $L = \sigma'(K')$. Donc, σ' est un isomorphisme de corps. □

Définition 6.12. *Soient K un corps, L_1/K et L_2/K des extensions de corps. Un homomorphisme de corps $\sigma : L_1 \to L_2$ est appelé* K-homomorphisme *si σ prolonge* $\mathrm{id} : K \to L_2$ *(c'est-à-dire, si $\sigma(x) = x$ pour tout $x \in K$).*

L'ensemble de tous les K-homomorphismes de L_1 dans L_2 est noté $\mathrm{Hom}_K(L_1, L_2)$.

Exemple 6.13. *Soient $K/\mathbb{Q}$ et $L/\mathbb{Q}$ deux extension et $\sigma : K \to L$ un homomorphisme de corps. Alors, σ est un $\mathbb{Q}$-homomorphisme.*

Corollaire 6.14. *Soit K un corps et $\overline{K}_1$ et $\overline{K}_2$ deux clôtures algébriques de K. Alors, il existe un isomorphisme de corps $\overline{K}_1 \to \overline{K}_2$ qui prolonge* id_K.

Démonstration. On prolonge l'identité $\mathrm{id} : K \to \overline{K}_2$ à $\overline{K}_1$ par la proposition 6.11. □

Corps de décomposition

Définition 6.15. *Soient K un corps et $(f_i)_{i\in I} \subseteq K[X]$ une famille de polynômes de degré ≥ 1. Une extension L/K est appelée* corps de décomposition de $(f_i)_{i\in I}$ sur K *si*

- *pour tout $i \in I$ le polynôme f_i se factorise complètement en facteurs linéaires dans $L[X]$ ($f_i(X) = b_i \prod_{j=1}^{\deg(f_i)}(X - c_{i,j})$ avec $c_{i,j} \in L$) et*
- *L est engendré sur K par tous les $c_{i,j}$ ($L = K(c_{i,j} \mid i \in I, 1 \leq j \leq \deg(f_i))$).*

Souvent la famille de polynôme ne consistera que d'un seul polynôme.

Exemple 6.16.
- *Le corps de décomposition de $X^2 - 2 \in \mathbb{Q}[X]$ sur $\mathbb{Q}$ est $\mathbb{Q}(\sqrt{2})$.*
- *Le corps de décomposition de $X^3 - 2 \in \mathbb{Q}[X]$ sur $\mathbb{Q}$ est $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ avec $\zeta_3 = e^{2\pi i/3}$.*
- *Le corps de décomposition de $\{X^2 - 2, X^2 - 3\} \subset \mathbb{Q}[X]$ est $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.*

Proposition 6.17. *Soient K un corps et $(f_i)_{i\in I} \subseteq K[X]$ une famille de polynômes de degré ≥ 1.*

(a) Il existe un corps de décomposition L de la famille $(f_i)_{i\in I}$ sur K. Il est algébrique sur K.

(b) Si L_1 est L_2 sont deux corps de décomposition de cette famille, alors il existe un K-isomorphisme $\sigma : L_1 \to L_2$.

Démonstration. (a) Soit $\overline{K}$ une clôture algébrique de K et soient $c_{i,j} \in \overline{K}$ les zéros des polynômes f_i. Alors, $L := K(c_{i,j} \mid i \in I, 1 \leq j \leq \deg(f_i))$ est un corps de décomposition. Comme L est engendré par des éléments qui sont algébriques sur K, il suit que L/K est une extension algébrique.

(b) Soit $\overline{L}_2$ une clôture algébrique de L_2 et $\mathrm{id}_K : K \to \overline{L}_2$ l'identité. Par la proposition 6.11 on peut prolonger σ en un K-homomorphisme $\sigma : L_1 \to \overline{L}_2$. On pose $d_{i,j} := \sigma(c_{i,j}) \in \overline{L}_2$. On a

$$b_i \prod_{j=1}^{\deg(f_i)} (X - c_{i,j}) = f_i(X) = f_i^\sigma(X) = b_i \prod_{j=1}^{\deg(f_i)} (X - d_{i,j})$$

et, comme L_2 est engendré sur K par les $d_{i,j}$ en tant que corps de décomposition sur K, alors, l'image $\sigma(L_1)$ est L_2, donc $L_1 \cong L_2$ par un K-isomorphisme. □

Définition 6.18. *Soit L/K une extension algébrique de corps. On l'appelle* normale *si tout polynôme irréductible $f \in K[X]$ qui possède un zero c_1 dans L se factorise complètement en facteurs linéaires dans $L[X]$, c'est-à-dire, $f(X) = b \prod_{i=1}^{\deg(f)}(X - c_i)$ avec $c_1, \ldots, c_{\deg(f)} \in L$.*

Proposition 6.19. *Soit L/K une extension algébrique (pas nécéssairement finie). Alors les assertions suivantes sont équivalentes :*

(i) L/K est normale.

(ii) L est un corps de décomposition d'une famille $(f_i)_{i\in I} \subseteq K[X]$ sur K.

(iii) Tout K-homomorphisme $\sigma : L \to \overline{L}$, où $\overline{L}$ est une clôture algébrique de L, satisfait $\sigma(L) = L$ et donc donne lieu à un K-isomorphisme $\sigma : L \to L$.

Démonstration. « (i) ⇒ (ii) » : Soit $S \subseteq L$ tel que $L = K(S)$. Pour tout $s \in S$ soit $f_s := \mathrm{mipo}_s(X) \in K[X]$ le polynôme minimal de s sur K. Par (i), tout f_s se factorise complètement dans $L[X]$ et par hypothèse L est engendré par $s \in S$, donc, par tous les zéros de tous les f_s.

« (ii) $\Rightarrow$ (iii) » : Pour tout $i \in I$, l'homomorphisme σ permute les racines de f_i : si $f_i(a) = 0$ pour $a \in L$, alors, $\sigma(a)$ est une autre racine de f_i (comme nous l'avons déjà vu plusieurs fois). Donc, l'image $\sigma(L)$ est engendré sur K par les mêmes éléments que L, donc, cette image est égale à L.

« (iii) $\Rightarrow$ (i) » : Soient $f \in K[X]$ irréductible et $a \in L$ tel que $f(a) = 0$. Soient $\overline{L}$ une clôture algébrique de L et $b \in \overline{L}$ tel que $f(b) = 0$. Par le lemme 6.9 (b) il existe un K-homomorphisme $\sigma : K(a) \to \overline{L}$ tel que $\sigma(a) = b$. Par la proposition 6.11 on peut le prolonger en K-homomorphisme $\sigma : L \to \overline{L}$. Par (iii) nous avons $L = \sigma(L) \ni \sigma(a) = b$. Donc L contient toutes les racines de f. □

Exemple 6.20. – *Les corps $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ et $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sont normaux sur $\mathbb{Q}$.*

- *Le corps $K := \mathbb{Q}(\sqrt[3]{2})$ n'est pas normal sur $\mathbb{Q}$, car le polynôme $X^3 - 2$ n'a qu'une seule de ses racines dans K. Alternativement, l'image de l'homomorphisme $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$ donné par $\sqrt[3]{2} \mapsto \zeta_3 \sqrt[3]{2}$ n'est pas contenue dans $\mathbb{Q}(\sqrt[3]{2})$.*
- *Toute extension L/K de degré 2 est normale : Si $L = K(a)$, alors L est le corps de décomposition du polynôme minimal de a sur K (comme le polynôme est de degré 2, s'il a un facteur linéaire dans $L[X]$, alors l'autre doit y être aussi).*
- *Si M/L et L/K sont normales, l'extension M/K peut quand-même être non-normale.*
  Par exemple, $\mathbb{Q}(\sqrt[4]{2}) \supsetneq \mathbb{Q}(\sqrt{2}) \supsetneq \mathbb{Q}$. La grande extension n'est pas normale pour les mêmes raison que le deuxième exemple. Par contre, les deux sous-extensions sont normales car elles sont de degrés 2.
- *Si $M/L/K$ sont des extensions de corps avec M/K normale, l'extension L/K peut être non-normale.*
  Par exemple : $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) \supsetneq \mathbb{Q}(\sqrt[3]{2}) \supsetneq \mathbb{Q}$.
- *Soient K un corps et $\overline{K}$ une clôture algébrique de K. Alors, $\overline{K}/K$ est normale (on peut prendre la famille de tous les polynômes de $K[X]$).*

Proposition 6.21. *Soient $M/L/K$ des extensions de corps. Si M/K est normale, alors M/L l'est aussi.*

Démonstration. M est un corps de décomposition d'une famille de polynômes $(f_i)_{i \in I} \subseteq K[X]$ sur K. Mais, M est encore un corps de décomposition de la même famille considérée sur L. □

Définition 6.22. *Soit L/K une extension algébrique. Une extension N/L est appelée* clôture normale de L/K *si*

- *N/K est normale et*
- *si $N/N_1/L$ telle que N_1/K est normale, alors $N = N_1$ (donc, N/K ne contient aucune sous-extension non-triviale qui est normale sur K et contient L).*

Proposition 6.23. *Soit L/K une extension algébrique.*

(a) Soient $\overline{L}$ une clôture algébrique de L sur K, $S \subseteq L$ tel que $L = K(S)$ et f_s le polynôme minimal de s sur K pour tout $s \in S$. Alors, le corps de décomposition M de la famille $(f_s)_{s \in S}$ sur K est une clôture normale de L/K.

En particulier, une clôture normale existe toujours.

(b) Si N est une clôture normale de L/K, alors N est le corps de décomposition sur K de la famille $(f_s)_{s \in S}$.

(c) Si L/K est finie, alors toute clôture normale N/K de L/K est aussi finie.

(d) Soit N/K une clôture normale de L/K. Alors, N est l'extension de K engendrée par tous les $\sigma(L)$ pour $\sigma \in \mathrm{Hom}_K(L, \overline{L})$.

(e) Si N_1/K et N_2/K sont deux clôtures normales de L/K, alors, il existe un K-isomorphisme $N_1 \cong N_2$.

Démonstration. (a) Les corps de décomposition donnent lieu à des extensions normales, donc M/K est normale. Soit $M/M'/L$ telle que M'/K est normale. On sait que M' doit contenir toutes les racines des f_s, car $f_s(s) = 0$ et $s \in L$. Donc, $M' = M$.

(b) Soit N une clôture normale de L/K. Comme dans (a) on sait que N doit contenir toutes les racines des f_s, car $f_s(s) = 0$ et $s \in L$. Donc N est un corps de décomposition sur K de la famille $(f_s)_{s\in S}$.

(c) Si L/K est finie, l'ensemble S peut être choisi fini. Donc, on obtient N comme l'extension engendrée par l'ensemble fini de toutes les racines des f_s.

(d) On montre d'abord $N \supseteq \sigma(L)$ pour tout $\sigma \in \mathrm{Hom}_K(L, \overline{L})$: L'image de σ est engendrée par les $\sigma(s)$ pour $s \in S$ (car L est engendré sur K par S). Mais, nous savons que $\sigma(s) \in \overline{L}$ est une racine de f_s et appartient donc à N.

On montre maintenant que N est contenu dans le corps engendré sur K par toutes les images $\sigma(L)$ pour $\sigma \in \mathrm{Hom}_K(L, \overline{L})$. Pour cela il suffit de démontrer que pour tout $s \in S$ toute racine de f_s est contenue dans un $\sigma(L)$. Soit t une autre racine de f_s. Nous avons déjà fait cet argument un nombre de fois : par le lemme 6.9 il existe un K-homomorphisme $\sigma : K(s) \to \overline{L}$ qui envoie s sur t. Par la proposition 6.11 nous pouvons prolonger σ en élément de $\mathrm{Hom}_K(L, \overline{L})$. Donc $t \in \sigma(L)$.

(e) Tous les deux sont des corps de décomposition de la famille $(f_s)_{s\in S}$, donc isomorphes par la proposition 6.17 (b). □

7 Extensions séparables

On se rappelle : Soient K un corps, $f \in K[X]$ un polynôme irréductible, $\overline{K}$ une clôture algébrique de K et $a \in \overline{K}$ t.q. $f(a) = 0$. Alors, nous avons la bijection

$$\{ \text{ racines de } f \text{ dans } \overline{K}\} \longrightarrow \mathrm{Hom}_K(K(a), \overline{K}),$$

où l'image de la racine b est l'unique K-homomorphisme σ tel que $\sigma(a) = b$ (voir le lemme 6.9).

On appellera un polynôme f séparable quand il a « autant de racines (dans $\overline{K}$) que possible » (c'est à dire $\deg(f)$). On appellera une extension L/K séparable quand elle admet « autant de K-homomorphismes $L \to \overline{K}$ que possible » (notion à préciser ci-dessous).

Exemple 7.1.
- *Le polynôme $X^2-2 \in \mathbb{Q}[X]$ a deux racines dans $\mathbb{C}$ et son degré est également 2.*
- *Le polynôme $X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$ a quatre racines dans $\mathbb{C}$ et son degré est également 4.*
- *Soit p un nombre premier. Le polynôme $X^p - T \in \mathbb{F}_p(T)[X]$ (où $\mathbb{F}_p(T) := \mathrm{Frac}(\mathbb{F}_p[T])$) est irréductible (comme nous l'avons vu par le critère d'Eisenstein), mais, avec $t \in \overline{\mathbb{F}_p(T)}$ tel que $t^p = T$ on a $X^p - T = (X - t)^p$, donc il n'y a qu'une seule racine bien que le degré soit p.*

Définition 7.2. *Soit K un corps et $\overline{K}$ une clôture algébrique de K. Soit $f \in K[X]$.*
- *Une racine $a \in \overline{K}$ de f est dite de* multiplicité r *si $(X-a)^r \mid f$ et $(X-a)^{r+1} \nmid f$.*
- *Le polynôme f est dit* séparable *si toutes ses racines (dans $\overline{K}$) ont la multiplicité 1. Il est clair que f est séparable si et seulement si le nombre de racines distinctes est égale au degré de f.*
- *Si f n'est pas séparable, on l'appelle* inséparable.

Lemme 7.3. *Soient K un corps et $f, g \in K[X]$.*

(a) Soit L/K une extension de corps. Soient $\mathrm{pgcd}_{K[X]}(f,g)$ le plus grand commun diviseur unitaire (pour qu'il soit unique) de f et g dans l'anneau principal $K[X]$, et $\mathrm{pgcd}_{L[X]}(f,g)$ l'analogue dans $L[X]$. Alors, $\mathrm{pgcd}_{K[X]}(f,g) = \mathrm{pgcd}_{L[X]}(f,g)$.

(b) Pour $f = \sum_{i=0}^{d} a_i X^i$ nous définissons la dérivée formelle *$f'(X) := \sum_{i=1}^{d} i a_i X^{i-1}$. Alors, on a*

$$(f+g)' = f' + g' \quad \text{et} \quad (fg)' = f'g + fg'.$$

Démonstration. (a) Par l'identité de Bézout nous avons

$$d_1 := \mathrm{pgcd}_{K[X]}(f,g) = f(X)a_1(X) + g(X)b_1(X)$$
$$d_2 := \mathrm{pgcd}_{L[X]}(f,g) = f(X)a_2(X) + g(X)b_2(X)$$

avec $a_1, b_1 \in K[X]$ et $a_2, b_2 \in L[X]$. Nous avons les divisibilités suivantes dans $L[X]$: $d_1 | f$, $d_1 \mid g$, donc $d_1 \mid d_2$; et de la même façon $d_2 | f$, $d_2 \mid g$, donc $d_2 \mid d_1$. Comme d_1 et d_2 sont unitaires, on obtient $d_1 = d_2$.

(b) C'est un calcul simple. (Noter que vous ne pouvez pas utiliser la règle d'Analyse 1 sauf pour les corps $\mathbb{R}$ et $\mathbb{C}$.) □

Proposition 7.4. *Soient K un corps, $\overline{K}$ une clôture algébrique et $f \in K[X]$ de degré ≥ 1.*

(a) Soit $a \in \overline{K}$ une racine de f. Alors, les assertions suivantes sont équivalentes :
- *(i) La multiplicité de a est $r > 1$.*
- *(ii) $f'(a) = 0$.*
- *(iii) $\mathrm{pgcd}_{K[X]}(f, f')(a) = 0$.*

(b) Soit f irréductible. Alors, les assertions suivantes sont équivalentes :
- *(i) f est séparable.*
- *(ii) $f' \neq 0$ (polynôme constant 0).*

Démonstration. (a) Soit $f(X) = c\prod_{i=1}^{d}(X - a_i)$ avec $a_i \in \overline{K}$ et $a = a_1 = a_2 = \cdots = a_r$ et $a \neq a_i$ pour $i > r$. On a

$$f'(X) = c\sum_{j=1}^{d}\prod_{i=1, i\neq j}^{d}(X - a_i).$$

Notez que par le lemme 7.3 le pgcd peut être calculé dans $\overline{K}[X]$, où il est évident. Les équivalences sont donc claires.

(b) « (i) ⇒ (ii) » : Si f est séparable, par (a) on a $\mathrm{pgcd}_{K[X]}(f, f')(a) \neq 0$ pour toute racine a de f (dans $\overline{K}$). Donc $f' \neq 0$.

