UFR MATHÉMATIQUES
Université Clermont Auvergne

Master 1 Mathématiques

Théorie des corps et algèbre bilinéaire

R. Taillefer
Rachel.Taillefer@uca.fr

2018-2019

version du 5 mai 2019, 5:19pm

Première partie

Théorie des corps

CHAPITRE 1

Extensions de corps

Dans tout ce cours, nous ne considèrerons que des corps **commutatifs**.

I EXTENSIONS DE CORPS

On rappelle qu'un sous-corps d'un corps k est un sous-anneau de k qui est stable par inverses.

Définition 1. *Soit E un corps et soit k un sous-corps de E.*

*On dit que E est une **extension** de k. On note souvent $k \subset E$ ou $\begin{matrix} E \\ | \\ k \end{matrix}$ une extension de corps.*

On rappelle que les seuls idéaux d'un corps k sont (0) et k, ce qui implique en particulier que tout morphisme de corps $k \to E$ est injectif.

Par conséquent, si $\sigma : k \to E$ est un morphisme de corps, on a un isomorphisme $k \cong \sigma(k)$ et E est une extension de $\sigma(k)$. On peut donc considérer E comme une extension de k.

Remarque. Soit E une extension d'un corps k. Alors E est en particulier un espace vectoriel sur k, qui peut être de dimension finie ou infinie.

Définition 2. *Soit $k \subset E$ une extension de corps.*

(i) *Si E est de dimension finie comme k-espace vectoriel, avec $\dim_k(E) = n$, alors on dit que l'extension $k \subset E$ est **finie, de degré** n, et on note $[E : k] = n$ le degré de l'extension.*

(ii) *Si E est de dimension infinie comme k-espace vectoriel, on dit que $k \subset E$ est une extension infinie.*

Remarque. Dans le cas d'une extension $k \subset E$ finie, c'est bien l'*extension* et non le corps E qui est fini.

Exemples. (1) Pour tout corps k, $k \subset k$ est une extension finie de degré 1.

(2) $\mathbb{C}$ est une extension de degré 2 de $\mathbb{R}$ (une base du $\mathbb{R}$-espace vectoriel $\mathbb{C}$ est donnée par $\{1, i\}$).

(3) $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}]$ où $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \mid (a, b) \in \mathbb{Q}^2\right\}$ est une extension finie de degré 2 (une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\sqrt{2}]$ est donnée par $\left\{1, \sqrt{2}\right\}$).

(4) Le corps des fractions rationnelles $k(X)$ est une extension infinie de k (la famille infinie $\left\{X^j \mid j \in \mathbb{N}\right\}$ de $k(X)$ est libre sur k).

Théorème 3. Soient $k \subset E \subset L$ des extensions de corps. Alors

(a) l'extension $k \subset L$ est finie si, et seulement si, les deux extensions $k \subset E$ et $E \subset L$ sont finies ;

(b) si $k \subset L$ est une extension finie alors

$$[L : k] = [L : E][E : k].$$

Démonstration. Soit $(e_i)_{i\in I}$ une base du k-espace vectoriel E et soit $(\ell_j)_{j\in J}$ une base du E-espace vectoriel L.

Alors $(e_i\ell_j)_{(i,j)\in I\times J}$ est une base du k-espace vectoriel L. En effet,

➢ Soit $x \in L$. Alors il existe une famille $(\lambda_j)_{j\in J}$ d'éléments de E, qui sont tous nuls sauf un nombre fini d'entre eux, telle que $x = \sum_{j\in J} \lambda_j\ell_j$. De plus, pour tout $j \in J$, il existe une famille $(\mu_{i,j})_{i\in I}$ d'éléments de k, qui sont tous nuls sauf un nombre fini d'entre eux, telle que $\lambda_j = \sum_{i\in I} \mu_{i,j}e_i$. On a alors $x = \sum_{(i,j)\in I\times J} \mu_{i,j}e_i\ell_j$ (somme finie), qui est une combinaison linéaire à coefficients dans k. Donc $(e_if_j)_{(i,j)\in I\times J}$ engendre le k-espace vectoriel L.

➢ Supposons que l'on ait $\sum_{(i,j)\in I'\times J'} \mu_{i,j}e_i\ell_j = 0$ avec $I' \subset I$ et $J' \subset J$ finies et $\mu_{i,j} \in k$ pour tous i, j. On a donc $\sum_{j\in J'} \left(\sum_{i\in I'} \mu_{i,j}e_i\right)\ell_j = 0$ avec, pour tout $j \in J'$, $\sum_{i\in I'} \mu_{i,j}e_i \in E$. Puisque $(\ell_j)_{j\in J}$ est libre sur E, on a donc $\sum_{i\in I'} \mu_{i,j}e_i = 0$ pour tout $j \in J'$. Puisque $(e_i)_{i\in I}$ est libre sur k, on a $\mu_{i,j} = 0$ pour tout $i \in I'$ et tout $j \in J'$. On en déduit donc que $(e_if_j)_{(i,j)\in I\times J}$ est libre sur k.

Par conséquent, $k \subset L$ est finie si et seulement si $I \times J$ est fini, ce qui est équivalent à I et J finies, c'est-à-dire à $k \subset E$ et $E \subset L$ finies.

De plus, si toutes ces extensions sont finies, on a

$$[L : k] = |I \times J| = |I| \cdot |J| = [E : k][L : E]. \qquad \checkmark$$

II Extensions algébriques

Définition 4. *Soit $k \subset E$ une extension de corps. Soit $\alpha \in E$.*
*On dit que α est **algébrique** sur k s'il est racine d'un polynôme non nul à coefficients dans k.*
*On dit que α est **transcendant** sur k s'il n'est pas algébrique sur k.*

Exemples. (1) $\sqrt{2} \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$ (racine de $X^2 - 2 \in \mathbb{Q}[X]$ non nul).

(2) $\omega_n = e^{2i\pi/n} \in \mathbb{C}$ est algébrique sur $\mathbb{Q}$ (racine du polynôme non nul $X^n - 1 \in \mathbb{Q}[X]$).

(3) $X \in k(X)$ est transcendant sur k (puisque la famille $\{X^n \mid n \in \mathbb{N}\}$ est libre sur k).

(4) Les nombres réels π et e sont transcendants sur $\mathbb{Q}$ (admis).

Remarque. Soient $k \subset E \subset L$ des extensions de corps et soit α un élément de L. Si α est algébrique sur k alors α est algébrique sur E.

En effet, si α est algébrique sur k alors il existe $P \in k[X]$ non nul tel que $P(\alpha) = 0$. Or $P \in E[X]$, donc α est algébrique sur E.

Définition-Proposition 5. *Soit $k \subset E$ une extension et soit $\alpha \in E$ un élément algébrique sur k.*
Alors il existe un unique polynôme irréductible et unitaire $M_\alpha \in k[X]$ tel que $M_\alpha(\alpha) = 0$.
De plus, pour tout $P \in k[X]$ tel que $P(\alpha) = 0$, on a $M_\alpha \mid P$.
*Le polynôme M_α est appelé **polynôme minimal** de α sur k.*

Démonstration. Soit $\varphi : k[X] \to E$ le morphisme d'anneaux défini par $\varphi(P) = P(\alpha)$. Par hypothèse, α est algébrique donc $\operatorname{Ker}\varphi \neq (0)$. De plus, l'anneau $k[X]$ est principal (k est un corps), donc l'idéal $\operatorname{Ker}\varphi$ est principal. Notons M_α le générateur unitaire de $\operatorname{Ker}\varphi$.

On a alors $k[X]/(M_\alpha) \cong \operatorname{Im}\varphi$, qui est un anneau intègre, donc (M_α) est un idéal premier non nul de l'anneau principal $k[X]$ et par conséquent M_α est irréductible.

Il existe donc un polynôme irréductible et unitaire $M_\alpha \in k[X]$ tel que $M_\alpha(\alpha) = 0$.

Soit maintenant P un polynôme tel que $P(\alpha) = 0$. Alors $P \in \operatorname{Ker}\varphi = (M_\alpha)$ donc $M_\alpha \mid P$. Si de plus P est irréductible, on en déduit que M_α et P sont associés. Finalement, si P est irréductible et unitaire, on obtient $P = M_\alpha$ et on a donc démontré l'unicité du polynôme irréductible et unitaire de $k[X]$ tel que $P(\alpha) = 0$. $\checkmark$

Exemples. (1) Le polynôme minimal de $\sqrt{2} \in \mathbb{R}$ sur $\mathbb{Q}$ est $X^2 - 2 \in \mathbb{Q}[X]$ (il est irréductible car il est de degré 2 et n'a pas de racine dans $\mathbb{Q}$).

(2) Soit p un nombre premier et soit $\omega_p = e^{2i\pi/n} \in \mathbb{C}$. On sait déjà que ω_p est algébrique sur $\mathbb{Q}$ et qu'il est racine de $X^p - 1$. Or $X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \cdots + X + 1)$. Posons $P(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$. Alors $P(X+1) = \dfrac{(X+1)^p - 1}{X} = \sum_{j=1}^{p} \binom{p}{j} X^{j-1}$. Ce polynôme est unitaire, son coefficient constant est p et ses autres coefficients non nuls sont les $\binom{p}{j}$ pour $2 \leqslant j \leqslant p-1$ qui sont multiples de p. Grâce au critère d'Eisenstein pour p, le polynôme $P(X+1)$ est irréductible et donc P est irréductible. C'est donc le polynôme minimal de ω_p sur $\mathbb{Q}$.

Définition 6. *Une extension $k \subset E$ est **algébrique** si tout élément de E est algébrique sur k.*

Proposition 7. Soit $k \subset E$ une extension. Si elle est finie, alors elle est algébrique.

Démonstration. Soit $k \subset E$ une extension finie de degré n. Soit $\alpha \in E$. La famille $\{1; \alpha; \alpha^2; \cdots; \alpha^n\}$ contient $n+1$ éléments, elle est donc liée sur k : il existe donc des éléments λ_i, $0 \leqslant i \leqslant n$, de k, qui ne sont pas tous nuls et tels que $\sum_{i=0}^{n} \lambda_i \alpha^i = 0$. Soit $P = \sum_{i=0}^{n} \lambda_i X^i \in k[X]$. Le polynôme P n'est pas nul et $P(\alpha) = 0$ donc α est algébrique sur k. ✓

Remarque. La réciproque est fausse : il existe des extensions algébriques qui ne sont pas finies. Voir Travaux Dirigés.

Définition-Proposition 8. *Soit $k \subset E$ une extension. Soit $\alpha \in E$.*

(a) *Le plus petit sous-anneau de E contenant k et α est $k[\alpha] = \{P(\alpha) \mid P \in k[X]\}$.*

(b) *Le plus petit sous-corps de E contenant k et α est $k(\alpha) = \left\{ \frac{P(\alpha)}{Q(\alpha)} \mid P \in k[X],\ Q \in k[X],\ Q(\alpha) \neq 0 \right\}$. C'est le corps des fractions de $k[\alpha]$.*

(c) *Soient $\alpha_1, \ldots \alpha_n$ des éléments de E. Le plus petit sous-corps de E contenant k et $\alpha_1, \ldots, \alpha_n$ est*

$$k(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{P(\alpha_1, \ldots, \alpha_n)}{Q(\alpha_1, \ldots, \alpha_n)} \mid P, Q \in k[X_1, \ldots, X_n], Q(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}.$$

(d) *Plus généralement, soit G une partie de E. Le plus petit sous-corps de E contenant k et G, noté $k(G)$, est l'intersection de tous les sous-corps de E contenant $k \cup G$. On dit que $k(G)$ est l'extension de k engendrée par G dans E.*

Remarque. On a $k(\alpha_1, \ldots, \alpha_n) = k(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$.

En effet, $k(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$ est un corps contenant $\alpha_1, \ldots, \alpha_{n-1}, \alpha_n$, donc il contient $k(\alpha_1, \ldots, \alpha_n)$. Réciproquement, on a $L := k(\alpha_1, \ldots, \alpha_{n-1}) \subset k(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n)$ et $\alpha_n \in k(\alpha_1, \ldots, \alpha_n)$. Le corps $k(\alpha_1, \ldots, \alpha_n)$ contient donc $L(\alpha_n)$ qui est le plus petit corps contenant L et α_n, donc $k(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) \subset k(\alpha_1, \ldots, \alpha_n)$.

Théorème 9. Soit $k \subset E$ une extension et soit $\alpha \in E$. Les assertions suivantes sont équivalentes.

(i) α est algébrique sur k.

(ii) $k[\alpha] = k(\alpha)$.

(iii) L'extension $k \subset k(\alpha)$ est finie.

(iv) L'extension $k \subset k(\alpha)$ est algébrique.

De plus, si ces conditions équivalentes sont vérifiées, le degré de l'extension $k \subset k(\alpha)$ est égal au degré du polynôme minimal de α sur k : on a $[k(\alpha) : k] = \deg M_\alpha$

Démonstration. ➢ (i)⇒(ii). Supposons que $\alpha \in E$ est algébrique sur k. Soit M_α son polynôme minimal. On a déjà vu que l'idéal (M_α) est le noyau du morphisme $\varphi\colon k[X] \to E$ défini par $\varphi(P) = P(\alpha)$. De plus, $\operatorname{Im}\varphi = k[\alpha]$. Puisque M_α est irréductible et $k[X]$ est principal, l'idéal (M_α) est maximal et $k[X]/(M_\alpha)$ est un corps, et par conséquent $k[\alpha]$ est un corps aussi. Or le plus petit corps contenant $k[\alpha]$ est son corps des fractions $k(\alpha)$, donc $k(\alpha) = k[\alpha]$.

➢ (ii)⇒(iii). Supposons que $k(\alpha) = k[\alpha]$. Considérons le morphisme $\varphi\colon k[X] \to E$ défini par $\varphi(P) = P(\alpha)$. Par définition, son image est $k[\alpha]$. Puisque $k[X]$ est principal, $\operatorname{Ker}\varphi = (M)$ avec $(M) \in k[X]$. Notons que M n'est pas nul car $k(\alpha)$ est un corps. On a donc $k(\alpha) = k[\alpha] \cong k[X]/(M)$.

Soit d le degré de M. Soit x un élément quelconque de $k(\alpha)$, il existe $P \in k[X]$ tel que $x = P(\alpha)$. Effectuons la division euclidienne de P par M : on a $P(X) = Q(X)M(X) + R(X)$ avec $\deg R < d$, donc $x = P(\alpha) = R(\alpha)$ est combinaison linéaire à coefficients dans k de $1, \alpha, \alpha^2, \dots, \alpha^{d-1}$. Ainsi, $k(\alpha)$ est de dimension finie inférieure à d sur k.

On en déduit que $k \subset k(\alpha)$ est finie de degré inférieur ou égal à d.

➢ Les deux implications (iii)⇒(iv) et (iv)⇒(i) sont évidentes.

Supposons que les conditions de l'énoncé soient remplies. La démonstration qui précède montre que $[k(\alpha) : k] \leqslant d$ où $d = \deg M_\alpha$. Supposons maintenant que $\sum_{i=0}^{d-1} \lambda_i \alpha^i = 0$ avec $\lambda_i \in k$ pour tout i. Soit $P = \sum_{i=0}^{d-1} \lambda_i X^i \in k[X]$. On a $P \in k[X]$ de degré inférieur à $d-1$ et $P(\alpha) = 0$. On sait alors que M_α divise P. Puisque $\deg M_\alpha = d$, on en déduit que $P = 0$. La famille $\left\{1, \alpha, \alpha^2, \dots, \alpha^{d-1}\right\}$ est donc libre. Puisqu'elle engendre $k(\alpha)$, c'est une base de $k(\alpha)$ et on a $[k(\alpha) : k] = d$. ✓

Exemple. Soit p un nombre premier et soit $\omega = e^{2i\pi/p} \in \mathbb{C}$. Alors $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1$.

En effet, on a déjà vu que le polynôme minimal de ω_p sur $\mathbb{Q}$ est $X^{p-1} + X^{p-2} + \cdots + X + 1$ qui est de degré $p - 1$.

Corollaire 10. Soit $k \subset E$ une extension et soient $\alpha_1, \dots, \alpha_n$ des éléments de E. Les assertions suivantes sont équivalentes.

(i) $\alpha_1, \dots, \alpha_n$ sont algébriques sur k.

(ii) L'extension $k \subset k(\alpha_1, \dots, \alpha_n)$ est finie.

(iii) L'extension $k \subset k(\alpha_1, \dots, \alpha_n)$ est algébrique.

Démonstration. La seule implication qui n'est pas évidente est (i)⇒(ii). Raisonnons par récurrence sur n.

Pour $n = 1$, c'est le théorème précédent.

Supposons donc que n éléments de E algébriques sur un sous-corps de E engendrent nécessairement une extension finie de ce sous-corps. Soient $\alpha_1, \dots, \alpha_{n+1}$ des éléments de E algébriques sur k. Par hypothèse de récurrence, l'extension $k \subset k(\alpha_1, \dots, \alpha_n)$ est finie. L'élément α_{n+1} est algébrique sur k donc sur $k(\alpha_1, \dots, \alpha_n)$, donc d'après le théorème, l'extension $k(\alpha_1, \dots, \alpha_n) \subset k(\alpha_1, \dots, \alpha_n)(\alpha_{n+1}) = k(\alpha_1, \dots, \alpha_n, \alpha_{n+1})$ est finie. On en déduit d'après le théorème 3 que l'extension $k \subset k(\alpha_1, \dots, \alpha_n, \alpha_{n+1})$ est finie. ✓

Remarque. Toute extension finie est de la forme $k(\alpha_1, \dots, \alpha_n)$ avec α_i algébriques.

Voir Travaux Dirigés.

Il suffit de prendre une base $\{a_1, \dots, \alpha_n\}$ de E sur k.

Corollaire 11. Soient $k \subset E \subset L$ des extensions. Alors $k \subset L$ est algébrique si, et seulement si, $k \subset E$ et $E \subset L$ sont algébriques.

Démonstration. Supposons que $k \subset L$ est algébrique. Alors tous les éléments de L, et en particulier tous les éléments de E sont algébriques sur k, donc $k \subset E$ est algébrique. De plus, tout élément de L est algébrique sur k, donc sur E et par conséquent $E \subset L$ est algébrique.

Réciproquement, supposons que $k \subset E$ et $E \subset L$ sont algébriques. Soit $\alpha \in L$. On doit démontrer que α est algébrique sur k. Il existe $\lambda_0, \dots, \lambda_d$ dans E tels que $\sum_{i=0}^{d} \lambda_i \alpha^i = 0$. Soit $E' = k(\lambda_1, \dots, \lambda_d)$. Puisque les λ_i sont dans E, ils sont algébriques sur k et donc l'extension $k \subset E'$ est finie. De plus, α est algébrique sur E' donc $E' \subset E'(\alpha)$ est finie. On en déduit que l'extension $k \subset E'(\alpha)$ est finie et donc que α est algébrique sur k. ✓

Définition 12. *Soient $k \subset E$ et $k \subset L$ des extensions de k. Un k-morphisme de E dans L est un morphisme de corps $E \to L$ qui est k-linéaire (on rappelle que E et L sont des espaces vectoriels sur k).*

Remarque. Un morphisme de corps $\varphi : E \to L$ est un k-morphisme de corps si, et seulement si, φ prolonge id_k, c'est-à-dire que $\varphi_{|k} = \mathrm{id}_k$.

Remarque. Soit $k \subset E$ une extension avec $E = k(\alpha_1, \dots, \alpha_n)$. Soit $k \subset L$ une autre extension et soit $\varphi : E \to L$ un k-morphisme. Alors φ est entièrement déterminé par les $\varphi(\alpha_i)$ pour $1 \leqslant i \leqslant n$.

En effet, si x est un élément quelconque de E, il s'écrit $x = \dfrac{P(\alpha_1, \dots, \alpha_n)}{Q(\alpha_1, \dots, \alpha_n)}$ avec $P, Q \in k[X]$ et $Q(\alpha_1, \dots, \alpha_n) \neq 0$. On a donc $\varphi(x) = \varphi(P(\alpha_1, \dots, \alpha_n))\varphi(Q(\alpha_1, \dots, \alpha_n))^{-1}$. De plus, puisque φ est un morphisme d'anneaux qui fixe les éléments de k, on en déduit que $\varphi(P(\alpha_1, \dots, \alpha_n)) = P(\varphi(\alpha_1), \dots, \varphi(\alpha_n))$ et $\varphi(Q(\alpha_1, \dots, \alpha_n)) = Q(\varphi(\alpha_1), \dots, \varphi(\alpha_n))$. Donc φ est entièrement déterminé par $\varphi(\alpha_1), \dots, \varphi(\alpha_n)$.

Proposition 13. Soit $k \subset E$ une extension *algébrique*. Alors tout k-endomorphisme de E est un k-automorphisme.

Démonstration. Soit $\varphi : E \to E$ un k-morphisme. Puisque φ est un morphisme de corps, il est injectif.

Soit $\alpha \in E$. Par hypothèse, α est algébrique sur k donc il existe $P = \sum_{i=0}^{d} \lambda_i X^i \in k[X]$ tel que $P(\alpha) = 0$. Notons R l'ensemble des racines de P dans E ; c'est un ensemble fini. De plus, si $r \in R$, alors $P(r) = 0$, donc $0 = \varphi(0) = \varphi(P(r)) = \varphi\left(\sum_{i=0}^{d} \lambda_i r^i\right) = \sum_{i=0}^{d} \lambda_i \varphi(r)^i = P(\varphi(r))$, donc $\varphi(r) \in R$.

Ainsi, φ induit une application $f : R \to R$, qui est injective puisque φ est injective, et qui est donc bijective puisque R est fini. En particulier, il existe $\beta \in R \subset E$ tel que $\alpha = f(\beta) = \varphi(\beta)$. Donc φ est surjectif. ✓

Proposition 14. Soit $k \subset E$ une extension. Soit $\mathcal{A}$ l'ensemble des éléments de E qui sont algébriques sur k. Alors $\mathcal{A}$ est un corps et $k \subset \mathcal{A}$ est une extension algébrique.

Démonstration. Voir Travaux Dirigés.

Il est clair que $k \subset \mathcal{A}$.

Une fois que l'on a démontré que $\mathcal{A}$ est un corps, il est clair que c'est une extension algébrique de k.

Démontrons dans un premier temps que $\mathcal{A}$ est un corps. Alors $k \subset \mathcal{A}$ sera bien une extension de corps algébrique.

On remarque que si $\alpha \in E$, alors $\alpha \in \mathcal{A}$ si, et seulement si, l'extension $k \subset k(\alpha)$ est finie.

Soient α et β des éléments de $\mathcal{A}$. Alors $k \subset k(\alpha, \beta)$ est une extension finie.

- ➢ On a $k \subset k(\alpha + \beta) \subset k(\alpha, \beta)$ donc $k \subset k(\alpha + \beta)$ est finie et donc $\alpha + \beta \in \mathcal{A}$.
- ➢ On a $k(-\alpha) = k(\alpha)$ finie, donc $-\alpha \in \mathcal{A}$.
- ➢ On a $k \subset k(\alpha\beta) \subset k(\alpha, \beta)$ donc $k \subset k(\alpha\beta)$ est finie et donc $\alpha\beta \in \mathcal{A}$.
- ➢ Supposons que $\alpha \neq 0$. Alors α est inversible dans E. Soit $P \in k[X]$ non nul, de degré d, tel que $P(\alpha) = 0$. Alors $P(\alpha^{-1}) = \alpha^{-d} P(\alpha) = 0$ donc $\alpha^{-1} \in \mathcal{A}$.

Ainsi, $\mathcal{A}$ est bien un sous-corps de E et donc une extension de k, qui est algébrique par définition de $\mathcal{A}$. ✓

Corollaire 15. Soit $k \subset E$ une extension, soit G une partie de E dont tous les éléments sont algébriques sur k. Alors $k \subset k(G)$ est une extension algébrique de k.

Démonstration. Voir Travaux Dirigés.

Notons $\mathcal{A}$ l'ensemble des éléments de $k(G)$ qui sont algébriques sur k. On a bien sûr $k \subset \mathcal{A} \subset k(G)$ et $G \subset \mathcal{A}$. De plus, on sait que $\mathcal{A}$ est un corps d'après la proposition précédente. Puisque $\mathcal{A}$ est un sous-corps de E qui contient k et G, il contient le plus petit corps de E qui contient k et G, c'est-à-dire $k(G)$. Par conséquent, $\mathcal{A} = k(G)$ et $k(G)$ est une extension algébrique de k. ✓

Définition 16. *Un **nombre algébrique** est un nombre complexe qui est algébrique sur* $\mathbb{Q}$.
On note $\mathbb{A}$ *l'ensemble des nombres algébriques.*

Remarque. D'après la proposition précédente, $\mathbb{A}$ est un corps et $\mathbb{Q} \subset \mathbb{A}$ est une extension algébrique.

Proposition 17. $\mathbb{A}$ est une extension algébrique de $\mathbb{Q}$ qui n'est pas finie.

Démonstration. Voir Travaux Dirigés.
Supposons que $\mathbb{Q} \subset \mathbb{A}$ soit une extension finie de degré d et soit p un nombre premier tel que $p > n+1$.
Soit $\omega = e^{2i\pi/p}$. On a déjà vu que ω est algébrique sur $\mathbb{Q}$, c'est-à-dire que $\omega \in \mathbb{A}$, donc $\mathbb{Q}(\omega) \subset \mathbb{A}$. Mais $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1 > n$ et on a obtenu une contradiction.
Donc $\mathbb{A}$ est une extension algébrique infinie de $\mathbb{Q}$. ✓

CHAPITRE 2

Décomposition des polynômes. Clôture algébrique.

I CORPS DE RUPTURE, CORPS DE DÉCOMPOSITION D'UN POLYNÔME

Définition 1. *Soit k un corps. Soit $f \in k[X]$ un polynôme non constant.*
*Un **corps de rupture** de f sur k est un corps E dont k est un sous-corps, dans lequel f a une racine α, et tel que $E = k(\alpha)$.*

Exemples. (1) $\mathbb{C}$ est un corps de rupture de X^2+1 sur $\mathbb{R}$. En effet, $\mathbb{C} = \mathbb{R}(i)$.
On remarque que $\mathbb{C} = \mathbb{R}[i] \cong \mathbb{R}[X]/(X^2+1)$.
(2) $\mathbb{Q}(\sqrt{2})$ est un corps de rupture de X^2-2 sur $\mathbb{Q}$. On remarque que $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[X]/(X^2-2)$.
(3) $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{3})$ sont des corps de rupture de X^4-5X^2+6 sur $\mathbb{Q}$.

Théorème 2. Soient k un corps et $f \in k[X]$ un polynôme non constant. Alors il existe un corps de rupture de f sur k.

Démonstration. Soit g un facteur irréductible de f. Soit $E = k[X]/(g)$. Puisque g est irréductible, E est un corps. On peut identifier k à un sous-corps de E via l'inclusion $k \hookrightarrow k[X] \twoheadrightarrow E$. De plus, si α est la classe de X dans E, on a bien $g(\alpha) = g(\overline{X}) = \overline{g(X)} = 0$ donc $f(\alpha) = 0$. Enfin, $E = k[\alpha] = k(\alpha)$. ✓

Proposition 3. (Prolongement des isomorphismes)
Soit $s\colon k \to k'$ un isomorphisme de corps. Soit $\overline{s}\colon k[X] \to k'[X]$ l'unique isomorphisme d'anneaux qui prolonge s et qui associe X à X, c'est-à-dire que $\overline{s}(\sum_{i=0}^d a_i X^i) = \sum_{i=0}^d s(a_i)X^i$. Soit $f \in k[X]$ un polynôme irréductible.

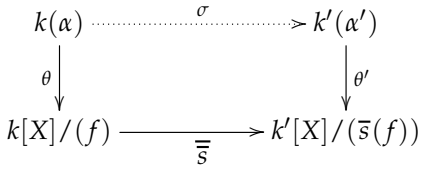
(i) Le polynôme $\overline{s}(f) \in k'[X]$ est irréductible.

(ii) Soient E (*resp.* E') une extension de k (*resp.* k') contenant une racine α (*resp.* α') de f (*resp.* $\overline{s}(f)$). Alors il existe un unique isomorphisme de corps $\sigma\colon k(\alpha) \to k(\alpha')$ qui prolonge s et tel que $\sigma(\alpha) = \alpha'$.

Démonstration. (i) Immédiat car $\overline{s}$ est un isomorphisme.

(ii) Commençons par démontrer l'unicité d'un tel isomorphisme. Soit $x = \sum_{i=0}^d \lambda_i \alpha^i \in k(\alpha) = k[\alpha]$, avec $\lambda_i \in k$ pour tout i. Si σ est un isomorphisme de corps tel que $\sigma_{|k} = s$ et $\sigma(\alpha) = \alpha'$, alors on doit avoir $\sigma(x) = \sum_{i=0}^d \sigma(\lambda_i)\sigma(\alpha)^i = \sum_{i=0}^d s(\lambda_i)(\alpha')^i$. Donc σ est unique.
Démontrons maintenant son existence. Le morphisme d'anneaux $k[X] \to k[\alpha] = k(\alpha)$ qui envoie $P(X)$ sur $P(\alpha)$ est surjectif ; son noyau contient (f) qui est un idéal maximal de $k[X]$ puisque f est irréductible et $k[X]$ est principal, donc il est égal à (f) ; finalement, on obtient un isomorphisme $k[X]/(f) \cong k(\alpha)$. Notons $\theta : k(\alpha) \to k[X]/(f)$ cet isomorphisme, qui associe $\overline{X}$ à α. De même, on a un isomorphisme $\theta' : k'(\alpha') \to k'[X]/(\overline{s}(f))$, qui associe $\overline{X}$ à α'.

On a donc



où $\overline{\overline{s}}$ est obtenu à partir de $\overline{s}$ par passage au quotient. Le morphisme $\overline{\overline{s}}$ est un isomorphisme puisque $\overline{s}$ est un isomorphisme et $\overline{s}((f)) = (\overline{s}(f))$. Alors $\sigma = (\theta')^{-1} \circ \overline{\overline{s}} \circ \theta$ est un isomorphisme qui vérifie les conditions requises. ✓

Corollaire 4. Soit k un corps. Soit $f \in k[X]$ un polynôme irréductible. Alors deux corps de rupture de f sur k sont k-isomorphes.

Démonstration. On applique la proposition 3 de prolongement des isomorphismes avec $k = k'$ et $s = \mathrm{id}_k$. ✓

Corollaire 5. Soit $k \subset E$ une extension. Soient α et α' deux éléments de E qui sont algébriques sur k. Les assertions suivantes sont équivalentes.

(i) Les polynômes minimaux de α et α' sur k sont égaux.

(ii) Il existe un (unique) k-isomorphisme de $k(\alpha)$ dans $k(\alpha')$ qui envoie α sur α'.

Démonstration. ➢ Supposons que α et α' ont le même polynôme minimal f sur k. On applique la proposition 3 de prolongement des isomorphismes avec $k = k'$ et $s = \mathrm{id}_k$ pour obtenir (ii).

➢ Soit $\sigma\colon k(\alpha) \to k(\alpha')$ un k-isomorphisme tel que $\sigma(\alpha) = \alpha'$. Si $P \in k[X]$, on a donc $\sigma(P(\alpha)) = P(\alpha')$. Soit M_α le polynôme minimal de α. Il est irréductible et unitaire. De plus, $M_\alpha(\alpha') = \sigma(M_\alpha(\alpha)) = \sigma(0) = 0$, donc α' est racine de M_α. Ainsi, M_α est le polynôme minimal de α sur k. ✓

Définition 6. *Si les conditions du corollaire 5 sont vérifiées, on dit que α et α' sont **conjugués** sur k.*

Exemples. ➢ Les éléments $\sqrt{2}$ et $-\sqrt{2}$ de $\mathbb{R}$ sont conjugués sur $\mathbb{Q}$ (leur polynôme minimal commun sur $\mathbb{Q}$ est $X^2 - 2$).

➢ Les éléments i et $-i$ de $\mathbb{C}$ sont conjugués sur $\mathbb{R}$ (leur polynôme minimal commun sur $\mathbb{R}$ est $X^2 + 1$). Plus généralement, si $(a, b) \in \mathbb{R}^2$, $a + ib$ et $a - ib$ sont conjugués sur $\mathbb{R}$ (racine du polynôme irréductible $X - a \in \mathbb{R}[X]$ si $b = 0$, racines du polynôme irréductible $X^2 - 2aX + a^2 + b^2 \in \mathbb{R}[X]$ si $b \neq 0$).

➢ Soit p un nombre premier. Les racines $p^{\text{ièmes}}$ de l'unité distinctes de 1 (dans $\mathbb{C}$) sont conjuguées sur $\mathbb{Q}$ (leur polynôme minimal commun sur $\mathbb{Q}$ est $\sum_{j=0}^{p-1} X^j$).

Définition 7. *Soit k un corps et soit $f \in k[X]$ un polynôme non constant. Un **corps de décomposition** de f sur k est un corps E dont k est un sous-corps et qui vérifie les deux conditions suivantes :*

(i) *f est scindé dans $E[X]$, c'est-à-dire qu'il existe $c \in k$ et $a_1, \ldots, a_n$ dans E tels que $f(x) = c(X - a_1) \cdots (X - a_n)$, et*

(ii) *$E = k(a_1, \ldots, a_n)$.*

Pour le théorème suivant, nous aurons besoin d'un lemme.

Lemme 8. Soit $s\colon k \to k'$ un isomorphisme de corps, soit $\overline{s}\colon k[X] \to k'[X]$ l'isomorphisme d'anneaux induit, soit $f \in k[X]$ un polynôme non constant, soit E un corps de décomposition de f sur k et soit E' un corps de décomposition de $\overline{s}(f)$ sur k'. Alors il existe un isomorphisme $\sigma\colon E \to E'$ qui prolonge s.

De plus, si $g \in k[X]$ est un facteur irréductible de f, si α est une racine de g dans E et si α' est une racine de $\overline{s}(g)$ dans E', alors on peut choisir σ de sorte que $\sigma(\alpha) = \alpha'$.

Démonstration. On raisonne par récurrence sur le degré de f.

➢ Si $\deg f = 1$, alors $E = k$ et $E' = k'$ et on peut prendre $\sigma = s$.

➢ Soit $n \in \mathbb{N}$, $n \geqslant 2$, tel que le résultat est vrai pour tous les corps k, k', tous les isomorphismes $s\colon k \to k'$ et tous les polynômes de $k[X]$ de degré inférieur ou égal à $n-1$.
Soit $s\colon k \to k'$ un isomorphisme de corps et soit $f \in k[X]$ un polynôme de degré n. Posons $E = k(\alpha_1, \dots, \alpha_n)$ et $E' = k'(\alpha'_1, \dots, \alpha'_n)$ où les α_i sont les racines de f et les α'_i sont les racines de $\overline{s}(f)$. Soit $g \in k[X]$ un facteur irréductible de f et soit α (*resp.* α') une racine de g (*resp.* de $\overline{s}(g)$). Quitte à renuméroter les α_i et les α'_i, on peut supposer que $\alpha = \alpha_1$ et $\alpha' = \alpha'_1$.
Soit $L = k(\alpha)$. D'après la proposition 3 de prolongement des isomorphismes, il existe un isomorphisme de corps $t\colon L \to L'$ qui prolonge s et tel que $t(\alpha) = \alpha'$. Soit $\overline{t}\colon L[X] \to L'[X]$ l'isomorphisme d'anneaux induit. Dans $L[X]$, on a $f(X) = (X-\alpha)h(X)$. On a donc $\overline{t}(f(X)) = (X-\alpha')\overline{t}(h(X))$. Notons que $E = L(\alpha_2, \dots, \alpha_n)$ est un corps de décomposition de h sur L et que $E' = L'(\alpha'_2, \dots, \alpha'_n)$ est un corps de décomposition de $\overline{t}(h)$ sur L'. Puisque $\deg h < n$, on peut appliquer l'hypothèse de récurrence, et il existe un isomorphisme de corps $\sigma\colon E \to E'$ qui prolonge t ; par conséquent, σ prolonge s et $\sigma(\alpha) = t(\alpha) = \alpha'$. ✓

Théorème 9. Soit k un corps et soit $f \in k[X]$ un polynôme non constant.

(i) Il existe un corps de décomposition pour f sur k.

(ii) Deux corps de décomposition de f sur k sont k-isomorphes.

Démonstration. (i) On démontre l'existence d'un corps de décomposition par récurrence sur le degré de f.

➢ Si f est de degré 1, alors k est un corps de décomposition de f sur k.

➢ Soit $d \geqslant 2$ tel que le résultat soit vrai pour tout polynôme de degré inférieur ou égal à $d-1$ sur tout corps k. Soit $f \in k[X]$ un polynôme de degré d. Soit L un corps de rupture de f : on a $L = k(\alpha)$ et $f(X) = (X-\alpha)g(X)$ dans $L[X]$. Puisque $\deg g \leqslant d-1$, par hypothèse de récurrence il existe un corps de décomposition de g sur L, égal à $L(\beta_1, \dots, \beta_{d-1})$. Alors $L(\beta_1, \dots, \beta_{d-1}) = k(\beta_1, \dots, \beta_{d-1}, \alpha)$ est un corps de décomposition de f sur k.

(ii) Pour démontrer l'unicité à k-isomorphisme près, on applique le lemme 8 avec $k = k'$ et $s = \mathrm{id}_k$. ✓

Exemples. (1) Les racines de $f(X) = (X^2-3)(X^3+1)$ dans $\mathbb{C}$ sont $\pm\sqrt{3}$, $e^{2i\pi/6} = \frac{1}{2}(1+i\sqrt{3})$, -1 et $e^{10i\pi/6} = \frac{1}{2}(1-i\sqrt{3})$ donc $\mathbb{Q}(\sqrt{3}, -\sqrt{3}, \frac{1}{2}(1+i\sqrt{3}), \frac{1}{2}(1-i\sqrt{3})) = \mathbb{Q}(i, \sqrt{3})$ est un corps de décomposition de f sur $\mathbb{Q}$.

(2) Les polynômes X^2-3 et X^2-2X-2 ont tous deux $\mathbb{Q}(\sqrt{3})$ comme corps de décomposition sur $\mathbb{Q}$.

II Clôture algebrique

Proposition 10. Soit k un corps. Les assertions suivantes sont équivalentes.

(i) Tout polynôme non constant de $k[X]$ est scindé dans $k[X]$, c'est-à-dire qu'il se décompose comme produit de polynômes de degré 1 de $k[X]$.

(ii) Tout polynôme irréductible de $k[X]$ est de degré 1.

(iii) Toute extension algébrique de k est triviale (égale à k).

(iv) Tout polynôme non constant de $k[X]$ admet au moins une racine dans k.

Démonstration. ➢ (i)⇒(ii). Puisque k est un corps, tout polynôme de degré 1 de $k[X]$ est irréductible. De plus, si f est un polynôme irréductible de $k[X]$, d'après (i) on peut écrire $f = \prod_{i=1}^{r} g_i$ avec $g_i \in k[X]$ de degré 1 pour tout i. On a donc deux décompositions d'un polynôme en produit de facteurs irréductibles, donc $r = 1$ et f est associé à g_1 puisque $k[X]$ est factoriel, donc f est de degré 1. (On peut aussi dire que $f = g_1 h$ avec $h = \prod_{i=2}^{r} g_i$, et puisque f est irréductible et g_1 n'est pas inversible, h est inversible donc constant, donc f et g_1 sont associés).

➢ (ii)⇒(iii). Soit $k \subset E$ une extension algébrique. Soit $\alpha \in E$ et soit M_α son polynôme minimal. Puisqu'il est irréductible, il est de degré 1. Il est également unitaire, donc $M_\alpha = X - \alpha \in k[X]$ et par conséquent $\alpha \in k$.

➢ (iii)⇒(iv). Soit $f \in k[X]$ et soit $k(\alpha)$ un corps de rupture de f sur k. Alors $k \subset k(\alpha)$ est algébrique, donc triviale, et donc $\alpha \in k$. Ainsi, f a bien une racine dans k.

➢ (iv)⇒(i). Par récurrence sur le degré du polynôme.

✓

Définition 11. *Un corps satisfaisant une des conditions équivalentes de la proposition précédente est dit* ***algébriquement clos****.*

Exemple. $\mathbb{Q}$ et $\mathbb{R}$ ne sont pas algébriquement clos.

Théorème 12. Le corps $\mathbb{C}$ est algébriquement clos.

Démonstration. Admis.

Avec les polynômes symétriques. Soit $P \in \mathbb{C}[X]$ un polynôme non constant. Nous devons démontrer que P a une racine dans $\mathbb{C}$.

Remarquons que $\overline{P}P \in \mathbb{R}[X]$ (où $\overline{P}$ désigne le conjugué de P). De plus, si P a une racine dans $\mathbb{C}$ alors $\overline{P}P$ aussi et si $\overline{P}P$ a une racine dans $\mathbb{C}$, alors soit P a une racine dans $\mathbb{C}$ soit $\overline{P}$ a une racine $\alpha \in \mathbb{C}$ mais alors $\overline{\alpha} \in \mathbb{C}$ est une racine de P. Ainsi, P a une racine complexe si, et seulement si, $\overline{P}P$ a une racine complexe et on peut donc supposer que $P \in \mathbb{R}[X]$. De plus, quitte à multiplier par l'inverse du coefficient dominant, on peut supposer que P est unitaire.

Posons $\deg P = d = 2^n q$ avec q impair. On va raisonner par récurrence sur $n \in \mathbb{N}$.

✦ Si $n = 0$, alors P est de degré impair et il a une racine réelle d'après le théorème des valeurs intermédiaires.

✦ Soit $n \geqslant 1$ tel que le résultat est vrai pour les polynômes de degré $2^{n-1}q'$ avec q' impair.

Soit L un corps de décomposition de P sur $\mathbb{C}$: P est scindé sur L, donc $P = (X - \alpha_1) \cdots (X - \alpha_d)$ avec $\alpha_i \in L$. On doit démontrer que l'un au moins des α_i est dans $\mathbb{C}$.

Notons $\sigma_1, \dots, \sigma_d$ les polynômes symétriques élémentaires en $X_1, \dots, X_d$ et posons $\widetilde{\sigma}_k = \sigma_k(\alpha_1, \dots, \alpha_d)$. D'après les relations coefficients-racines, pour tout k on a $\widetilde{\sigma}_k \in \mathbb{R}$.

Pour tout $(i,j) \in \mathbb{N}^2$ avec $1 \leqslant i, j \leqslant d$ et tout $c \in \mathbb{R}$, on pose $\beta_{ij}^{(c)} = \alpha_i + \alpha_j + c\alpha_i\alpha_j$; nous allons démontrer que pour tout c, l'un des $\beta_{ij}^{(c)}$ est dans $\mathbb{C}$. Pour cela, on considère les polynômes

$$\widetilde{Q}_c = \prod_{1 \leqslant i,j \leqslant d} (X - \beta_{ij}^{(c)}) \in L[X],\ c \in \mathbb{R}.$$

On a $\widetilde{Q}_c = Q_c(\alpha_1, \dots, \alpha_d)$ où $Q_c = \prod_{1 \leqslant i,j \leqslant d}(X - X_i - X_j - cX_iX_j) \in \mathbb{R}[X][X_1, \dots, X_d]$. Le polynôme Q_c est un polynôme symétrique en $X_1, \dots, X_d$, donc il existe un polynôme $T \in \mathbb{R}[X][X_1, \dots, X_d]$ tel que $Q_c = T(\sigma_1, \dots, \sigma_d)$. On en déduit que $\widetilde{Q}_c = T(\widetilde{\sigma}_1, \dots, \widetilde{\sigma}_d) \in \mathbb{R}[X]$ puisque les $\widetilde{\sigma}_k$ sont réels.

De plus, $\deg Q_c = \sum_{i=1}^{n}(d - i + 1) = \frac{d(d+1)}{2} = 2^{n-1}q'$ avec $q' = q(d+1)$ impair. Donc d'après l'hypothèse de récurrence Q_c a une racine γ_c dans $\mathbb{C}$.

Par conséquent, pour tout $c \in \mathbb{R}$, il existe $(i(c), j(c)) \in [\![1\,;d]\!]^2$ tel que $\gamma_c = \beta_{i(c)j(c)}^{(c)} = \alpha_{i(c)} + \alpha_{j(c)} + c\alpha_{i(c)}\alpha_{j(c)} \in \mathbb{C}$.

Puisque $\mathbb{R}$ est infini et que les indices $(i(c), j(c))$ parcourent un ensemble fini, il existe des nombres réels $c_1 \neq c_2$ tels que $(i(c_1), j(c_1)) = (i(c_2), j(c_2))$. Notons $r = i(c_1) = i(c_2)$ et $s = j(c_1) = j(c_2)$. Alors $\gamma_{c_1} = \alpha_r + \alpha_s + c_1\alpha_r\alpha_s \in \mathbb{C}$ et $\gamma_{c_2} = \alpha_r + \alpha_s + c_2\alpha_r\alpha_s \in \mathbb{C}$. Posons $u = \alpha_r + \alpha_s$ et $v = \alpha_r\alpha_s$. Alors $(c_1 - c_2)v = \gamma_{c_1} - \gamma_{c_2} \in \mathbb{C}$ donc $v \in \mathbb{C}$ et $u = \gamma_{c_1} - c_1 v \in \mathbb{C}$. De plus, α_r et α_s sont les racines de $X^2 - uX + v \in \mathbb{C}[X]$, et l'on sait que ces racines sont complexes.

On a donc démontré que les racines α_r et α_s de P sont dans $\mathbb{C}$, donc P a bien une racine complexe. ✓

Proposition 13. Tout corps algébriquement clos est infini.

Démonstration. Soit k un corps fini, posons $k = \{a_1, \dots, a_n\}$. Soit $f(X) = \prod_{i=1}^{n}(X - a_i) + 1$. Pour tout i on a $f(a_i) \neq 0$ donc f n'a pas de racine dans k. Donc k n'est pas algébriquement clos. ✓

Définition 14. *Soit k un corps. Une clôture algébrique $\overline{k}$ de k est une extension algébrique $k \subset \overline{k}$ telle que $\overline{k}$ est algébriquement clos.*

Théorème 15. Tout corps admet une clôture algébrique.

Démonstration. Admis.

Soit k un corps. Soit $\mathcal{F}$ l'ensemble des polynômes non constants de $k[X]$.

Soit $(x_f)_{f\in\mathcal{F}}$ une famille d'indéterminées indexée par $\mathcal{F}$ et soit A l'anneau $A = k[x_f]_{f\in\mathcal{F}}$: il s'agit de l'ensemble des polynômes en les x_f, chaque polynôme ne faisant intervenir qu'un nombre fini d'indéterminées.

Soit I l'idéal de A engendré par $\left\{f(x_f) \mid f \in \mathcal{F}\right\}$.

Montrons que $I \neq A$, par l'absurde. Supposons que $I = A$. Alors $1 \in I$, donc il s'écrit comme combinaison linéaire finie de $f(x_f)$, $f \in \mathcal{F}$, à coefficients dans A. Il existe une famille finie $\{f_1, \dots, f_n\}$ d'éléments de $\mathcal{F}$ et des éléments $g_1, \dots, g_n$ de A tels que

$$1 = \sum_{i=1}^{n} g_i f_i(x_{f_i}).$$

Pour tout i, posons $X_i = x_{f_i}$. On a un nombre fini de polynômes $g_1, \dots, g_n$, qui font donc intervenir un nombre fini d'indéterminées $X_1, \dots, X_n, X_{n+1}, \dots, X_r$ où $X_{n+1}, \dots, X_r$ sont des indeterminées de la forme x_f avec $f \neq f_i$ pour tout i. On a donc $1 = \sum_{i=1}^{n} g_i(X_1, \dots, X_r) f_i(X_i)$.

Soit E un corps de décomposition de $\prod_{i=1}^{n} f_i$: il contient donc, pour tout i, une racine α_i de f_i. Pour $n+1 \leqslant i \leqslant r$, posons $\alpha_i = 0$. Alors on a

$$1 = \sum_{i=1}^{n} g_i(\alpha_1, \dots, \alpha_r) f_i(\alpha_i) = 0.$$

On a obtenu une contradiction, donc $I \neq A$.

Soit $\mathfrak{m}$ un idéal maximal de A qui contient I. Alors $k_1 = A/\mathfrak{m}$ est un corps qui contient k (puisque $\mathfrak{m}$ ne contient pas de constante), comme sous-corps donc k_1 est une extension de k. De plus, la classe de x_f dans k_1 est une racine de f dans k_1, c'est donc un élément algébrique sur k. Puisque k_1 est engendré par les classes des x_f pour $f \in \mathcal{F}$, qui sont toutes des éléments algébriques sur k, l'extension $k \subset k_1$ est algébrique d'après le corollaire 15 du chapitre 1.

On a ainsi construit une extension algébrique $k \subset k_1$ telle que tout polynôme non constant de $k[X]$ (mais pas nécessairement ceux de $k_1[X]$) a une racine dans k_1.

On recommence la construction pour obtenir une extension algébrique $k_1 \subset k_2$ telle que tout polynôme non constant de $k_1[X]$ (mais pas nécessairement ceux de $k_2[X]$) a une racine dans k_2.

On construit ainsi une chaîne $k \subset k_1 \subset k_2 \subset \ldots \subset k_n \subset \ldots$ de corps telle que pour tout n, l'extension $k_n \subset k_{n+1}$ est algébrique et tout polynôme non constant de $k_n[X]$ admet une racine dans k_{n+1}. Notons que pour tout n, l'extension $k \subset k_n$ est aussi algébrique.

Posons $\overline{k} = \bigcup_{n\in\mathbb{N}} k_n$ (avec $k_0 = k$). Alors $\overline{k}$ est un corps, qui est une extension de k. De plus, si x est un élément de $\overline{k}$, il est dans l'un des k_n donc il est algébrique sur k ; ainsi, l'extension $k \subset \overline{k}$ est algébrique.

Enfin, si f est un polynôme non constant à coefficients dans $\overline{k}$, c'est un polynôme de $k_n[X]$ pour un n, donc il admet une racine dans $k_{n+1} \subset \overline{k}$; ainsi, $\overline{k}$ est algébriquement clos. ✓

Exemple. $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$, mais pas de $\mathbb{Q}$ (car $\mathbb{Q} \subset \mathbb{C}$ n'est pas algébrique).

Théorème 16. Soit $E \subset L$ une extension algébrique et soit Ω un corps algébriquement clos.
Pour tout morphisme de corps $E \to \Omega$, il existe un morphisme de corps $L \to \Omega$ qui le prolonge.

modifié le 14/02/2019

Démonstration. Soit $\varphi\colon E \to \Omega$ un k-morphisme.

Soit $\mathcal{E} = \left\{(F, f) \mid E \subset F \subset L,\ f\colon F \to \Omega,\ f_{|E} = \varphi\right\}$. L'ensemble $\mathcal{E}$ n'est pas vide puisqu'il contient (E, φ).

On définit une relation d'ordre (partiel) sur $\mathcal{E}$ en posant

$$(F, f) \preccurlyeq (F', f') \iff F \subset F' \text{ et } f'_{|F} = f.$$

Nous allons démontrer que $(\mathcal{E}, \preccurlyeq)$ est un ensemble inductif pour ensuite appliquer le lemme de Zorn.

Soit $\mathcal{F} = \{(F_i, f_i) \in \mathcal{E} \mid i \in I\}$ une famille totalement ordonnée d'éléments de $\mathcal{E}$. On doit démontrer qu'elle admet un majorant dans $\mathcal{E}$. Posons $F = \cup_{i\in I} F_i$: c'est un corps contenant E et contenu dans L.

Soit $f : F \to \Omega$ défini de la façon suivante : si $x \in F$, il existe $i \in I$ tel que $x \in F_i$, et on pose $f(x) = f_i(x)$. L'application f est bien définie : s'il existe $j \in I$ tel que $x \in F_j$, on doit vérifier que $f_i(x) = f_j(x)$. Puisque $\mathcal{F}$ est totalement ordonnée, on a par exemple $(F_i, f_i) \preccurlyeq (F_j, f_j)$ et donc $F_i \subset F_j$ et $f_{j|F_i} = f_i$, donc $f_j(x) = f_i(x)$. On vérifie que f est un morphisme de corps. D'abord, pour tout $i \in I$ on a $1 \in F_i$ donc $f(1) = f_i(1) = 1$. Soient x et y deux éléments de F. Il existe donc i et j dans I tels que $x \in F_i$ et $y \in F_j$. Puisque $\mathcal{F}$ est totalement ordonné, en particulier on a par exemple $F_i \subset F_j$ donc x et y sont dans le corps F_j, ainsi que $x + y$ et xy. On a donc $f(x+y) = f_j(x+y) = f_j(x) + f_j(y) = f(x) + f(y)$ et $f(xy) = f_j(xy) = f_j(x)f_j(y) = f(x)f(y)$. De plus, $f_{|E} = (f_i)_{|E} = \varphi$ (pour n'importe quel $i \in I$). Ainsi, $(F, f) \in \mathcal{E}$ et c'est un majorant de $\mathcal{F}$. Donc l'ensemble $\mathcal{E}$ est inductif.