« (ii) $\Rightarrow$ (i) » : Comme $f' \neq 0$ et $\deg(f') < \deg(f)$ et f est irréductible, on a $\mathrm{pgcd}_{K[X]}(f, f') = 1$, car le pgcd est un diviseur de f et de f'. Donc par (a) la multiplicité de toute racine a est 1 et donc f est séparable. □

Définition 7.5. *Un corps K est appelé* parfait *si tout polynôme irréductible $f \in K[X]$ est séparable.*

Exemple 7.6.
- *Tout corps de caractéristique 0 est parfait.*
  Raison : Pour $f \in K[X]$ de degré ≥ 1, on a toujours $f' \neq 0$ (le degré diminue par 1).
- *Tout corps algébriquement clos est parfait.*
  Raison : Les seuls polynômes irréductibles sont linéaires et donc trivialement séparables.
- *Le corps $\mathbb{F}_p(T) = \mathrm{Frac}(\mathbb{F}_p[T])$ n'est pas parfait.*
  Raison : Le polynôme $X^p - T \in \mathbb{F}_p(T)[X]$ est irréductible et inséparable.

Définition 7.7. *Soit L/K une extension algébrique de corps.*

(a) On appelle $a \in L$ séparable sur K *si son polynôme minimal $\mathrm{mipo}_a(X) \in K[X]$ sur K est séparable.*

(b) On appelle L/K séparable *si tout $a \in L$ est séparable sur K.*

(c) Soit $\overline{K}$ une clôture algébrique de K. On pose

$$[L : K]_s := \#\mathrm{Hom}_K(L, \overline{K})$$

et on l'appelle le degré de séparabilité de l'extension L/K.

Noter que $[L : K]_s$ est indépendant du choix de $\overline{K}$ car toute autre clôture algébrique de K est K-isomorphe à la clôture $\overline{K}$ que nous avons choisie.

Lemme 7.8. *Soit K un corps, $\overline{K}$ une clôture algébrique de K, $a \in \overline{K}$ et $f := \mathrm{mipo}_a \in K[X]$ son polynôme minimal sur K. Alors :*

(a) $[K(a) : K]_s$ est égal au nombre de zéros de f dans $\overline{K}$, donc $[K(a) : K]_s \leq [K(a) : K]$.

(b) a est séparable sur $K \Leftrightarrow [K(a) : K] = [K(a) : K]_s$.

Démonstration. Immédiat à cause de la bijection

$$\{ \text{ racines de } f \text{ dans } \overline{K}\} \longrightarrow \mathrm{Hom}_K(K(a), \overline{K}).$$

□

Proposition 7.9. *Soient $M/L/K$ des extensions algébriques de corps. Le degré de séparabilité est multiplicatif :*

$$[M : K]_s = [M : L]_s \cdot [L : K]_s.$$

Démonstration. Soient $\overline{K}$ une clôture algébrique de K et

$$\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_i \mid i \in I\} \quad \text{et} \quad \mathrm{Hom}_L(M, \overline{K}) = \{\tau_j \mid j \in J\}.$$

On suppose que le premier ensemble est en bijection avec I et le deuxième en bijection avec J. Pour tout $i \in I$ on choisit une prolongation $\overline{\sigma}_i : \overline{K} \to \overline{K}$ de σ_i (possible par la proposition 6.11).

Soient $i, k \in I$ et $j, \ell \in J$ tels que $\overline{\sigma}_i \circ \tau_j = \overline{\sigma}_k \circ \tau_\ell$. On montre : $i = k$ et $j = \ell$.

Comme $\tau_j|_L = \tau_\ell|_L = \mathrm{id}_L$ on obtient d'abord $\sigma_i = \overline{\sigma}_i|_L = \overline{\sigma}_k|_L = \sigma_k$, donc $i = k$. On multipliant l'égalité $\overline{\sigma}_i \circ \tau_j = \overline{\sigma}_i \circ \tau_\ell$ par $\overline{\sigma}_i^{-1}$ on voit $\tau_j = \tau_\ell$, donc $j = \ell$.

Nous montrons : $\mathrm{Hom}_K(M, \overline{K}) = \{\overline{\sigma}_i \circ \tau_j \mid i \in I, j \in J\}$. Par ce qui précède cet ensemble est en bijection avec $I \times J$; nous obtenons donc l'assertion de la proposition.

L'inclusion « $\supseteq$ » est évidente. Regardons l'autre « $\subseteq$ ». Soit $\tau \in \mathrm{Hom}_K(M, \overline{K})$. On considère $\tau|_L \in \mathrm{Hom}_K(L, \overline{K})$; donc il existe un $i \in I$ tel que $\tau|_L = \sigma_i$. Notons que $\overline{\sigma}_i^{-1} \circ \tau|_L = \mathrm{id}_L$. Donc $\overline{\sigma}_i^{-1} \circ \tau \in \mathrm{Hom}_L(M, \overline{K})$, donc il existe $j \in J$ tel que $\overline{\sigma}_i^{-1} \circ \tau = \tau_j$, alors $\tau = \overline{\sigma}_i \circ \tau_j$, ce qu'il fallait démontrer. □

Dans la preuve suivante nous allons le fait : *Soient $L/M/K$ des extensions de corps et $a \in L$. Si a est séparable sur K, alors a est séparable sur M.* La raison est la suivante : Soient $f \in K[X]$ et $g \in M[X]$ les polynômes minimaux de a sur K et sur M respectivement. Par hypothèse f est séparable. Comme g est un diviseur de f, alors g est aussi séparable, donc a est séparable sur M.

Proposition 7.10. *Soit L/K une extension finie de corps. Les assertion suivantes sont équivalentes :*

(i) *L/K est séparable.*

(ii) *Il existe des éléments $a_1, \ldots, a_n \in L$ séparables sur K tels que $L = K(a_1, \ldots, a_n)$.*

(iii) $[L : K] = [L : K]_s$.

Démonstration. « (i) $\Rightarrow$ (ii) » : Clair. Tout ensemble fini de générateurs est composé d'éléments séparables.

« (ii) $\Rightarrow$ (iii) » : Le fait précédent, lemme 7.8 et multiplicativité du degré et du degré de séparabilité.

« (iii) $\Rightarrow$ (i) » : Soient $a_1, \ldots, a_n \in L$ tels que $L = K(a_1, \ldots, a_n)$. Les inégalités $[K(a_1) : K]_s \leq [K(a_1) : K]$ et $[K(a_1, \ldots, a_i, a_{i+1}) : K(a_1, \ldots, a_i)]_s \leq [K(a_1, \ldots, a_i, a_{i+1}) : K(a_1, \ldots, a_i)]$ pour $1 \leq i \leq n-1$ provenant du Lemme 7.8 ensemble avec la multiplicativité montre $[L : K]_s \leq [L : K]$ avec égalité si et seulement si tout a_i est séparable pour $i = 1, \ldots, n$. Ceci montre que tout $a_1 \in L$ est séparable sur K. □

Ajoutons encore une version infinie de la proposition précédente.

Proposition 7.11. *Soit L/K une extension algébrique de corps. Elle est séparable si et seulement si elle est engendrée par des éléments séparables sur K.*

Démonstration. Soit $\{a_i\}_{i \in I} \subseteq L$ un ensemble de générateurs séparables (pour un ensemble I). Tout $b \in L$ se trouve déjà dans $K(a_j \mid j \in J) \subseteq L$ pour un sous-ensemble fini $J \subseteq I$. Ce corps est séparable par la proposition 7.10. □

Proposition 7.12 (Existence d'élément primitif)**.** *Soit K un corps infini et L/K une extension finie et séparable. Alors, il existe $a \in L$ tel que $L = K(a)$, donc L est une extension simple de K.*

Noter que le résultat est aussi vrai pour les corps finis ; mais la preuve en est différente (voir la feuille 10).

Démonstration. Soit $\overline{K}$ une clôture algébrique de K. Sans perte de généralité nous pouvons supposer $L = K(b, c)$. Soient $f = \mathrm{mipo}_b$ et $g = \mathrm{mipo}_c$ les polynômes minimaux de b et c sur K et $b = b_1, b_2, \ldots, b_n, c = c_1, c_2, \ldots, c_m \in \overline{K}$ leurs zéros. Nous choisissons $y \in K$ tel que pour tout $1 \leq i \leq n$ et $2 \leq j \leq m$ nous avons $y \neq \frac{b_i - b}{c_j - c}$ (ici on utilise que K contient assez d'éléments) et nous posons $a := b + yc$.

On montre $b, c \in K(a)$, donc $K(a) = K(b, c)$.

Posons $h(X) := f(a - yX) \in K(a)[X]$. On a $h(c) = f(a - yc) = f(b) = 0$. Mais, $h(c_j) \neq 0$ pour tout $2 \leq j \leq m$ pour la raison suivante : Par choix de y nous avons $b_i - b \neq y(c - c_j)$ donc $b_i \neq b + yc - yc_j = a - yc_j$ pour tout $q \leq i \leq n$. Alors, $h(c_j) = f(a - yc_j) \neq 0$ car $a - yc_j$ est différent de toutes les racines de f. Donc, $\mathrm{pgcd}_{K(a)[X]}(h, g) = X - c$, donc $c \in K(a)$, donc $b \in K(a)$. □

Corps finis

Lemme 7.13. *Soit K un corps fini (c'est-à-dire : $\#K < \infty$). Alors :*

(a) $\mathrm{car}(K) = p > 0$*, un nombre premier et l'homomorhpisme naturel $\mathbb{F}_p \to K$ est injectif ; donc on considère K comme une extension de $\mathbb{F}_p$.*

(b) Il existe $n \in \mathbb{N}$ tel que $\#K = p^n$.

(c) $\mathrm{Frob}_p : K \to K, \quad x \mapsto x^p$ *est un homomorphisme de corps, « l'homomorphisme de Frobenius » (voir la définition-lemme 3.5).*

Démonstration. (a) et (c) ont déjà été démontrés.

(b) Comme K est une extension de $\mathbb{F}_p$, c'est un $\mathbb{F}_p$-espace vectoriel de dimension $n = [K : \mathbb{F}_p]$ (forcement finie, car K est finie). Donc $K \cong (\mathbb{F}_p)^n$ en tant que $\mathbb{F}_p$-espace vectoriel. Donc $\#K = p^n$. □

Théorème 7.14. *Soit p un nombre premier et n un nombre naturel. Soit $f(X) := X^{p^n} - X \in \mathbb{F}_p[X]$.*

(a) Si K est un corps de cardinal p^n, alors, K est un corps de décomposition de f sur $\mathbb{F}_p$.

(b) Tout corps de décomposition N de f sur $\mathbb{F}_p$ est un corps de cardinal p^n.

(c) Si K_1 et K_2 sont deux corps de cardinal p^n, alors, ils sont isomorphes. On note $\mathbb{F}_{p^n}$ tout corps de cardinal p^n. (C'est justifié car il est unique à isomorphisme près.)

(d) $\mathbb{F}_{p^n}/\mathbb{F}_p$ est une extension de corps séparable et normale qui est de degré n.

Attention ! Ne pas confondre $\mathbb{F}_{p^n}$ avec $\mathbb{Z}/p^n\mathbb{Z}$. Les deux sont différents dès que $n > 1$.

Démonstration. On fait la preuve en plusieurs étapes.

- La dérivée formelle de f est $f'(X) = -1$, donc $\mathrm{pgcd}(f, f') = 1$. Par la proposition 7.4 (a) tout zéro de f dans N est de multiplicité 1. Donc, f est séparable. En conséquence, $N/\mathbb{F}_p$ est séparable et le nombre de racines distinctes de f dans N est égal au degré du polynôme, donc égal à p^n.
- Soit K est un corps de cardinal p^n. Alors, $K^\times = K \setminus \{0\}$ est un groupe d'ordre $p^n - 1$. Alors pour tout $a \in K^\times$ on a : $a^{p^n - 1} = 1$, donc $a^{p^n} - a = 0$, donc, $f(a) = 0$. Evidemment, $f(0) = 0$. On conclut : $f(a) = 0$ pour tout $a \in K$. Donc, K est égal à l'ensemble des racines de f. On obtient que K est un corps de décomposition de f et donc (a).

- On veut montrer (b) maintenant. Soit N un corps de décomposition de f sur $\mathbb{F}_p$. On pose $R := \{a \in N \mid f(a) = 0\} \subseteq N$. Noter que $\#R = p^n$ à cause de la séparabilité de f.
- On montre que R est un sous-corps de N : Soient $a, b \in R$, donc $a^{p^n} = a$ et $b^{p^n} = b$. Cela implique :
  - $0^{p^n} = 0$ et $1^{p^n} = 1$, donc $0, 1 \in R$;
  - $(a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b$, donc $a + b \in R$;
  - $(-a)^{p^n} = (-1)^{p^n} a^{p^n} = -a$, donc, $-a \in R$ (noter que pour $p = 2$ il n'y a rien à démontrer et pour $p > 2$ on a $(-1)^{p^n} = -1$) ;
  - $(a \cdot b)^{p^n} = a^{p^n} \cdot b^{p^n} = a \cdot b$, donc $a \cdot b \in R$;
  - si $a \neq 0$, alors $\left(\frac{1}{a}\right)^{p^n} = \frac{1}{a^{p^n}} = \frac{1}{a}$, donc $\frac{1}{a} \in R$.
- Donc R est un sous-corps du corps de décomposition de f qui contient toutes les racines de f. Par la définition du corps de décomposition, on conclut $R = N$. Donc, $\#N = p^n$. Cela montre (b).
- (c) L'unicité provient du fait que les corps de décomposition sont unique à isomorphisme près.
- (d) $\mathbb{F}_{p^n}/\mathbb{F}_p$ est normale, car c'est un corps de décomposition, et elle est séparable, car f l'est. Le cardinal implique l'assertion concernant le degré.

□

8 Extensions galoisiennes

Soit L/K une extension normale. On se rappelle que par la Proposition 6.19 tout élément σ de $\mathrm{Hom}_K(L, \overline{L})$ satisfait $\sigma(L) = L$ et donne donc lieu à un K-isomorphisme $L \to L$. On note l'ensemble des K-isomorphismes $L \to L$ par $\mathrm{Aut}_K(L)$. C'est clairement un groupe pour la composition d'applications avec élément neutre l'identité id_L.

Nous avons donc pour L/K une extension finie et normale

$$\#\,\mathrm{Aut}_K(L) = \#\mathrm{Hom}_K(L, \overline{L}) = [L : K]_s \leq [L : K] \tag{8.3}$$

avec égalité si et seuelement si L/K est aussi séparable.

Définition 8.1. *Soit L/K une extension algébrique. Elle est appelée* galoisienne *si elle est normale et séparable. On pose*

$$\mathrm{Gal}(L/K) := G(L/K) := \mathrm{Aut}_K(L)$$

(l'ensemble des K-homomorphisme $L \to L$) et on l'appelle groupe de Galois de L/K.

Lemme 8.2. *Soit L/K une extension galoisienne finie. Alors $\#\,\mathrm{Gal}(L/K) = [L : K]$.*

Démonstration. Conséquence de l'équation (8.3) et de la séparabilité. □

Exemple 8.3. – *$\mathbb{C}/\mathbb{R}$ est une extension galoisienne : elle est normale (par exemple, car le degré est 2) et séparable (par exemple, car la caractéristique est 0).*
$\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, \mathbb{C}) = \{\mathrm{id}_{\mathbb{C}}, c\}$ *où c est la conjugaison complexe.*

– *Soit $\mathbb{N} \ni d \neq 0, 1$ un nombre qui n'est pas un carré de façon que $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ est une extension de degré 2 qui est galoisienne. Nous avons :*

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$$

où σ est déterminé uniquement par $\sigma(\sqrt{d}) = -\sqrt{d}$.

– *Soient p un nombre premier et $\zeta_p := e^{2\pi i/p}$. On pose $K := \mathbb{Q}(\zeta_p)$ (le p-ième corps cyclotomique). Alors $K/\mathbb{Q}$ est une extension galoisienne. Son groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ est cyclique d'ordre $p-1$.*
En effet : Nous connaissons le polynôme minimal de ζ_p sur $\mathbb{Q}$. C'est le p-ième polynôme cyclotomique $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + 1 \in \mathbb{Q}[X]$. Ses racines sont toutes les puissance ζ_p^j pour $j = 1, 2, \ldots, p-1$. Donc il est clair que $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ est galoisienne.
Donc, nous pouvons directement écrire $p-1$ homomorphismes $K \to K$:

$$\sigma_j : K \to K \text{ déterminé uniquement par } \sigma_j(\zeta_p) = \zeta_p^j$$

pour $j \in \{1, 2, \ldots, p-1\}$ et comme le cardinal de $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ est $p-1$, nous avons trouvé les éléments de ce groupe.
*Il faut encore voir que le groupe est cyclique. On se rappelle que $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times$ est cyclique. Nous définissons le p-*ième caractère cyclotomique *:*

$$\chi_p : \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to (\mathbb{Z}/p\mathbb{Z})^\times$$

comme suit : Soit $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Nous avons $\tau(\zeta_p) = \zeta_p^{\chi(\tau)}$ pour un $\chi(\tau) \in (\mathbb{Z}/p\mathbb{Z})^\times$. Cette application est clairement bijective. On calcule qu'il s'agit d'un homomorphisme (donc d'un isomorphisme) de groupes :

$$\zeta_p^{\chi(\tau_1\tau_2)} = \tau_1(\tau_2(\zeta_p)) = \tau_1(\zeta_p^{\chi(\tau_2)}) = \big(\tau_1(\zeta_p)\big)^{\chi(\tau_2)} = \big(\zeta_p^{\chi(\tau_1)}\big)^{\chi(\tau_2)} = \zeta_p^{\chi(\tau_1)\chi(\tau_2)}.$$

Dans les exercices vous allez voir que ce même résultat est valable pour tout entier positif n et pas seulement pour les nombres premiers p.