On en déduit, grâce au lemme de Zorn, que $\mathcal{E}$ admet un élément maximal $(\hat{E}, \hat{f}) \in \mathcal{E}$.

Démontrons que $\hat{E} = L$. Si $\hat{E} \subsetneq L$, alors il existe $\alpha \in L$ tel que $\alpha \notin \hat{E}$. Puisque L est algébrique sur E, l'élément α admet un polynôme minimal $M_\alpha = \sum_{i=0}^{d} a_i X^i \in E[X]$. Le polynôme $\sum_{i=0}^{d} \hat{f}(a_i) X^i \in \Omega[X]$ admet au moins une racine β dans Ω. On applique la proposition 3 de prolongement des isomorphismes avec $s : \hat{E} \xrightarrow{\hat{f}} \operatorname{Im} \hat{f}$ et $\alpha' = \beta$ pour obtenir un isomorphisme $\sigma : \hat{E}(\alpha) \to (\operatorname{Im} \hat{f})(\beta)$ (qui prolonge s), qui induit $g : \hat{E}(\alpha) \to \Omega$ en composant avec l'injection $(\operatorname{Im} \hat{f})(\beta) \hookrightarrow \Omega$. On a alors $(\hat{E}(\alpha), g) \in \mathcal{E}$ et $(\hat{E}, \hat{f}) \prec (\hat{E}(\alpha), g)$, ce qui contredit la maximalité de $(\hat{E}, \hat{f}) \in \mathcal{E}$.

Donc $\hat{E} = L$ et ainsi $(L, \hat{f}) \in \mathcal{E}$. Par conséquent, $\hat{f}$ est un prolongement de φ à L. ✓

Remarque. Si $k \subset E \subset L$ sont des extensions avec $E \subset L$ algébrique et si Ω est une clôture algébrique de k, alors on peut préciser la conclusion du théorème :

Pour tout k-morphisme $E \to \Omega$, il existe un k-morphisme $L \to \Omega$ qui le prolonge.

Corollaire 17. Soit $k \subset L$ une extension algébrique et soit $\overline{k}$ une clôture algébrique de k. Alors L se plonge dans $\overline{k}$, c'est-à-dire qu'il existe un k-morphisme (injectif) $L \to \overline{k}$.

Démonstration. On applique le théorème avec $k = E$. ✓

Corollaire 18. Soient k et k' deux corps, soit $t : k \to k'$ un isomorphisme de corps et soit Ω (resp. Ω') une clôture algébrique de k (resp. k'). Alors il existe un isomorphisme de corps $\varphi : \Omega \to \Omega'$ qui prolonge t.

En particulier, deux clôtures algébriques de k sont k-isomorphes.

modifié le 14/02/2019

Démonstration. Notons $i : k \hookrightarrow \Omega$ et $i' : k' \hookrightarrow \Omega'$ les inclusions.

L'extension $k \subset \Omega$ est algébrique et $i' \circ t : k \to \Omega'$ est un morphisme de corps. D'après le théorème, il existe un morphisme de corps $\varphi : \Omega \to \Omega'$ qui prolonge $i' \circ t$. Notons que φ est injectif.

De même, il existe un morphisme de corps $\psi : \Omega' \to \Omega$ qui prolonge $i \circ t^{-1}$.

Alors $\varphi \circ \psi : \Omega' \to \Omega'$ est un endomorphisme de corps. De plus, $\varphi \circ \psi_{|k'} = \varphi \circ i \circ t^{-1} = \varphi_{|t^{-1}(k)} \circ t^{-1} = i' \circ t \circ t^{-1} = i'$ donc $\varphi \circ \psi$ est un k'-endomorphisme et donc un k'-automorphisme puisque $k' \subset \Omega'$ est algébrique. On en déduit en particulier que φ est surjectif. C'est donc un isomorphisme et $\varphi_{|k} = i' \circ t$. ✓

Remarque. Il y a plusieurs isomorphismes entre deux clôtures algébriques en général, on ne peut donc pas parler de «la» clôture algébrique.

Remarque. Soit $k \subset E$ une extension algébrique. Soit $\overline{k}$ une clôture algébrique de k et soit $\overline{E}$ une clôture algébrique de E. Alors $\overline{E} \cong \overline{k}$.

En effet, $\overline{E}$ est un corps algébriquement clos et l'extension $E \subset \overline{E}$ est algébrique donc l'extension $k \subset \overline{E}$ est algébrique aussi. Ainsi, $\overline{E}$ est une clôture algébrique de k et elle est donc isomorphe à $\overline{k}$.

CHAPITRE 3

Caractéristique d'un corps. Corps finis

I SOUS-CORPS PREMIER ET CARACTÉRISTIQUE D'UN CORPS

Définition 1. *Un corps est dit **premier** s'il n'a pas de sous-corps autre que lui-même.*

Proposition 2. Tout corps admet un sous-corps premier, qui est l'intersection de tous ses sous-corps.

Soit k un corps et soit $\varphi\colon \mathbb{Z} \to k$ l'application définie par $\varphi(n) = n \cdot 1_k$. C'est un morphisme d'anneaux, donc son noyau $\operatorname{Ker}\varphi$ est un idéal de $\mathbb{Z}$, il est donc de la forme $p\mathbb{Z}$ avec $p \in \mathbb{N}$.

Définition 3. *Soit k un corps et soit $\varphi\colon \mathbb{Z} \to k$ le morphisme d'anneaux défini par $\varphi(n) = n \cdot 1_k$. Soit $p \in \mathbb{N}$ l'entier tel que $\operatorname{Ker}\varphi = p\mathbb{Z}$.*
*Alors p est appelé la **caractéristique** de k.*

Remarque. Soit k un corps de caractéristique $p > 0$. On remarque que pour tout $x \in k$ on a $px = 0$. En effet, $px = p \cdot 1_k \cdot x = \varphi(p)x = 0 \cdot x = 0$.

Théorème 4. Soit k un corps et soit p la caractéristique de k.

(a) Si $p = 0$ alors le sous-corps premier de k est isomorphe à $\mathbb{Q}$.

(b) Si $p > 0$ alors p est premier et le sous-corps premier de k est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Démonstration. Notons que tout sous-corps de k contient nécessairement 1_k et donc $\operatorname{Im}\varphi$.

(a) Supposons que $p = 0$, c'est-à-dire que $\varphi : \mathbb{Z} \to k$ est injectif et $\operatorname{Im}\varphi \cong \mathbb{Z}$. Le sous-corps premier de k contient $\operatorname{Im}\varphi$ et donc il est égal à $\operatorname{Frac}(\operatorname{Im}\varphi)$, qui est isomorphe à $\operatorname{Frac}(\mathbb{Z}) = \mathbb{Q}$.

(b) Supposons que $p > 0$, c'est-à-dire que le noyau de $\varphi : \mathbb{Z} \to k$ est $p\mathbb{Z}$. Alors $\operatorname{Im}\varphi \cong \mathbb{Z}/p\mathbb{Z}$ par le premier théorème d'isomorphisme. Or $\operatorname{Im}\varphi$ est un sous-anneau de k donc il est intègre, et donc p est premier et $\mathbb{Z}/p\mathbb{Z}$ est un corps et $\operatorname{Im}\varphi$ aussi. Donc $\operatorname{Im}\varphi$ est le sous-corps premier de k et il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. ✓

Lemme 5. Soit k un corps de caractéristique $p > 0$. Alors pour tout $(x, y) \in k^2$ on a

$$(x + y)^p = x^p + y^p.$$

Démonstration. Puisque k est commutatif, les éléments x et y commutent et on peut appliquer la formule du binôme de Newton : $(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + \sum_{i=1}^{p-1} \binom{p}{i} x^i y^{p-i} + y^p$.
Nous allons vérifier que pour tout i tel que $1 \leqslant i \leqslant p-1$, le coefficient $\binom{p}{i}$ est un multiple de p dans $\mathbb{Z}$, qui vaut donc 0 dans k.
Par définition de $\binom{p}{i}$, on a la relation suivante dans $\mathbb{Z}$:

$$i!(p-i)!\binom{p}{i} = p \cdot (p-1)!$$

donc le nombre premier (irréductible) p divise le produit $i!(p-i)!\binom{p}{i}$, donc d'après le lemme de Gauss, il divise l'un des facteurs du produit.
Mais p ne divise aucun des entiers m tels que $1 \leqslant m \leqslant i$ (car $i < p$) ou $1 \leqslant m \leqslant p-i$ (car $p-i < p$), donc toujours d'après le lemme de Gauss p ne divise pas $i!(p-i)!$. Par conséquent, p divise $\binom{p}{i}$. ✓

II Corps finis

Remarque. Si k est un corps fini, son sous-corps premier est donc fini et par conséquent la caractéristique de k est un nombre premier p.

Théorème 6. Soit k un corps (commutatif) et soit G un sous-groupe fini (multiplicatif) de k^*. Alors G est cyclique.

Rappel. Soit G un groupe abélien fini non trivial. Alors G est isomorphe au produit direct de ses sous-groupes de Sylow.

Si on pose $|G| = p_1^{n_1} \cdots p_s^{n_s}$ avec $p_1, \ldots, p_s$ des nombres premiers distincts et $n_1, \ldots, n_s$ dans $\mathbb{N}^*$, alors le p_i-sous-groupe de Sylow H_i, qui est d'ordre $p_i^{n_i}$, est isomorphe à un produit direct de groupes cycliques $C_{p_i^{r_1}} \cdots C_{p_i^{r_m}}$ avec $1 \leqslant r_1 \leqslant \cdots \leqslant r_m$ uniques et $r_1 + \cdots + r_m = n_i$, d'après le théorème de Kronecker.

Démonstration. Soit G un sous-groupe fini de k^*, qui est donc un groupe abélien fini. Supposons que G n'est pas trivial, d'ordre $p_1^{n_1} \cdots p_s^{n_s}$ avec $p_1, \ldots, p_s$ des nombres premiers distincts et $n_1, \ldots, n_s$ dans $\mathbb{N}^*$. On a alors $G \cong H_1 \times H_2 \times \cdots \times H_s$ avec H_i le p_i-sous-groupe de Sylow de G. Selon le rappel, on a $H_i \cong C_{p_i^{r_1}} \cdots C_{p_i^{r_m}}$ avec $1 \leqslant r_1 \leqslant \cdots \leqslant r_m$ uniques et $r_1 + \cdots + r_m = n_i$. Notons que $|H_i| \geqslant p_i^{r_m}$. Tous les éléments x de H_i vérifient $x^{p_i^{r_m}} = 1$, ce sont donc des racines du polynôme $X^{p_i^{r_m}} - 1$ de $k[X]$. Puisque k est intègre, ce polynôme a au plus $p_i^{r_m}$ racines, donc $|H_i| \leqslant p_i^{r_m}$. On en déduit que $|H_i| = p_i^{r_m}$ et donc que $H_i \cong C_{p_i}^{r_m}$ est cyclique d'ordre $p_i^{r_m}$.
On a donc $G \cong C_{p_1^{u_1}} \times \cdots C_{p_s^{u_s}}$, qui est isomorphe à un groupe cyclique d'après le théorème Chinois.

Autre démonstration. Posons $n = |G|$.
Soit d un diviseur de n. S'il existe un élément a de G d'ordre d, alors G a un sous-groupe cyclique $H = \langle a \rangle \cong C_d$ d'ordre d. Pour tout élément y de H on a $y^d = 1$, donc y est racine du polynôme $X^d - 1 \in k[X]$, qui a donc au moins d racines. Puisque k est intègre, ce polynôme a au plus d racines, il en a donc exactement d, qui sont précisément les éléments de H. De plus, le nombre d'éléments d'ordre d de H est $\varphi(d)$ où φ est l'indicatrice d'Euler.
Ainsi, pour tout diviseur d de G, le nombre d'éléments $N(d)$ de G d'ordre d est soit 0, soit $\varphi(d)$ et on a $N(d) \leqslant \varphi(d)$.
On sait que l'ordre de tout élément de G divise n, donc on a

$$n = |G| = \sum_{d|n} N(d) \leqslant \sum_{d|n} \varphi(d).$$

Mais en raisonnant dans le groupe cyclique C_n, on sait aussi que $n = \sum_{d|n} \varphi(d)$. On en déduit donc que pour tout diviseur d de n on a $N(d) = \varphi(d)$ et en particulier que $N(n) = \varphi(n) > 0$, c'est-à-dire que G contient un élément d'ordre n. Par conséquent, G est cyclique d'ordre n. ✓

Théorème 7. Soit k un corps fini. Alors il existe un nombre premier p (qui est la caractéristique de k) et un nombre entier $r \in \mathbb{N}^*$ tels que $|k| = p^r$.

Réciproquement, si p est un nombre premier et si $r \in \mathbb{N}^*$, il existe un corps à p^r éléments, unique à isomorphisme près.

Démonstration. Supposons que k est un corps fini. Son sous-corps premier est donc isomorphe à $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Alors k est un espace-vectoriel sur $\mathbb{F}_p$, nécessairement de dimension finie $r \in \mathbb{N}^*$. Le nombre d'éléments de k est donc p^r.
Réciproquement, soit p un nombre premier et soit $r \in \mathbb{N}^*$. Posons $q = p^r$. Soit $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$. Soit $\mathcal{R}$ l'ensemble des racines de $f := X^q - X \in \mathbb{F}_p[X]$ dans $\overline{\mathbb{F}_p}$. On a $f'(X) = qX^{q-1} - 1 = -1$

puisque q est multiple de p et $\mathbb{F}_p$ est de caractéristique p. Ainsi, toutes les racines de f sont simples. Par conséquent, $|\mathcal{R}| = q$.

Démontrons que $\mathcal{R}$ est un corps.

➢ 0 et 1 sont dans $\mathcal{R}$.

➢ Si x et y sont dans $\mathcal{R}$, alors $(x+y)^q = x^q + y^q = x + y$ donc $x + y \in \mathcal{R}$ et $(xy)^q = x^q y^q = xy$ donc $xy \in \mathcal{R}$.

➢ Si $x \in \mathcal{R}$, alors $(-x)^q = (-1)^q x^q = (-1)^q x$. Si $p > 2$, alors q est impair et on a $(-x)^q = -x$ et donc $-x \in \mathcal{R}$. Si $p = 2$, alors $-x = x \in \mathcal{R}$.

➢ Si $x \in \mathcal{R}$, $x \neq 0$, alors $(x^{-1})^q = (x^q)^{-1} = x^{-1}$ donc $x^{-1} \in \mathcal{R}$.

Donc $\mathcal{R}$ est un sous-corps de $\overline{\mathbb{F}_p}$, de cardinal q.

Il reste à démontrer l'unicité à isomorphisme près d'un corps à q éléments. Soit E un corps à q éléments. Son sous-corps premier est nécessairement isomorphe à $\mathbb{F}_p$ (car p est le seul nombre premier qui divise q). Le groupe multiplicatif E^* est cyclique d'ordre $q-1$, donc pour tout $x \in E^*$ on a $x^{q-1} = 1$. On en déduit que pour tout $x \in E$ on a $x^q = x$. L'extension $\mathbb{F}_p \subset E$ est algébrique (car finie), donc E se plonge dans $\overline{\mathbb{F}_p}$ via $\sigma : E \to \overline{\mathbb{F}_p}$. Ainsi, les éléments de $\sigma(E)$ sont des racines de $f = X^q - X$ dans $\overline{\mathbb{F}_p}$. Donc $\sigma(E) \subset \mathcal{R}$, et comme $|\sigma(E)| = |E| = |\mathcal{R}|$, on a $\sigma(E) = \mathcal{R}$. Donc $E \cong \mathcal{R}$. ✓

Remarque. On peut démontrer que tout corps fini est commutatif (admis).

Définition 8. *Soient p un nombre premier et $r \in \mathbb{N}^*$. On note $\mathbb{F}_{p^r}$ le corps à p^r éléments.*

Remarques. (1) On a démontré que tout corps à p^r éléments est isomorphe au corps de décomposition de $X^{p^r} - X$ sur $\mathbb{F}_p$ et que tout élément de ce corps est racine de ce polynôme.

(2) Le groupe $\mathbb{F}_{p^r}^*$ est cyclique d'ordre $p^r - 1$.

(3) Le groupe additif $\mathbb{F}_{p^r}$ est un produit de r groupes cycliques d'ordre p ; en effet, tous les éléments x de $\mathbb{F}_{p^r}$ vérifient $px = 0$.

Attention : cet isomorphisme n'est pas un isomorphisme d'anneaux (ou de corps) ! !

III Racines de l'unité et polynômes cyclotomiques

Soit $n \in \mathbb{N}^*$. On note $\mu_n = \{z \in \mathbb{C} \mid z^n = 1\}$ le groupe des racines $n^{\text{ièmes}}$ de l'unité. C'est un groupe cyclique d'ordre n.

Une racine $n^{\text{ième}}$ de l'unité est dite **primitive** si elle engendre le groupe μ_n, et l'ensemble des racines primitives $n^{\text{ièmes}}$ de l'unité est noté μ_n^*. On rappelle que

➢ si $\omega \in \mu_n^*$ et $k \in \mathbb{Z}$, alors $\omega^k \in \mu_n^*$ si, et seulement si, n et k sont premiers entre eux, et

➢ $|\mu_n^*| = \varphi(n)$ où φ est la fonction indicatrice d'Euler.

Définition 9. *On appelle **corps cyclotomique** un corps de la forme $\mathbb{Q}(\omega)$ avec $\omega \in \mu_n^*$.*

Notre objectif ici est de déterminer le degré $[\mathbb{Q}(\omega) : \mathbb{Q}]$, qui est le degré du polynôme minimal de ω sur $\mathbb{Q}$.

Définition 10. *Soit $n \in \mathbb{N}^*$. Le $n^{ième}$ **polynôme cyclotomique** $\Phi_n \in \mathbb{C}[X]$ est défini par*

$$\Phi_n(X) = \prod_{\zeta \in \mu_n^*} (X - \zeta).$$

On remarque que Φ_n est unitaire et que ses racines, les éléments de μ_n^*, sont simples.

Proposition 11. On a $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Démonstration. Les deux polynômes sont unitaires. Ils ont le même degré, puisque $\deg \Phi_d = |\mu_d^*| = \varphi(d)$ et $\sum_{d|n} \varphi(d) = n$. Il suffit donc de vérifier qu'ils ont les mêmes racines dans $\mathbb{C}$.
Soit x une racine de $X^n - 1$, on a $x^n = 1$ donc x est une racine de l'unité dont l'ordre d divise n, c'est donc un élément de μ_d^* et par conséquent une racine de Φ_d.
Soit x une racine de $\prod_{d|n} \Phi_d(X)$, il existe donc d tel que $d|n$ et x est racine de Φ_d. On a donc $x \in \mu_d^*$ et donc $x^d = 1$. Mais $d|n$ donc $x^n = (x^d)^{n/d} = 1$ et x est racine de $X^n - 1$. ✓

Exemples. ➢ $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$, $\Phi_4(X) = X^2 + 1$.

➢ Si p est un nombre premier, $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1$.

➢ Détermination de Φ_6. On a $X^6 - 1 = \Phi_6(X)\Phi_3(X)\Phi_2(X)\Phi_1(X)$ et $X^3 - 1 = \Phi_3(X)\Phi_1(X)$. Or $X^6 - 1 = (X^3 - 1)(X^3 + 1)$ donc $X^3 + 1 = \Phi_6(X)\Phi_2(X)$ avec $\Phi_2(X) = X + 1$, donc finalement $\Phi_6(X) = X^2 - X + 1$.

Corollaire 12. Pour tout $n \in \mathbb{N}^*$, on a $\Phi_n(X) \in \mathbb{Z}[X]$.

Nous aurons besoin du lemme suivant.

Lemme 13. Soit A un anneau factoriel et soit K son corps des fractions. Soient $P, Q \in A[X]$ des polynômes unitaires. On suppose qu'il existe $R \in K[X]$ tel que $P = QR$. Alors $R \in A[X]$ et R est unitaire.

Démonstration. Puisque Q est unitaire, on peut effectuer la division euclidienne de P par Q dans $A[X]$, et on obtient $P = GQ + H$ avec $G, H \in A[X]$ et $\deg H < \deg Q$. Dans $K[X]$, la division euclidienne est la même, et elle est unique. On en déduit que $H = 0$ et $R = G \in A[X]$. Pour le dernier point, il suffit de comparer les coefficients dominants. ✓

Démonstration du corollaire. Par récurrence sur n, en utilisant le lemme.

➢ Pour $n = 1$, on l'a déjà vu.

➢ Soit $n \in \mathbb{N}$, $n \geqslant 2$, tel que $\Phi_r \in \mathbb{Z}[X]$ pour tout $r < n$. Par hypothèse de récurrence, le polynôme $Q(X) = \prod_{\substack{r|n \\ r \neq n}} \Phi_r(X)$ est dans $\mathbb{Z}[X]$ et il est unitaire.
On sait que $X^n - 1 = \Phi_n(X)Q(X)$ dans $\mathbb{C}[X]$, et puisque $X^n - 1$ et $Q(X)$ sont dans $\mathbb{Z}[X]$, le quotient $\Phi_n(X)$ est dans $\mathbb{Q}(X)$; puisque c'est un polynôme, il est dans $\mathbb{Q}[X]$. On peut donc appliquer le lemme : le polynôme Φ_n est dans $\mathbb{Z}[X]$ (et il est unitaire). ✓

Théorème 14. Pour tout $n \in \mathbb{N}^*$, le polynôme $\Phi_n(X)$ est irréductible dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$. C'est le polynôme minimal de toute racine primitive $n^{\text{ième}}$ de l'unité $\omega \in \mu_n^*$ sur $\mathbb{Q}$.
En particulier, on a $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$.

Démonstration. Démontrons que Φ_n est irréductible dans $\mathbb{Z}[X]$. Soit $P \in \mathbb{Z}[X]$ un facteur irréductible de Φ_n et soit $Q \in \mathbb{Z}[X]$ tel que $\Phi_n = PQ$. Notons que puisque Φ_n est unitaire, les coefficients dominants de P et Q sont égaux et sont dans $\{-1; 1\}$, on peut donc supposer que P et Q sont unitaires. Nous allons démontrer que $\Phi_n = P$.
Vérifions d'abord que toute racine de Φ_n est racine de P. Pour un entier $s \in \mathbb{N}^*$, notons $\ell(s)$ le nombre de facteurs premiers dans la décomposition en produit de nombres premiers de s.
Soit $\zeta \in \mathbb{C}$ une racine de P fixée. Si ω est une racine de Φ_n, c'est-à-dire une racine primitive $n^{\text{ième}}$ de l'unité, alors il existe $s \in \mathbb{N}^*$, premier avec n, tel que $\omega = \zeta^s$. Nous allons démontrer par récurrence sur $\ell(s)$ que ζ^s est racine de P.

➢ Si $\ell(s) = 0$, c'est-à-dire si $s = 1$, il n'y a rien à faire.

➢ Supposons que $\ell(s) = 1$, c'est-à-dire que $s = p$ est un nombre premier qui ne divise pas n. Nous devons démontrer que ζ^p est une racine de P. Supposons par l'absurde que ζ^p n'est pas une racine de P. Notons que $\zeta^p = \omega$ est une racine de Φ_n, donc ζ^p est une racine de Q. Par conséquent, ζ est une racine de $Q(X^p)$. Comme P est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$, c'est le polynôme minimal de ζ sur $\mathbb{Q}$ et donc P divise $Q(X^p)$ dans $\mathbb{Q}[X]$, et donc dans $\mathbb{Z}[X]$ d'après le lemme 13. Réduisons l'égalité $\Phi_n = PQ$ modulo p, on a donc

$$\overline{\Phi_n} = \overline{PQ} \text{ dans } \mathbb{F}_p[X].$$

On a aussi $\overline{Q(X^p)} = \overline{Q(X)}^p$. En effet, posons $Q(X) = \sum_{i=0}^{d} a_i X^i$; puisque $\mathbb{F}_p$ est l'ensemble des racines du polynôme $X^p - X$ dans $\overline{\mathbb{F}_p}$, et en utilisant le fait que $\mathbb{F}_p$ est de caractéristique p, on a $\overline{a_i}^p = \overline{a_i}$ pour tout i et on en déduit que $\overline{Q(X)}^p = \sum_{i=0} \overline{a_i}^p X^{ip} = \sum_{i=0}^{d} \overline{a_i}(X^p)^i = \overline{Q(X^p)}$. Comme P divise $Q(X^p)$ dans $\mathbb{Z}[X]$, on en déduit que $\overline{P}$ divise $\overline{Q}^p$ dans $\mathbb{F}_p[X]$. Soit S un facteur irréductible de $\overline{P}$ dans $\mathbb{F}_p[X]$. D'après le lemme de Gauss, S divise aussi $\overline{Q}$ et donc S^2 divise $\overline{PQ} = \overline{\Phi_n}$ qui divise $\overline{X^n - 1} = X^n - \overline{1}$ dans $\mathbb{F}_p[X]$. Mais $(X^n - \overline{1})' = \overline{n}X^{n-1}$, qui n'est pas nul puisque p ne divise pas n. Dans l'anneau factoriel $\mathbb{F}_p[X]$, les seuls diviseurs non inversibles de $\overline{n}X^{n-1}$ sont, à association près, les X^k avec $1 \leqslant k \leqslant n-1$, qui ne divisent pas $X^n - \overline{1}$, donc $X^n - \overline{1}$ n'a pas de facteur carré. On a donc obtenu une contradiction et par conséquent ζ^p est une racine de P.

➢ Soit s premier à n tel que $r := \ell(s) > 1$ et tel que le résultat est vrai pour tout s' premier à n avec $\ell(s') < \ell(s)$. Posons $s = p_1 \dots p_r$ avec $p_1, \dots, p_r$ premiers qui ne divisent pas n. Par hypothèse de récurrence, $\zeta' = \zeta^{p_1 \cdots p_{r-1}}$ est une racine de P. La démonstration pour $\ell(s) = 1$ montre alors que $\omega = (\zeta')^{p_r}$ est aussi une racine de P.

Nous avons donc démontré par récurrence que toute racine de Φ_n est racine de P. Puisque les racines de Φ_n sont simples, on en déduit que Φ_n divise P (dans $\mathbb{C}[X]$) et donc, puisque P divise Φ_n, que $\Phi_n = P$. Finalement, Φ_n est irréductible dans $\mathbb{Z}[X]$.