– *Soit $\zeta_3 = e^{2\pi i/3}$. On considère l'extension $K := \mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ qui est galoisienne (la séparabilité est claire car nous sommes en caractéristique 0, et la normalité a été montrée dans un exemple précédent). Son degré est 6. On va maintenant calculer les éléments de son groupe de Galois $\mathrm{Gal}(K/\mathbb{Q})$.*
On va d'abord prolonger l'identité $\mathbb{Q} \hookrightarrow \mathbb{C}$ à $K' := \mathbb{Q}(\zeta_3)$; c'est un cas spécial de l'exemple précédent : le polynôme minimal de ζ_3 est $X^2 + X + 1 \in \mathbb{Q}[X]$ et ses deux racines sont ζ_3 et ζ_3^2. Donc nous avons deux prolongations

$$\sigma_i : \mathbb{Q}(\zeta_3) \to \mathbb{C}$$

données par $\sigma_1(\zeta_3) = \zeta_3$ et $\sigma_2(\zeta_3) = \zeta_3^2$. (On sait que $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ est galoisienne, mais nous n'allons pas utiliser ce fait.)
Le polynôme $X^3 - 2$ reste irréductible sur $\mathbb{Q}(\zeta_3)[X]$ (par exemple, par la multiplicativité des degrés et le fait que 2 et 3 sont premiers entre eux). Donc pour tout $i \in \{1, 2\}$ nous pouvons prolonger σ_i à $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ de trois manières qui sont déterminées par :

$$\sigma_{i,1}(\sqrt[3]{2}) = \sqrt[3]{2}, \quad \sigma_{i,2}(\sqrt[3]{2}) = \zeta_3\sqrt[3]{2}, \quad \sigma_{i,3}(\sqrt[3]{2}) = \zeta_3^2\sqrt[3]{2}.$$

Par la normalité de $\mathbb{Q}(\sqrt[3]{2},\zeta_3)/\mathbb{Q}$ ces $\mathbb{Q}$-homomorphismes donnent des éléments dans le groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\zeta_3)/\mathbb{Q})$. Nous avons donc calculé les éléments du groupe de Galois. Notons encore que $\sigma_{1,1}$ est l'identité.

- *Soit K un corps fini de caractéristique p et de cardinal p^n. Nous avons vu dans la section précédente que $K/\mathbb{Q}_p$ est séparable et normale, donc, galoisienne. Son degré est n.*
  Nous calculons le groupe de Galois $\mathrm{Gal}(K/\mathbb{F}_p)$. Pour cela on se rappelle du Frobenius $\mathrm{Frob}_p : K \to K$ donné par $x \mapsto x^p$; c'est un automorphisme de corps.
  Nous savons que $\mathrm{Frob}_p^n = \mathrm{id}_K$. On veut montrer que n est l'ordre de Frob_p. Soit $1 \leq i < n$; supposons que $\mathrm{Frob}_p^i = \mathrm{id}$. Alors, tout élément de K satisfait $x^{p^i} = x$, donc $K \subseteq \mathbb{F}_{p^i}$, ce qui est une contradiction. Donc, l'ordre de Frob_p est bien n.
  Nous pouvons conclure que $\mathrm{Gal}(K/\mathbb{F}_p)$ est un groupe cyclique d'ordre p engendré par Frob_p.
- *Soit K un corps et $f \in K[X]$ un polynôme irréductible et séparable. Alors le corps de décomposition L de f sur K est une extension galoisienne de K.*
  Raison : Elle est normale, est elle est engendré par les racines de f, donc par des éléments séparables. Nous nous rappelons que nous avons vu que les extensions engendrées par des éléments séparables sont séparables.

Lemme 8.4. *Soient $L/E/K$ des extensions de corps telles que L/K est galoisienne. Alors :*

(a) L/E est galoisienne et $\mathrm{Gal}(L/E)$ est le sous-groupe de $\mathrm{Gal}(L/K)$ composé des ces éléments de $\mathrm{Gal}(L/K)$ qui sont des E-homomorphismes (c'est-à-dire, $\sigma(e) = e$ pour tout $e \in E$).

(b) Si E/K est aussi galoisienne (ce qui n'est pas automatique !), alors l'application

$$\pi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K), \quad \sigma \mapsto \sigma|_E$$

est un homomorphisme de groupes qui est surjectif. Son noyau est égal à $\mathrm{Gal}(L/E)$.

Démonstration. (a) Nous avons vu les deux propriétés : normale (proposition 6.21) et séparable (appliquer la proposition 7.10). Nous avons

$$\mathrm{Gal}(L/E) = \mathrm{Aut}_E(L) \subseteq \mathrm{Aut}_K(L) = \mathrm{Gal}(L/K).$$

(b) Comme E/K est supposée normale, pour tout K-homomorphisme $\sigma : L \to L$ on a toujours $\sigma(E) = E$. Donc $\sigma|_E \in \mathrm{Gal}(E/K)$, et l'application π est bien définié. Il est clair que π est un homomorphisme.

On montre la surjectivité : Soit $\tau \in \mathrm{Gal}(E/K)$. En utilisant la proposition 6.11 on prolonge l'application

$$E \xrightarrow{\tau} E \hookrightarrow L \hookrightarrow \overline{L}$$

en un K-homomorphisme $\tilde{\tau} : L \to \overline{L}$. La normalité de L/K implique que $\tilde{\tau}(L) = L$, donc $\tilde{\tau}|_L \in \mathrm{Gal}(L/K)$ et satisfait $\pi(\tilde{\tau}) = \tau$.

Pour calculer le noyau de π, soit $\sigma \in \mathrm{Gal}(L/K)$. Par définition $\pi(\sigma) = \sigma|_E = \mathrm{id}_E$ si et seulement si $\sigma \in \mathrm{Gal}(L/E)$. □

Définition-Lemme 8.5. *Soit L un corps et $G \subseteq \mathrm{Aut}(L)$. On pose $L^G := \{x \in L \mid \forall\, \sigma \in G :\ \sigma(x) = x\ \}$. C'est un corps qui est appelé* le sous-corps de L fixé par G *ou* le sous-corps des G-invariants de L.

Démonstration. Facile à vérifier. □

Proposition 8.6. *Soit L un corps, $G \subseteq \mathrm{Aut}(L)$ un groupe fini et $K := L^G$. Alors L/K est une extension galoisienne avec $\mathrm{Gal}(L/K) = G$.*

Démonstration. Cette preuve se fait en plusieurs étapes :

- Notons que $G \leq \mathrm{Aut}_K(L)$. Nous avons par l'égalité (8.3) :

$$n := \#G \leq \#\,\mathrm{Aut}_K(L) \leq [L : K].$$

- Soit $a \in L$. On va construire un polynôme séparable dans $K[X]$ qui annulle a.
  On le fait comme suit : Soit $S := \{\sigma(a) \mid \sigma \in G\} = \{a = a_1, a_2, \ldots, a_r\}$; c'est un ensemble fini, car G est fini ; il contient a, car $\mathrm{id}_L \in G$. On pose

$$f_a(X) := \prod_{i=1}^{r}(X - \tau(a_i)) \in L[X].$$

  Il est clair que $f_a(a) = 0$ et qu'il est séparable Il faut donc montrer que les coefficients de f appartiennent à K. Soit $\tau \in G$. Noter que l'application $S \to S$, donnée par $a \mapsto \tau(a)$ est une bijection (car $G \to G$, donnée par $\sigma \mapsto \tau\sigma$ est une bijection). On calcule

$$\tau(f_a(X)) = \prod_{i=1}^{r}(X - \tau(a_i)) = \prod_{i=1}^{r}(X - a_i) = f_a(X),$$

  où la deuxième égalité est due à la bijection précédente (les facteurs du polynôme sont permutés mais pas changés !). De l'égalité $\tau(f_a) = f_a$ pour tout $\tau \in G$ on conclut que $f \in K[X]$.
- Nous trouvons donc que tout élément $a \in L$ est séparable. Donc L/K est séparable. En plus L/K est normale parce que L est un corps de décomposition de la famille $\{f_a\}_{a\in L}$. Donc L/K est une extension galoisienne.
- Soit $a \in L$ un élément primitif qui existe à cause de la proposition 7.12. Le polynôme minimal $g_a := \mathrm{mipo}_a \in K[X]$ de a sur K divise f_a. Donc nous avons $[L : K] = \deg(g_a) \leq \deg(f_a) = r \leq n$.
- En comparant avec la prémière inégalité en haut, nous trouvons

$$G = \mathrm{Aut}_K(L) = \mathrm{Gal}(L/K).$$

□

En fait, la preuve donne une manière d'écrire le polynôme minimal (voir exercices).

Corollaire 8.7. *Soit L/K une extension normale et $G := \mathrm{Aut}_K(L)$ soit fini. Alors :*

(a) *L/L^G est une extensions galoisienne avec $\mathrm{Gal}(L/L^G) = G$.*

(b) *$[L^G : K]_s = 1$.*

(c) *Si L/K est séparable (donc galoisienne), alors $K = L^G$.*

Démonstration. (a) C'est encore une fois l'assertion de la proposition 8.6.

(b) Il est clair que $K \leq L^G$. Nous avons la chaine d'inclusions

$$G = \mathrm{Gal}(L/L^G) = \mathrm{Aut}_{L^G}(L) \leq \mathrm{Aut}_K(L) = G,$$

donc nous avons l'égalité partout.

Soit $\overline{K}$ une clôture algébrique de K. Soit $\sigma : L^G \to \overline{K}$ un K-homomorphisme. On peut le prolonger à un K-homomorphisme $\tilde{\sigma} : L \to \overline{K}$ à cause de la proposition 6.11. La normalité de L/K implique $\tilde{\sigma}(L) = L$, donc $\tilde{\sigma} \in \mathrm{Aut}_K(L)$. On conclut $\tilde{\sigma} \in \mathrm{Aut}_{L^G}(L)$. Alors, $\tilde{\sigma}|_{L^G} = \sigma = \mathrm{id}_{L^G}$. Donc, $\mathrm{Hom}_K(L^G, \overline{K}) = \{\mathrm{id}_{L^G}\}$ et alors $[L^G : K]_s = 1$.

(c) Comme L/K est séparable, alors L^G/K l'est aussi. Donc $[L^G : K]_s = [L^G : K] = 1$ et $L^G = K$. □

Théorème 8.8 (Théorème principal de la théorie de Galois)**.** *Soient L/K une extension galoisienne finie et $G := \mathrm{Gal}(L/K)$. Alors :*

(a) Les applications

$$\begin{array}{ccc} \{\text{ Sous-groupes de } G\} & \overset{\Phi}{\underset{\Psi}{\rightleftarrows}} & \{\text{ Corps } E \text{ tels que } L/E/K\}, \\ H & \overset{\Phi}{\longmapsto} & L^H \\ \mathrm{Gal}(L/E) & \overset{\Psi}{\longmapsto} & E \end{array}$$

sont des bijections.

(b) Soit $H \leq G$ un sous-groupes. Les assertions suivantes sont équivalentes :

(i) $H \lhd G$ est un sous-groupe normal.

(ii) L^H/K est une extension normale (donc galoisienne).

(c) Si L^H/K est normale, alors l'application

$$\pi : G \to \mathrm{Gal}(L^H/K), \quad \sigma \mapsto \sigma|_{L^H}$$

induit un isomorphisme de groupes $G/H \cong \mathrm{Gal}(L^H/K)$.

Démonstration. (a) On vérifie $\Phi \circ \Psi = \mathrm{id}$ et $\Psi \circ \Phi = \mathrm{id}$.

Soit E un corps tel que $L/E/K$. Alors :

$$\Phi(\Psi(E)) = \Phi(\mathrm{Gal}(L/E)) = L^{\mathrm{Gal}(L/E)} = E,$$

où la dernière égalité est due au corollaire 8.7 (c).

Soit $H \leq G$ un sous-groupe. Alors :

$$\Psi(\Phi(H)) = \Psi(L^H) = \mathrm{Gal}(L/L^H) = H,$$

où la dernière égalité a été démontrée dans le corollaire 8.7 (a).

(b) On fait d'abord un petit calcul : Soit $\sigma \in G$ et $H \leq G$ un sous-groupe. Alors

$$\sigma(L^H) = L^{\sigma H \sigma^{-1}}.$$

En effet : $a \in \sigma(L^H) \Leftrightarrow \sigma^{-1}(a) \in L^H \Leftrightarrow h \circ \sigma^{-1}(a) = \sigma^{-1}(a)$ pour tout $h \in H \Leftrightarrow \sigma \circ h \circ \sigma^{-1}(a) = a$ pour tout $h \in H \Leftrightarrow a \in L^{\sigma H \sigma^{-1}}$.

Nous pouvons maintenant démontrer l'assertion ainsi :

$$\begin{aligned} L^H \quad &\overset{\text{prop. 6.19}}{\Leftrightarrow} \quad \sigma(L^H) = L^H \quad \forall\, \sigma \in G \\ &\Leftrightarrow \quad L^{\sigma H \sigma^{-1}} = L^H \quad \forall\, \sigma \in G \\ &\overset{\text{(a)}}{\Leftrightarrow} \quad H = \sigma H \sigma^{-1} \quad \forall\, \sigma \in G \\ &\overset{\text{déf.}}{\Leftrightarrow} \quad H \lhd G \text{ est un sous-groupe normal.} \end{aligned}$$

(c) Le lemme 8.4 nous donne pour le corps L^H et le théorème d'isomorphismes :

$$G/H \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/L^H) \xrightarrow{\pi\ \sim} \mathrm{Gal}(L^H/K).$$

□

Exemple 8.9. – *Soit L/K une extension galoisienne dont le groupe de Galois $G = \mathrm{Gal}(L/K)$ est cyclique d'ordre 6, donc isomorphe à $\mathbb{Z}/6\mathbb{Z}$. La liste des sous-groupe complète de $\mathbb{Z}/6\mathbb{Z}$ est la suivante : $\{0\}, 3\mathbb{Z}/6\mathbb{Z}, 2\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}$. Donc il y a 4 sous-corps de L/K dont les degrés sur K sont 6, 3, 2, 1.*

– *Nous avons déjà calculé le groupe de Galois de $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}$.*
On calcule maintenant tous les sous-corps de $K := \mathbb{Q}(\zeta_3, \sqrt[3]{2})$. Un résultat de la feuille 11 dit que le groupe de Galois $G := \mathrm{Gal}(K/\mathbb{Q})$ est le groupe symétrique S_3.
Plus précisement : Nous prenons les deux homomorphismes : $\sigma, \tau : K \to K$ définis uniquement par :

$$\sigma(\zeta_3) = \zeta_3^2, \quad \sigma(\sqrt[3]{2}) = \sqrt[3]{2}, \quad \tau(\zeta_3) = \zeta_3, \quad \tau(\sqrt[3]{2}) = \zeta_3 \sqrt[3]{2}.$$

L'ordre de σ est 3 et l'ordre de τ est 2. Ces deux éléments engendrent G. Voici la liste des sous-groupes de G et des corps fixés par ces groupes.
  – *$H := \{\mathrm{id}\}$, $K^H = K$.*
  – *$H := G$, $K^H = \mathbb{Q}$.*
  – *$H := \langle\tau\rangle \lhd G$ est un sous-groupe normal (car l'indice est 2 ; c'est le groupe alterné $A_3 \lhd S_3$), $K^H = \mathbb{Q}(\zeta_3)$.*
  – *$H := \langle\sigma\rangle \leq G$, $K^H = \mathbb{Q}(\sqrt[3]{2})$.*
  – *$H := \langle\tau\sigma\tau^{-1}\rangle \leq G$, $K^H = \tau(\mathbb{Q}(\sqrt[3]{2})) = \mathbb{Q}(\tau(\sqrt[3]{2})) = \mathbb{Q}(\zeta_3\sqrt[3]{2})$.*
  – *$H := \langle\tau^2\sigma\tau^{-2}\rangle \leq G$, $K^H = \tau^2(\mathbb{Q}(\sqrt[3]{2})) = \mathbb{Q}(\tau^2(\sqrt[3]{2})) = \mathbb{Q}(\zeta_3^2\sqrt[3]{2})$.*

– *Soit K un corps fini de caractéristique p et de cardinal p^n. Nous avons vu que $\mathrm{Gal}(K/\mathbb{F}_p)$ est cyclique d'ordre n engendré par le Frobenius Frob_p.*
Donc $\mathrm{Gal}(K/\mathbb{F}_p)$ est isomorphe au groupe $\mathbb{Z}/n\mathbb{Z}$. Les sous-groupes sont précisement donnés par $a\mathbb{Z}/n\mathbb{Z}$ pour $a \mid n$. La théorie de Galois nous redonne donc le résultat que les sous-corps de $\mathbb{F}_{p^n}$ sont précisement $\mathbb{F}_{p^n}^{\langle \mathrm{Frob}_p^a \rangle} = \mathbb{F}_{p^a}$ pour les diviseurs a de n.