Enfin, le polynôme Φ_n est irréductible dans $\mathbb{Z}[X]$ donc il est irréductible dans $\mathbb{Q}[X]$. C'est donc le polynôme minimal de chacune de ses racines, qui sont les racines primitives $n^{\text{ièmes}}$ de l'unité. ✓

CHAPITRE 4

Théorie de Galois des extensions finies

L'objectif de ce chapitre est d'étudier les extensions de corps en utilisant des groupes associés.

I GROUPE DE GALOIS

Définition 1. *Soit $k \subset E$ une extension de corps. Le **groupe de Galois de E sur k** est le groupe des k-automorphismes de E (pour la loi de composition).*
On le note $\mathrm{Gal}(E/k)$ (ou parfois $\mathrm{Aut}_k(E)$).

Exemples. ➢ On a $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z} \cong \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$.
Vérifions par exemple le deuxième isomorphisme. Soit $s \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$. Alors s est entièrement déterminé par $s(\sqrt{2})$. On a $s(\sqrt{2})^2 = s(\sqrt{2}^2) = s(2) = 2$ donc $s(\sqrt{2}) = \pm\sqrt{2}$. Si $s(\sqrt{2}) = \sqrt{2}$, alors $s = \mathrm{id}_{\mathbb{Q}(\sqrt{2})}$. D'autre part, on sait qu'il existe un $\mathbb{Q}$-automorphisme σ de $\mathbb{Q}(\sqrt{2})$ tel que $\sigma(\sqrt{2}) = -\sqrt{2}$ car $\sqrt{2}$ et $-\sqrt{2}$ sont conjugués, d'après le corollaire 5 du chapitre 2. Il est clair que $\sigma \circ \sigma = \mathrm{id}_{\mathbb{Q}(\sqrt{2})}$. Finalement, on a $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\mathrm{id}; \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$.
Pour $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ on raisonne de même, ce groupe est constitué de $\mathrm{id}_{\mathbb{C}}$ et de la conjugaison complexe.
➢ $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$? Posons $\alpha = \sqrt[3]{2}$. Soit s un $\mathbb{Q}$-automorphisme de $\mathbb{Q}(\alpha)$. Alors s est entièrement déterminé par $s(\alpha)$. On doit avoir $(s(\alpha))^3 = s(\alpha^3) = s(2) = 2$ donc $s(\alpha) \in \{\alpha, j\alpha, j^2\alpha\}$. Mais $j \notin \mathbb{Q}(\alpha)$ donc $s(\alpha) = \alpha$. On en déduit que $s = \mathrm{id}$.
Finalement, $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$.

Remarque. $\mathrm{Gal}(E/k)$ est un sous-groupe du groupe de tous les automorphismes de corps $\mathrm{Aut}(E)$ de E. Si k est le sous-corps premier de E, alors $\mathrm{Gal}(E/k) = \mathrm{Aut}(E)$.

Lemme 2. Soit $k \subset E \subset L$ des extensions et soit $s : E \to L$ un k-morphisme. Soit α un élément de E algébrique sur k.

(i) Si α est racine de $P \in k[X]$, alors $s(\alpha)$ est racine de P.

(ii) Les éléments α et $s(\alpha)$ sont conjugués.

Démonstration. (i) Exercice.

(ii) Soit M_α le polynôme minimal de α sur k. Alors $s(\alpha)$ est racine de M_α et M_α est irréductible et unitaire, donc M_α est le polynôme minimal de $s(\alpha)$ sur k. ✓

Proposition 3. Soit $k \subset E$ une extension finie. Alors $\mathrm{Gal}(E/k)$ est un groupe fini.

Démonstration. Soit $k \subset E$ une extension finie. Alors il existe $\alpha_1, \ldots, \alpha_n$ dans E tels que $E = k(\alpha_1, \ldots, \alpha_n)$. Si $s \in \mathrm{Gal}(E/k)$, on sait qu'il est déterminé par les $s(\alpha_i)$ pour $1 \leqslant i \leqslant n$. De plus, pour tout i, α_i est algébrique sur k et α_i et $s(\alpha_i)$ sont conjugués donc il n'y a qu'un nombre fini de possibilités pour $s(\alpha_i)$. Finalement, il n'y a qu'un nombre fini de possibilités pour s. ✓

Soit $f \in k[X]$. Si E et E' sont deux corps de décomposition de f, on sait qu'il existe un k-isomorphisme $\sigma : E \to E'$. On en déduit un isomorphisme de groupes

$$\begin{array}{ccc} \mathrm{Gal}(E/k) & \to & \mathrm{Gal}(E'/k) \\ s & \mapsto & \sigma \circ s \circ \sigma^{-1}. \end{array}$$

Ceci donne un sens à la définition suivante.

Définition 4. *Soit $f \in k[X]$ un polynôme non constant. Le **groupe de Galois de f sur** k est le groupe de Galois de l'extension $k \subset E$ où E est un corps de décomposition de f sur k.*
On le note $\mathrm{Gal}_k(f)$.

Le groupe de Galois d'un polynôme est un outil essentiel pour étudier ses racines. Nous le verrons dans le chapitre 5.

Théorème 5. Soit $f \in k[X]$ un polynôme non constant. Soit $\mathcal{R}_f$ l'ensemble des racines de f dans une clôture algébrique de k. Posons $m = \left|\mathcal{R}_f\right| \leqslant \deg f$.

Alors le groupe de Galois $\mathrm{Gal}_k(f)$ opère sur $\mathcal{R}_f$, et cette action est transitive si f est irréductible sur k.

De plus, cette action induit un morphisme de groupes injectif

$$\mathrm{Gal}_k(f) \hookrightarrow S(\mathcal{R}_f) \cong S_m$$

(autrement dit, l'action est fidèle).

Démonstration. Soit E un corps de décomposition de f sur k. Alors $\mathrm{Gal}_k(f) = \mathrm{Gal}(E/k)$. Par définition de $\mathrm{Gal}(E/k)$, ce groupe opère sur E (par automorphismes : pour $s \in \mathrm{Gal}(E/k)$ et $x \in E$, $s \cdot x = s(x)$). De plus, cette action se restreint à $\mathcal{R}_f$ d'après le lemme 2. Plus précisément, si $s \in \mathrm{Gal}(E/k)$ et si α est une racine de f, alors $s \cdot \alpha = s(\alpha) \in \mathcal{R}_f$.

Si f est irréductible, le lemme 8 du chapitre 2 montre que l'action de $\mathrm{Gal}(E/k)$ sur $\mathcal{R}_f$ est transitive.

Considérons le morphisme de groupes $\varphi : \mathrm{Gal}_k(f) \to S(\mathcal{R}_f)$ induit par cette action : $\varphi(s)(\alpha) = s(\alpha)$. Soit $s \in \mathrm{Gal}(E/k)$ tel que $\varphi(s) = \mathrm{id}_{\mathcal{R}_f}$. Puisque s est un k-automorphisme de $E = k(\mathcal{R}_f)$, il est entièrement déterminé par les $s(\alpha)$ pour $\alpha \in \mathcal{R}_f$. Mais par hypothèse, on a $s(\alpha) = \alpha$ pour tout $\alpha \in \mathcal{R}_f$, donc $s = \mathrm{id}_E$. On a démontré que φ est injectif. ✓

Nous avons associé un groupe à une extension de corps. Nous allons maintenant définir une extension à partir de groupes d'automorphismes.

Définition-Proposition 6. *Soit E un corps et soit G un sous-groupe de $\mathrm{Aut}(E)$. On pose*

$$E^G = \{x \in E \mid \forall s \in G,\ s(x) = x\}.$$

*Alors E^G est un sous-corps de E, appelé le **corps des invariants de** G.*

Démonstration. Exercice. ✓

Remarquons que si $k \subset L \subset E$ sont des extensions de corps, alors $\mathrm{Gal}(E/L)$ est un sous-groupe de $\mathrm{Gal}(E/k)$.

On a donc construit deux applications

$$\begin{array}{ccc} \{\text{sous-extensions } k \subset L \subset E\} & \rightleftarrows & \{\text{sous-groupes de } \mathrm{Gal}(E/k)\} \\ k \subset L \subset E & \mapsto & \mathrm{Gal}(E/L) \\ k \subset E^H \subset E & \hookleftarrow & H. \end{array}$$

Il est alors naturel de se demander si ce sont des bijections réciproques. Plus précisément, nous allons étudier la question suivante.

Question. *Soit $k \subset E$ une extension (algébrique). On a toujours $k \subset E^{\mathrm{Gal}(E/k)}$.*
A quelles conditions sur $k \subset E$ a-t-on $k = E^{\mathrm{Gal}(E/k)}$?

Exemples. (1) On considère l'extension $\mathbb{R} \subset \mathbb{C}$. Le groupe de Galois $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ est égal à $\{1, s\}$ avec $s : \mathbb{C} \to \mathbb{C}$ la conjugaison complexe.
Dans ce cas on a $\mathbb{C}^{\mathrm{Gal}(\mathbb{C}/\mathbb{R})} = \mathbb{R}$.

(2) On considère l'extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$. On a déjà vu que $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{(2)})/\mathbb{Q}) = \{1\}$, donc $\mathbb{Q}(\sqrt[3]{(2)})^{\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{(2)})/\mathbb{Q})} = \mathbb{Q}(\sqrt[3]{(2)}) \neq \mathbb{Q}$.

II Extensions normales

Définition-Proposition 7. *Soit $k \subset E$ une extension algébrique et soit $\overline{E}$ une clôture algébrique de E. Les assertions suivantes sont équivalentes.*

(i) *Tout polynôme irréductible $f \in k[X]$ ayant une racine dans E a toutes ses racines dans E.*

(ii) *Tout k-morphisme $t : E \to \overline{E}$ est à valeurs dans E, et donc est un élément de $\mathrm{Gal}(E/k)$.*

*Une extension algébrique satisfaisant une de ces conditions équivalentes est dite **normale**.*

Démonstration. ➢ On suppose que (i) est vérifiée. Soit $t : E \to \overline{E}$ un k-morphisme. Soit $\alpha \in E$. Alors α est algébrique sur k et on sait donc que $t(\alpha)$ est conjugué à α. Soit M_α le polynôme minimal de α sur k, c'est un polynôme irréductible de $k[X]$ qui a une racine dans E, donc d'après l'hypothèse (i) toutes ses racines sont dans E, et par conséquent $t(\alpha) \in E$. Donc t est un k-endomorphisme de E et puisque E est une extension algébrique de k, t est un k-automorphisme de E (proposition 13 du chapitre 1).

➢ On suppose que (ii) est vérifiée. Soit $f \in k[X]$ un polynôme irréductible qui a une racine α dans E. Soit β une autre racine de f dans $\overline{E}$. D'après la proposition 3 du chapitre 2 de prolongement des isomorphismes, il existe un unique k-isomorphisme $\sigma : k(\alpha) \to k(\beta)$ tel que $\sigma(\alpha) = \beta$. Si on compose avec l'injection naturelle de $k(\beta)$ dans $\overline{E}$, on obtient un k-morphisme $k(\alpha) \to \overline{E}$, qui se prolonge en un k-morphisme de $\tilde{\sigma} : E \to \overline{E}$ d'après le théorème 16 du chapitre 2. Par hypothèse (ii), $\tilde{\sigma}$ est un k-automorphisme de E, donc $\beta = \sigma(\alpha) = \tilde{\sigma}(\alpha)$ est dans E. ✓

Proposition 8. Soit $k \subset E$ une extension finie. Les assertions suivantes sont équivalentes.

(i) $k \subset E$ est normale.

(ii) E est un corps de décomposition sur k d'un polynôme $f \in k[X]$.

Démonstration. Soit $f \in k[X]$ et soit E un corps de décomposition de f sur k. Posons $E = k(\alpha_1, \ldots, \alpha_n)$ où $\alpha_1, \ldots, \alpha_n$ sont les racines de f dans une clôture algébrique $\overline{E}$ de E.
Soit $t : E \to \overline{E}$ un k-morphisme ; il est déterminé par les $t(\alpha_i)$. Pour tout i, $t(\alpha_i)$ est une racine de f, donc c'est l'un des α_j et donc t est à valeurs dans E. L'extension $k \subset E$ est donc normale.
Réciproquement, soit $k \subset E$ une extension normale finie. Puisqu'elle est finie, il existe $\alpha_1, \ldots, \alpha_n$ dans E tels que $E = k(\alpha_1, \ldots, \alpha_n)$. Soit $f = \prod_{i=1}^n M_{\alpha_i}$ où $M_{\alpha_i} \in k[X]$ est le polynôme minimal de α_i sur k.
Chaque M_{α_i} est irréductible sur k et $\alpha_i \in E$ donc par hypothèse toutes les racines de M_{α_i} sont dans E. Ainsi, f est scindé dans $E[X]$ donc E contient un corps de décomposition de f sur k. De plus, tout corps de décomposition de f sur k doit contenir tous les α_i, puisque ce sont des racines de f, donc doit contenir E. Finalement, E est un corps de décomposition de f sur k. ✓

Exemples. (1) L'extension $\mathbb{R} \subset \mathbb{C}$ est normale puisque $\mathbb{C}$ est un corps de décomposition de $X^2 + 1$ sur $\mathbb{R}$.

(2) L'extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ n'est pas normale car le polynôme $X^3 - 2 \in \mathbb{Q}[X]$ a une racine dans $\mathbb{Q}(\sqrt[3]{2})$ mais pas toutes.

Proposition 9. Soit $k \subset E$ une extension finie. Alors il existe une extension finie $E \subset \hat{E}$ telle que l'extension finie $k \subset \hat{E}$ soit normale.

Démonstration. On pose $E = k(\alpha_1, \ldots, \alpha_n)$. Soit $f = \prod_{i=1}^n M_{\alpha_i}$. Soit $\hat{E}$ un corps de décomposition de f sur k. Alors $k \subset E \subset \hat{E}$, les extensions sont finies et $k \subset \hat{E}$ est normale. ✓

Exemple. $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, j)$.

Proposition 10. Soient $k \subset E \subset L$ des extensions algébriques telles que $k \subset L$ est normale. Alors

(i) $E \subset L$ est normale ;

(ii) $k \subset E$ est normale si, et seulement si, pour tout $s \in \mathrm{Gal}(L/k)$ on a $s(E) = E$.

Démonstration. (i) Soit $t\colon L \to \overline{L}$ un E-morphisme. C'est donc un k-morphisme et puisque $k \subset L$ est normale, t est à valeurs dans L. Ainsi, $E \subset L$ est normale.

(ii) Supposons que $k \subset E$ est normale. Soit $s \in \mathrm{Gal}(L/k)$. Soit $\overline{L}$ une clôture algébrique de L ; c'est également une clôture algébrique de E.

On a un k-morphisme $E \xrightarrow{s_{|E}} L \hookrightarrow \overline{L} \cong \overline{E}$ et puisque $k \subset E$ est normale, il est à valeurs dans E, autrement dit, $s(E) \subset E$. Ainsi, s est un k-endomorphisme de E et donc un k-automorphisme de E, donc $s(E) = E$.

Réciproquement, supposons que pour tout $s \in \mathrm{Gal}(L/k)$ on a $s(E) = E$. Soit $t\colon E \to \overline{E}$ un k-morphisme. Puisque l'extension $E \subset L$ est algébrique, il se prolonge en un k-morphisme $\widehat{t}\colon L \to \overline{E}$. Or $\overline{E} \cong \overline{L}$ donc $\widehat{t}\colon L \to \overline{L}$. Puisque l'extension $k \subset L$ est normale, $\widehat{t}$ est à valeurs dans L, donc induit un élément de $\mathrm{Gal}(L/k)$. Par hypothèse, on a donc $\widehat{t}(E) = E$ et donc t est à valeurs dans E. On a démontré que $k \subset E$ est normale. ✓

III Extensions séparables

Définition 11. *Soit k un corps.*

(i) *Soit $f \in k[X]$ un polynôme non constant. On dit que f est **séparable** (sur k) s'il n'a que des racines simples (dans E, un corps de décomposition de f sur k).*

(ii) *Soit $k \subset E$ une extension algébrique. On dit qu'un élément $a \in E$ est **séparable** sur k si son polynôme minimal sur k est séparable sur k.*

(iii) *On dit qu'une extension algébrique $k \subset E$ est **séparable** si tout élément $a \in E$ est séparable sur k.*

Proposition 12. Soit $f \in k[X]$ un polynôme irréductible. Alors f est séparable si et seulement si $f'(X) \neq 0$. Ainsi,

(i) si $\mathrm{car}(k) = 0$, alors f est séparable ;

(ii) si $\mathrm{car}(k) = p > 0$, alors f est séparable si et seulement si $f \notin k[X^p]$.

Démonstration. Soit E un corps de décomposition de f.

Supposons que f n'est pas séparable sur k. Alors f admet une racine multiple $a \in E$. On a donc $f(a) = 0$ et $f'(a) = 0$. De plus, f est irréductible et admet a comme racine, donc il est associé au polynôme minimal de a. Or on a $f'(a) = 0$, donc f divise f'. Puisque $\deg f > \deg f'$, on en déduit que $f' = 0$.

Réciproquement, si $f' = 0$ alors toute racine de f est une racine multiple de f, donc f n'est pas séparable.

Précisons ce que cela signifie en fonction de la caractéristique de k. Remarquons d'abord que si on pose $f(X) = \sum_{i=0}^{d} a_i X^i$, alors $f'(X) = \sum_{i=1}^{d} i a_i X^{i-1}$ qui est nul si et seulement si $i a_i = 0$ pour tout i avec $0 \leqslant i \leqslant d$.

(i) Supposons que $\mathrm{car}(k) = 0$. Si $f' = 0$, alors pour tout $i > 0$ on a $a_i = 0$ donc f est constant donc f n'est pas irréductible (il est inversible ou nul). Par conséquent, tout polynôme irréductible est séparable.

(ii) Supposons maintenant que $\mathrm{car}(k) = p > 0$.

Si f n'est pas séparable, c'est-à-dire que $f' = 0$, alors $i a_i = 0$ pour tout i avec $0 \leqslant i \leqslant d$. Si i n'est pas un multiple de p, alors $i \neq 0$ dans k et donc $a_i = 0$. On en déduit que

$$f(X) = \sum_{\substack{0 \leqslant i \leqslant d \\ p \mid i}} a_i X^i = \sum_{\substack{j \in \mathbb{N} \\ 0 \leqslant pj \leqslant d}} a_{pj} X^{pj} \in k[X^p].$$

Réciproquement, si $f \in k[X^p]$, alors il existe $g \in k[X]$ tel que $f(X) = g(X^p)$, donc $f'(X) = g'(X^p) p X^{p-1} = 0$, donc f n'est pas séparable. ✓

Corollaire 13. Si $\mathrm{car}(k) = 0$, alors toute extension algébrique est séparable.

Exemple. Soit k un corps de caractéristique $p > 0$ (par exemple $\mathbb{F}_{p^2}$) et soit $\alpha \in k$ un élément qui n'a pas de racine p-ième dans k (par exemple un générateur du groupe cyclique $\mathbb{F}_{p^2}^*$). Alors $X^p - \alpha$ est irréductible sur k (Voir Travaux Dirigés.) mais il n'est pas séparable sur k.

Lemme 14. Soient $k \subset E \subset L$ des extensions algébriques. On suppose que $k \subset L$ est séparable. Alors les extensions $k \subset E$ et $E \subset L$ sont séparables.

Démonstration. Par hypothèse, tous les éléments de L et donc en particulier les éléments de E sont séparables sur k, donc $k \subset E$ est séparable. De plus, si $\alpha \in L$, alors le polynôme minimal de α sur E divise le polynôme minimal de α sur k qui est séparable par hypothèse, donc α est séparable sur E, et l'extension $E \subset L$ est donc séparable. ✓

Remarque. De la même manière, on démontre que si $k \subset E \subset L$ sont des extensions algébriques et si $\alpha \in L$ est un élément séparable sur k, alors α est séparable sur E.

Définition-Proposition 15. *Soit $k \subset E$ une extension finie. Soit Ω un corps algébriquement clos. Soit $t : k \to \Omega$ un morphisme de corps tel que l'extension $t(k) \subset \Omega$ soit algébrique. Alors l'ensemble*

$$\Phi_{t,\Omega} = \left\{ f : E \to \Omega \mid f \text{ morphisme de corps tel que } f_{|k} = t \right\}$$

*des morphismes de corps qui prolongent t est fini, et son cardinal ne dépend pas du choix du couple (t, Ω). On note $[E : k]_s$ ce cardinal, que l'on appelle **degré séparable de l'extension** $k \subset E$.*

Si $E = k(\alpha)$, alors $[E : k]_s$ est égal au nombre de racines distinctes *du polynôme minimal de α sur k (dans un corps de décomposition de ce polynôme).*

Démonstration. Soit (t', Ω') un autre tel couple. Alors Ω (resp. Ω') est une clôture algébrique de $t(k)$ (resp. de $t'(k)$). Notons $v : t(k) \to k$ la réciproque de l'isomorphisme $t : k \to t(k)$. On a un isomorphisme de corps $t' \circ v : t(k) \to t'(k)$. D'après le corollaire 18 du chapitre 2, on en déduit qu'il existe un isomorphisme $\varphi : \Omega \to \Omega'$ qui prolonge $t' \circ v$, c'est-à-dire que $\varphi_{|t(k)} = t' \circ v$ et donc $\varphi \circ t = t' \circ v \circ t = t'$. On en déduit alors une bijection $\Phi_{t,\Omega} \to \Phi_{t',\Omega'}$ qui à $f \in \Phi_{t,\Omega}$ associe $\varphi \circ f$.
Puisque $k \subset E$ est finie, on peut écrire $E = k(\alpha_1, \ldots, \alpha_n)$ avec $\alpha_1, \ldots, \alpha_n$ algébriques sur k. Choisissons une clôture algébrique Ω de E et soit $t : k \hookrightarrow E \hookrightarrow \Omega$ le plongement ; ainsi, tout élément f de $\Phi_{t,\Omega}$ est un k-morphisme. Pour tout i avec $1 \leqslant i \leqslant n$, l'élément $f(\alpha_i)$ est une racine du polynôme minimal de α_i sur k, il n'y donc qu'un nombre fini de possibilités pour $f(\alpha_i)$. Puisque f est entièrement déterminé par les $f(\alpha_i)$, on en déduit que $\Phi_{t,\Omega}$ est fini.
Dans le cas particulier où $E = k(\alpha)$, ce qui précède montre que le cardinal de $\Phi_{t,\Omega}$ est inférieur ou égal au nombre de conjugués de α dans Ω (sans compter les multiplicités), c'est-à-dire le nombre de racines distinctes de M_α. De plus, si β est un conjugué de α, on sait qu'il existe un k-isomorphisme $k(\alpha) \to k(\beta)$ qui induit un k-morphisme $E = k(\alpha) \to \Omega$, c'est-à-dire un élément de $\Phi_{t,\Omega}$, et deux conjugués distincts de α induisent des éléments distincts de $\Phi_{t,\Omega}$. On en déduit l'égalité recherchée. ✓

Remarque. Il découle de la démonstration précédente que si α est un élément algébrique sur k, alors $[k(\alpha) : k]_s \leqslant \deg M_\alpha = [k(\alpha) : k]$.

Proposition 16. Soient $k \subset E \subset L$ des extensions finies. Alors

$$[L : k]_s = [L : E]_s [E : k]_s.$$

Démonstration. Soit $t : k \to \overline{k}$ un plongement de k dans une clôture algébrique $\overline{k}$ de k.
Soit $r = [E : k]_s$ et posons $\Phi_{t,\overline{k}} = \left\{ f : E \to \overline{k} \mid f \text{ morphisme de corps et } f_{|k} = t \right\} = \{f_1, \ldots, f_r\}$.
Soit $i \in \{1, \ldots, r\}$. On sait que $\overline{k}$ est une clôture algébrique de E. De plus, on a un morphisme de corps $f_i : E \to \overline{k}$. Soit $q = [L : E]_s$ et posons $\Phi'_{f_i,\overline{k}} = \left\{ g : L \to \overline{k} \mid g \text{ morphisme de corps et } g_{|E} = f_i \right\} = \{g_{i,1}, \ldots, g_{i,q}\}$. On rappelle que q ne dépend pas de i d'après la définition-proposition 15.

Pour tout (i,j), $g_{i,j}$ est un prolongement de t à L. De plus, si h est un prolongement de t à L, alors $h_{|E}$ est un prolongement de t à E, donc c'est l'un des f_i et donc h est l'un des $g_{i,j}$.
Finalement, $\{g_{i,j} \mid 1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant q\}$ est l'ensemble des prolongements distincts de t à L et par conséquent $[L : k]_s = rq = [E : k]_s[L : E]_s$. ✓

Proposition 17. Soit $k \subset E$ une extension finie. Alors

$$[E : k]_s \leqslant [E : k].$$

Démonstration. On a déjà vu que si $E = k(\alpha)$ avec α algébrique sur k, alors $[E : k]_s \leqslant [E : k]$.
Dans le cas général d'une extension finie $k \subset E$, on a $E = k(\alpha_1, \ldots, \alpha_n)$ avec $\alpha_1, \ldots, \alpha_n$ algébriques sur k. Posons $E_r = k(\alpha_1, \ldots, \alpha_r)$ pour tout r avec $1 \leqslant r \leqslant n$ et $E_0 = k$. Alors $E_r \subset E_{r+1} = E_r(\alpha_{r+1})$ est une extension finie et $[E_{r+1} : E_r]_s \leqslant [E_{r+1} : E_r]$.
En utilisant la formule de la proposition précédente, on obtient

$$[E : k]_s = \prod_{i=0}^{n-1} [E_{r+1} : E_r]_s \leqslant \prod_{i=0}^{n-1} [E_{r+1} : E_r] = [E : k].$$ ✓

Proposition 18. Soit $k \subset E$ une extension finie. Alors $k \subset E$ est séparable si, et seulement si, $[E : k]_s = [E : k]$.