– *Soit L/K une extension finie de corps finis. Soit p^n le cardinal de L. Donc L/K est une extension galoisienne de groupe de Galois cyclique $\langle \mathrm{Frob}_p^a \rangle$ où p^a est le cardinal de K.*

Voici un corollaire simple mais pas évident !

Corollaire 8.10. *Soit L/K une extension séparable et fini. Alors, l'ensemble $\{E \text{ corps} \mid L/E/K\}$ est fini.*

Démonstration. Sans perte de généralité nous pouvons remplacer L par une clôture normale. Donc, on peut supposer que L/K est une extension galoisienne. Il est clair que son groupe de Galois $\mathrm{Gal}(L/K)$ qui est un groupe fini ne possède qu'un nombre fini de sous-groupes (déjà l'ensemble des sous-ensembles de G est fini). Donc par le théorème 8.8 il n'existe qu'un nombre fini de corps E tels que $L/E/K$. □

Proposition 8.11. *Soit L/K une extension de corps. Soient $L/L_1/K$ et $L/L_2/K$ des extensions telles que L_1/K et L_2/K sont galoisiennes et finies.*

(a) Le corps $L_1L_2 := K(L_1, L_2)$ (extension de K dans L engendrée par les éléments de L_1 et L_2) est une extension galoisienne et finie de K.

(b) La restriction

$$\mathrm{Gal}(L_1L_2/L_2) \to \mathrm{Gal}(L_1/(L_1 \cap L_2)), \quad \sigma \mapsto \sigma|_{L_1}$$

est un isomorphisme de groupes.

(c) L'application

$$\varphi : \mathrm{Gal}(L_1L_2/K) \to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K), \quad \sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2})$$

est un homomorphisme de groupes injectif d'image

$$\mathrm{im}(\varphi) = \{(\sigma, \tau) \in \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) \mid \sigma|_{L_1 \cap L_2} = \tau|_{L_1 \cap L_2}\}.$$

Démonstration. Exercice. □

Définition 8.12. *Une extension galoisienne L/K est appelée* abélien (cyclique) *si $\mathrm{Gal}(L/K)$ est abélien (cyclique).*

Corollaire 8.13. *Soient L_1/K et L_2/K deux extensions abéliennes contenu dans un corps L. Alors, L_1L_2/K est aussi une extension abélienne.*

Démonstration. $\mathrm{Gal}(L_1L_2/K)$ est un sous-groupe de $\mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$ qui est abélien (par la proposition 8.11), donc $\mathrm{Gal}(L_1L_2/K)$ est abélien. □

9 Résolubilité par radicaux

Dans cette section nous regardons la motiviation de Galois pour sa théorie, la résolubilité des équations polynômiaux par radicaux.

– $f(X) := X^2 + aX + b \in \mathbb{Q}[X]$. Nous avons

$$f(x) = 0 \Leftrightarrow x = \frac{1}{2}(-a \pm \sqrt{a^2 - 4b}),$$

donc les racines de f peuvent être exprimées par des expressions « radicales », autrement dit, les racines de f appartiennent à une extension de $\mathbb{Q}$ qui peut être engendrée par des radicaux.

– $f(X) := X^3 + 3aX + 2b \in \mathbb{Q}[X]$. Soit $\zeta := \zeta_3 := e^{2\pi i/3}$. Nous avons

$$f(x) = 0 \Leftrightarrow x = u + v \text{ ou } x = \zeta^2 u + \zeta v \text{ ou } x = \zeta u + \zeta^2 v,$$

où $u = \sqrt[3]{-b + \sqrt{b^2 + a^3}}$ et $v = \sqrt[3]{-b - \sqrt{b^2 + a^3}}$. Donc ici aussi les racines de f peuvent être exprimées par des expressions « radicales », autrement dit, les racines de f appartiennent à une extension de $\mathbb{Q}$ qui peut être engendrée par des radicaux.

– Il existe aussi une formule en termes de radicaux pour les polynômes de degré 4.

Définition 9.1. *Soit K un corps parfait.*

(a) Une extension finie L/K s'appelle résoluble par radicaux *s'il existe des corps*

$$K = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n$$

tels que

– *$L \subseteq E_n$ et*

– *pour tout $1 \leq i \leq n$ il existe $a_i \in E_{i-1}$ et $n_i \in \mathbb{N}$ tels que $E_i = E_{i-1}(\sqrt[n_i]{a_i})$ ou $E_i = E_{i-1}(\zeta_{n_i})$.*

(b) Une équation polynômielle $f(x) = 0$ avec $f(X) \in K[X]$ s'appelle résoluble par radicaux sur K *si un corps de décomposition de f sur K est résoluble par radicaux sur K.*

Cela veut dire que les racines de f (qui appartiennent, comme on le sait, au corps de décomposition) peuvent être exprimées par des radicaux.

Définition-Lemme 9.2. *Soient K un corps parfait et $n \in \mathbb{N}_{>0}$. Soit μ_n l'ensemble des racines (dans une clôture algébrique $\overline{K}$ de K) du polynôme $X^n - 1 \in K[X]$. On appelle μ_n* le groupe des n-ièmes racines d'unités. *C'est un groupe cyclique (pour la multiplication de K).*

Alors $K(\mu_n)$ est galoisien sur K et le groupe de Galois $\mathrm{Gal}(K(\mu_n)/K)$ est un groupe abélien. On appelle $K(\mu_n)$ la n-ième extension cyclotomique de K.

Démonstration.

– μ_n est un groupe : Soient $a, b \in \mu_n$, donc $a^n = b^n = 1$. Alors, $\left(\frac{a}{b}\right)^n = \frac{a^n}{b^n} = 1$, donc $\frac{a}{b} \in \mu_n$. On en conclut que μ_n est un groupe.

– Que μ_n est cyclique provient de l'exercice 1(b) de la feuille 9 qui dit que tout sous-groupe fini de $K^\times$ est cyclique.

– L'extension $K(\mu_n)/K$ est galoisienne : séparable car K est parfait et normale car c'est le corps de décomposition du polynôme $X^n - 1 \in K[X]$.

– L'application

$$\phi : \mathrm{Gal}(K(\mu_n)/K) \to \mathrm{Aut}(\mu_n), \quad \sigma \mapsto (\zeta \mapsto \sigma(\zeta))$$

est un homomorphisme de groupes injectif. Ici, $\mathrm{Aut}(\mu_n)$ est l'ensemble des automorphismes du groupe μ_n, c'est-à-dire l'ensemble des isomorphismes de groupes $\mu_n \to \mu_n$.
Cette assertion est claire.

– $\mathrm{Aut}(\mu_n)$ est un groupe abélien : Comme μ_n est cyclique, on peut choisir un générateur $\zeta \in \mu_n$ et tout automorphisme $\sigma \in \mathrm{Aut}(G)$ est uniquement déterminé par $\sigma(\zeta)$. On a $\sigma(\zeta) = \zeta^m$ pour un $m \in \mathbb{N}$. Le groupe est abélien car la composition de deux automorphismes multiplie les exposantes, et la multiplication dans $\mathbb{Z}$ est commutative.

□

Lemme 9.3. *Soient K un corps parfait, $a \in K$ et $n \in \mathbb{N}_{>0}$. Soit $L := K(\sqrt[n]{a})$. On suppose que K contient μ_n.*

Alors l'extension L/K est galoisienne et le groupe de Galois $\mathrm{Gal}(L/K)$ est un sous-groupe de μ_n et donc cyclique (et abélien).

Démonstration. L'extension L/K est galoisienne, car elle est séparable (comme K est parfait) et normale (c'est un corps de décomposition de $X^n - a$; ici on utilise que μ_n appartient à K). On définit l'application de Kummer

$$\psi : \mathrm{Gal}(L/K) \to \mu_n, \quad \sigma \mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}.$$

Elle est clairement injective car les K-homomorphisme $L \to L$ sont déterminé par l'image de $\sqrt[n]{a}$. C'est un homomorphisme de groupes :

$$\psi(\sigma \circ \tau) = \frac{\sigma(\tau(\sqrt[n]{a}))}{\sqrt[n]{a}} = \frac{\sigma(\psi(\tau)\sqrt[n]{a})}{\sqrt[n]{a}} = \psi(\tau)\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} = \psi(\tau)\psi(\sigma) = \psi(\sigma)\psi(\tau)$$

où on a utilisé que τ agit trivialement sur μ_n, donc sur l'image de ψ. □

Lemme 9.4. *Soit K un corps parfait tel que $\mu_n \subseteq L$. Soient L/K une extension galoisienne avec groupe de Galois $G := \mathrm{Gal}(L/K)$ et $a \in L$. Soit N/K la clôture normale (donc galoisienne) sur K de $L(\sqrt[n]{a})$ (qui est vu comme un sous-corps d'une clôture algébrique de L).*

Alors, N/L est une extension abélienne.

Démonstration. On définit le polynôme

$$f(X) := \prod_{\sigma \in G} (X^n - \sigma(a)) \in L[X].$$

Comme il est clairement invariant par tout $\tau \in G$, il en suit que $f \in K[X]$. La clôture normale N de $L(\sqrt[n]{a})$ sur K est le corps de décomposition de f sur K, car il est normal et tous les $\sqrt[n]{\sigma(a)}$ doivent y appartenir pour $\sigma \in G$.

Comme $\mu_n \subseteq K$ on peut donc voir N comme le compositum de tous les corps $L(\sqrt[n]{\sigma(a)})$ pour $\sigma \in G$. Par le corollaire 8.13 et le lemme 9.3 on obtient qu'en effet N/L est abélienne. □

Définition 9.5. *Soit G un groupe fini. On l'appelle* résoluble *s'il existe une suite de sous-groupes*

$$G_n = \{1\} \leq G_{n-1} \leq G_{n-2} \leq \cdots \leq G_1 \leq G_0 = G$$

telle que

- *pour tout $1 \leq i \leq n$ on a $G_i \lhd G_{i-1}$ (sous-groupe normal) et*
- *G_{i-1}/G_i est un groupe abélien.*

Théorème 9.6. *Soient K un corps parfait et L/K une extension finie qui est résoluble par radicaux. Alors, il existe une extension finie et galoisienne N/K telle que*

- *$L \subseteq N$ et*
- *le groupe de Galois $\mathrm{Gal}(N/K)$ est résoluble.*

Démonstration. Par définition nous avons des corps

$$K = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n$$

tels que

- $L \subseteq E_n$ et
- pour tout $1 \leq i \leq n$ il existe $a_i \in E_{i-1}$ et $n_i \in \mathbb{N}$ tels que $E_i = E_{i-1}(\sqrt[n_i]{a_i})$ ou $E_i = E_{i-1}(\zeta_{n_i})$.

On pose $M := \operatorname{ppcm}(n_i \mid 0 \leq i \leq n)$ et on définit $L_0 := K(\mu_M)$ (et $L_{-1} := K$). Notez que $\mu_{n_i} \subseteq L_0$ pour tout $0 \leq i \leq n$ et que L_0/K est une extension abélienne par la définition-lemme 9.2. Pour tout $1 \leq i \leq n$ on définit récursivement L_i comme la clôture galoisienne sur K de $L_{i-1}E_i$. Par le lemme 9.4 L_i/L_{i-1} est abélienne, c'est-à-dire $\operatorname{Gal}(L_i/L_{i-1})$ est abélienne.

Le corps recherché est $N := L_n$. Par construction nous avons

$$\operatorname{Gal}(L_n/L_n) \trianglelefteq \operatorname{Gal}(L_n/L_{n-1}) \trianglelefteq \operatorname{Gal}(L_n/L_{n-2}) \trianglelefteq \cdots \trianglelefteq \operatorname{Gal}(L_n/L_0) \trianglelefteq \operatorname{Gal}(L_n/L_{-1})$$

et tous les quotients $\operatorname{Gal}(L_n/L_{i-1})/\operatorname{Gal}(L_n/L_i) \cong \operatorname{Gal}(L_i/L_{i-1})$ pour $0 \leq i \leq n$ sont des groupes abéliens. Donc $\operatorname{Gal}(L_n/L_{-1}) = \operatorname{Gal}(N/K)$ est un groupe résoluble. □

Remarque 9.7. *Par la théorie de Kummer on peut montrer que l'assertion réciproque tu théorème est également vraie : Si K est un corps parfait et N/K est une extension finie et galoisienne de groupe de Galois résoluble, alors toute extension L/K avec $L \subseteq N$ est résoluble par radicaux.*

Malheureusement, on n'aura pas le temps pour développer ceci.

Proposition 9.8. *Soit K un corps et $L := K(A_1, \ldots, A_n) := \operatorname{Frac}(K[A_1, \ldots, A_n])$ le corps de fonctions à n variables sur K. Le* polynôme général de degré n sur K *est*

$$f(X) := \sum_{i=0}^{n} A_i X^i \in L[X].$$

Soit N un corps de décomposition de f sur L.

Alors, N/L est une extension galoisienne de groupe de Galois $\operatorname{Gal}(N/L) \cong S_n$, le groupe symétrique (des permutations de l'ensemble $\{1, 2, \ldots, n\}$).

Démonstration. Soient $t_1, \ldots, t_n \in N$ tels que

$$f(X) = \prod_{i=1}^{n} (X + t_i) \in N[X].$$

Par l'exercice 6(b) de la feuille 13 l'homomorphisme d'anneaux

$$\psi : K[T_1, \ldots, T_n] \to N, \quad T_i \mapsto t_i$$

est injectif. Il induit le K-isomorphisme

$$\psi : K(T_1, \ldots, T_n) := \operatorname{Frac}(K[T_1, \ldots, T_n]) \to N, \quad T_i \mapsto t_i$$

(la surjectivité est claire).

Donc $f(X)$ est un polynôme séparable car ses racines sont distinctes. On en conclut que N/L est une extension galoisienne.

Soit $\sigma \in \mathrm{Gal}(N/L)$. Il permute les t_i. Pour $i \in \{1, \ldots, n\}$ on définit la permutation $\varphi(\sigma) \in S_n$ par la règle $\sigma(t_i) = t_{\varphi(\sigma)(i)}$. Alors, nous avons l'application

$$\varphi : \mathrm{Gal}(N/K) \to S_n, \quad \sigma \mapsto \varphi(\sigma),$$

qui est injective parce que σ est uniquement déterminé par les images des t_i. C'est un homomorphisme de groupes :

$$t_{\varphi(\sigma\tau)(i)} = \sigma(\tau(t_i)) = \sigma(t_{\varphi(\tau)(i)}) = t_{\varphi(\sigma)(\varphi(\tau)(i))}.$$

Il faut démontrer que φ est un isomorphisme de groupes. Pour tout $\alpha \in S_n$, nous définissons un isomorphisme d'anneaux

$$\sigma : K[T_1, \ldots, T_n] \to K[T_1, \ldots, T_n], \quad g(T_1, \ldots, T_n) \mapsto g(T_{\alpha(1)}, \ldots, T_{\alpha(n)})$$

(l'inverse est donné par l'inverse de la permutation α). On en obtient un K-isomorphisme

$$\sigma : K(T_1, \ldots, T_n) \to K(T_1, \ldots, T_n),$$

et donc un K-isomorphisme $\sigma : L \to L$ via ψ. Par construction nous avons $\varphi(\sigma) = \alpha$. Donc, nous avons démontré la surjectivité de φ. □

Définition 9.9. *Soit G un groupe.*

(a) Soient $a, b \in G$. L'élément $[a, b] := aba^{-1}b^{-1} \in G$ s'appelle le commutateur de a, b.

(b) Soient $H_1, H_2 \leq G$ des sous-groupes.

$$[H_1, H_2] := \langle [a, b] \mid a \in H_1, b \in H_2 \rangle.$$

(c) $DG := G' := [G, G]$ s'appelle le sous-groupe des commutateurs de G.

(d) Pour $i \geq 0$ on définit $D^iG := \underbrace{DD \ldots D}_{i\text{-fois}} G$.

Proposition 9.10. *Soit G un groupe.*

(a) $[G, G] \trianglelefteq G$ est un sous-groupe normal.

(b) Pour tout $N \trianglelefteq G$ sous-groupe normal :

$$G/N \text{ est abélien } \Leftrightarrow [G, G] \subseteq N.$$

(c) Les assertions suivantes sont équivalentes :

(i) G est résoluble.