Démonstration. ➢ Traitons d'abord le cas où $E = k(\alpha)$.
Si α est séparable sur k, alors les racines de M_α sont simples et on a donc $[k(\alpha) : k]_s = [k(\alpha) : k]$. Réciproquement, si $[k(\alpha) : k]_s = [k(\alpha) : k]$ alors le nombre de racines distinctes de M_α est égal au degré de M_α, donc toutes les racines de M_α sont simples et donc α est séparable sur k. On a donc

$$\circledast \qquad \alpha \text{ séparable sur } k \iff [k(\alpha) : k]_s = [k(\alpha) : k].$$

On en déduit que, si $k \subset k(\alpha)$ est séparable, alors α est séparable sur k donc $[k(\alpha) : k]_s = [k(\alpha) : k]$.
Démontrons la réciproque. Supposons que $[k(\alpha) : k]_s = [k(\alpha) : k]$. Soit $\beta \in k(\alpha)$. Nous devons démontrer que β est séparable sur k.
On a $k \subset k(\beta) \subset k(\alpha)$. Donc $[k(\alpha) : k(\beta)]_s[k(\beta) : k]_s = [k(\alpha) : k]_s = [k(\alpha) : k] = [k(\alpha) : k(\beta)][k(\beta) : k]$. De plus, puisque α est séparable sur k, il est séparable sur $k(\beta)$. On en déduit d'après $\circledast$ que $[k(\alpha) : k(\beta)]_s = [k(\alpha) : k(\beta)]$. Par conséquent, $[k(\beta) : k]_s = [k(\beta) : k]$ et donc β est séparable sur k d'après $\circledast$.

➢ Traitons maintenant le cas général. Puisque $k \subset E$ est finie, on a $E = k(\alpha_1, \ldots, \alpha_n)$ avec $\alpha_1, \ldots, \alpha_n$ algébriques sur k. Posons $E_r = k(\alpha_1, \ldots, \alpha_r)$ pour $1 \leqslant r \leqslant n$ et $E_0 = k$. On a $E_{r+1} = E_r(\alpha_{r+1})$ pour $0 \leqslant r \leqslant n-1$.
Si $k \subset E$ est séparable, alors α_i est séparable sur k et donc sur E_{i-1} pour tout i, et donc $[E_i : E_{i-1}]_s = [E_i : E_{i-1}]$ pour tout i. On a donc

$$[E : k]_s = \prod_{i=1}^{n} [E_i : E_{i-1}]_s = \prod_{i=1}^{n} [E_i : E_{i-1}] = [E : k].$$

Réciproquement, supposons que $[E : k]_s = [E : k]$. Soit $\beta \in E$, on doit démontrer que β est séparable sur k. On a $k \subset k(\beta) \subset E$. De plus,

$$[k(\beta) : k]_s = \frac{[E : k]_s}{[E : k(\beta)]_s} = \frac{[E : k]}{[E : k(\beta)]_s} \geqslant \frac{[E : k]}{[E : k(\beta)]} = [k(\beta) : k].$$

Or on sait en général que $[k(\beta) : k]_s \leqslant [k(\beta) : k]$, donc on a $[k(\beta) : k]_s = [k(\beta) : k]$ et on déduit de $\circledast$ que β est séparable sur k. ✓

Corollaire 19. Soit $k \subset E$ une extension et soient $\alpha_1, \ldots, \alpha_n$ des éléments de E algébriques sur k. Alors l'extension $k \subset k(\alpha_1, \ldots, \alpha_n)$ est séparable si, et seulement si, tous les α_i sont séparables sur k.

Démonstration. Si $k \subset k(\alpha_1, \ldots, \alpha_n)$, alors les α_i sont séparables sur k par définition d'une extension séparable.
Supposons que tous les α_i sont séparables sur k. Posons $E_r = k(\alpha_1, \ldots, \alpha_r)$ pour $1 \leqslant r \leqslant n$ et $E_0 = k$. Alors α_i est séparable sur E_{i-1}. On a donc

$$[E_n : k]_s = \prod_{i=1}^{n} [E_i : E_{i-1}]_s \overset{\circledast}{=} \prod_{i=1}^{n} [E_i : E_{i-1}] = [E_n : k]$$

donc $k \subset E_n$ est séparable d'après la proposition. ✓

Corollaire 20. Soient $k \subset E \subset L$ des extensions algébriques. Les assertions suivantes sont équivalentes.

(i) $k \subset L$ est séparable.

(ii) $k \subset E$ et $E \subset L$ sont séparables.

Démonstration. Nous avons déjà vu l'implication (i)⇒(ii) dans le lemme 14.

Réciproquement, supposons que $k \subset E$ et $E \subset L$ sont séparables.

➢ Si $k \subset L$ est une extension finie, alors $[L : k]_s = [L : E]_s[E : k]_s = [L : E][E : k] = [L : k]$ donc $k \subset L$ est séparable.

➢ Sinon, soit $\alpha \in L$ et soit $P \in E[X]$ son polynôme minimal sur E ; posons $P(X) = \sum_{i=0}^{d} a_i X^i$ avec $a_i \in E$. Soit $E' = k(a_0, \ldots, a_d)$. Les éléments a_i sont algébriques sur k donc l'extension $k \subset E'$ est finie. Soit $L' = E'(\alpha)$. L'extension $E' \subset L'$ est également finie. De plus, les a_i sont séparables sur k (ils sont dans E) donc $k \subset E'$ est séparable. L'élément $\alpha \in L$ est séparable sur E donc P est séparable ; or $P \in E'[X]$ et $P(\alpha) = 0$ donc le polynôme minimal de α sur E' divise P, donc il est séparable et donc α est séparable sur E'. L'extension $E' \subset L'$ est donc séparable. On déduit du cas fini que $k \subset L'$ est séparable (finie) et donc que $\alpha \in L'$ est séparable sur k.

Finalement, l'extension $k \subset L$ est séparable. ✓

Proposition 21. Soit $k \subset E$ une extension finie normale. Alors $|\mathrm{Gal}(E/k)| = [E : k]_s$.

Démonstration. Soit $\overline{k}$ une clôture algébrique de k. Rappelons que $[E : k]_s$ est fini et que c'est le nombre d'éléments de $\Phi = \left\{ t : E \to \overline{k} \mid t \text{ est un } k\text{-morphisme} \right\}$. Notons que $\overline{k}$ est une clôture algébrique de E.

Si $s \in \mathrm{Gal}(E/k)$, en composant avec $\sigma : E \hookrightarrow \overline{k}$ on en déduit un élément $\sigma \circ s$ de Φ, et si $s \neq s'$, on a $\sigma \circ s \neq \sigma \circ s'$, donc on obtient une injection $f : \mathrm{Gal}(E/k) \hookrightarrow \Phi$. D'autre part, si $t \in \Phi$, puisque $k \subset E$ est normale, t est à valeurs dans E donc définit un élément $\overline{t}$ de $\mathrm{Gal}(E/k)$ tel que $f(\overline{t}) = \sigma \circ \overline{t} = t$. On a donc une bijection f entre $\mathrm{Gal}(E/k)$ et Φ, qui sont donc de même cardinal. ✓

Remarque. Si $k \subset E$ est une extension finie quelconque, la démonstration montre que $|\mathrm{Gal}(E/k)| \leqslant [E : k]_s$ (car f est toujours injective).

Définition 22. *Soit $k \subset E$ une extension. Un élément $\alpha \in E$ est un **élément primitif** de l'extension si $E = k(\alpha)$.*

Théorème 23. (Théorème de l'élément primitif.)
Toute extension finie et séparable admet un élément primitif.

Démonstration. Soit $k \subset E$ une extension finie séparable.

➢ Premier cas : k est un corps fini. Notons q le cardinal de k. L'extension $k \subset E$ est finie, donc E est aussi un corps fini, de cardinal q^n où $n = [E : k]$. Le groupe E^* est donc cyclique, soit α un générateur de ce groupe. On a $k(\alpha) \subset E$. De plus, tout élément de E^* est une puissance de α, donc $E = k(\alpha)$.

➢ Second cas : k est un corps infini. Il existe $\alpha_1, \ldots, \alpha_n$ dans E, 2 à 2 distincts, tels que $E = k(\alpha_1, \ldots, \alpha_n)$. Si $n = 1$ il n'y a rien à faire, supposons donc que $n = 2$.

Soient $t_1, \ldots, t_r : E \to \overline{k}$ les k-morphismes distincts. On sait que $r = [E : k]_s = [E : k]$. Considérons le polynôme

$$f(X) = \prod_{1 \leqslant i \neq j \leqslant r} \left((t_i - t_j)(\alpha_1) + (t_i - t_j)(\alpha_2) X \right) \in \overline{k}[X].$$

Pour tout i, t_i est entièrement déterminé par $t_i(\alpha_1)$ et $t_i(\alpha_2)$, donc si $i \neq j$, on doit avoir $t_i(\alpha_1) \neq t_j(\alpha_1)$ ou $t_i(\alpha_2) \neq t_j(\alpha_2)$. On en déduit que $f \neq 0$. Puisque k est infini, il existe $c \in k$ tel que $f(c) \neq 0$, et donc pour tout $i \neq j$ on a $(t_i - t_j)(\alpha_1) + (t_i - t_j)(\alpha_2)c \neq 0$, c'est-à-dire que $(t_i - t_j)(\alpha_1 + c\alpha_2) \neq 0$ ou encore $t_i(\alpha_1 + c\alpha_2) \neq t_j(\alpha_1 + c\alpha_2)$. Donc les restrictions des t_i à $k(\alpha_1 + c\alpha_2)$ sont des k-morphismes distincts, et on a donc $[k(\alpha_1 + c\alpha_2) : k]_s \geqslant r$. D'autre part, on a $k \subset k(\alpha_1 + c\alpha_2) \subset E$, l'extension $k \subset k(\alpha_1 + c\alpha_2)$ est donc séparable et on a

$$r \leqslant [k(\alpha_1 + c\alpha_2) : k]_s = [k(\alpha_1 + c\alpha_2) : k] \leqslant [E : k] = r$$

dont on déduit que $E = k(\alpha_1 + c\alpha_2)$.

On conclut par récurrence sur n. ✓

Remarque. La démonstration du théorème dans le cas où k est fini n'utilise pas le fait que l'extension est séparable. Par conséquent, toute extension finie d'un corps fini admet un élément primitif.

En fait, une extension finie d'un corps fini est toujours séparable. Voir Travaux Dirigés.

En effet, soit $\mathbb{F}_q \subset \mathbb{F}_{q^r}$ un extension finie où q est une puissance d'un nombre premier p. On sait que $\mathbb{F}_{q^r}$ est le corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^{q^r} - X$, dont les racines sont simples puisque son polynôme dérivé est $q^r X^{q^r-1} - 1 = -1 \neq 0$. Ainsi toutes les racines de $X^{q^r} - X$ dans $\mathbb{F}_{q^r}$ sont séparables sur $\mathbb{F}_p$, donc $\mathbb{F}_p \subset \mathbb{F}_{q^r}$ est séparable et donc $\mathbb{F}_q \subset \mathbb{F}_{q^r}$ est séparable.

Une autre démonstration consiste à considérer le morphisme de corps $\varphi : \mathbb{F}_q \to \mathbb{F}_q$ défini par $\varphi(a) = a^p$, qui est un isomorphisme puisqu'il est injectif et $\mathbb{F}_q$ est fini. Soit $\alpha \in \mathbb{F}_{q^r}$ et soit $M_\alpha \in \mathbb{F}_q[X]$ son polynôme minimal sur $\mathbb{F}_q$. Supposons que α, et donc M_α, n'est pas séparable. On sait donc qu'il existe $f \in \mathbb{F}_q[X]$ tel que $M_\alpha(X) = f(X^p)$. Posons $f(X) = \sum_{i=0}^{d} a_i X^i$. Puisque φ est un isomorphisme, pour tout i il existe $b_i \in \mathbb{F}_q$ tel que $a_i = b_i^p$. On a donc $M_\alpha(X) = f(X^p) = \sum_{i=0}^{d} b_i^p X^{ip} = \left(\sum_{i=0}^{d} b_i X^i\right)^p$, ce qui contredit le fait que M_α est irréductible dans $\mathbb{F}_q[X]$.

IV Théorèmes fondamentaux de la théorie de Galois

Définition 24. *Une **extension galoisienne** est une extension $k \subset E$ qui est normale et séparable.*

Ainsi, une extension $k \subset E$ est galoisienne si et seulement si elle est algébrique et, pour tout $\alpha \in E$, le polynôme minimal de α est scindé à racines simples dans $E[X]$.

Remarque. Pour toute extension finie $k \subset E$, on a $|\mathrm{Gal}(E/k)| \leqslant [E : k]_s$. Si de plus $k \subset E$ est une extension normale finie, alors $|\mathrm{Gal}(E/k)| = [E : k]_s$ (voir Proposition 21).

Enfin, si $k \subset E$ est une extension galoisienne finie, on a $[E : k] = |\mathrm{Gal}(E/k)|$.

Remarque. Soit $k \subset E$ une extension galoisienne finie. On sait qu'elle admet un élément primitif.

Soit $\alpha \in E$. Alors α est un élément primitif de l'extension si, et seulement si, pour tout $s \in \mathrm{Gal}(E/k)$ avec $s \neq \mathrm{id}_E$, on a $s(\alpha) \neq \alpha$.

En effet :

- Si $E = k(\alpha)$, alors tout élément s de $\mathrm{Gal}(E/k)$ est entièrement déterminé par $s(\alpha)$. En particulier, si $s \neq \mathrm{id}_E$, alors $s(\alpha) \neq \mathrm{id}_E(\alpha) = \alpha$.
- Réciproquement, supposons que pour tout $s \in \mathrm{Gal}(E/k)$ avec $s \neq \mathrm{id}_E$, on ait $s(\alpha) \neq \alpha$. On a alors une injection $\mathrm{Gal}(E/k) \hookrightarrow \Phi_{\iota,\overline{k}} = \left\{f : k(\alpha) \to \overline{k} \mid f_{|k} = \iota\right\}$ où ι est l'injection naturelle $\iota : k \hookrightarrow \overline{k}$.

On en déduit donc que

$$|\mathrm{Gal}(E/k)| \leqslant [k(\alpha) : k]_s \leqslant [k(\alpha) : k] \leqslant [E : k] = |\mathrm{Gal}(E/k)|.$$

Toutes ces inégalités sont donc des égalités, par conséquent $[k(\alpha) : k] = [E : k]$ et $E = k(\alpha)$.

Remarque. Si $k \subset L \subset E$ sont des extensions avec $k \subset E$ galoisienne, alors $L \subset E$ est galoisienne. En effet, elle est algébrique puisque $k \subset E$ l'est, elle est normale d'après la proposition 10 et elle est séparable d'après le corollaire 20.

Théorème 25. Soit $k \subset E$ une extension algébrique. Les assertions suivantes sont équivalentes.

(i) $k \subset E$ est galoisienne.

(ii) $E^{\mathrm{Gal}(E/k)} = k$.

Démonstration. ➢ (i)⇒(ii). Supposons que $k \subset E$ est galoisienne. On a toujours $k \subset E^{\mathrm{Gal}(E/k)}$. Soit maintenant $\alpha \in E \setminus k$ et démontrons que $\alpha \notin E^{\mathrm{Gal}(E/k)}$.

Puisque $\alpha \notin k$, le polynôme minimal M_α de α est de degré > 1, donc il a une autre racine β. Puisque l'extension $k \subset E$ est normale, $\beta \in E$, et puisque l'extension $k \subset E$ est séparable, $\beta \neq \alpha$. D'après le corollaire 5 du chapitre 2, il existe un k-isomorphisme $t : k(\alpha) \to k(\beta)$, que l'on peut considérer comme un k-morphisme $k(\alpha) \to \overline{k}$. Les extensions $k \subset k(\alpha) \subset E$ sont algébriques, donc d'après le

théorème 16 du chapitre 2, il existe un k-morphisme $\widehat{t}\colon E \to \overline{k}$ qui prolonge t. Notons que $\overline{k}$ est une clôture algébrique de E, donc puisque l'extension $k \subset E$ est normale, $\widehat{t}$ est à valeurs dans E, il définit donc un élément de $\mathrm{Gal}(E/k)$ qui ne fixe pas α. Donc $\alpha \notin E^{\mathrm{Gal}(E/k)}$.

Finalement, $E^{\mathrm{Gal}(E/k)} = k$.

➢ (ii)⇒(i). Supposons que $E^{\mathrm{Gal}(E/k)} = k$. Soit $\alpha \in E$ et soit M_α son polynôme minimal sur k. On note $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ les racines distinctes de M_α dans E. Notons que $n \leqslant \deg M_\alpha$. Pour tout $s \in \mathrm{Gal}(E/k)$ et pour tout i, il existe j tel que $s(\alpha_i) = \alpha_j$; en effet, $s(\alpha_i) \in E$ et $s(\alpha_i)$ est une racine de M_{α_i}. Ainsi, le k-morphisme s (injectif) permute les α_i. Posons $f(X) = \prod_{i=1}^{n}(X - \alpha_i) \in E[X]$. Soit $s \in \mathrm{Gal}(E/k)$ et soit $\overline{s} : E[X] \to E[X]$ son unique prolongement à $E[X]$ tel que $\overline{s}(X) = X$. Alors $\overline{s}(f(X)) = f(X)$, donc tous les coefficients de f sont dans $E^{\mathrm{Gal}(E/k)} = k$, et donc $f(X) \in k[X]$. Mais $f(\alpha) = f(\alpha_1) = 0$ donc M_α divise f, et puisque $\deg f \leqslant \deg M_\alpha$ et f est unitaire, les polynômes f et M_α sont égaux. On en déduit que les racines de M_α sont toutes dans E et sont 2 à 2 distinctes. On a démontré que $k \subset E$ est galoisienne. ✓

Théorème 26. Soient E un corps et G un groupe fini d'automorphismes de E. Alors l'extension $E^G \subset E$ est galoisienne finie et $[E : E^G] = |G|$. De plus, $G = \mathrm{Gal}(E/E^G)$.

Nous utiliserons le lemme suivant.

Lemme 27. Soit $k \subset E$ une extension algébrique séparable. Supposons qu'il existe $n \in \mathbb{N}^*$ tel que pour tout $\alpha \in E$, on a $[k(\alpha) : k] \leqslant n$. Alors l'extension $k \subset E$ est finie et $[E : k] \leqslant n$.

Démonstration. Soit $\alpha \in E$ tel que le degré $[k(\alpha) : k]$ soit maximal. Démontrons que $E = k(\alpha)$. Soit $\beta \in E$. Puisque l'extension $k \subset E$ est séparable et $k \subset k(\alpha, \beta) \subset E$, l'extension $k \subset k(\alpha, \beta)$ est également séparable, et elle est finie. D'après le théorème de l'élément primitif, il existe $c \in k(\alpha, \beta)$ tel que $k(\alpha, \beta) = k(c)$. On a donc $k(\alpha) \subset k(c)$. Par conséquent on a $[k(\alpha) : k] \leqslant [k(c) : k] \leqslant [k(\alpha) : k]$ puisque $[k(\alpha) : k]$ est maximal, et donc $k(\alpha) = k(c)$. Finalement, on a $\beta \in k(c) = k(\alpha)$. Donc $E = k(\alpha)$ et on en déduit le résultat. ✓

Démonstration du théorème 26. Soit $\alpha \in E$.

➢ Démontrons que α est algébrique sur E^G. Considérons l'orbite $\Omega_\alpha = \{s(\alpha) \mid s \in G\}$ de α sous l'action de G, qui est finie puisque G est fini. Soient $\sigma_1, \ldots, \sigma_r$ des éléments de G tels que $\Omega_\alpha = \{\sigma_1(\alpha), \ldots, \sigma_r(\alpha)\}$ et $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ si $i \neq j$. Soit $t \in G$. Pour tout i on a $t(\sigma_i(\alpha)) \in \Omega_\alpha$ donc il existe j tel que $t(\sigma_i(\alpha)) = \sigma_j(\alpha)$. Puisque t est injectif, il définit une permutation des $\sigma_i(\alpha)$.

Soit $f(X) = \prod_{i=1}^{r}(X - \sigma_i(\alpha)) \in E[X]$. Soit $\overline{t}\colon E[X] \to E[X]$ l'unique morphisme d'anneaux qui prolonge t et tel que $\overline{t}(X) = X$. Alors $\overline{t}(f(X)) = f(X)$, donc les coefficients de $f(X)$ sont dans E^G et on a $f(X) \in E^G[X]$. Or $\alpha \in \Omega_\alpha$, donc $f(\alpha) = 0$ et donc α est algébrique sur E^G.

➢ Soit P le polynôme minimal de α sur E^G. Alors P divise f, dont toutes les racines sont simples et dans E, donc P est scindé à racines simples dans $E[X]$.

➢ Remarquons de plus que $[E^G(\alpha) : E^G] = \deg P \leqslant \deg f = r \leqslant |G|$.

Ceci est vrai pour tout $\alpha \in E$, donc nous avons démontré que $E^G \subset E$ est une extension galoisienne et que pour tout $\alpha \in E$ on a $[E^G(\alpha) : E^G] \leqslant |G|$, donc d'après le lemme $E^G \subset E$ est galoisienne finie avec $[E : E^G] \leqslant |G|$.

De plus, il est clair que $G \subset \mathrm{Gal}(E/E^G)$ donc $|G| \leqslant \left|\mathrm{Gal}(E/E^G)\right| = [E : E^G] \leqslant |G|$ (où l'égalité du milieu découle d'une remarque page 26), donc on a bien $G = \mathrm{Gal}(E/E^G)$. ✓

Corollaire 28. Soit $k \subset E$ une extension finie. Les assertions suivantes sont équivalentes.

(i) $k \subset E$ est galoisienne.

(ii) $E^{\mathrm{Gal}(E/k)} = k$.

(iii) $[E : k] = |\mathrm{Gal}(E/k)|$.

Démonstration. ➢ Nous avons déjà vu que (i)⇔(ii) et (i)⇒(iii).

➢ (iii)⇒(ii). Soit $G = \mathrm{Gal}(E/k)$. Puisque $k \subset E$ est une extension finie, G est fini. On sait donc que $E^G \subset E$ est galoisienne finie et que $[E : E^G] = |G|$ d'après le théorème 26. Par hypothèse on a aussi $[E : k] = |G|$. Puisque $k \subset E^G$ on en déduit que $E^G = k$. ✓

Proposition 29. Soit $n \in \mathbb{N}^*$, soit k un corps de caractéristique nulle ou première à n contenant toutes les racines $n^{\text{ièmes}}$ de l'unité (c'est-à-dire toutes les racines de $X^n - 1 \in k[X]$), soit $a \in k$ et soit α une racine du polynôme $X^n - a$ (dans un corps de décomposition de $X^n - a$ sur k).

Alors l'extension $k \subset k(\alpha)$ est galoisienne et $\mathrm{Gal}(k(\alpha)/k)$ est un groupe cyclique d'ordre d avec $d \mid n$. De plus, $\alpha^d \in k$.

Démonstration. Soit U_n l'ensemble des racines $n^{\text{ièmes}}$ de l'unité dans k. Ce sont toutes les racines du polynôme $X^n - 1$. Elles forment un sous-groupe fini du groupe multiplicatif k^*, donc U_n est un groupe cyclique. De plus, le polynôme $P = X^n - 1$ n'a que des racines simples, car $P' = nX^{n-1}$ et P n'ont pas de racine commune (on utilise ici le fait que la caractéristique de k ne divise pas n et donc que P' n'est pas nul donc son unique racine est 0), donc U_n est un groupe cyclique d'ordre n.

Soit ω un générateur de U_n. Alors $U_n = \{\omega^j \mid 0 \leqslant j \leqslant n-1\}$. Les racines de $X^n - a$ sont les $\omega^j\alpha$ avec $0 \leqslant j < n$; en effet, ce sont des racines de $X^n - a$ et il y a n éléments distincts, donc ce sont toutes les racines de $X^n - a$. En particulier, α est séparable sur k. De plus, pour tout j on a $\omega^j\alpha \in k(\alpha)$ donc $k(\alpha)$ est un corps de décomposition de $X^n - a$ sur k. L'extension $k \subset k(\alpha)$ est donc galoisienne.

Notons $G = \mathrm{Gal}(k(\alpha)/k)$. Pour tout $s \in G$, $s(\alpha)$ est une racine de $X^n - a$ donc $s(\alpha) = \omega_s\alpha$ où ω_s est une racine $n^{\text{ième}}$ de l'unité.

On considère l'application $\varphi : G \to U_n$ qui à s associe ω_s. C'est un morphisme de groupes (en effet, si s et t sont dans G, alors $\omega_{s\circ t}\alpha = s \circ t(\alpha) = s(\omega_t\alpha) = \omega_t s(\alpha) = \omega_t\omega_s\alpha$ puisque $\omega_t \in k$). Le morphisme φ est injectif ; en effet, si $s \in \mathrm{Ker}\,\varphi$, alors $\varphi(s) = 1$ donc $s(\alpha) = \alpha$; mais s est entièrement déterminé par $s(\alpha)$, donc $s = \mathrm{id}_{k(\alpha)}$. Par conséquent, G est isomorphe à un sous-groupe de U_n, qui est cyclique d'ordre n, donc G est cyclique d'ordre d qui divise n.

Enfin, pour tout $s \in G$ l'élément ω_s est une racine $d^{\text{ième}}$ de l'unité et $s(\alpha^d) = s(\alpha)^d = (\omega_s\alpha)^d = \varphi_s^d\alpha^d = \alpha^d$ donc $\alpha^d \in k(\alpha)^G$. Mais $k(\alpha)^G = k$ puisque $k \subset k(\alpha)$ est galoisienne, donc $\alpha^d \in k$. ✓

Théorème 30. (Correspondance de Galois.) Soit $k \subset E$ une extension galoisienne finie. On a une correspondance bijective, qui renverse les inclusions,

$$\begin{array}{ccc} \{\text{sous-extensions } k \subset L \subset E\} & \rightleftarrows & \{\text{sous-groupes de } \mathrm{Gal}(E/k)\} \\ k \subset L \subset E & \mapsto & \mathrm{Gal}(E/L) \\ k \subset E^H \subset E & \hookleftarrow & H. \end{array}$$

De plus, si $k \subset L \subset E$, alors l'extension $k \subset L$ est galoisienne si, et seulement si, le sous-groupe $\mathrm{Gal}(E/L)$ est normal dans $\mathrm{Gal}(E/k)$, et on a alors $\mathrm{Gal}(L/k) \cong \mathrm{Gal}(E/k)/\mathrm{Gal}(E/L)$.

Démonstration. Si $k \subset L \subset E$ est une sous-extension, alors $L \subset E$ est une extension galoisienne donc $L = E^{\mathrm{Gal}(E/L)}$.

Si H est un sous-groupe de $\mathrm{Gal}(E/k)$, c'est en particulier un sous-groupe fini d'automorphismes de E, donc $k \subset E^H \subset E$ avec $E^H \subset E$ galoisienne et $\mathrm{Gal}(E/E^H) = H$ (Théorème 26).

On a donc établi la correspondance bijective. Montrons maintenant que $k \subset L$ est galoisienne si, et seulement si, $\mathrm{Gal}(E/L)$ est normal dans $\mathrm{Gal}(E/k)$.

Soit $k \subset L \subset E$ une sous-extension.

Puisque $k \subset E$ est séparable, $k \subset L$ est séparable, elle est donc galoisienne si, et seulement si, elle est normale, ce qui est équivalent d'après la proposition 10 à

$$\forall s \in \mathrm{Gal}(E/k),\ s(L) = L.$$

Soit $s \in \mathrm{Gal}(E/k)$. Montrons que $\mathrm{Gal}(E/s(L)) = s\,\mathrm{Gal}(E/L)\,s^{-1}$:

➢ soit $t \in \mathrm{Gal}(E/L)$, pour tout $x' \in s(L)$ on a $s^{-1}(x') \in L$ donc $s \circ t \circ s^{-1}(x') = s(s^{-1}(x')) = x'$ donc $s \circ t \circ s^{-1} \in \mathrm{Gal}(E/s(L))$. Donc $s\,\mathrm{Gal}(E/L)\,s^{-1} \subset \mathrm{Gal}(E/s(L))$.

➢ soit $t \in \mathrm{Gal}(E/s(L))$, de même, on a $s^{-1} \circ t \circ s \in \mathrm{Gal}(E/L)$ donc $t = s \circ (s^{-1} \circ t \circ s) \circ s^{-1} \in s\,\mathrm{Gal}(E/L)\,s^{-1}$.

Supposons que $\mathrm{Gal}(E/L) \lhd \mathrm{Gal}(E/k)$. Pour tout $s \in \mathrm{Gal}(E/k)$ on a, en utilisant ce qui précède, $\mathrm{Gal}(E/s(L)) = s\,\mathrm{Gal}(E/L)\,s^{-1} = \mathrm{Gal}(E/L)$. On déduit donc de la correspondance bijective déjà démontrée que $s(L) = L$. Ainsi, $k \subset L$ est normale.

Supposons que $k \subset L$ est normale. Alors pour tout $s \in \mathrm{Gal}(E/k)$ on a $s(L) = L$ donc $s\,\mathrm{Gal}(E/L)\,s^{-1} = \mathrm{Gal}(E/s(L)) = \mathrm{Gal}(E/L)$ et donc $\mathrm{Gal}(E/L) \lhd \mathrm{Gal}(E/k)$.

Il reste à démontrer que sous ces conditions, on a $\mathrm{Gal}(L/k) \cong \mathrm{Gal}(E/k)/\mathrm{Gal}(E/L)$. Puisque $k \subset L$ est normale, pour tout $s \in \mathrm{Gal}(E/k)$ on a $s(L) = L$. On peut donc considérer $s_{|L} \in \mathrm{Gal}(L/k)$ et définir une application $\varphi : \mathrm{Gal}(E/k) \to \mathrm{Gal}(L/k)$ par $\varphi(s) = s_{|L}$. C'est un morphisme de groupes.

Le morphisme φ est surjectif. En effet, si $t \in \mathrm{Gal}(L/k)$ on peut considérer $L \xrightarrow{t} L \to \overline{k}$, qui se prolonge en $s : E \to \overline{k}$, qui est à valeurs dans E puisque $k \subset E$ est normale ; on a donc $s \in \mathrm{Gal}(E/k)$, et $\varphi(s) = t$.
Il reste à déterminer le noyau de φ. Soit $s \in \mathrm{Gal}(E/k)$ tel que $\varphi(s) = \mathrm{id}_L$. Alors $s \in \mathrm{Gal}(E/L)$ donc $\mathrm{Ker}\,\varphi \subset \mathrm{Gal}(E/L)$. Réciproquement, si $s \in \mathrm{Gal}(E/L)$ on a bien sûr $\varphi(s) = \mathrm{id}_L$ donc $s \in \mathrm{Ker}\,\varphi$.
On conclut grâce au premier théorème d'isomorphisme que $\mathrm{Gal}(E/k)/\mathrm{Gal}(E/L) \cong \mathrm{Gal}(L/k)$. ✓

Exemple. Soit $E = \mathbb{Q}(\sqrt[3]{2}, j)$. Posons $\alpha = \sqrt[3]{2}$.

➢ E est un corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$, donc l'extension $\mathbb{Q} \subset E$ est normale. De plus, $\mathrm{car}(\mathbb{Q}) = 0$ donc elle est séparable. Elle est donc galoisienne, et finie.
Déterminons son degré. on a $[E : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$. Le polynôme $X^3 - 2 \in \mathbb{Q}[X]$ est unitaire irréductible sur $\mathbb{Q}$ et admet α pour racine, donc c'est le polynôme minimal de α sur $\mathbb{Q}$ et $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Le polynôme $X^2 + X + 1$ est unitaire irréductible sur $\mathbb{Q}(\alpha)$ (puisqu'il est de degré 2 et n'admet pas de racine dans $\mathbb{Q}(\alpha) \subset \mathbb{R}$), il admet j comme racine donc c'est le polynôme minimal de j sur $\mathbb{Q}(\alpha)$ et on a $[E : \mathbb{Q}(\alpha)] = 2$. Finalement $[E : \mathbb{Q}] = 6$.

➢ Soit $G = \mathrm{Gal}(E/\mathbb{Q})$. Ce qui précède montre que G est un groupe d'ordre 6. D'après le théorème de synthèse de la fin du chapitre 4 du premier semestre, on sait que G est soit cyclique, soit isomorphe au groupe symétrique S_3.
De plus, α et $j\alpha$ sont conjugués sur $\mathbb{Q}(j)$; en effet, $[\mathbb{Q}(\alpha, j) : \mathbb{Q}(j)] = \frac{[E:\mathbb{Q}]}{[\mathbb{Q}(j):\mathbb{Q}]} = \frac{6}{2} = 3$ donc le polynôme minimal de α sur $\mathbb{Q}(j) = 3$, mais $X^3 - 2$ est un polynôme annulateur de α donc il est multiple du polynôme minimal de α sur $\mathbb{Q}(j)$ donc égal à ce dernier puisqu'il est de même degré. Il existe donc un $\mathbb{Q}(j)$-automorphisme s de E, qui est en particulier un élément de G, tel que $s(j) = j$ et $s(\alpha) = j\alpha$. De même, il existe $t \in G$ tel que $t(\alpha) = \alpha$ et $t(j) = j^2$. On remarque que $s^3 = \mathrm{id}$ et $t^2 = \mathrm{id}$. De plus, $t \circ s \circ t^{-1} \circ s^{-1} = s \neq \mathrm{id}$ donc G n'est pas abélien et donc G est isomorphe à S_3. Les éléments de G sont donc $1, s, s^2 = s^{-1}, t, s \circ t \circ s^{-1}, s^{-1} \circ t \circ s$.

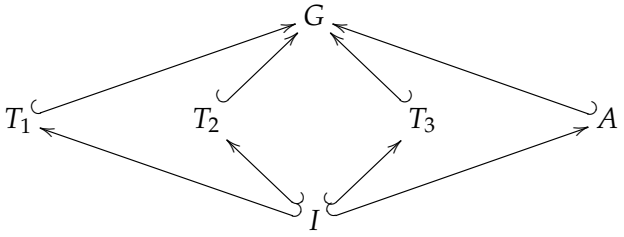
➢ Les sous-groupes de $G \cong S_3$ sont d'ordres $1, 2, 3$ ou 6 et sont les suivants.

✧ Sous-groupe d'ordre 1 : $I = \{\mathrm{id}\}$.

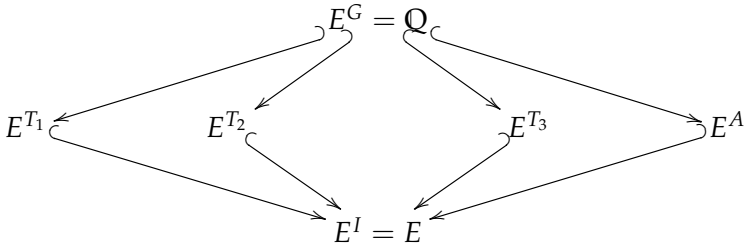
✧ Sous-groupes d'ordre 2 : $T_1 = \{\mathrm{id}, t\}$, $T_2 = \{\mathrm{id}, s \circ t \circ s^{-1}\}$ et $T_3 = \{\mathrm{id}, s^{-1} \circ t \circ s\}$.

✧ Sous-groupe d'ordre 3 : $A = \{\mathrm{id}, s, s^2\}$ (groupe alterné A_3).

✧ Sous-groupe d'ordre 6 : G.



➢ En utilisant la correspondance entre les sous-groupes de G et les sous-extensions de $\mathbb{Q} \subset E$, on en déduit que les sous-extensions de $\mathbb{Q} \subset E$ sont les $\mathbb{Q} \subset L \subset E$ avec $L = E^H$ où H parcourt les sous-groupes de G :



Notons que puisque $|T_i| = 2$ on a $[E : E^{T_i}] = 2$ et donc $[E^{T_i} : \mathbb{Q}] = 3$. De même, $[E : E^A] = 3$ et donc $[E^A : \mathbb{Q}] = 2$.
On vérifie que $E^{T_1} = \mathbb{Q}(\alpha)$, $E^{T_2} = \mathbb{Q}(j\alpha)$, $E^{T_3} = \mathbb{Q}(j^2\alpha)$, $E^A = \mathbb{Q}(j)$. Par exemple, on a $t(\alpha) = \alpha$ donc $\alpha \in E^{T_1}$ donc $\mathbb{Q}(\alpha) \subset E^{T_1}$ et $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3 = [E^{T_1} : \mathbb{Q}]$ donc $\mathbb{Q}(\alpha) = E^{T_1}$.

➢ Les sous-extensions qui sont galoisiennes sont toutes les $E^H \subset E$ où $H \in \{T_1, T_2, T_3, A\}$, ainsi que $\mathbb{Q} \subset E^A$ puisque $A \lhd G$ (et c'est le seul sous-groupe normal non-trivial de G). De plus on a $\mathrm{Gal}(E^A/\mathbb{Q}) \cong G/A \cong \mathbb{Z}/2\mathbb{Z}$.

➢ On peut vérifier que $c = j + \alpha$ est un élément primitif de l'extension $\mathbb{Q} \subset E$: d'après une remarque page 26, il suffit pour cela de vérifier que pour tout $\sigma \in G$ avec $\sigma \neq \mathrm{id}$, on a $\sigma(c) \neq c$.

CHAPITRE 5

Applications

I CONSTRUCTIONS À LA RÈGLE ET AU COMPAS

A. Formalisme algébrique

Soit $\mathbb{P}_0$ un ensemble de points du plan euclidien $\mathbb{R}^2$. On autorise deux types de constructions :

➢ tracer une droite passant par deux points de $\mathbb{P}_0$,

➢ tracer un cercle de centre un point de $\mathbb{P}_0$ et de rayon la distance entre deux points de $\mathbb{P}_0$.

Définition 1. *Tout point de $\mathbb{R}^2$ obtenu comme intersection de droites ou de cercles suivant les opérations ci-dessus est dit **constructible en une étape à partir de** $\mathbb{P}_0$.*

*Un point M du plan est dit **constructible** s'il existe une suite finie de points $M_1, M_2, \dots, M_n = M$ tels que pour tout i avec $1 \leqslant i \leqslant n$, le point M_i est constructible en une étape à partir de $\mathbb{P}_0 \cup \{M_1, \dots, M_{i-1}\}$.*

Lemme 2. Soit D une droite passant par les points $A = (a_1, a_2)$ et $B = (b_1, b_2)$. Alors D a une équation de la forme $\alpha x + \beta y + \gamma = 0$ avec α, β, γ dans $\mathbb{Q}(a_1, a_2, b_1, b_2)$.

Soit $\mathscr{C}$ un cercle de centre $A = (a_1, a_2)$ et de rayon BC avec $B = (b_1, b_2)$ et $C = (c_1, c_2)$. Alors $\mathscr{C}$ a une équation de la forme $x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0$ avec α, β, γ dans $\mathbb{Q}(a_1, a_2, b_1, b_2, c_1, c_2)$.

Démonstration. La droite $D = (AB)$ a pour équation $x - a_1 = 0$ si $a_1 = b_1$ et $y - a_2 = (x - a_1)\dfrac{b_2 - a_2}{b_1 - a_1}$ si $a_1 \neq b_1$.
Le cercle $\mathscr{C}$ a pour équation $(x - a_1)^2 + (y - a_2)^2 = (c_1 - b_1)^2 + (c_2 - b_2)^2$. ✓

Supposons $\mathbb{R}^2$ rapporté à un système de coordonnées : $M = (x, y)$ en identifiant le point à ses coordonnées. Soit K_0 le sous-corps de $\mathbb{R}$ engendré par les coordonnées des points de $\mathbb{P}_0$.

Notons que K_0 est de caractéristique nulle, donc il contient $\mathbb{Q}$. On a donc des extensions $\mathbb{Q} \subset K_0 \subset \mathbb{R}$.

Avec les notations de la définition 1, si on pose $M_i = (x_i, y_i)$, soit $K_i = K_{i-1}(x_i, y_i)$ pour $1 \leqslant i \leqslant n$. On a donc une chaîne d'extensions $\mathbb{Q} \subset K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \mathbb{R}$.

Théorème 3. Avec les notations ci-dessus, les degrés des extensions $K_0 \subset K_0(x)$ et $K_0 \subset K_0(y)$ sont des puissances de 2.

Lemme 4. Les degrés $[K_{i-1}(x_i) : K_{i-1}]$ et $[K_{i-1}(y_i) : K_{i-1}]$ sont égaux à 1 ou 2.

Démonstration. Le point $M_i = (x_i, y_i)$ est construit en une étape à partir de $\mathbb{P}_0 \cup \{M_1, \dots, M_{i-1}\}$. C'est donc l'intersection de

(a) deux droites (non parallèles) ou

(b) une droite et un cercle ou

(c) deux cercles (non concentriques).

Etudions ces trois cas.

(a) Soient D et D' deux droites telles que $M_i = D \cap D'$. Soient $\alpha x + \beta y + \gamma = 0$ et $\alpha' x + \beta' y + \gamma' = 0$ leurs équations respectives avec $\alpha, \beta, \gamma, \alpha', \beta', \gamma'$ dans K_{i-1} et $\alpha\beta' - \beta\alpha' \neq 0$. Les coordonnées de M_i forment l'unique solution du système linéaire

$$\begin{cases} \alpha x + \beta y + \gamma = 0 \\ \alpha' x + \beta' y + \gamma' = 0 \end{cases}$$

donc x_i et y_i sont dans K_{i-1} et on a $[K_{i-1}(x_i) : K_{i-1}] = 1$ et $[K_{i-1}(y_i) : K_{i-1}] = 1$.

(b) Soit D une droite et soit C un cercle tels que $M_i = D \cap C$. Soit $\alpha x + \beta y + \gamma = 0$ une équation de D et soit $x^2 + y^2 - 2\alpha' x - 2\beta' y + \gamma' = 0$ une équation de C avec $\alpha, \beta, \gamma, \alpha', \beta', \gamma'$ dans K_{i-1}. Les coordonnées de M_i forment alors une solution du système

$$\begin{cases} \alpha x + \beta y + \gamma = 0 \\ x^2 + y^2 - 2\alpha' x - 2\beta' y + \gamma' = 0. \end{cases}$$

Si $\beta = 0$ alors $x_i \in K_{i-1}$, et si $\beta \neq 0$ on substitue $y = -\frac{\alpha x + \gamma}{\beta}$ dans la deuxième équation pour obtenir un polynôme de degré inférieur ou égal à 2 dont x_i est racine. Le polynôme minimal de x_i sur K_{i-1} le divise, donc il est de degré 1 ou 2 et donc $[K_{i-1}(x_i) : K_{i-1}] = 1$ ou 2.
De même, $[K_{i-1}(y_i) : K_{i-1}] = 1$ ou 2.

(c) Soient C et C' deux cercles tels que $M_i = C \cap C'$. Soient $x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0$ et $x^2 + y^2 - 2\alpha' x - 2\beta' y + \gamma' = 0$ leurs équations respectives avec $\alpha, \beta, \gamma, \alpha', \beta', \gamma'$ dans K_{i-1} et $(\alpha, \beta) \neq (\alpha', \beta')$. Les coordonnées de M_i forment alors une solution du système

$$\begin{cases} x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0 \\ x^2 + y^2 - 2\alpha' x - 2\beta' y + \gamma' = 0. \end{cases}$$

En faisant la différence des deux équations, on est ramenés à un système tel que celui du cas précédent, et on en déduit que $[K_{i-1}(x_i) : K_{i-1}] = 1$ ou 2 et que $[K_{i-1}(y_i) : K_{i-1}] = 1$ ou 2. ✓

Démonstration du théorème. D'après le lemme précédent, $[K_i : K_{i-1}] = [K_{i-1}(x_i, y_i) : K_{i-1}(x_i)][K_{i-1}(x_i) : K_{i-1}]$ est une puissance de 2. En effet, le degré de y_i sur K_{i-1} est égal à 1 ou 2 et il est multiple du degré de y_i sur $K_{i-1}(x_i)$, qui est égal à 1 ou 2.
Donc par récurrence $[K_n : K_0]$ est une puissance de 2.
De plus, $[K_n : K_0] = [K_n : K_0(x)][K_0(x) : K_0]$ donc $[K_0(x) : K_0]$ est aussi une puissance de 2. ✓

B. Applications à quelques problèmes géométriques

Avant de nous intéresser à ces problèmes bien connus, faisons les remarques suivantes.

On supposera toujours que $|\mathbb{P}_0| > 1$ et on choisira un repère de telle sorte que $O = (0, 0)$ et $I = (1, 0)$ soient dans $\mathbb{P}_0$.

Remarque. Si on sait construire des points M et N tels que $MN = \alpha$, alors on sait construire le point $(\alpha, 0)$ à la règle et au compas.

Remarque. On sait construire, à la règle et au compas, une droite perpendiculaire à une droite donnée et passant par un point donné.

En effet, soit $D = (AB)$ une droite et soit C un point. Si (AC) ou (BC) est orthogonale à D, c'est terminé.

Supposons que $C \neq A$ et que (AC) ne soit pas orthogonale à D. Le cercle de centre C et de rayon CA rencontre la droite D en un autre point M. On sait alors tracer la médiatrice de $[AM]$ (c'est la droite passant par les points d'intersection des cercles de centres A et M et de rayon AM), qui contient C et qui est perpendiculaire à D.

Si $C = A$, on fait la même construction avec B.

B.1. Duplication du cube

Question. *Peut-on construire, à la règle et au compas, l'arête d'un cube dont le volume soit le double de celui d'un cube d'arête donnée ?*

Considérons comme cube initial un cube d'arête $[OI]$. Soit $\mathbb{P}_0 = \{O, I\}$. Alors $K_0 = \mathbb{Q}$.

Supposons que l'on puisse construire des points M et N tels que $MN^3 = 2$; alors le point $A = (\alpha, 0)$ tel que $\alpha^3 = 2$ serait également constructible. Dans ce cas, α serait une racine du polynôme $X^3 - 2 \in \mathbb{Q}[X]$, qui est irréductible sur $\mathbb{Q}$, donc on aurait $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, qui n'est pas une puissance de 2. Le point A n'est donc pas constructible à partir de $\mathbb{P}_0$ et le cube d'arête MN avec $MN^3 = 2$ non plus.

La réponse est donc non.

B.2. Trisection de l'angle

Question. *Peut-on construire, à la règle et au compas, deux droites qui partagent un angle donné en trois parties égales ?*

La réponse est non en général. Vérifions-le pour l'angle $\frac{\pi}{3}$. On prend à nouveau $\mathbb{P}_0 = \{O, I\}$ et donc $K_0 = \mathbb{Q}$. Le point P obtenu par intersection du cercle de centre O et de rayon OI avec la médiatrice de $[OI]$ nous permet de construire l'angle $\frac{\pi}{3}$.

On voudrait construire un angle θ tel que $3\theta = \frac{\pi}{3}$. Il s'agit de construire le point $M = (\cos\theta, \sin\theta)$.

Supposons que M est constructible.

On sait construire, à la règle et au compas, la perpendiculaire à l'axe des abscisses passant par M. On peut donc construire le point de coordonnées $(\alpha, 0)$ avec $\alpha = \cos\theta$.

On a alors $\frac{1}{2} = \cos\frac{\pi}{3} = \cos(3\theta) = 4\cos^3\theta - 3\cos\theta = 4\alpha^3 - 3\alpha$ donc $8\alpha^3 - 6\alpha - 1 = 0$. Le polynôme $f(X) = 8X^3 - 6X - 1 \in \mathbb{Q}[X]$ est irréductible (critère d'Eisenstein appliqué à $f(X-1)$ avec $p = 3$) et admet α comme racine, donc $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ n'est pas une puissance de 2 : contradiction.

B.3. Quadrature du cercle

Question. *Peut-on construire, à la règle et au compas, l'arête d'un carré dont l'aire soit égale à celle d'un disque donné ?*

Considérons le disque D de rayon $[OI]$. Soit $\mathbb{P}_0 = \{O, I\}$. Alors $K_0 = \mathbb{Q}$. L'aire de D est π : on cherche à construire un carré dont l'aire est π, c'est-à-dire dont l'arête est de longueur $\sqrt{\pi}$.

Supposons que l'on sache construire un segment de longueur $\sqrt{\pi}$. On sait donc construire le point A tel que $IA = \sqrt{\pi}$ et (IA) soit orthogonale à l'axe des abscisses en I. Soit d la droite orthogonale à (OA) passant par A : elle rencontre l'axe des abscisses en B.

On a alors trois triangles rectangles semblables : OAB, OIA et AIB. On en déduit que $\frac{IA}{OI} = \frac{IB}{IA}$ et donc que $IB = OI \cdot IA^2 = IA^2 = \pi$. On sait donc construire un segment de longueur π et par conséquent $(\pi, 0)$ est constructible.

Mais alors l'extension $\mathbb{Q} \subset \mathbb{Q}(\pi)$ serait finie (de degré une puissance de 2), ce qui contredit le fait que π est transcendant.

La réponse est donc non.

II Résolubilité par radicaux des équations polynômiales

Dans toute cette partie, k sera un corps de caractéristique nulle.

On cherche les solutions d'une équation $f(x) = 0$ où $f \in k[X]$. Si $\deg f \in \{1, 2, 3, 4\}$, il existe des formules générales qui permettent d'obtenir des solutions de $f(x) = 0$ comme des expressions algébriques (obtenues avec les opérations $+, -, \times, \div$) faisant intervenir des radicaux (c'est-à-dire des racines $n^{\text{ièmes}}$ d'éléments de k), valables pour tout $f \in k[X]$. Nous allons voir que ce n'est plus le cas si $\deg f \geqslant 5$.

Définition 5. *Une extension $k \subset E$ est **radicale** s'il existe $\alpha_1, \dots, \alpha_n$ dans E et $p(1), \dots, p(n)$ dans $\mathbb{N}^*$ tels que*

➢ $\alpha_1^{p(1)} \in k$,

➢ *pour tout $i \in \{2, \dots, n\}$ on a $\alpha_i^{p(i)} \in k(\alpha_1, \dots, \alpha_{i-1})$,*

➢ $E = k(\alpha_1, \dots, \alpha_n)$.

*Les α_i forment une **suite de radicaux** pour l'extension $k \subset E$.*

Remarque. Notons qu'une extension radicale est nécessairement finie (pour tout i, α_i est algébrique sur $k(\alpha_1, \dots, \alpha_{i-1})$).

Remarque. Soit $\alpha_1, \dots, \alpha_n$ une suite de radicaux pour une extension radicale $k \subset E$. Quitte à ajouter ou enlever des éléments α_i, on peut supposer que

① pour tout i, il existe $p(i) \in \mathbb{N}^*$ *premier* tel que $\alpha_1^{p(1)} \in k$ et $\alpha_i^{p(i)} \in k(\alpha_1, \dots, \alpha_{i-1})$ pour $i \geqslant 2$ et

② $\alpha_1 \notin k$ et, pour tout $i \geqslant 2$, $\alpha_i \notin k(\alpha_1, \dots, \alpha_{i-1})$.

En effet, pour le point ①, supposons que par exemple $p(1) = q_1 \cdots q_r$ soit la décomposition en produit de facteurs premiers de $p(1)$. On considère alors la suite $\alpha_{1,1} = \alpha_1^{q_1 \cdots q_{r-1}}$, $\alpha_{1,2} = \alpha_1^{q_1 \cdots q_{r-2}}$, …, $\alpha_{1,r-1} = \alpha_1^{q_1}$, $\alpha_{1,r} = \alpha_1$. Alors $\alpha_{1,1}^{q_r} = \alpha_1^{p(1)} \in k$ et pour tout $j \geqslant 2$ on a $\alpha_{1,j}^{q_{r-j+1}} \in k(\alpha_{1,1}, \dots, \alpha_{1,j-1})$. De plus, $k(\alpha_{1,1}, \dots, \alpha_{1,r}) = k(\alpha_1)$. On fait de même pour les autres $p(i)$.

Pour le point ②, il suffit ensuite d'enlever les éléments qui sont dans le corps engendré par k et les éléments précédents, la suite obtenue vérifiera encore la propriété ①.

Remarque. (Pas traitée en cours.) Soient $k \subset L \subset E$ des extensions. On vérifie facilement que si $k \subset L$ et $L \subset E$ sont radicales, alors $k \subset E$ est radicale, et que si $k \subset E$ est radicale alors $L \subset E$ est radicale. Cependant, on peut avoir $k \subset E$ radicale et $k \subset L$ non radicale.

Donnons un exemple. Soit ω une racine primitive $7^{\text{ème}}$ de l'unité dans $\mathbb{C}$ et soit $\alpha = \omega + \omega^{-1} \in \mathbb{Q}(\omega)$. Il est clair que l'extension $\mathbb{Q} \subset \mathbb{Q}(\omega)$ est radicale. Vérifions que $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ n'est pas radicale.

Déterminons d'abord le degré de $\mathbb{Q} \subset \mathbb{Q}(\alpha)$. L'extension $\mathbb{Q} \subset \mathbb{Q}(\omega)$ est galoisienne (corps de décomposition de Φ_7 et $\mathrm{car}(\mathbb{Q}) = 0$), de degré 6, et son groupe de Galois G est formé des automorphismes s_k de $\mathbb{Q}(\omega)$ définis par $s_k(\omega) = \omega^k$ pour $1 \leqslant k \leqslant 6$. Notons que G est abélien, donc tous ses sous-groupes sont normaux dans G et donc pour toute extension intermédiaire $\mathbb{Q} \subset L \subset \mathbb{Q}(\omega)$, l'extension $\mathbb{Q} \subset L$ est galoisienne.