(ii) Il existe $i \in \mathbb{N}$ tel que $D^iG = \{1\}$.

Démonstration. (a) D'abord on remarque que $[G,G]$ est l'ensemble de tous les produits finis de commutateurs car $[a,b][b,a] = aba^{-1}b^{-1}bab^{-1}a^{-1} = 1$. Pour voir que $[G,G]$ est un sous-groupe normal de G il suffit donc de faire le calcul suivant :

$$g[a,b]g^{-1} = gaba^{-1}b^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} = [gag^{-1}, gbg^{-1}] \in [G,G]$$

pour tout $g, a, b \in G$.

(b) « $\Rightarrow$ » : Supposons que G/N est abélien. Alors, $0 = [aN, bN] = [a,b]N$. Donc $[a,b] \in N$ pour tout $a, b \in G$.

« $\Leftarrow$ » : Supposons que $[G,G] \subseteq N$. Donc, $aba^{-1}b^{-1} \in N$, donc $abN = baN$ pour tout $a, b, \in G$, montrant que G/N est abélien.

(c) « (i) $\Rightarrow$ (ii) » : Supposons que G est résoluble. Alors, il existe des sous-groupes

$$\{1\} = G_n \trianglelefteq G_{n-1} \trianglelefteq G_{n-2} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = G$$

tels que G_i/G_{i+1} est abélien pour tout $0 \leq i \leq n-1$.

On démontre par récurrence $D^iG \subseteq G_i$ (ce qui implique $D^nG = \{1\}$).

Pour $i = 0$, on a $D^iG = G \subseteq G_0 = G$. Supposons l'assertion vraie pour i. On la démontre pour $i+1$. Comme G_i/G_{i+1} est abélien, on obtient de (b) que $DG_i \subseteq G_{i+1}$. Par hypothèse $D^iG \subseteq G_i$, donc $D^{i+1}G = D(D^iG) \subseteq DG_i \subseteq G_{i+1}$. □

Proposition 9.11. *Soit $n \in \mathbb{N}_{>0}$.*

(a) Le groupe symétrique S_n est engendré par les transpositions $(i \quad j)$ pour $i, j \in \{1, 2, \ldots, n\}$ distincts.

(b) Le groupe alterné A_n est engendré par les 3-cycles $(i \;\; j \;\; k)$ pour $i, j, k \in \{1, 2, \ldots, n\}$ distincts.

(c) $[S_n, S_n] = A_n$.

(d)
$$[A_n, A_n] = \begin{cases} \{1\} & \text{si } n = 1, 2, 3, \\ \{(1), (1\;\;2)(3\;\;4), (1\;\;3)(2\;\;4), (1\;\;4)(2\;\;3)\} & \text{si } n = 4, \\ A_n & \text{si } n \geq 5. \end{cases}$$

(e) Le groupe S_n est résoluble si et seulement si $n \leq 4$.

Démonstration. (a) C'est une conséquence direct du calcul

$$(a_1 \;\; a_2 \;\; \ldots \;\; a_r) = (a_1 \;\; a_2) \circ (a_2 \;\; a_3) \circ \cdots \circ (a_{r-1} \;\; a_r).$$

(b) Par (a) tout $\sigma \in A_n$ est le produit d'un nombre pair de transpositions. Donc il faut considérer les produits de deux transpositions et les exprimer en 3-cycles. Ça marche ainsi :

– $(a_1 \;\; a_2) \circ (a_3 \;\; a_4) = (a_1 \;\; a_3 \;\; a_2) \circ (a_1 \;\; a_3 \;\; a_4)$ si a_1, a_2, a_3, a_4 sont distincts.

– $(a_1 \;\; a_2) \circ (a_2 \;\; a_3) = (a_1 \;\; a_2 \;\; a_3)$ si a_1, a_2, a_3 sont distincts.

– $(a_1 \;\; a_2) \circ (a_1 \;\; a_2) = (1)$ si a_1, a_2 sont distincts.

(c) Comme S_n/A_n est abélien (isomorphe à $\mathbb{Z}/2\mathbb{Z}$ si $n \geq 3$ par la signature), on a par la proposition 9.10 que $[S_n, S_n] \subseteq A_n$. Soit $(a_1 \;\; a_2 \;\; a_3)$ un 3-cycle. On a

$$(a_1 \;\; a_2 \;\; a_3) = (a_1 \;\; a_3)(a_2 \;\; a_3)(a_1 \;\; a_3)^{-1}(a_2 \;\; a_3)^{-1} = [(a_1 \;\; a_3), (a_2 \;\; a_3)] \in [S_n, S_n].$$

Comme tout élément de A_n est un produit de 3-cycles, on obtient $A_n \subseteq [S_n, S_n]$.

(d) $n = 1, 2, 3, 4$ sont vérifiés par des calculs directs. Pour $n \geq 5$ il suffit d'exprimer tout 3-cycle $(a_1 \ \ a_2 \ \ a_3)$ comme un commutateur. C'est facile car on peut choisir a_4, a_5 tels que a_1, a_2, a_3, a_4, a_5 sont distincts et l'on a

$$(a_1 \ \ a_2 \ \ a_3) = (a_1 \ \ a_2 \ \ a_4)(a_1 \ \ a_3 \ \ a_5)(a_1 \ \ a_2 \ \ a_4)^{-1}(a_1 \ \ a_3 \ \ a_5)^{-1} = [(a_1 \ \ a_2 \ \ a_4), (a_1 \ \ a_3 \ \ a_5)].$$

(e) Pour $n \geq 5$ la proposition 9.10 montre que S_n n'est pas résoluble. Les cas $n = 1, 2, 3, 4$ sont vérifiés par des calculs directs et faciles. □

Corollaire 9.12 (Abel)**.** *Soit K un corps parfait. L'équation générale de degré n sur K est résoluble en radicaux si et seulement si $n \leq 4$.*

Démonstration. Proposition 9.11 et théorème 9.6. □

Donc pour $n \geq 5$ il n'existe pas de formule pour exprimer les solutions de l'équation générale de degré n en utilisant uniquement $+, -, \cdot, /, \sqrt[\bullet]{\bullet}$.

10 Constructions à la règle et au compas – n-gons réguliers

Définition-Lemme 10.1. *Soit $n \in \mathbb{N}$. Si $2^n + 1$ est un nombre premier, alors n est une puissance de 2.*
Tout nombre premier de la forme $2^{2^r} + 1$ est appelé nombre premier de Fermat.

Démonstration. Exercice sur la feuille 13. □

Les seuls nombres premiers de Fermat connus sont 3, 17, 257, 65537.

Théorème 10.2 (Gauß)**.** *Soit $n \in \mathbb{N}_{\geq 3}$. Les assertions suivantes sont équivalentes :*

(i) Etant donné deux points C et P, le n-gon régulier de centre C et avec P comme un des sommets est constructible à la règle et au compas.

(ii) $\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$ est une puissance de 2.

(iii) Il existe des nombres premiers de Fermat distincts $p_1, \ldots, p_s$ et $m \in \mathbb{N}$ tels que

$$n = 2^m p_1 p_2 \cdots p_s.$$

Démonstration. Sans perte de généralité nous pouvons prendre $C = 0$ et $P = 1$. La construction de l'n-gon régulier est équivalente à la construction d'un deuxième sommet, donc à $\zeta_n = e^{2\pi i/n}$ (on obtient les autres par des réflexions). Par l'exercice 2 de la feuille 12 on a $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, donc $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$.

« (i) $\Rightarrow$ (ii) » : Le corollaire 5.8 du théorème principal sur la constructibilité à la règle et au compas montre que le degré $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ doit être une puissance de 2.

« (ii) $\Rightarrow$ (i) » : Par le théorème principal sur la constructibilité à la règle et au compas (théorème 5.7) il suffit de montrer qu'il existe des corps

$$\mathbb{Q} = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_r$$

tels que $\zeta_n \in L_r$ et $[L_i : L_{i-1}] = 2$ pour tout $1 \leq i \leq r$. Nous avons que $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ est un groupe fini abélien d'ordre 2^r pour un $r \in \mathbb{N}$. L'exercice 4 (b) de la feuille 13 montre l'existence de sous-groupes

$$\{1\} = G_r \lhd G_{r-1} \lhd \cdots \lhd G_1 \lhd G_0 = G,$$

tels que $(G_i : G_{i-1}) = 2$ pour $1 \leq i \leq r$. La correspondance du théorème principal de la théorie de Galois 8.8 le traduit en la suite de corps recherchée.

« (ii) $\Rightarrow$ (iii) » : Soit $n = 2^m p_1^{e_1} \cdot \cdots \cdot p_s^{e_s}$ la factorisation de n en nombres premiers distincts. Nous avons $\varphi(n) = 2^{m-1}(p_1 - 1)p_1^{e_1-1} \cdot \cdots \cdot (p_s - 1)p_s^{e_s-1} = 2^r$. Donc $e_1 = e_2 = \cdots = e_s = 1$ et $p_i - 1$ est une puissance de 2 pour tout $1 \leq i \leq s$. Par la définition-lemme 10.1, p_i est un nombre premier de Fermat pour tout $1 \leq i \leq s$.

« (iii) $\Rightarrow$ (ii) » : Nous avons $\varphi(n) = 2^{m-1}(p_1 - 1) \cdot \cdots \cdot (p_s - 1)$ qui est une puissance de 2. □

Remarque 10.3. *Dans le théorème 10.2 on peut remplacer (i) par :*

(i') Etant donné deux points P_1, P_2 du plan, un n-gon régulier dont un côté est le segment $\overline{P_1\ P_2}$ est constructible à la règle et au compas.

La raison est la suivante :

Admettons (i) : Alors, il est possible de construire l'angle $\frac{2\pi}{n}$; donc, il est possible de construire l'angle $\frac{n-2}{n}\pi$; c'est l'angle entre deux côtés voisins du n-gon. Donc, il est possible de contruire le n-gon ayant $\overline{P_1\ P_2}$ comme un de ses côtés.

Admettons (i') : Si on a le n-gon régulier, il est facile de construire son centre (Comment ?). Ayant son centre, on a l'angle $\frac{2\pi}{n}$. A l'aide de cet angle on peut construire les n-gon réguliers avec le centre et un des sommets donnés.

Exercices : Algèbre 3

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Hoan-Phung Bui

Feuille 1

18/09/2012

Les exercices sont à rendre le 25/09/2012 au début du cours.

Vos solutions aux exercices vont être notées A (bien), B (moins bien), C (insuffisant). La note que vous obtenez pour vos exercices ainsi que pour vos résultats aux devoirs surveillés comptent pour la note finale du cours : une moyenne de A compte 2 points sur 20 et une moyenne de B 1 point et C 0 points. Par exemple, si vous avez eu une moyenne de B dans vos exercices et si vous obtenez une 13 dans l'examen, la note finale sera 14.

1. Cet exercice vous explique comment obtenir le polynôme minimal d'une matrice. D'abord vous apprenez une méthode générale pour le calculer. Mais, vous verrez aussi que – heureusement – souvent il suffit de connaître le polynôme caractéristique (plus parfois un petit calcul). Rappelons qu'une conséquence du théorème de Cayley-Hamilton est que le polynôme minimal de la matrice M est un diviseur du polynôme caractéristique. Puisque M est de degré n, comme vous le savez, le polynôme caractéristique est aussi de degré n. En conséquence le polynôme minimal est de degré au plus n ; il peut être plus petit !

   Voici la *méthode de Krylov* pour calculer le polynôme minimal de M :

   Soient K un corps et $M \in \mathrm{Mat}_{n\times n}(K)$. Soit $(e_1, \ldots, e_n)$ la base canonique.
   - Pour tout $1 \leq i \leq n$:
     Calculez la combinaison linéaire non nulle la plus courte

     $$0 = a_0 e_i + a_1 M e_i + a_2 M^2 e_i + \cdots + a_{r-1} M^{r-1} e_i + M^r e_i.$$

     Ainsi, vous obtenez le polynôme $g_i(X) := a_0 + a_1 X + a_2 X^2 + \cdots + a_{r-1} X^{r-1} + X^r \in K[X]$.
   - Calculez $m_M(X) := \mathrm{ppcm}(g_1(X), \ldots, g_n(X))$. C'est le polynôme minimal !

   Notez que souvent vous pouvez abrégez cette méthode : si, par exemple, le degré de g_1 est n, vous savez déjà que g_1 est le polynôme minimal (et est égal au polynôme caractéristique).

   (a) Les coefficients des matrices suivantes sont dans $\mathbb{Q}$. Donnez pour chacune des matrices suivantes le polynôme caractéristique et le polynôme minimal. Ne faites pas de grands calculs ! Les résultats sont faciles à obtenir (par exemple, en utilisant les critères pour la diagonalisation).

$$M_1 := \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, M_2 := \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}, M_3 := \begin{pmatrix} a & 1 \\ 0 & b \end{pmatrix} \text{ avec } a \neq b,$$

$$M_4 := \begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix}, M_5 := \begin{pmatrix} a & 1 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix}, M_6 := \begin{pmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix},$$

$$M_7 := \begin{pmatrix} a & 1 & 1 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix}, M_8 := \begin{pmatrix} a & 1 & 1 \\ 0 & b & 1 \\ 0 & 0 & c \end{pmatrix} \text{ avec } a \neq b \neq c \neq a.$$

(b) (Exercice supplémentaire) Même question pour :

$$M_9 := \begin{pmatrix} a_1 & 1 & 0 & \dots & 0 \\ 0 & a_2 & 1 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & a_{n-1} & 1 \\ 0 & \dots & \dots & 0 & a_n \end{pmatrix} \text{ avec } a_i \neq a_j \text{ pour } i \neq j,$$

$$M_{10} := \begin{pmatrix} a & \epsilon_1 & 0 & \dots & 0 \\ 0 & a & \epsilon_2 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & a & \epsilon_{n-1} \\ 0 & \dots & \dots & 0 & a \end{pmatrix} \text{ avec } \epsilon_i \in \{0,1\} \text{ pour } 1 \leq i \leq n-1.$$

(c) Même question pour :

$$N_1 := \begin{pmatrix} 0 & -1 & 1 \\ 3 & 4 & -3 \\ 2 & 2 & -1 \end{pmatrix}, N_2 := \begin{pmatrix} 3 & 0 & 1 \\ -5 & 0 & -1 \\ -4 & -2 & 2 \end{pmatrix}, N_3 := \begin{pmatrix} 4 & 1 & 0 \\ -6 & -1 & 0 \\ -4 & -2 & 2 \end{pmatrix}.$$

(d) (Exercice supplémentaire) Démontrez que la méthode de Krylov marche, c'est-à-dire, démontrez l'assertion $m_M(X) := \mathrm{ppcm}(g_1(X), \dots, g_n(X))$.

2. Dans cet exercice vous obtenez la réduction de Jordan des matrices de l'exercice 1.

(a) Pour les matrices de l'exercice 1 (a) et 1 (c), donnez la/une réduction de Jordan.

Ne calculez pas de base ni de matrice de changement de base. Dans cette exercice il nous suffit la matrice. Puisque vous connaissez le polynôme minimal et le polynôme caractéristique, vous n'avez aucun calcul à faire !

(b) (Exercice supplémentaire) Même question pour les matrices de 1 (b).

(c) Pour la matrice N_1 de l'exercice 1 (c), calculez une matrice C telle que $C^{-1}N_1C$ est une réduction de Jordan de N_1.

3. (Exercice supplémentaire) Soit K un corps algébriquement clos. Par définition (qu'on verra un peu plus tard dans le cours) cela veut dire que chaque polynôme normalisé $f(X) \in K[X]$ peut être écrit comme $f(X) = \prod_{i=1}^{n}(X - a_i)$ avec $a_1, \dots, a_n \in K$. Soit $M = (m_{i,j})_{1 \leq i,j \leq n} \in \mathrm{Mat}_{n \times n}(K)$. La *trace* de M est definie comme $\mathrm{tr}(M) = \sum_{i=1}^{n} m_{i,i}$.

Trouvez une formule qui exprime $\mathrm{tr}(M)$ et $\det(M)$ en termes des coefficients du polynôme caractéristique $\mathrm{car}_M(X)$.

Il est très utile d'utiliser la réduction de Jordan. Vous pouvez sans preuve employer que le déterminant et la trace d'une matrice sont indépendants sous conjugaison.

À propos. Pour illustrer qu'une assertion fausse comme $0 = 1$ implique tout, on dit qu'Einstein a donné l'exemple suivant : « Si $0 = 1$, alors $1 = 2$. L'ensemble dont les éléments sont le pape et moi a deux éléments. Mais, puisque $1 = 2$, cet ensemble n'a qu'un élément, ce qui implique que je suis le pape. »

Exercices : Algèbre 3

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Hoan-Phung Bui

Feuille 2

25/09/2012

Les exercices sont à rendre le 02/10/2012 au début du cours.

1. Soient A un anneau factoriel et K son corps des fractions. Démontrez les assertions suivantes :
   (a) Tout $z \in K \setminus \{0\}$ s'écrit de façon unique comme produit
   $$z = u \cdot \prod_{p \in \mathbb{P}} p^{v_p(z)}$$
   avec $u \in A^\times$, $v_p(z) \in \mathbb{Z}$ et on a $v_p(z) \neq 0$ seulement pour un nombre fini de $p \in \mathbb{P}$.
   (b) Pour tous $x, y \in K$ on a $v_p(xy) = v_p(x) + v_p(y)$. Pour que cette égalité ait un sens si $x = 0$ ou $y = 0$ on pose $a + \infty = \infty$ et $\infty + \infty = \infty$.
   (c) On a : $x \in A \Leftrightarrow v_p(x) \geq 0 \; \forall \, p \in \mathbb{P}$.
   (d) Soit $x \in A$. On a : $v_p(x) = 0$ pour tout $p \in \mathbb{P} \Leftrightarrow x \in A^\times$.
2. Soient A un anneau factoriel et K son corps des fractions. Soit $0 \neq f \in K[X]$. Démontrez les assertions suivantes :
   (a) On a que $v_p(f) \neq 0$ seulement pour un nombre fini de $p \in \mathbb{P}$.
   (b) $v_p(f) \geq 0 \; \forall \, p \in \mathbb{P} \Leftrightarrow f \in A[X]$.
   (c) Si $0 \neq f(X) = \sum_{i=0}^{r} a_i X^i \in A[X]$, alors $v_p(f) = v_p(\mathrm{pgcd}(a_0, a_1, \ldots, a_r))$.
   (d) Il existe $a \in K \setminus \{0\}$ tel que $af \in A[X]$ est un polynôme primitif.
   (e) Pour tout $a \in K \setminus \{0\}$ on a $v_p(af) = v_p(a) + v_p(f)$.
3. (Exercice supplémentaire) Soient A, B des anneaux commutatifs, $\phi : A \to B$ un homomorphisme d'anneaux et $b_1, \ldots, b_n \in B$.
   Montrez qu'il existe un unique homomorpisme d'anneaux
   $$\Phi : A[X_1, \ldots, X_n] \to B$$
   tel que $\Phi(X_i) = b_i$ pour tout $i = 1, \ldots, n$ et $\Phi|_R = \phi$.
   Cette propriété abstraite (mais, parfois utile !) s'appelle *propriété universelle de l'anneau des polynômes*.

À propos. Évariste Galois, né le 25 octobre 1811 à Bourg-la-Reine, mort le 31 mai 1832 à Paris, est un mathématicien français, qui a donné son nom à une branche des mathématiques, la théorie de Galois.

Mort à la suite d'un duel à l'âge de vingt ans, il laisse un manuscrit élaboré trois ans plus tôt, dans lequel il établit qu'une équation algébrique est résoluble par radicaux si et seulement si le groupe de permutation de ses racines a une certaine structure, qu'Emil Artin appellera justement résoluble. Son Mémoire sur les conditions de résolubilité des équations par radicaux, publié par Joseph Liouville quatorze

ans après sa mort, a été considéré par ses successeurs, en particulier Sophus Lie, comme le déclencheur du point de vue structural et méthodologique des mathématiques modernes.

Républicain radical, il prit une part active aux événements qui suivirent les Trois Glorieuses.

Les démêlés de Galois avec les autorités, tant scientifiques que politiques, les zones d'ombre entourant sa mort prématurée, contrastant avec l'importance désormais reconnue de ses travaux, ont contribué à en faire l'incarnation du génie romantique malheureux et d'une jeunesse prometteuse et mal aimée. Il a été célébré en octobre 2011 à l'occasion du bicentenaire de sa naissance.

(Source : fr.wikipedia.org/wiki/Evariste_Galois)

Exercices : Algèbre 3

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Hoan-Phung Bui

Feuille 3

02/10/2012

Ces exercices qui ne sont pas à rendre vous préparent au devoir surveillé du 10/10/2012.

1. Révisez les exemples et exercices concernant la réduction de Jordan.
2. Trouvez tous les polynômes irréductibles de degré au plus 4 dans $\mathbb{F}_2[X]$.
3. Démontrez que les polynômes suivants sont irréductibles :
   (1) $5X^3 + 63X^2 + 168 \in \mathbb{Q}[X]$,
   (2) $X^6 + X^3 + 1 \in \mathbb{Q}[X]$,
   (3) $X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$,
   (4) $X^4 - 3X^3 + 3X^2 - X + 1 \in \mathbb{Q}[X]$,
   (5) $X^9 + XY^7 + Y \in \mathbb{Q}[X, Y]$,
   (6) $X^2 - Y^3 \in \mathbb{C}[X, Y]$.

   Les deux critères (réduction et Eisenstein) vont vous aider, mais ne suffiront pas toujours.
4. (Exercice supplémentaire)
   (a) *(Variante du critère de réduction)* Soient A un anneau factoriel et K son corps des fractions. Soient $f(X) = \sum_{i=0}^{d} a_i X^i \in A[X]$ un polynôme non constant et p un élément premier de A qui ne divise pas a_d. Supposons que $\overline{f}(X) := \sum_{i=0}^{d} \overline{a_i} X^i$ est irréductible dans $A/(p)[X]$ où $\overline{a_i}$ est la classe de a_i dans $A/(p)$.

   Montrez que f est un élément irréductible dans $K[X]$.

   (Vous pouvez utiliser le critère de réduction formulé dans le cours.)

   (b) Démontrez aussi une *variante du critère d'Eisenstein* : La condition que le polynôme soit primitif peut être enlevée si la conclusion est l'irréductibilité dans $K[X]$.
5. (Exercice supplémentaire) Démontrez les assertions suivantes :
   (a) Le polynôme $X^4 + 1 \in \mathbb{Q}[X]$ est irréductible.
   (b) Pour tout nombre premier p on a :
      (i) Il existe $a \in \mathbb{Z}$ t.q. $a^2 \equiv -1 \mod p$ ou
      (ii) il existe $b \in \mathbb{Z}$ t.q. $b^2 \equiv 2 \mod p$ ou
      (iii) il existe $c \in \mathbb{Z}$ t.q. $c^2 \equiv -2 \mod p$.
   (c) Pour tout nombre premier p le polynôme $X^4 + 1 \in \mathbb{F}_p[X]$ possède un diviseur de degré 2 (qui n'est pas nécessairement irréductible).

   (Aide : Considérer $X^4 + 1 = (X^2 + aX + b)(X^2 + cX + d)$ et utiliser (b).)

À propos. *Ferdinand Gotthold Max Eisenstein (16 avril 1823 - 11 octobre 1852).*

Comme Galois et Abel, Eisenstein est mort avant l'âge de 30 ans, et comme Abel, sa mort est due à la tuberculose. Il est né et mort à Berlin, Allemagne. Il fit ses études à l'Université de Berlin où Dirichlet était son professeur. Bernhard Riemann a suivi des cours donnés par Eisenstein.

Gauß aurait déclaré : « Il n'y a que trois mathématiciens qui feront date : Archimède, Newton et Eisenstein ». Bien que cette déclaration soit assez improbable, Eisenstein a créé une œuvre remarquable. Il n'est pas seulement connu pour son critère d'irréductibilité, mais aussi pour les séries d'Eisenstein dans la théorie des formes modulaires et la réciprocité d'Eisenstein (qui généralise celle de Gauß), pour en nommer quelques-uns de ses accomplissements.

(Partiellement tiré de : `http ://fr.wikipedia.org/wiki/Gotthold_Eisenstein`)

Exercices : Algèbre 3

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Hoan-Phung Bui

Feuille 4

09/10/2012

Les exercices sont à rendre le 16/10/2012 au début du cours.

Tout corps est supposé commutatif pour le reste du cours.

1. (a) Nous savons que $K := \mathbb{F}_2[X]/(X^2+X+1)$ est un corps de cardinal 4. Déterminer sa caractéristique et son corps premier.
   (b) Plus généralement : Soit K un corps de caractéristique $p > 0$ et $f \in K[X]$ un polynôme irréductible. Déterminer la caractéristique de $K[X]/(f(X))$.
2. Soient K un corps de caractéristique $p > 0$ et $n \in \mathbb{N}$. On pose $q := p^n$. Démontrer que pour tout $a, b \in K$ on a $(a+b)^q = a^q + b^q$.
3. Soient L/K une extension de corps et $a \in L$. Démontrer que l'application *évaluation*

$$\mathrm{ev}_a : K[X] \to L, \quad \sum_{i=0}^{d} c_i X^i \mapsto \sum_{i=0}^{d} c_i a^i$$

   est un homomorphisme d'anneaux.
4. (a) Démontrer que $\mathbb{Q}[i] \subset \mathbb{C}$ (avec $i = \sqrt{-1}$) est un corps (donc égal à $\mathbb{Q}(i)$). Quel est son degré sur $\mathbb{Q}$?
   (b) Démontrer que $\mathbb{R}[i] \subseteq \mathbb{C}$ (avec $i = \sqrt{-1}$) est égal à $\mathbb{C}$. Quel est son degré sur $\mathbb{R}$?
   (Exercice supplémentaire :) Quel est son degré sur $\mathbb{Q}$?
   (c) Soit p un nombre premier et $n \geq 1$ un nombre naturel. Démontrer que $\mathbb{Q}[\sqrt[n]{p}] \subset \mathbb{R}$ est un corps (donc égal à $\mathbb{Q}(\sqrt[n]{p})$). Quel est son degré sur $\mathbb{Q}$?
   (d) (Exercice supplémentaire) Soit p un nombre premier et $\zeta_p := e^{2\pi i/p} \in \mathbb{C}$. Démontrer que $\mathbb{Q}[\zeta_p] \subset \mathbb{C}$ est un corps (donc égal à $\mathbb{Q}(\zeta_p)$). Quel est son degré sur $\mathbb{Q}$?
5. (Exercice supplémentaire) Soient L/K une extension de corps de degré 2^k (pour un $k \in \mathbb{N}$), $a \in L$ et $f \in K[X]$ un polynôme irréductible de degré d tel que $f(a) = 0$ et d est impair. Démontrez que $a \in K$.

À propos : Historique de la résolution des équations polynomiales – le degré 2.

Les équations du second degré sont au centre de l'algèbre babylonienne, dès avant le 18ème siècle AC. La tablette d'argile BM 13901 a été qualifiée de "véritable petit manuel d'algèbre, consacré à l'équation du second degré et aux systèmes d'équations, et donnant les procédures résolutoires fondamentales".

Al-Khawarizmi (∼783-∼850) : mathématicien, géographe, astrologue et astronome perse (Perse = Iran actuel) est à l'origine des mots "algorithme" et "algèbre". Son apport en mathématiques fut tel qu'il est également surnommé "le père de l'algèbre" avec Diophante d'Alexandrie ((∼200/214-∼284/298), mort à 84 ans, également connu pour son épitaphe permettant de retrouver l'âge qu'il avait à sa mort).

Al-Khawarizmi étudie les équations du second degré dans un ouvrage intutilé "Abrégé du calcul par la restauration (al-jabr) et la comparaison (al-muqābala)". Il distingue six cas d'équations du premier ou second degré dans lesquels les paramètres a, b et c sont tous positifs :
1. les carrés égalent les racines : $ax^2 = bx$,
2. les carrés égalent les nombres : $ax^2 = c$,
3. les racines égalent les nombres : $bx = c$,
4. les carrés et les racines égalent les nombres : $ax^2 + bx = c$,
5. les carrés et les nombres égalent les racines : $ax^2 + c = bx$,
6. les racines et les nombres égalent les carrés : $bx + c = ax^2$.

Sources :

- Jean Doyen, Problèmes et méthodes en mathématiques (cours donné à l'ULB durant l'année académique 2008-2009)
- Wikipédia

Exercices : Algèbre 3

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Hoan-Phung Bui

Feuille 5

16/10/2012

Les exercices sont à rendre le 23/10/2012 au début du cours.

---

1. Calculer le polynôme minimal sur $\mathbb{Q}$ de $\sqrt{7}$, $\sqrt[5]{7}$, $\frac{1+\sqrt{5}}{2}$.
2. Soient L/K une extension de corps et $a \in L$. On suppose $K[a] = K(a)$. Ecrire une preuve directe (sans utiliser les résultats du cours) qui montre que a est algébrique sur K.
3. Soient L/K une extension de corps et $a_1, \ldots, a_n \in L$.
   Démontrer l'équivalence des deux assertions suivantes :
   (i) L'extension $K(a_1, a_2, \ldots, a_n)/K$ est finie.
   (ii) Tous les a_i pour $i = 1, \ldots, n$ sont algébriques sur K.
   Vous pouvez utiliser les résultats du cours.
4. Soit $f = X^3 + 3X - 3 \in \mathbb{Q}[X]$ et $\alpha \in \mathbb{C}$ un zéro de f.
   (a) Démontrer que 1, α, α^2 est une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\alpha)$.
   (b) Représenter α^{-1} et $(1+\alpha)^{-1}$ comme combinaison $\mathbb{Q}$-linéaire de $1, \alpha, \alpha^2$.
   (c) Calculer le polynôme minimal de $\beta := \alpha^2 - \alpha + 2$ sur $\mathbb{Q}$.
5. (Exercice supplémentaire) Soient L/K une extenstion algébrique de corps et A un sous-anneau de L tel que $K \subseteq A \subseteq L$. Démontrer ou contredire l'assertion : A est un corps.

À propos : Historique de la résolution des équations polynomiales – le degré 3.

Omar Khayyām (1048-1131) : mathématicien, astronome et poète persan résoud géométriquement les équations du 3ème degré dans sont "Traité d'algèbre" en 1074.
Exemple : $x^3 + px = q$, avec $p, q > 0$
Posons $p = a^2$ et $q = a^2 b$ (où $a, b > 0$) et considérons la parabole $x^2 = ay$ et le cercle $x^2 + y^2 = bx$. L'abscisse de l'intersection (non triviale) est racine de l'équation.

Scipione del Ferro (1465-1526) : professeur à l'Université de Bologne, a une idée originale : considérons l'équation $x^3 + px + q = 0$ (on peut toujours ramener un polynôme de degré 3 sous cette forme avec un changement de variables). Posons $x = u + v$, l'équation devient

$$(u+v)^3 + p(u+v) + q = 0 \Rightarrow (u^3 + v^3 + q) + (u+v)(3uv + p) = 0.$$

Il suffit alors de trouver u et v tels que

$$u^3 + v^3 = -q,$$
$$u^3 v^3 = \frac{-p^3}{27}$$

ce qui est facile.
A l'époque les nombres négatifs n'étaient pas aimés $\Rightarrow$ on distinguait 3 types d'équations du 3ème degré :

$x^3 + px = q$, $x^3 = px + q$, $x^3 + q = px$, avec $p, q > 0$.
A sa mort en 1526, Scipione del Ferro révèle son secret à son élève Antonio Maria del Fiore mais uniquement pour le premier type. Fiore clame qu'il sait résoudre les équations du 3ème degré.

Niccolo Fontana Tartaglia (1499-1557) : professeur de mathématiques à Venise, s'attaque seul au problème. Dans la nuit du 12 au 13 février 1535 il découvre la formule permettant de résoudre toutes les équations du 3ème degré.
Fiore lance un défi public (disputatio) à Tartaglia : 30 équations du 3ème degré à résoudre. Prix du vainqueur : 30 banquets. Tartaglia gagne mais refuse le prix.
Anecdote : Tartaglia est le surnom de Niccolo Fontana (tartagliare : bredouiller, bégayer). Niccolo Fontana habitait à Brescia qui fut prise par les Français en 1512. Il fut blessé par les soldats à la mâchoire, il ne meurt pas mais conservera un défaut de parole toute sa vie.

Girolamo Cardano (1501-1576) : médecin, astrologue, mathématicien, ingénieur vivant à Milan. Il apprend que Tartaglia peut résoudre les équations du 3ème degré. Il l'invite chez lui en 1539 et le harcèle jusqu'à ce que Tartaglia accepte de lui révéler sa méthode sous la forme d'un poème obscur que Cardano arrive néanmois à déchiffrer. Tartaglia fait jurer à Cardano de ne jamais révéler le secret.
Cardano connaît donc la formule de résolution de toutes les équations du 3ème degré et l'applique à divers exemples. L'équation

$$x^3 - 15x - 4 = 0$$

possède $x = 4$ comme racine. Mais la formule donne

$$x = \sqrt[3]{2 + 11\sqrt{-1}} + \sqrt[3]{2 - 11\sqrt{-1}},$$

une vraie torture mentale pour Cardano (les nombres complexes n'ont pas encore été introduits).
En 1543 Cardano apprend que Scipione del Ferro avait résolu bien avant Tartaglia les équations du 3ème degré. Cardano pensa alors que rien ne l'empêchait de publier la solution de del Ferro. En 1547 Cardano publie "Arts Magna" avec les résolutions des équations du 3ème et 4ème degré (Ferrari). Depuis lors la formule de résolution des équations du 3ème degré s'appelle "formule de Cardan".