Le polynôme $f(X) = \prod_{k=1}^{6}(X - s_k(\alpha))$ est à coefficients dans $\mathbb{Q}(\omega)^G = \mathbb{Q}$ et admet α comme racine. Notons que $f(X) = g(X)^2$ avec $g(X) = \prod_{k=1}^{3}(X - s_k(\alpha))$ car $s_{7-k}(\alpha) = s_k(\alpha)$ pour tout k. Le calcul de g donne $g(X) = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$, qui est irréductible (par exemple avec le test des racines entières puisqu'il est de degré 3). C'est donc le polynôme minimal de α sur $\mathbb{Q}$. Ainsi, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. En particulier, puisque 3 est premier, pour tout $z \in \mathbb{Q}(\alpha) \setminus \mathbb{Q}$ on a $\mathbb{Q}(z) = \mathbb{Q}(\alpha)$.

Supposons que $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ soit radicale et soit $\beta_1, \dots, \beta_n$ une suite de radicaux pour l'extension. Quitte à supprimer des β_j, on peut supposer que $\beta_1 \notin \mathbb{Q}$. On a donc $\mathbb{Q}(\beta_1) = \mathbb{Q}(\alpha)$. De plus, par hypothèse, il existe $n \in \mathbb{N}$, $n \geqslant 2$ tel que $\beta_1^n = q \in \mathbb{Q}$.

L'extension $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ est galoisienne et son groupe de Galois est d'ordre 3. On en déduit que les conjugués de β_1 sont dans $\mathbb{Q}(\beta_1)$ et que β_1 a exactement deux conjugués γ_1 et γ_2 tels que β_1, γ_1 et γ_2 sont deux à deux distincts. De plus, γ_1 et γ_2 sont des racines du polynôme minimal de β sur $\mathbb{Q}$ qui divise $X^n - q$, donc $\gamma_1^n = \gamma_2^n = \beta_1^n = q$. On en déduit que $\frac{\gamma_1}{\beta_1}$ et $\frac{\gamma_2}{\beta_1}$, qui sont des éléments de $\mathbb{Q}(\beta_1) \subset \mathbb{R}$, sont des racines $n^{\text{èmes}}$ de l'unité. Mais les seules racines $n^{\text{èmes}}$ de l'unité qui sont dans $\mathbb{R}$ sont 1 et -1, on en déduit qu'au moins deux éléments parmi β_1, γ_1 et γ_2 sont égaux, et on a obtenu une contradiction.

Donc $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\omega)$ avec $\mathbb{Q} \subset \mathbb{Q}(\omega)$ radicale et $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ non radicale.

Théorème 6. Si k est un corps de caractéristique nulle et si $k \subset E$ est une extension normale radicale, alors $\mathrm{Gal}(E/k)$ est résoluble.

Nous utiliserons le lemme suivant.

Lemme 7. Soit k un corps de caractéristique nulle. Soit $k \subset E$ une extension, soit $n \in \mathbb{N}^*$ et soit $\varepsilon \in E$ une racine primitive $n^{\text{ème}}$ de l'unité.

Alors $\mathrm{Gal}(k(\varepsilon)/k)$ est abélien (et même cyclique si n est premier).

Démonstration. Voir Travaux Dirigés.

Puisque ε est une racine primitive $n^{\text{ème}}$ de l'unité, pour tout $s \in \mathrm{Gal}(k(\varepsilon)/k)$ l'élément $s(\varepsilon)$ est aussi une racine primitive $n^{\text{ème}}$ de l'unité, et par conséquent il existe $q_s \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que $s(\varepsilon) = \varepsilon^{q_s}$.

Soit $\psi : \mathrm{Gal}(k(\varepsilon)/k) \to (\mathbb{Z}/n\mathbb{Z})^\times$ définie par $\psi(s) = q_s$. Si s et t sont dans $\mathrm{Gal}(k(\varepsilon)/k)$, alors $s \circ t(\varepsilon) = s(\varepsilon^{q_t}) = (s(\varepsilon))^{q_t} = (\varepsilon^{q_s})^{q_t} = \varepsilon^{q_s q_t}$ donc $\psi(s \circ t) = \psi(s)\psi(t)$ et ψ est un morphisme de groupes. Si $\psi(s) = 1$, alors $s(\varepsilon) = \varepsilon$ et donc $s = \mathrm{id}$ (puisque s est déterminé par $s(\varepsilon)$). Donc ψ est injectif.

Finalement, $\mathrm{Gal}(k(\varepsilon)/k)$ s'identifie à un sous-groupe du groupe abélien $(\mathbb{Z}/n\mathbb{Z})^\times$.

Si de plus n est premier, alors $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique donc $\mathrm{Gal}(k(\varepsilon)/k)$ aussi. ✓

Démonstration du théorème. On raisonne par récurrence sur le nombre n d'éléments d'une suite de radicaux vérifiant les propriétés ① et ②.

➢ Si $n = 0$, c'est évident.

➢ Soit $n > 0$ tel que le résultat soit vrai pour les extensions normales radicales possédant une suite de radicaux vérifiant ① et ② et de longueur $n-1$. Soit $E = k(\alpha_1, \dots, \alpha_n)$ une extension normale radicale telle que $(\alpha_1, \dots, \alpha_n)$ vérifie ① et ②.

Il existe un nombre premier $p \in \mathbb{N}^*$ tel que $\alpha_1^p \in k$. Soit M_{α_1} le polynôme minimal de α_1 sur k. Puisque l'extension $k \subset E$ est normale, M_{α_1} est scindé dans $E[X]$, et toutes ses racines sont simples puisque la caractéristique est nulle. De plus, $\alpha_1 \notin k$ donc $\deg M_{\alpha_1} \geqslant 2$. Il existe donc une racine $\beta \neq \alpha$ de M_{α_1} dans E et par conséquent il existe $s \in \mathrm{Gal}(E/k)$ tel que $s(\alpha_1) = \beta$. Puisque $\alpha_1^p \in k$, on a alors $\alpha_1^p = s(\alpha_1^p) = \beta^p$.

Posons $\varepsilon = \alpha_1\beta^{-1}$. Alors $\varepsilon \neq 1$ et $\varepsilon^p = 1$ donc, puisque p est premier, $1, \varepsilon, \dots, \varepsilon^{p-1}$ sont les racines $p^{\text{ièmes}}$ de l'unité distinctes.

Soit $L = k(\varepsilon)$, on a une suite d'extensions $k \subset L \subset L(\alpha_1) \subset E$. L'extension $k \subset E$ est galoisienne donc l'extension $L \subset E$ est galoisienne. D'après la proposition 29 du chapitre 4, l'extension $L \subset L(\alpha_1)$ est galoisienne de groupe de Galois cyclique. Le théorème de correspondance de Galois implique alors que $\mathrm{Gal}(E/L(\alpha_1))$ est normal dans $\mathrm{Gal}(E/L)$ et que $\mathrm{Gal}(L(\alpha_1)/L) \cong \mathrm{Gal}(E/L)/\mathrm{Gal}(E/L(\alpha_1))$.

On a $E = L(\alpha_1)(\alpha_2, \dots, \alpha_n)$. On en déduit que $L(\alpha_1) \subset E$ est radicale et normale et qu'elle a une suite de radicaux vérifiant ① et ② de longueur $n-1$. D'après l'hypothèse de récurrence, $\mathrm{Gal}(E/L(\alpha_1))$ est résoluble.

De plus, le groupe $\mathrm{Gal}(L(\alpha_1)/L)$ est abélien (cyclique), donc résoluble. On en déduit donc que $\mathrm{Gal}(E/L)$ est résoluble (il admet un sous-groupe normal résoluble $\mathrm{Gal}(E/L(\alpha_1))$ et son quotient par ce sous-groupe est $\mathrm{Gal}(L(\alpha_1)/L)$, résoluble).

Enfin, L est un corps de décomposition de $X^p - 1$ sur k donc $k \subset L$ est normale, donc galoisienne, donc $\mathrm{Gal}(L/k) \cong \mathrm{Gal}(E/k)/\mathrm{Gal}(E/L)$ avec $\mathrm{Gal}(L/k)$ abélien d'après le lemme 7, donc résoluble, et $\mathrm{Gal}(E/L)$ est résoluble, donc $\mathrm{Gal}(E/k)$ est résoluble. ✓

B. Résolubilité des polynômes

Définition 8. *Soit k un corps de caractéristique nulle. Soit $f \in k[X]$ et soit E un corps de décomposition de f sur k.*

*On dit que l'équation polynomiale $f(x) = 0$, ou que le polynôme f, est **résoluble par radicaux** sur k s'il existe un corps L contenant E tel que l'extension $k \subset L$ soit radicale.*

Remarque. Chaque racine peut être obtenue à partir d'éléments de k par les opérations algébriques usuelles $(+, -, \times, \div)$ et en prenant des racines $n^{\text{ièmes}}$, mais pas toutes de la même manière.

Théorème 9. Soit k un corps de caractéristique nulle et soit $f \in k[X]$ un polynôme résoluble par radicaux sur k.

Alors le groupe $\mathrm{Gal}_k(f)$ est résoluble.

Lemme 10. Soit $k \subset L$ une extension radicale. Alors il existe une extension $L \subset N$ telle que $k \subset N$ soit normale et radicale.

Démonstration. Posons $L = k(\alpha_1, \dots, \alpha_n)$ avec, pour tout i, $p(i) \in \mathbb{N}^*$ tel que $\alpha_i^{p(i)} \in k(\alpha_1, \dots, \alpha_{i-1})$.
Pour tout i, notons $M_{\alpha_i} \in k[X]$ le polynôme minimal de α_i sur k et considérons le polynôme $f = \prod_{i=1}^{n} M_{\alpha_i} \in k[X]$.
Soit N un corps de décomposition de f sur k. Alors $k \subset N$ est normale, démontrons qu'elle est radicale.
Pour tout $i \in \{1, \dots, n\}$, notons $\beta_{i1} = \alpha_i, \beta_{i2}, \dots, \beta_{id_i}$ les racines de M_{α_i}, où $d_i = \deg M_{\alpha_i}$. Définissons une chaîne de corps $K_0 = k \subset K_1 \subset \dots \subset K_n = N$ récursivement par $K_i = K_{i-1}(\beta_{i1}, \dots, \beta_{id_i})$ pour $1 \leqslant i \leqslant n$. Nous savons déjà que $\beta_{i1}^{p(i)} = \alpha_i^{(p(i))} \in K_{i-1}$ pour tout i. Montrons que pour tout i et pour tout j avec $2 \leqslant j \leqslant d_i$, on a $\beta_{ij}^{p(i)} \in K_{i-1}$.
D'après le lemme 8 du chapitre 2, si E_i est un corps de décomposition de M_{α_i} sur k il existe $\sigma \in \mathrm{Gal}(E_i/k)$ tel que $\sigma(\alpha_i) = \beta_{ij}$. On a alors $\beta_{ij}^{p(i)} = \sigma(\alpha_i^{p(i)}) \in \sigma(K_{i-1})$. Or pour tout ℓ, σ permute les $\beta_{\ell j}$ (ce sont les racines de $M_{\alpha_\ell} \in k[X]$), donc $\sigma(K_{i-1}) = K_{i-1}$. Donc $\beta_{ij}^{p(i)} \in K_{i-1} \subset k(\beta_{11}, \dots, \beta_{1n}, \beta_{21}, \dots, \beta_{i,j-1})$.
On en déduit finalement que $k \subset L = k(\beta_{11}, \beta_{12}, \cdots, \beta_{n,d_n})$ est radicale. ✓

Démonstration du théorème 9. On suppose que f est résoluble par radicaux sur k. Soit E un corps de décomposition de f sur k et L une extension de E telle que $k \subset L$ soit radicale.
D'après le lemme précédent, il existe une extension $L \subset N$ telle que $k \subset N$ soit normale et radicale.
D'après le théorème 6, le groupe de Galois $\mathrm{Gal}(N/k)$ est résoluble.
Notons que l'extension $k \subset N$ est galoisienne puisqu'on est en caractéristique 0. L'extension $k \subset E$ est également galoisienne, donc d'après le théorème de correspondance de Galois, le groupe de Galois $\mathrm{Gal}(N/E)$ est normal dans le groupe $\mathrm{Gal}(N/k)$ et $\mathrm{Gal}_k(f) = \mathrm{Gal}(E/k) \cong \mathrm{Gal}(N/k)/\mathrm{Gal}(N/E)$ est isomorphe à un quotient du groupe résoluble $\mathrm{Gal}(N/k)$, il est donc résoluble. ✓

Remarque. La réciproque du théorème est également vraie : si $\mathrm{Gal}_k(f)$ est résoluble, alors f est résoluble par radicaux sur k. (Admis.)

Proposition 11. Soit p un nombre premier et soit $f \in \mathbb{Q}[X]$ un polynôme *irréductible* de degré p. Si f a exactement deux racines complexes non réelles, alors $\mathrm{Gal}_{\mathbb{Q}}(f)$ est isomorphe à S_p.

Démonstration. Voir Travaux Dirigés.
$\mathbb{C}$ est algébriquement clos, donc dans $\mathbb{C}[X]$, le polynôme f est scindé, et toutes ses racines sont simples (f irréductible et $\mathrm{car}(\mathbb{Q}) = 0$). Donc le groupe de Galois est un sous-groupe de S_p (permute les racines de f).
Soit E un corps de décomposition de f sur $\mathbb{Q}$. Alors $[E : \mathbb{Q}]$ est un multiple de p donc p divise $\left|\mathrm{Gal}_{\mathbb{Q}}(f)\right|$. Puisque p est premier, il existe un élément d'ordre p dans $\mathrm{Gal}_{\mathbb{Q}}(f)$. Or les seuls éléments de S_p d'ordre p sont les p-cycles, donc $\mathrm{Gal}_{\mathbb{Q}}(f)$ contient un p-cycle.
La conjugaison dans $\mathbb{C}$ induit un $\mathbb{Q}$-automorphisme de E qui laisse invariantes les $p-2$ racines réelles et échange les deux racines complexes, le groupe $\mathrm{Gal}_{\mathbb{Q}}(f)$ contient donc une transposition.
Quitte à changer l'ordre des racines de f dans E, on peut supposer que $\mathrm{Gal}_{\mathbb{Q}}(f)$ contient $\begin{pmatrix} 1 & 2 & 3 & \cdots & p \\ 2 & 1 & 3 & \cdots & p \end{pmatrix}$ et $\begin{pmatrix} 1 & 2 & \cdots & p-1 & p \\ 2 & 3 & \cdots & p & 1 \end{pmatrix}$, qui engendrent S_p, donc $\mathrm{Gal}_{\mathbb{Q}}(f) = S_p$. ✓

Corollaire 12. Le polynôme $X^5 - 6X + 3$ n'est pas résoluble par radicaux.

Démonstration. Voir Travaux Dirigés.
En utilisant le critère d'Eisenstein avec $p = 3$, on vérifie que le polynôme est irréductible sur $\mathbb{Q}$, et l'étude de la fonction $x \mapsto x^5 - 6x + 3$ montre qu'il a trois racines réelles distinctes. D'après la proposition, $\mathrm{Gal}(X^5 - 6X + 2/\mathbb{Q}) \cong S_5$, qui n'est pas résoluble, donc $X^5 - 6X + 3$ n'est pas résoluble par radicaux sur $\mathbb{Q}$. ✓

Lemme 13. Soit $\mathbb{R} \subset E$ une extension finie de degré impair. Alors $E = \mathbb{R}$.

Démonstration. Soit $\alpha \in E$. Soit M_α le polynôme minimal de α sur $\mathbb{R}$. On a $\deg M_\alpha = [\mathbb{R}(\alpha) : \mathbb{R}] = \dfrac{[E : \mathbb{R}]}{[E : \mathbb{R}(\alpha)]}$, qui est impair. D'après le théorème des valeurs intermédiaires, M_α a une racine réelle. Puisque M_α est irréductible sur $\mathbb{R}$, il est de degré 1 et donc $\alpha \in \mathbb{R}$. ✓

Lemme 14. Il n'existe pas d'extension quadratique de $\mathbb{C}$.

Démonstration. C'est une conséquence du fait (connu) que tout polynôme de degré 2 à coefficients dans $\mathbb{C}$ admet une racine dans $\mathbb{C}$. ✓

Lemme 15. Soit $\mathbb{C} \subset E$ une extension galoisienne de degré 2^n avec $n \in \mathbb{N}$. Alors $n = 0$ et $E = \mathbb{C}$.

Démonstration. Soit $G = \mathrm{Gal}(E/\mathbb{C})$. Puisque $\mathbb{C} \subset E$ est galoisienne, on a $|G| = [E : \mathbb{C}] = 2^n$.
D'après le lemme 14, on ne peut pas avoir $n = 1$. Supposons par l'absurde que $n > 1$.
D'après le premier théorème de Sylow, il existe un sous-groupe H de G d'ordre 2^{n-1}. Puisque H est d'indice 2 dans G, il est normal dans G. On déduit de la correspondance de Galois que l'extension $\mathbb{C} \subset E^H$ est galoisienne de degré $\left|\mathrm{Gal}(E^H/\mathbb{C})\right| = \left|\mathrm{Gal}(E/\mathbb{C})/\mathrm{Gal}(E/E^H)\right| = |G/H| = \dfrac{2^n}{2^{n-1}} = 2$.
D'après le lemme 14 on a obtenu une contradiction.
On a donc bien $n = 0$. ✓

Démonstration du théorème de d'Alembert-Gauss. Soit $f \in \mathbb{C}[X]$ un polynôme non constant. Nous devons démontrer que f a une racine dans $\mathbb{C}$.
Remarquons que $\overline{f}f \in \mathbb{R}[X]$ (où $\overline{f}$ désigne le polynôme conjugué de f). De plus, f a une racine dans $\mathbb{C}$ si, et seulement si, $\overline{f}f$ a une racine dans $\mathbb{C}$. On peut donc supposer que $f \in \mathbb{R}[X]$.
Soit E un corps de décomposition de f sur $\mathbb{R}$ et soit $L = E(i)$. Alors L est un corps de décomposition du polynôme $f(X)(X^2+1)$ sur $\mathbb{R}$, donc $\mathbb{R} \subset L$ est une extension normale, qui est donc galoisienne puisque $\mathrm{car}(\mathbb{R}) = 0$. Soit $G = \mathrm{Gal}(L/\mathbb{R})$.
On a $\mathbb{R} \subset \mathbb{C} \subset L$ donc l'extension $\mathbb{R} \subset L$ est de degré pair (multiple de $[\mathbb{C} : \mathbb{R}] = 2$). Posons $[L : \mathbb{R}] = 2^n m$ avec $n \in \mathbb{N}^*$ et $m \in \mathbb{N}^*$ impair.
Soit H un 2-sous-groupe de Sylow de G. Alors H est d'indice m dans G. De plus, l'extension $L^H \subset L$ est galoisienne et $H = \mathrm{Gal}(L/L^H)$ donc $[L^H : \mathbb{R}] = \dfrac{[L : \mathbb{R}]}{[L : L^H]} = \dfrac{|G|}{|H|} = m$ d'après le théorème de correspondance de Galois. D'après le lemme 13, on a $L^H = \mathbb{R}$ et $m = 1$. Donc $[L : \mathbb{R}] = 2^n$, ce qui implique que $[L : \mathbb{C}] = 2^{n-1}$ et donc grâce au lemme 15 on a $L = \mathbb{C}$.
Puisque f admet une racine dans L, il a une racine dans $\mathbb{C}$. ✓

Deuxième partie

Algèbre bilinéaire

CHAPITRE 6

Formes bilinéaires symétriques ; formes quadratiques ; orthogonalité

Dans la suite K est un corps de **caractéristique différente de** 2 et V est un K-espace vectoriel de dimension finie.

I GÉNÉRALITÉS SUR LES FORMES BILINÉAIRES

Définition 1. *Une **forme bilinéaire sur** V est une application $b : V \times V \longrightarrow K$ linéaire en chaque variable, c'est-à-dire telle que pour tout $(u, v, w) \in V^3$ et pour tout $\lambda \in K$,*

$$b(u+v,w) = b(u,w) + b(v,w), \qquad b(\lambda u, w) = \lambda b(u,w),$$
$$b(u,v+w) = b(u,v) + b(u,w), \qquad b(u,\lambda w) = \lambda b(u,w).$$

Exemples. ➢ Les produits scalaires sur les espaces vectoriels réels sont des formes bilinéaires.
➢ $b : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ définie par $b((x_1,x_2),(y_1,y_2)) = x_1y_1 - x_2y_2$ est une forme bilinéaire sur $\mathbb{R}^2$.
➢ $b : \mathbb{C}^2 \times \mathbb{C}^2 \to \mathbb{C}$ définie par $b((x_1,x_2),(y_1,y_2)) = x_1y_1 + x_1y_2$ est une forme bilinéaire sur $\mathbb{C}^2$.

Définition 2. *Soit b une forme bilinéaire sur V et soit $\mathcal{B} = \{e_1, \ldots, e_n\}$ une base de V. Posons $b_{ij} = b(e_i, e_j)$. La matrice $M_{\mathcal{B}}(b) = (b_{ij}) \in \mathcal{M}_n(K)$ est appelée la **matrice de b relativement à la base $\mathcal{B}$**.*

Le résultat suivant montre qu'une forme bilinéaire est entièrement déterminée par sa matrice dans une base. La preuve est un simple calcul laissé en exercice.

Proposition 3. Soit b une forme bilinéaire sur V, soit $\mathcal{B} = \{e_1, \ldots, e_n\}$ une base de V et soit $M_{\mathcal{B}}(b) = (b_{ij})$ la matrice de b relativement à la base $\mathcal{B}$. On a

$$b\left(\sum_{i=1}^n \lambda_i e_i, \sum_{i=1}^n \mu_i e_i\right) = \sum_{i,j=1}^n \lambda_i \mu_j b_{ij} = (\lambda_1, \ldots, \lambda_n) \cdot M_{\mathcal{B}}(b) \cdot {}^t(\mu_1, \ldots, \mu_n)$$

Réciproquement, si $M = (m_{ij}) \in \mathcal{M}_n(K)$, il existe une unique forme bilinéaire b sur V telle que $M_{\mathcal{B}}(b) = M$, c'est-à-dire $b(e_i, e_j) = m_{ij}$, pour tous i, j.

La matrice d'une forme bilinéaire dans une base dépend du choix de la base. La preuve du résultat suivant est une vérification directe, laissée en exercice.

Proposition 4. Soit b une forme bilinéaire sur V, et soient $\mathcal{B} = \{e_1, \ldots, e_n\}$ et $\mathcal{B}' = \{e'_1, \ldots, e'_n\}$ des bases de V. On a

$$M_{\mathcal{B}'}(b) = {}^tDM_{\mathcal{B}}(b)D$$

où $D = (d_{ij}) \in \mathrm{GL}_n(K)$ est la matrice inversible définie par $e'_i = \sum_{j=1}^n d_{ji}e_j$ pour tout i (matrice de passage).

Ce résultat mène à la définition suivante.

Définition 5. *On dit que deux matrices $M, N \in M_n(K)$ sont **congruentes** s'il existe $D \in \mathrm{GL}_n(K)$ telle que $M = {}^tDND$.*

Définition 6. *Soient b_1 et b_2 des formes bilinéaires sur des espaces vectoriels V_1 et V_2. On dit que b_1 et b_2 **équivalentes** s'il existe un isomorphisme K-linéaire $f : V_1 \longrightarrow V_2$ tel que*

$$\forall v, w \in V_1, \quad b_2(f(v), f(w)) = b_1(v, w)$$

Il est clair que la relation «être équivalente» est une relation d'équivalence sur les formes bilinéaires. *L'objectif principal de la théorie des formes bilinéaires est de les classifier à équivalence près*. En fait le problème se ramène au cas $V_1 = V_2$, mais il peut être plus commode dans certaines situations de considérer des formes bilinéaires définies sur des espaces différents.

Au niveau matriciel, le problème de classification prend la forme suivante.

Proposition 7. Soient b_1 et b_2 des formes bilinéaires sur des espaces vectoriels V_1 et V_2. Les assertions suivantes sont équivalentes.

(i) b_1 et b_2 sont équivalentes.

(ii) Pour toute base $\mathcal{B}$ de V_1, il existe une base $\mathcal{C}$ de V_2 telle que $M_{\mathcal{B}}(b_1) = M_{\mathcal{C}}(b_2)$.

(iii) Il existe des bases $\mathcal{B}$ de V_1 et $\mathcal{C}$ de V_2 dans lesquelles $M_{\mathcal{B}}(b_1) = M_{\mathcal{C}}(b_2)$.

En particulier, lorsque $V_1 = V_2 = V$, les assertions suivantes sont équivalentes.

(i) b_1 et b_2 sont équivalentes.

(ii) Pour toute base $\mathcal{B}$ de V, il existe une base $\mathcal{C}$ de V telle que $M_{\mathcal{B}}(b_1) = M_{\mathcal{C}}(b_2)$.

(iii) Il existe des bases $\mathcal{B}$ et $\mathcal{C}$ de V telles que $M_{\mathcal{B}}(b_1) = M_{\mathcal{C}}(b_2)$.

(iv) Il existe une base $\mathcal{B}$ de V telle que les matrices $M_{\mathcal{B}}(b_1)$ et $M_{\mathcal{B}}(b_2)$ soient congruentes.

(v) Dans toute base $\mathcal{B}$ de V, les matrices $M_{\mathcal{B}}(b_1)$ et $M_{\mathcal{B}}(b_2)$ sont congruentes.

Démonstration. (i)⇒ (ii) Supposons b_1 et b_2 équivalentes : il existe un isomorphisme K-linéaire $f : V_1 \longrightarrow V_2$ tel que pour tous $v, w \in V_1$, on a $b_2(f(v), f(w)) = b_1(v, w)$. Soit $\mathcal{B} = \{e_1, \ldots, e_n\}$ une base de V_1, et considérons la base $f(\mathcal{B}) = \{f(e_1), \ldots, f(e_n)\}$ de V_2. Alors la matrice de b_1 dans la base $\mathcal{B}$ et la matrice de b_2 dans la base $f(\mathcal{B})$ sont égales.

(ii)⇒(iii) Evident.