Raphaël Bombelli (1526-1572) : ingénieur en hydraulique à Bologne, a le courage d'aller plus loin : posons $\sqrt{-1} = i$ (1572), a-t-on $\sqrt[3]{2 + 11i} + \sqrt[3]{2 - 11i} = 4$? OUI car $(2+i)^3 = 2+11i$ et $(2-i)^3 = 2-11i$.

Sources :

- Jean Doyen, Problèmes et méthodes en mathématiques (cours donné à l'ULB durant l'année académique 2008-2009)
- Wikipédia

Exercices : Algèbre 3

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Hoan-Phung Bui

Feuille 6

23/10/2012

Les exercices sont à rendre le 30/10/2012 au début du cours.

1. (Exercice pas à rendre) Décrivez les constructions suivantes en utilisant uniquement les opérations **règle** et **compas** du cours :
   (a) Tracer la droite perpendiculaire à une droite donnée passant par un point donné.
   (b) Tracer la droite passant par un point donné et parallèle à une droite donnée.
   (c) Tracer la médiatrice d'un segment donné.
   (d) Additionner deux angles.
   (e) Réflexion d'un point par rapport à une droite donnée.
   (f) Construction du triangle équilatéral à partir d'un segment donné.
   (g) Tracer la bisectrice d'un angle.
2. Soit $P_0 \subseteq \mathbb{C}$ tel que $0, 1 \in P_0$ et $z, z_1, z_2 \in \mathcal{X}(P_0)$. Démontrer :
   (a) $z_1 + z_2 \in \mathcal{X}(P_0)$;
   (b) $-z \in \mathcal{X}(P_0)$;
   (c) $|z| \in \mathcal{X}(P_0)$;
   (d) $e^{\pi i/3} \in \mathcal{X}(P_0)$;
   (e) $|z_1| \cdot |z_2| \in \mathcal{X}(P_0)$;
   (f) $\frac{1}{|z|} \in \mathcal{X}(P_0)$ (pour $z \neq 0$) ;
   (g) $z_1 \cdot z_2 \in \mathcal{X}(P_0)$;
   (h) $\frac{1}{z} \in \mathcal{X}(P_0)$ (pour $z \neq 0$) ;
   (i) $\pm\sqrt{z} \in \mathcal{X}(P_0)$.

   Indication : Pour (e) et (f) utiliser le théorème de Thalès (allemand : Strahlensatz) et pour (i) utiliser le théorème de Thalès sur le cercle (allemand : Satz von Thales).
3. Soit $P_0 \subseteq \mathbb{C}$ un sous-ensemble. Démontrer que l'opération **compas** peut être remplacée par l'opération suivante sans changer l'ensemble de points constructibles :
   Pour tous $r_1, r_2 \in P_0$ tracer le cercle de centre r_1 passant par r_2.
4. Soit $P_0 \subseteq \mathbb{C}$ un sous-corps tel que $\overline{P_0} = P_0$ et $i \in P_0$. Soit $z \in P_1$. Démontrer $[P_0(z) : P_0] \leq 2$.
5. (Exercice supplémentaire) Démontrer que l'heptagon (le polygône régulier à 7 cotés) ne peut pas être construit à la règle et au compas.

   Indication : Construire l'heptagon est équivalent à construire la 7-ième racine d'unité $e^{2\pi i/7}$, dont on connaît le polynôme minimal.

À propos : Historique de la résolution des équations polynomiales – le degré 4.

Ludovico Ferrari (1522-1565) : mathematicien italien, découvre vers 1540 une méthode de résolution des équations du 4ème degré en se ramenant à une équation du 3ème degré.

René Descartes (1596-1650) : mathématicien français, donne en 1637 une méthode plus simple dans le "Discours de la méthode" (annexe intitulée "Géométrie") :
Prenons l'équation $x^4 + px^2 + qx + r = 0$. Si $q = 0$ on est ramené à une équation de degré 2 $\Rightarrow$ on peut supposer $q \neq 0$. On essaie de factoriser ce polynôme :

$$\begin{aligned} x^4 + px^2 + qx + r &= (x^2 + kx + m)(x^2 - kx + n) \\ &= x^4 + (m + n - k^2)x^2 + k(n - m)x + mn. \end{aligned}$$

En identifiant les coefficients et en divisant par $k \neq 0$ (car $q \neq 0$) on obtient

$$\begin{aligned} m + n &= p + k^2, \\ n - m &= \frac{q}{k}, \\ mn &= r. \end{aligned}$$

$$\begin{aligned} n &= \frac{1}{2}(p + k^2 + \frac{q}{k}), \\ m &= \frac{1}{2}(p + k^2 - \frac{q}{k}), \\ mn &= r. \end{aligned}$$

En remplaçant m et n dans la 3ème équation, on obtient

$$k^6 + 2pk^4 + (p^2 - 4r)k^2 - q^2 = 0.$$

On trouve ainsi k, ce qui nous permet de calculer m et n.
Descartes qualifie les racines réelles de vraies si > 0, fausses si < 0 et les racines non-réelles d'"imaginaires".

Sources :

- Jean Doyen, Problèmes et méthodes en mathématiques (cours donné à l'ULB durant l'année académique 2008-2009)
- Wikipédia

Exercices : Algèbre 3

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Hoan-Phung Bui

Feuille 7

30/10/2012

Ces exercices qui ne sont pas à rendre vous préparent au devoir surveillé du 07/11/2012.

1. Soit $a = \sqrt[5]{7} \in \mathbb{C}$.
   (a) Calculer le polynôme minimal f de a sur $\mathbb{Q}$.
   (b) Factoriser f dans $\mathbb{C}[X]$.
   Indication : $\zeta_5 := e^{2\pi i/5}$.
   (c) Ecrire tous les homomorphismes de corps $\mathbb{Q}(\sqrt[5]{7}) \to \mathbb{C}$.
2. Considérer l'extension de corps $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$.
   (a) Calculer le polynôme minimal f de $\alpha := \sqrt{2+\sqrt{2}}$ sur $\mathbb{Q}$.
   (b) Calculer l'inverse de α pour la base $1, \alpha, \ldots, \alpha^{d-1}$ où d est le degré de f.
   (c) Factoriser f dans $\mathbb{C}[X]$.
   (d) Ecrire tous les homomorphismes de corps $\mathbb{Q}(\sqrt{2+\sqrt{2}}) \to \mathbb{C}$.
3. Soit L/K une extension algébrique.
   (a) Soient $\alpha, \beta \in L$ tels que $[K(\alpha) : K] = m$, $[K(\beta) : K] = n$ et $\gcd(n, m) = 1$. Démontrer :
   $$[K(\alpha, \beta) : K] = mn.$$
   (b) Soient $\alpha_1, \ldots, \alpha_n \in L$ et $f_1, \ldots, f_n \in K[X]$ les polynômes minimaux correspondants. Démontrer :
   $$[K(\alpha_1, \ldots, \alpha_n) : K] \leq \prod_{i=1}^{n} \deg(f_i).$$
4. Soit K un corps algébriquement clos. Démontrer que le nombre d'éléments de K est infini.
   Indication : Supposer le contraire : $K = \{a_1, \ldots, a_n\}$. Ecrire un polynôme non-constant $f \in K[X]$ tel que $f(a_i) = 1$ pour tout $i = 1, \ldots, n$. Pour trouver ce polynôme il peut être utile de se rappeler comment on démontre que le nombre de nombres premiers est infini.
5. (Exercice supplémentaire) Soit K un corps. Le but de cet exercice est de démontrer qu'il existe une clôture algébrique de K.
   (a) Soit $M := \{f \in K[X] \mid \deg(f) \geq 1\}$. Soit $R := K[(X_f)_{f \in M}]$ l'anneau des polynômes dans les variables X_f où f parcourt l'ensemble M. Soit $\mathfrak{a} := (f(X_f)\ f \in M) \lhd R$, l'idéal de R engendré par tous les éléments $f(X_f)$ pour $f \in M$.
   Démontrer : $\mathfrak{a} \neq R$.
   Indication : Pour une contradiction, représenter $1 = \sum_{i=1}^{n} g_i f_i(X_{f_i})$ avec $g_1, \ldots, g_n \in R$ et certains $f_1, \ldots, f_n \in M$. Trouver une extension K'/K et $\alpha_i \in K'$ tels que $f_i(\alpha_i) = 0$. En déduire la contradiction.

(b) Soit $\mathfrak{m} \lhd R$ un idéal maximal tel que $\mathfrak{a} \subseteq \mathfrak{m}$ (qui existe par un résultat démontré en Algèbre 2) et poser $L := R/\mathfrak{m}$.

Conclure que L est une extension de corps de K.

(c) Démontrer que tout $f \in M$ possède un zéro dans L.

Nous avons donc démontré jusqu'à ici : Soit K un corps. Il existe un corps $L(K)$ tel que tout polynôme $f \in K[X]$ de degré ≥ 1 possède un zéro dans $L(K)$.

Indication : Imiter la preuve de l'existence du corps de rupture.

(d) Poser $K_0 := K$ et par récurrence pour tout $n \geq 1$: $K_n := L(K_{n-1})$. Poser $M := \bigcup_{n=0}^{\infty} K_n$.

Démontrer que M est algébriquement clos.

Indication : Tout $f \in M[X]$ doit appartenir à un $K_n[X]$.

(e) Poser $\overline{K} = K_M$ et conclure que $\overline{K}$ est une clôture algébrique de K.

À propos : Historique de la résolution des équations polynomiales – le degré $n \geq 5$.

Niels Henrik Abel (1802-1829) : mathématicien norvégien, mort à 26 ans de tubercolose, prouve en 1824, que l'équation générale du n-ème degré n'est pas résoluble par radicaux dès que $n \geq 5$. Remarquons que certaines équations particulières le sont, par exemple $ax^5 + b = 0$. On peut alors se poser la question suivante : Quelles sont les équations de degré ≥ 5 qui sont résolubles par radicaux ?
A l'occasion du bicentenaire de la naissance d'Abel, l'Académie norvégienne des sciences et des lettres a annoncé en 2001 qu'un nouveau prix serait créé pour les mathématiciens : le prix Abel. Le prix est décerné chaque année depuis 2003 et récompense un mathématicien pour l'ensemble de son oeuvre.

Evariste Galois (1811-1832) : mathématicien français, mort à 20 ans lors d'un duel, fournit la réponse : il trouve une condition nécessaire et suffisante pour déterminer si oui ou non une équation de degré n est résoluble (théorie de Galois !).

Sources :

- Jean Doyen, Problèmes et méthodes en mathématiques (cours donné à l'ULB durant l'année académique 2008-2009)
- Wikipédia

Exercices : Algèbre 3

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Hoan-Phung Bui

Feuille 8

06/11/2012

Les exercices sont à rendre le 13/11/2012 au début du cours.

1. Considérer l'extension de corps $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$.

   Est-ce que c'est une extension de corps *normale* ? Pourquoi ?

   Indication : Cette extension a déjà été étudiée sur la feuille 7 et les résultats peuvent aider.
2. Soit $f = X^4 - 3 \in \mathbb{Q}[X]$.
   (a) Démontrer que $L = \mathbb{Q}(\sqrt[4]{3}, i)$ est un corps de décomposition de f sur $\mathbb{Q}$.
   (b) Quel est le degré de l'extension $L/\mathbb{Q}$?
3. (a) Calculez un corps de décomposition L sur $\mathbb{Q}$ du polynôme $f(X) = X^5 - 7$. Quel est le degré de l'extension $L/\mathbb{Q}$?

   Indication : Est-ce que $f(X)$ est irréductible ? Considérer le corps $\mathbb{Q}(\zeta_5)$ où $\zeta_5 = e^{2\pi i/5}$. Vous trouvez le polynôme minimal de ζ_5 sur $\mathbb{Q}$ dans le cours. Factoriser-le dans $\mathbb{C}$. Choisir deux éléments qui engendrent L. Pour déterminer le degré $[L : \mathbb{Q}]$ vous pouvez utiliser un exercice de la feuille 7.

   (b) (Exercice supplémentaire) Même question pour $f(X) = X^6 + X^3 + 1$.

   Indication : Pour calculer les racines, poser d'abord $Y = X^3$.
4. Soient K un corps, $f \in K[X]$ un polynôme de degré $n > 0$ et L un corps de décomposition de f sur K. Démontrer que $[L : K]$ divise $n!$.

   Indication : Récurrence sur des corps arbitraires. Soit $f \in K[X]$ un polynôme de degré n. Distinguer les cas : f irréductible sur K ou f réductible. Si f est réductible, alors $f = gh$ et on utilise l'hérédité pour g et h. Si f est irréductible, soit a une racine de f dans L. Considérer l'extension $K(a)/K$; lequel est son degré ? Trouver un polynôme $g \in K(a)[X]$ de degré strictement plus petit que n, dont le corps de décomposition sur $K(a)$ est égal à L. Utiliser maintenant l'hérédité.
5. (Exercice supplémentaire). Démontrer que $\overline{\mathbb{Q}}$ est dénombrable.

   Indication : L'ensemble de polynômes dans $\mathbb{Q}[X]$ est dénombrable, donc l'ensemble de leurs zéros l'est aussi.

À propos. L'hôtel de Hilbert à Göttingen possède un nombre infini de chambres. Aujourd'hui toutes les chambres sont occupées. Malgré cela, l'hôtelier Hilbert peut toujours accueillir un nouveau client.

En effet supposons que les chambres sont numérotées par tous les nombres entiers (à partir de 1). Il suffit que l'hôtelier demande à l'occupant de la première chambre de s'installer dans la seconde, à celui de la seconde de s'installer dans la troisième, et ainsi de suite. Les clients déjà logés le restent. La première chambre est libre et peut accueillir le nouveau client.

Mais l'hôtelier peut aussi accueillir une infinité de nouveaux clients. Pour ce faire il faut que le client occupant la chambre numéro 1 prenne la chambre numéro 2, l'occupant de la numéro 2 la numéro 4, celui de la numéro 3 la numéro 6, et ainsi de suite. Chacun occupe une chambre de numéro double de celui

de sa chambre précédente, de telle sorte que toutes les chambres de numéro impair deviennent libres. Et puisqu'il existe une infinité de nombres impairs, l'hôtelier peut accueillir une infinité de nouveaux clients.

Pour être plus précis, il faudrait dire que l'hôtel peut toujours accueillir un ensemble *dénombrable* de clients. Par contre, si tous les nombres réels arrivent et chacun veut une chambre, l'hôtel ne suffira pas car l'ensemble des nombres réels n'est pas dénombrable (par l'argument de la diagonale de Cantor).

(Adapté et corrigé de : `http ://fr.wikipedia.org/wiki/Hôtel_de_Hilbert`)

Exercices : Algèbre 3

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Hoan-Phung Bui

Feuille 9

13/11/2012

Les exercices sont à rendre le 20/11/2012 au début du cours.

1. Soit K un corps et $G \leq K^\times$ un sous-groupe fini du groupe multiplicatif de K. Soit n l'ordre de G et $m := \max(\mathrm{ord}(g) \mid g \in G)$. Comme l'ordre $\mathrm{ord}(g)$ de tout élément $g \in G$ divise l'ordre du groupe G (c'est un fait bien connu de la théorie des groupes), on a $m \mid n$. Démontrer :
   (a) Tout $g \in G$ est un zéro du polynôme $f(X) := X^m - 1 \in K[X]$.
   (b) G est un groupe cyclique, c'est-à-dire, il peut être engendré par un seul élément.
2. Soit K un corps, $\overline{K}$ une clôture algébrique de K et $m \in \mathbb{N}_{>0}$. Nous supposons que soit K est de caractéristique 0, soit la caractéristique de K ne divise pas m. Démontrer :
   (a) Le polynôme $f := X^m - 1 \in K[X]$ est séparable sur K.
   (b) Il existe $g \in \overline{K}^\times$ d'ordre m dans le groupe multiplicatif $\overline{K}^\times$.
3. On considère l'extension $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})/\mathbb{Q}$. Démontrer que $\sqrt[3]{2}\sqrt[4]{5}$ est un élément primitif pour cette extension, c'est-à-dire $\mathbb{Q}(\sqrt[3]{2}\sqrt[4]{5}) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})$.
   Indication : Chercher $n, m \in \mathbb{N}$ tel que $4 \mid n$, $3 \mid m$ et $n \equiv 1 \mod 3$ ainsi $m \equiv 1 \mod 4$ et utiliser-les.
4. Soit K un corps de caractéristique $p > 0$, $\overline{K}$ une clôture algébrique de K et $a \in K$. Démontrer :
   Pour tout $n \in \mathbb{N}$ et pour tout $a \in K$ il existe un et un seul $b \in \overline{K}$ tel que $b^{p^n} = a$.
5. (Exercice supplémentaire) Soit K un corps de caractéristique $p > 0$, $\overline{K}$ une clôture algébrique de K et $f \in K[X]$ irréductible. Soit $r \in \mathbb{N}$ le maximum tel qu'il existe un polynôme $h \in K[X]$ avec la propriété $f(X) = h(X^{p^r})$. Soit $g \in K[X]$ tel que $g(X^{p^r}) = f(X)$. Démontrer :
   (a) g est irréductible et séparable.
   (b) La multiplicité de toute racine de f est égale à p^r.
   (c) Les zéros de f dans $\overline{K}$ sont précisement les uniques (voir l'autre exercice) p^n-ième racines des zéros de g dans $\overline{K}$.
   (d) Soit $a \in \overline{K}$ un zéro de f. Alors : $[K(a) : K] = p^r[K(a) : K]_s$.
6. Soit p un nombre premier.
   (a) Soit $\mathbb{F}_p(X) := \mathrm{Frac}(\mathbb{F}_p[X])$.
   Démontrer : $[\mathbb{F}_p(X) : \mathbb{F}_p(X^p)] = p$ et $[\mathbb{F}_p(X) : \mathbb{F}_p(X^p)]_s = 1$.
   (b) (Exercice supplémentaire) Soit $\mathbb{F}_p(X, Y) := \mathrm{Frac}(\mathbb{F}_p[X, Y])$.
   Démontrer : $[\mathbb{F}_p(X, Y) : \mathbb{F}_p(X^p, Y^p)] = p^2$ et $[\mathbb{F}_p(X, Y) : \mathbb{F}_p(X^p, Y^p)]_s = 1$.

À propos : Il n'existe pas d'ensemble de tous les ensembles.

En effet, supposons par l'absurde que l'ensemble de tous les ensembles existe ; appelons le Ω. Nous pouvons alors considérer le sous-ensemble A de Ω formé des ensembles X tels que X n'est pas un élément de l'ensemble X :

$$A = \{X \in \Omega | X \notin X\}\,.$$

Qu'en est-il alors de A ? Si A est un élément de A ($A \in A$), alors par définition de A, A n'est pas un élément de A ($A \notin A$). Et si A n'est pas un élément de A ($A \notin A$), alors par définition de A, A est un élément de A ($A \in A$). Aucune de ces deux options n'est donc possible.

Pour lever ce paradoxe, les mathématiciens ont introduit la notion de *catégorie*, mais ceci est une autre histoire.

Exercices : Algèbre 3

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Hoan-Phung Bui

Feuille 10

20/11/2012

Les exercices sont à rendre le 27/11/2012 au début du cours.

1. Finir la feuille 9 (Exercices 5 (d) et 6).
2. Soit K un corps fini de caractéristique p. L'exercice 1 de la feuille 9 montre que le groupe multiplicatif $K^\times = K \setminus \{0\}$ est cyclique.

   Utiliser ce fait pour démontrer qu'il existe $a \in K$ tel que $K = \mathbb{F}_p(a)$.
3. Soit K un corps fini de caractéristique $p > 2$. Considérons

$$\phi : K^\times \to K^{\times 2} := \{r^2 \mid r \in K^\times\}, \quad \phi(x) = x^2.$$

   (a) Démontrer que ϕ est un homomorphisme de groupes qui est surjectif. Ici on regarde $K^\times$ et $K^{\times 2}$ comme groupe pour la multiplication.

   (b) Calculer le cardinal du noyau de ϕ.

   (c) Soit $G := K^\times / K^{\times 2}$ le groupe quotient. Définir un isomorphisme de groupes $G \to (\mathbb{Z}/2\mathbb{Z}, +)$.

   (d) Démontrer l'équivalence suivante :

   (i) $p \equiv 1 \pmod 4$.

   (ii) Il existe $i \in \mathbb{F}_p$ tel que $i^2 = -1$ dans $\mathbb{F}_p$.
4. Soit K un corps fini. Soit $a := \prod_{x \in K^\times} x$.

   (a) Démontrer $x = -1$ (dans K).

   (b) Déduire que pour tout nombre premier p on a : $p \mid ((p-1)! + 1)$.

   (c) Démontrer que si $n \in \mathbb{N}_{\geq 2}$ n'est pas premier, alors $n \nmid ((n-1)! + 1)$.
5. (Exercice supplémentaire) Soient K un corps de caractéristique $p > 0$, L/K une extension et $\alpha \in L$ algébrique sur K. Démontrer l'équivalence suivante :

   (i) α est séparable sur K.

   (ii) $K(\alpha) = K(\alpha^p)$.

   Indication : Utiliser l'exercice 5 de la feuille 9.

À propos : Le paradoxe de Monty Hall

Vous êtes le candidat à un jeu télévisé et le présentateur vous propose de choisir votre prix. On vous place devant trois portes fermées. Derrière l'une de ces portes se trouve un cadeau merveilleux (la démonstration de l'hypothèse de Riemann par exemple) mais les deux autres portes ne cachent rien d'intéressant... Vous choisissez une porte. Une fois cela fait le présentateur ouvre une porte non intéressante parmi les deux portes restantes (exercice : une telle porte existe !). On vous propose maintenant de changer votre choix, quelle est la stratégie optimale ?

Exercices : Algèbre 3

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Hoan-Phung Bui

Feuille 11

27/11/2012

Les exercices sont à rendre le 04/12/2012 au début du cours.

---

1. Soient $M/L/K$ des extensions algébriques. On suppose que M/K est normale.
   Démontrer : $\#\mathrm{Hom}_K(L, M) = [L : K]_s$.
2. Soit $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
   (a) Démontrer que $K/\mathbb{Q}$ est une extension galoisienne.
   (b) Calculer les éléments de son groupe de Galois $\mathrm{Gal}(K/\mathbb{Q})$.
   (c) Est-ce que $\mathrm{Gal}(K/\mathbb{Q})$ est abélien ou cyclique ? Démontrer la réponse.
3. Soit $p > 2$ un nombre premier. Soit K le corps de décomposition de $X^p - 2$ sur $\mathbb{Q}$.
   (a) Démontrer que $K/\mathbb{Q}$ est une extension galoisienne.
   (b) Calculer les éléments de son groupe de Galois $\mathrm{Gal}(K/\mathbb{Q})$.
   (c) Est-ce que $\mathrm{Gal}(K/\mathbb{Q})$ est abélien ou cyclique ? Démontrer la réponse.
4. Au cours les éléments du groupe de Galois $G := \mathrm{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q})$ ont été calculés.
   Démontrer que G est isomorphe au groupe symétrique S_3.
5. (Exercice supplémentaire) Soient $p_1, p_2, \ldots, p_n$ des nombres premiers distincts.
   Démontrer que $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n})/\mathbb{Q}$ est une extension galoisienne avec groupe de Galois isomorphe à $\underbrace{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}}_{n \text{ facteurs}}$.

À propos. Concernant les déductions logiques...

"Hering ist gut. Schlagsahne ist gut.
Wie gut muss erst Hering mit Schlagsahne sein !"
Kurt Tucholsky, zitiert nach : Thiele, Mathematische Beweise.

Traduction belge libre : « Les gauffres sont bonnes. Les frites sont bonnes.
Comment les gauffres aux frites doivent être bonnes ! »

Exercices : Algèbre 3

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Hoan-Phung Bui

Feuille 12

04/12/2012

Ces exercices qui ne sont pas à rendre et ceux des feuilles précédentes vous préparent au devoir surveillé du 12/12/2012.

---

1. Soit L/K une extension galoisienne de degré 4. Soit G son groupe de Galois.
   (a) On suppose que G est cyclique. Combien de sous-corps possède l'extension L/K ? Quels sont leurs degrés sur K ?
   (b) On suppose que G n'est pas cyclique. Combien de sous-corps possède l'extension L/K ? Quels sont leurs degrés sur K ?

   Indication : Théorème principal de la théorie de Galois.
2. Soit $n \in \mathbb{N}$. Soit $K \subseteq \mathbb{C}$ le corps de décomposition du polynôme $X^n - 1 \in \mathbb{Q}[X]$. Soit μ_n le sous-groupe de $\mathbb{C}^\times$ (pour la multiplication) qui est composé de tous les éléments de $\mathbb{C}^\times$ dont l'ordre divise n.
   (a) Montrer (en donnant les bonnes citations du cours) que $K/\mathbb{Q}$ est une extension galoisienne.
   (b) Montrer que $K = \mathbb{Q}(\zeta_n)$.
   (c) On pose $\zeta_n = e^{2\pi i/n} \in \mathbb{C}^\times$. Montrer que μ_n est d'ordre n et $\mu_n = \{\zeta_n^j \mid j = 0, \dots, n-1\}$.
   (d) Montrer que l'application $\mathbb{Z}/n\mathbb{Z} \to \mu_n$ donnée par $j \mapsto \zeta_n^j$ est un isomorphisme de groupes (pour l'addition de $\mathbb{Z}/n\mathbb{Z}$).
   (e) Montrer l'équivalence des deux assertions suivantes :
      (i) L'ordre de ζ_n^j dans $\mu(n)$ est égal à n. (On appelle un tel ζ_n^j une n-ième racine *primitive* d'unité.)
      (ii) $j \in (\mathbb{Z}/n\mathbb{Z})^\times$.
   (f) On pose $\Phi_n(X) = \prod_{j \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta_n^j) \in \mathbb{C}[X]$.
   Démontrer $\Phi_n(X) \in \mathbb{Q}[X]$.
   Indication : Soit G le groupe de Galois. Montrer que $\sigma(\Phi_n) = \Phi_n$ pour tout $\sigma \in G$.
   (g) Démontrer : $X^n - 1 = \prod_{d|n, d>0} \Phi_d(X)$ où d parcourt les diviseurs positifs de n.
   (h) Démontrer par récurrence en n que $\Phi_n(X)$ appartient à $\mathbb{Z}[X]$.
   Indication : Utiliser le résultat de Gauß (voir le cours).
   (i) Soit $\Phi_n(X) = f(X) \cdot g(X)$ avec $f, g \in \mathbb{Z}[X]$. Soit $\zeta \in \mathbb{C}$ tel que $f(\zeta) = 0$. Soit p un nombre premier qui ne divise pas p. Démontrer que $f(\zeta^p) = 0$.
   Indication : Le polynôme $X^n - 1 \in \mathbb{F}_p[X]$ est séparable. Soient $\overline{f}$ la réduction de f modulo p, et $\overline{g}$ celle de g. Donc $\gcd(\overline{f}, \overline{g}) = 1$. Si $g(\zeta_n^p) = 0$, déduire une contradiction en utilisant $\overline{g}(X^p) = (\overline{g}(X))^p$.
   (j) Démontrer que Φ_n est le polynôme minimal de ζ_n.
   Indication : Ecrire $j \in (\mathbb{Z}/n\mathbb{Z})^\times$ en facteurs premiers et utiliser le point précédent.

(k) Démontrer que le *n-ième caractère cyclotomique*

$$\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times,$$

donné par la règle $\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}$ est un isomorphisme de groupes.

3. Soit $n \geq 3$ un nombre premier.
   (a) Démontrer $\mathbb{Q}(\zeta_n)$ possède un et un seul sous-corps K tel que $[\mathbb{Q}(\zeta_n) : K] = 2$.
   (b) Donner un élément $a \in K$ tel que $K = \mathbb{Q}(a)$.
4. Soit K un corps et $f \in K[X]$ un polynôme irréductible et séparable. Soit L un corps de décomposition de f sur K. Donc L/K est une extension galoisienne. On suppose $G := \mathrm{Gal}(L/K)$ est un groupe abélien.
   Démontrer : $L = K(a)$ pour toute racine $a \in L$ de f.
   Indication : Théorème principal de la théorie de Galois.
5. (Exercice supplémentaire) Soit L/K une extension galoisienne finie et $H \leq \mathrm{Gal}(L/K)$ un sous-groupe.
   (a) Soit $a \in L$. On suppose que l'on a l'égalité $H = \{\sigma \in G \mid \sigma(a) = a\}$. Démontrer : $L^H = K(a)$.
   (b) Démontrer qu'il existe $a \in L$ avec la propriété $H = \{\sigma \in G \mid \sigma(a) = a\}$.
6. (Exercice supplémentaire) Soit L un corps algébriquement clos et $\sigma \in \mathrm{Aut}(L)$ d'ordre fini. On pose $K := L^{\langle\sigma\rangle}$ où $\langle\sigma\rangle$ est le sous-groupe de $\mathrm{Aut}(L)$ engendré par σ. Soit M/K une extension finie.
   Démontrer M/K est galoisienne et $\mathrm{Gal}(M/K)$ est un groupe cyclique.

À propos : Le problème de Syracuse

On prend un nombre entier positif. S'il est pair on le divise par 2, sinon on le multiplie par 3 et on lui ajoute 1. On répète ensuite cette opération avec le nouveau nombre obtenu. Est-il vrai qu'on obtiendra toujours le nombre 1 après un certain nombre d'étapes ?

Cette conjecture a un énoncé très simple mais se révèle être incroyablement compliqué. Paul Erdős a dit à propos de cette conjecture : « Les mathématiques ne sont pas encore prêtes pour de tels problèmes. » Il a offert d'ailleurs $500 à celui qui prouverait ou réfuterait cette conjecture.

Exercices : Algèbre 3

Semestre d'hiver 2012/2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Hoan-Phung Bui

Feuille 13

11/12/2012

Les exercices sont à rendre le 18/12/2012 au début du cours.

1. Soient L/K une extension finie et galoisienne et $G := \mathrm{Gal}(L/K)$ son groupe de Galois. On va décrire le polynôme minimal sur K de $a \in L$.

   Soit $S := \{\sigma(a) \mid \sigma \in G\}$. On numérote les éléments de S comme $a_1, a_2, a_3, \ldots, a_r$ et on pose

   $$f(X) := \prod_{i=1}^{r}(X - a_i) \in L[X].$$

   Démontrer :

   (a) $f(a) = 0$.

   (b) $f \in K[X]$.

   (c) f est irréductible comme élément de $K[X]$.

   Donc, f est le polynôme minimal de a sur K.

2. Soit L/K une extension galoisienne et finie. Soient $L/L_1/K$ et $L/L_2/K$ des extensions. On pose $H_i := \mathrm{Gal}(L/L_i)$ pour $i = 1, 2$. Démontrer :

   (a) $L_1 \subseteq L_2 \quad \Leftrightarrow \quad H_2 \subseteq H_1$.

   (b) $L_1L_2 = L^{H_1 \cap H_2}$. Ici $L_1L_2 := K(L_1, L_2)$ est l'extension de K dans L engendrée par les éléments de L_1 et L_2.

   (c) $L_1 \cap L_2 = L^H$ où $H = \langle H_1, H_2 \rangle$ est le sous-groupe de G engendré par H_1 et H_2.

3. Soit L/K une extension de corps. Soient $L/L_1/K$ et $L/L_2/K$ des extensions telles que L_1/K et L_2/K sont galoisiennes et finies. Démontrer :

   (a) Le corps $L_1L_2 := K(L_1, L_2)$ est une extension galoisienne et finie de K.

   (b) La restriction

   $$\mathrm{Gal}(L_1L_2/L_2) \to \mathrm{Gal}(L_1/(L_1 \cap L_2)), \quad \sigma \mapsto \sigma|_{L_1}$$

   est un isomorphisme de groupes.

   (c) L'application

   $$\varphi : \mathrm{Gal}(L_1L_2/K) \to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K), \quad \sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2})$$

   est un homomorphisme de groupes.

   (d) φ est injectif.

   (e) $\mathrm{im}(\varphi) = \{(\sigma, \tau) \in \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) \mid \sigma|_{L_1 \cap L_2} = \tau|_{L_1 \cap L_2}\}$.

4. Soit G un groupe abélien fini d'ordre $p^n > 1$ où p est un nombre premier. Démontrer :
   (a) Il existe un élément $g \in G$ d'ordre p.
   (b) Il existe des sous-groupes normaux
   $$\{1\} = G_n \lhd G_{n-1} \lhd G_{n-2} \lhd \cdots \lhd G_1 \lhd G_0 = G$$
   tels que G_{i-1}/G_i est cyclique d'ordre p.
   Indication : Utiliser (a), regarder le quotient $G/\langle g \rangle$ et itérer.
5. (a) Soient $a, b \in \mathbb{Z}$, $a \neq b$ et $n \in \mathbb{N}$. Démontrer : $(a-b) \mid (a^n - b^n)$.
   (b) Soit $n = rs$ avec r pair et s impair. On suppose que $2^n + 1$ est un nombre premier. Démontrer : $s = 1$.
6. (Exercice supplémentaire) Soit K un corps.
   (a) Démontrer par récurrence l'assertion suivante :

   Pour tout $n \in \mathbb{N}$ et tout corps K on a :
   Si L est une extension algébrique de $K(X_1, \ldots, X_n) := \mathrm{Frac}(K[X_1, \ldots, X_n])$ et aussi de $K(T_1, \ldots, T_m) := \mathrm{Frac}(K[T_1, \ldots, T_m])$ avec $m \geq n$, alors $m = n$.

   (b) Soit L une extension algébrique de $K(X_1, \ldots, X_n) := \mathrm{Frac}(K[X_1, \ldots, X_n])$ telle qu'il existe $t_1, \ldots, t_n \in L$ avec $L = K(t_1, \ldots, t_n)$.
   Alors, le homomorphisme d'anneaux
   $$\varphi : K[T_1, \ldots, T_n] \to L, \quad T_i \mapsto t_i$$
   est injectif.

À propos. Koffer von Göttingen