(iii)⇒(i) Supposons qu'il existe une base $\mathcal{B} = \{e_1, \ldots, e_n\}$ de V_1 et une base $\mathcal{C} = \{e'_1, \ldots, e'_n\}$ de V_2 telles $M_{\mathcal{B}}(b_1) = M_{\mathcal{C}}(b_2)$. Alors l'unique isomorphisme linéaire $f : V_1 \to V_2$ tel que $f(e_i) = e'_i$, pour tout i, vérifie $b_2(f(v), f(w)) = b_1(v, w)$ pour tous $v, w \in V_1$.

Supposons que $V_1 = V_2 = V$. Les assertions (i), (ii) et (iii) sont équivalentes d'après ce qui précède. L'équivalence avec les autres assertions se montre directement en utilisant la proposition 4. ✓

On définit maintenant des invariants importants associés à une forme bilinéaire. Comme à l'habitude, le rang d'une matrice est par définition la dimension de l'image de l'application linéaire qu'elle définit.

Définition-Proposition 8. *Soit $b : V \times V \longrightarrow K$ une forme bilinéaire. Le **rang de** b est le rang de la matrice de b relativement à une base de V. Il ne dépend pas du choix de la base de V, et si b_1 et b_2 sont deux formes bilinéaires équivalentes, on a* $\operatorname{rang}(b_1) = \operatorname{rang}(b_2)$.

*On dit que b est **non dégénérée** lorsque* $\operatorname{rang}(b) = \dim(V)$, *c'est-à-dire lorsque la matrice de b est inversible.*

Le résultat se montre grâce les propositions 4 et 7 (les rangs de deux matrices congruentes étant égaux), mais on peut aussi le montrer grâce au résultat important suivant.

Proposition 9. Soit $b : V \times V \longrightarrow K$ une forme bilinéaire et soit

$$\begin{aligned} \Psi_b : V &\longrightarrow V^* \\ v &\longmapsto \Psi_b(v) = b(-, v),\ \Psi_b(v)(w) = b(w, v) \end{aligned}$$

Alors Ψ_b est une application linéaire et $\operatorname{rang}(b) = \operatorname{rang}(\Psi_b) = \dim(\operatorname{Im}(\Psi_b))$. En particulier b est non dégénérée si et seulement Ψ_b est un isomorphisme.

Démonstration. La linéarité de Ψ_b est une vérification facile. Si $\mathcal{B} = \{e_1, \dots, e_n\}$ est une base de V, de base duale $\mathcal{B}^* = \{e_1^*, \dots, e_n^*\}$, on a $\Psi_b(e_j) = \sum_{i=1}^n b(e_i, e_j) e_i^*$ pour tout j. La matrice de Ψ_b relativement aux bases $\mathcal{B}$ et $\mathcal{B}^*$ est donc $M_{\mathcal{B}}(b)$, d'où le résultat. ✓

Définition-Proposition 10. *Soit $b : V \times V \longrightarrow K$ une forme bilinéaire. Soit $(K^*)^2 = \left\{x^2 \mid x \in K^*\right\}$; c'est un sous-groupe de K^*.*

*Le **discriminant de** b est défini par*

$$\operatorname{discr}(b) = \begin{cases} 0 & \text{si } \det(M) = 0 \\ \overline{\det(M)} \in K^*/(K^*)^2 & \text{sinon} \end{cases}$$

où M est la matrice de b relativement à une base de V. Il ne dépend pas du choix de la base de V, et si b_1 et b_2 sont deux formes bilinéaires équivalentes, on a $\operatorname{discr}(b_1) = \operatorname{discr}(b_2)$.

Exemples. Si b est la forme bilinéaire sur $\mathbb{R}^2$ dont la matrice associée dans la base canonique est $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ alors $\operatorname{discr}(b) = \overline{-1}$.

Si b est la forme bilinéaire sur $\mathbb{C}^2$ dont la matrice associée dans la base canonique est $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ alors $\operatorname{discr}(b) = \overline{-1} = \overline{i^2} = \overline{1}$.

Démonstration. Soient M et N les matrices respectives de b dans des bases de V. Alors $M = {}^tDND$ pour une matrice inversible D. On a donc $\det(M) = \det(N)\det(D)^2 \in \det(N)(K^*)^2 = \overline{\det(N)}$.
La preuve de la dernière assertion est similaire. ✓

II Formes bilinéaires symétriques et formes quadratiques

On ne considère désormais que des formes bilinéaires symétriques. La définition est la suivante.

Définition 11. *On dit qu'une forme bilinéaire $b : V \times V \longrightarrow K$ est **symétrique** si*

$$\forall u, v \in V,\ b(u, v) = b(v, u)$$

Rappelons qu'une matrice $A = (a_{ij}) \in \mathcal{M}_n(K)$ est dite symétrique si ${}^tA = A$, c'est-à-dire si $a_{ij} = a_{ji}$ pour tous i, j. On note $\operatorname{Sym}_n(K)$ l'ensemble des matrices symétriques $n \times n$: c'est un sous-espace vectoriel de $\mathcal{M}_n(K)$, de dimension $\frac{n(n+1)}{2}$.

On voit facilement qu'une forme bilinéaire est symétrique si et seulement si sa matrice dans une (ou toute) base est symétrique.

Proposition 12. Soient $b, b' : V \times V \longrightarrow K$ deux formes bilinéaires symétriques telles que pour tout $u \in E$, on a $b(u,u) = b'(u,u)$. Alors $b = b'$.

Démonstration. Soient $u, v \in V$. On a

$$b(u+v,u+v) = b(u,u) + b(v,v) + 2b(u,v) \quad \text{et} \quad b'(u+v,u+v) = b'(u,u) + b'(v,v) + 2b'(u,v)$$

Cela donne $b(u,v) = b'(u,v)$ pour tous $u, v \in V$ (on rappelle que la caractéristique de K n'est pas 2), d'où $b = b'$. ✓

Le résultat précédent et sa preuve justifient la définition suivante.

Définition 13. *Soit $q : V \to K$ une application. On dit que q est une **forme quadratique sur** V s'il existe une forme bilinéaire symétrique $b : V \times V \longrightarrow K$ telle que*

$$\forall u \in V,\ q(u) = b(u,u)$$

La forme bilinéaire b est alors unique, on la note b_q, et on a $b_q(u,v) = \frac{1}{2}(q(u+v) - q(u) - q(v))$.

Réciproquement, si $b : V \times V \longrightarrow K$ est une forme bilinéaire symétrique, on lui associe la forme quadratique q_b définie par $q_b(u) := b(u,u)$.

Il est donc complètement équivalent de se donner une forme bilinéaire symétrique ou une forme quadratique.

Exemples. ➢ On prend $V = K^2$ et $q(u) = x_1^2 + x_2^2$ pour tout $u = (x_1, x_2) \in V$. Alors q est une forme quadratique et pour $v = (y_1, y_2)$ on a $b_q(u,v) = x_1y_1 + x_2y_2$.

➢ On prend $V = K^2$ et $q(u) = x_1^2 - x_2^2 + 6x_1x_2$. Alors q est une forme quadratique et $b_q(u,v) = x_1y_1 - x_2y_2 + 3x_1y_2 + 3x_2y_1$.

➢ Plus généralement, soit $V = K^n$. Pour tout $u = (x_1, \ldots, x_n) \in V$, on pose

✧ $q_1(u) = ax_i^2$ pour un $a \in K$;

✧ $q_2(u) = ax_ix_j$ pour un $a \in K$.

Alors q_1 et q_2 sont des formes quadratiques, de formes bilinéaires associées définies par

✧ $b_{q_1}(u,v) = ax_iy_i$;

✧ $b_{q_2}(u,v) = \frac{a}{2}x_iy_j + \frac{a}{2}y_ix_j$

pour tout $v = (y_1, \ldots, y_n) \in V$.

➢ On prend $V = \mathbb{R}^2$ et $b = \langle , \rangle$ un produit scalaire sur $\mathbb{R}^2$. On note $\|.\|$ la norme associée à b. Alors $q_b = \|.\|^2$.

La terminologie «forme quadratique» est justifiée par l'expression dans une base.

Proposition 14. Soit $q : V \longrightarrow K$ une application et soit $\mathcal{B} = \{e_1, \ldots, e_n\}$ une base de V. Les assertions suivantes sont équivalentes.

(i) q est une forme quadratique.

(ii) Il existe $A = (a_{ij}) \in \mathrm{Sym}_n(K)$ telle que si $u = \sum_{i=1}^n x_ie_i$, alors

$$q(u) = \sum_{i=1}^n a_{ii}x_i^2 + 2\sum_{i<j} a_{ij}x_ix_j.$$

Démonstration. Soit b une forme bilinéaire sur V et soit $A = (a_{ij}) \in \mathrm{Sym}_n(K)$ la matrice de b relativement à $\mathcal{B}$. Alors pour tout $u = \sum_{i=1}^n x_i e_i$ on a

$$\begin{aligned} b(u,u) &= b\left(\sum_{i=1}^n x_i e_i, \sum_{j=1}^n x_j e_j\right) = \sum_{i=1}^n \sum_{j=1}^n x_i x_j b(e_i,e_j) = \sum_{i=1}^n \sum_{j=1}^n x_i x_j a_{ij} \\ &= \sum_{i=1}^n a_{ii} x_i^2 + \sum_{i=1}^n \sum_{j\neq i} a_{ij} x_i x_j = \sum_{i=1}^n a_{ii} x_i^2 + \sum_{1\leqslant i<j\leqslant n} a_{ij} x_i x_j + \sum_{1\leqslant j<i\leqslant n} a_{ij} x_i x_j \\ &= \sum_{i=1}^n a_{ii} x_i^2 + \sum_{1\leqslant i<j\leqslant n} a_{ij} x_i x_j + \sum_{1\leqslant i<j\leqslant n} a_{ji} x_i x_j = \sum_{i=1}^n a_{ii} x_i^2 + 2 \sum_{1\leqslant i<j\leqslant n} a_{ij} x_i x_j, \end{aligned}$$

la dernière égalité découlant du fait que A est symétrique.

➢ (i)⇒(ii). Supposons que q est une forme quadratique, de forme bilinéaire associée b. Le calcul précédent montre alors que $q(u) = b(u,u) = \sum_{i=1}^n a_{ii} x_i^2 + 2\sum_{1\leqslant i<j\leqslant n} a_{ij} x_i x_j$.

➢ (ii)⇒(i). Supposons que pour tout $u = \sum_{i=1}^n x_i e_i \in V$ on ait $q(u) = \sum_{i=1}^n a_{ii} x_i^2 + 2\sum_{1\leqslant i<j\leqslant n} a_{ij} x_i x_j$. Soit b la forme bilinéaire symétrique sur V dont la matrice relativement à la base $\mathcal{B}$ est A. Alors le calcul précédent montre que $b(u,u) = q(u)$ pour tout $u \in V$ donc q est une forme quadratique de forme bilinéaire associée b. ✓

Ainsi, une fois qu'une base de V est fixée, la forme quadratique q s'exprime comme un polynôme homogène de degré 2 en les coordonnées du vecteur, d'où le nom de forme quadratique.

De plus, si A est diagonale, alors $q(u) = \sum_{i=1}^n a_{ii} x_i^2$ est une combinaison linéaire de carrés. Nous allons voir que, moyennant un changement de base, on peut toujours se ramener à ce cas.

La notion d'équivalence pour les formes bilinéaires symétriques prend la forme suivante au niveau des formes quadratiques.

Définition-Proposition 15. *Soient $b_1 : V_1 \times V_1 \longrightarrow K$ et $b_2 : V_2 \times V_2 \longrightarrow K$ des formes bilinéaires symétriques et soient q_1, q_2 les formes quadratiques associées. Alors b_1 et b_2 sont équivalentes si et seulement s'il existe un isomorphisme linéaire $f : V_1 \longrightarrow V_2$ tel que $q_2 \circ f = q_1$.*

*On dit que **deux formes quadratiques sont équivalentes** quand leurs formes bilinéaires sont équivalentes, c'est-à-dire quand la condition précédente est vérifiée.*

La vérification est facile (exercice).

III Orthogonalité

Définition 16. *Soit $b : V \times V \longrightarrow K$ une forme bilinéaire symétrique.*

*On dit que deux vecteurs $u, v \in V$ sont b-**orthogonaux** (ou simplement orthogonaux s'il n'y a pas d'ambigüité) si $b(u,v) = 0$.*

*Une famille de vecteurs S est dite (b-)**orthogonale** si les vecteurs de S sont deux à deux orthogonaux, elle est dite (b-)**orthonormée** si elle est orthogonale et si $b(u,u) = 1$ pour tout $u \in S$.*

Proposition 17. Soit $b : V \times V \longrightarrow k$ une forme bilinéaire symétrique et soit $S \subset V$ une famille orthogonale telle que $b(u,u) \neq 0$ pour tout $u \in S$. Alors la famille S est linéairement indépendante.

Démonstration. Soient $v_1, \ldots, v_n \in S$ et $\lambda_1, \ldots, \lambda_n \in K$ tels que $\sum_{i=1}^n \lambda_i v_i = 0$. Pour tout i on a

$$0 = b(\sum_{j=1}^n \lambda_j v_j, v_i) = \sum_{j=1}^n \lambda_j b(v_j, v_i) = \lambda_i b(v_i, v_i)$$

d'où $\lambda_i = 0$ et le résultat. ✓

Remarque. L'hypothèse de la proposition est bien «$b(u,u) \neq 0$ pour tout $u \in S$» et non «$u \neq 0$ pour tout $u \in S$». En effet, contrairement au cas où b est un produit scalaire, on peut avoir $u \neq 0$ et $b(u,u) = 0$ (on dit alors que u est *isotrope*).

Par exemple, soit b la forme bilinéaire sur $\mathbb{R}^2$ donnée par $b((x_1,x_2),(y_1,y_2)) = x_1y_2 + x_2y_1$. Alors $u = (0,1) \neq 0$ mais $b(u,u) = 0$. Notons que b est non-dégénérée.

Définition 18. *Soit b une forme bilinéaire symétrique sur V. Si S est une partie de V, le b-**orthogonal** de S (ou l'orthogonal de S pour b) est le sous-ensemble*

$$S^{\perp_b} := \{u \in V \mid \forall v \in S,\ b(u,v) = 0\}$$

On le note $S^\perp$ lorsqu'il n'y a pas d'ambigüité.

Les propriétés suivantes sont des vérifications immédiates.

Proposition 19. Soit b une forme bilinéaire symétrique sur V et soit S une partie de V.

(i) $S^\perp$ est un sous-espace vectoriel de V, et $S \subset (S^\perp)^\perp$.

(ii) Si $S \subset T$, alors $T^\perp \subset S^\perp$.

(iii) Si W est un sous-espace vectoriel de V et $\{w_1, \dots, w_p\}$ est une famille génératrice de W, alors

$$W^\perp = \{u \in V \mid \forall i = 1, \dots, p,\ b(u, w_i) = 0\} = \{w_1, \dots, w_r\}^\perp.$$

Autrement dit, $(\mathrm{vect}\{S\})^\perp = S^\perp$.

Remarque. Attention, même si S est un sous-espace vectoriel de V, on peut avoir $S \subsetneq (S^\perp)^\perp$.
Par exemple, soit b la forme bilinéaire sur $\mathbb{R}^2$ donnée par $b((x_1,x_2),(y_1,y_2)) = x_1y_1$.
Soit $S = \mathrm{vect}\{(1,0)\}$. Alors $S^\perp = \mathrm{vect}\{(0,1)\}$ et $(S^\perp)^\perp = \mathbb{R}^2 \supsetneq S$.

Le résultat suivant est très important.

Théorème 20. Soit $b : V \times V \longrightarrow K$ une forme bilinéaire symétrique, et soit $W \subset V$ un sous-espace vectoriel.

(i) b est non dégénérée si, et seulement si, $V^\perp = \{0\}$.

(ii) Si b est non dégénérée, alors $\dim(V) = \dim(W) + \dim(W^\perp)$, et $W = (W^\perp)^\perp$.

(iii) Si $W \cap W^\perp = \{0\}$, alors $V = W \oplus W^\perp$.

Démonstration. (i) Soit $\Psi_b : V \to V^*$ l'application linéaire définie par $\Psi_b(v) = b(-,v)$ pour tout $v \in V$. On sait d'après la proposition 9 que b est non dégénérée si, et seulement si, Ψ_b est un isomorphisme. On constate que $\mathrm{Ker}\,\Psi_b = V^\perp$. Or Ψ_b est un isomorphisme si et seulement si Ψ_b est injectif. On en déduit donc que b est non dégénérée si et seulement si $V^\perp = \{0\}$.

(ii) On suppose que b est non dégénérée. L'application linéaire

$$\begin{aligned} \Psi_b^W \colon V &\longrightarrow W^* \\ v &\longmapsto b(v,-)_{|W} \end{aligned}$$

est surjective. En effet, si $f \in W^*$, on peut prolonger f à $g \in V^*$, or b est non dégénérée donc Ψ_b est surjective, donc $g = \Psi_b(v)$ et alors $f = g_{|W} = \Psi_b^W(v)$. Le noyau de Ψ_b^W est $W^\perp$, donc le théorème du rang donne $\dim(V) = \dim(W) + \dim(W^\perp)$, comme annoncé. On a alors aussi $\dim(V) = \dim(W^\perp) + \dim((W^\perp)^\perp)$, donc $\dim((W^\perp)^\perp) = \dim(W)$ et donc comme $W \subset (W^\perp)^\perp$, on a bien $W = (W^\perp)^\perp$.

(iii) L'application linéaire

$$\begin{aligned} (\Psi_b^W)_{|W} \colon W &\longrightarrow W^* \\ w &\longmapsto b(w,-)_{|W} \end{aligned}$$

a pour noyau $W \cap W^\perp$. Si cet espace est nul, alors $(\Psi_b^W)_{|W}$ est injective et c'est donc un isomorphisme (la restriction de b à W est donc non-dégénérée). En particulier $\Psi_b^W \colon V \to W^*$ est surjective, et le théorème du rang donne donc à nouveau $\dim(V) = \dim(W) + \dim(W^\perp)$. Puisque $W \cap W^\perp = \{0\}$, on en déduit que $V = W \oplus W^\perp$. ✓

Remarque. On peut avoir une forme bilinéaire b sur V non-dégénérée dont la restriction à un sous-espace W est dégénérée.

Par exemple, si b est la forme bilinéaire symétrique sur $\mathbb{R}^2$ associée à la forme quadratique $q : \mathbb{R}^2 \to \mathbb{R}$ définie par $q(x_1, x_2) = x_1^2 - x_2^2$ et si $W = \text{vect}\{(1,1)\}$, alors b est non-dégénérée mais sa restriction à W est nulle.

Le résultat suivant est un cas particulier de la proposition 12.

Proposition 21. Soit $b : V \times V \longrightarrow K$ une forme bilinéaire symétrique non nulle. Alors il existe $v \in V$ tel que $q(v) = b(v,v) \neq 0$.

On peut maintenant montrer l'existence d'une base orthogonale pour une forme bilinéaire symétrique quelconque.

Théorème 22. Soit $b : V \times V \longrightarrow K$ une forme bilinéaire symétrique. Alors V possède une base orthogonale pour b. Il existe donc une base de V dans laquelle la matrice de b soit diagonale

$$\begin{pmatrix} a_1 & 0 & & 0 \\ 0 & \ddots & & 0 \\ & & a_r & \\ 0 & 0 & & 0_{n-r} \end{pmatrix}$$

où tous les a_i sont non nuls et $r = \text{rang}(b)$.

Démonstration. On procède par récurrence sur $n = \dim(V)$.

Si $n = 1$ le résultat est évident.

Soit $n > 1$ tel que le résultat est vrai pour les formes bilinéaires symétriques sur les espaces vectoriels de dimension $< n$. Supposons que $b \neq 0$, sinon le résultat est évident. Soit $v \in V$ tel que $b(v,v) \neq 0$ (proposition précédente), et soit $W = \text{vect}\{v\}$. On a $W \cap W^\perp = \{0\}$, donc $V = W \oplus W^\perp$ par le théorème 20. On a $\dim(W^\perp) = n - 1$, donc par hypothèse de récurrence il existe une base b-orthogonale $\mathcal{B}$ de $W^\perp$, et ainsi $\{v\} \cup \mathcal{B}$ est une base b-orthogonale de V. En ordonnant cette base de manière adéquate, on obtient la forme demandée pour la matrice de b dans cette base, et il est clair que l'entier r est le rang de b. ✓

Remarque. Il résulte de ce théorème que si $b : V \times V \longrightarrow K$ est une forme bilinéaire symétrique, il existe un sous-espace $E \subset V$ tel que $V = V^\perp \oplus E$ (cette somme directe étant b-orthogonale, c'est-à-dire que tous les vecteurs d'un des sous-espaces sont orthogonaux aux vecteurs de l'autre sous-espace) et $\dim(E) = \text{rang}(b)$.

En effet, si $\mathcal{B} = \{e_1, \ldots, e_n\}$ est une base relativement à laquelle la matrice de b est celle de l'énoncé du théorème, $V^\perp = \text{vect}\{e_{r+1}, \ldots, e_n\}$ donc $E = \text{vect}\{e_1, \ldots, e_r\}$ convient.

Il y a bien entendu une version de ce théorème pour les formes quadratiques et pour les matrices symétriques.

C'est le résultat de réduction le plus général sur un corps quelconque. Si on fait des hypothèses supplémentaires sur K, nous allons voir que l'on peut obtenir des résultats plus précis.

CHAPITRE 7

Classification des formes bilinéaires symétriques

I FORMES BILINÉAIRES SYMÉTRIQUES SUR UN CORPS ALGÉBRIQUEMENT CLOS

Dans le cas où le corps de base est algébriquement clos, le théorème 22 du chapitre précédent peut être affiné de la manière suivante, pour obtenir une classification complète des formes bilinéaires symétriques dans ce cas.

Théorème 1. Soit $b : V \times V \longrightarrow K$ une forme bilinéaire symétrique. Supposons que tout élément de K admet une racine carrée dans K (cela est vrai si K est algébriquement clos). Alors il existe une base de V dans laquelle la matrice de b est diagonale de la forme

$$\begin{pmatrix} I_r & 0 \\ 0 & 0_{n-r} \end{pmatrix}$$

où $r = \text{rang}(b)$.

En particulier deux formes bilinéaires symétriques $b_1, b_2 : V \times V \longrightarrow K$ sont équivalentes si, et seulement si, elles ont même rang.

Démonstration. Soit r le rang de b et soit $\{e_1, \ldots, e_n\}$ une base b-orthogonale : $b(e_i, e_j) = \delta_{ij} a_i$ avec $a_1, \ldots, a_r$ non nuls et $a_i = 0$ pour $i > r$. Pour $i \leqslant r$, soit $c_i \in K$ tel que $c_i^2 = a_i$. La base $\left\{c_1^{-1} e_1, \ldots, c_r^{-1} e_r, e_{r+1}, \ldots, e_n\right\}$ convient.

Supposons que b_1 et b_2 soient équivalentes. Soit $\mathcal{B}$ une base de V. Les matrices de b_1 et b_2 relativement à la base $\mathcal{B}$ sont congruentes d'après la proposition 7 du chapitre 6, donc elles ont même rang.

Supposons que b_1 et b_2 aient le même rang r. Ce qui précède montre qu'il existe des bases $\mathcal{B}$ et $\mathcal{C}$ de V telles que $M_{\mathcal{B}}(b_1) = A = M_{\mathcal{C}}(b_2)$ avec $A = \begin{pmatrix} I_r & 0 \\ 0 & 0_{n-r} \end{pmatrix}$. On en déduit que b_1 et b_2 sont équivalentes d'après la proposition 7 du chapitre 6. ✓

Corollaire 2. On suppose que tout élément de K admet une racine carrée dans K.

(i) Deux formes quadratiques sur V sont équivalentes si, et seulement si, elles ont même rang.

(ii) Deux matrices symétriques sont congruentes si, et seulement si, elles ont même rang.

De plus, les matrices $\begin{pmatrix} I_r & 0 \\ 0 & 0_{n-r} \end{pmatrix}$ pour $0 \leqslant r \leqslant n$ forment des représentants de ces classes de congruence.

(iii) Il y a $n+1$ classes d'équivalence de formes quadratiques ou de formes bilinéaires symétriques.
Il y a $n+1$ classes de congruence de matrices symétriques.

A. Théorèmes généraux

On commence par la forme la plus générale de la loi d'inertie de Sylvester.

Théorème 3. (Loi d'inertie de Sylvester) Soit K un sous-corps de $\mathbb{R}$ et soit $b : V \times V \longrightarrow K$ une forme bilinéaire symétrique. Il existe une base $\{e_1, \dots, e_n\}$ de V dans laquelle la matrice de b est diagonale de la forme

$$\begin{pmatrix} a_1 & 0 & & & & & 0 \\ 0 & \ddots & & & & & \\ & & a_p & & & & \\ 0 & & & -a_{p+1} & & & 0 \\ & & & & \ddots & & \\ & & & & & -a_r & \\ 0 & & & & & & 0_{n-r} \end{pmatrix}$$

avec $r = \operatorname{rang}(b)$, $(a_1, \dots, a_r) \in K^r$ et $a_i > 0$ pour tout i, $1 \leqslant i \leqslant r$. Le couple d'entiers $(p, r-p)$ ne dépend pas du choix d'une telle base, on le note $\operatorname{sign}(b)$, et on dit que c'est la **signature** de la forme bilinéaire b.

Deux formes bilinéaires symétriques équivalentes ont même signature.

Démonstration. L'existence d'une telle base est une conséquence directe du Théorème 22 du chapitre 6, en ordonnant les vecteurs de la base de manière adéquate.

Il faut maintenant montrer l'indépendance de p du choix de la base. On utilise la forme quadratique q associée à b.

Soit $\mathcal{B} = \{e_1, \dots, e_n\}$ une base de V dans laquelle la matrice de b est la matrice de l'énoncé. Remarquons que $\mathcal{B}$ est b-orthogonale et que $q(e_i) = \begin{cases} a_i & \text{si } 1 \leqslant i \leqslant p \\ -a_i & \text{si } p < i \leqslant r \\ 0 & \text{si } r < i \leqslant n. \end{cases}$

Soit $\mathcal{B}' = \{e'_1, \dots, e'_n\}$ une autre base b-orthogonale de V, telle que $q(e'_i) = \begin{cases} a'_i > 0 & \text{si } 1 \leqslant i \leqslant p' \\ -a'_i < 0 & \text{si } p' < i \leqslant r \\ 0 & \text{si } r < i \leqslant n. \end{cases}$

Posons

$$F = \operatorname{vect}\{e_1, \dots, e_p\}, \qquad G = \operatorname{vect}\{e_{p+1}, \dots, e_n\}$$
$$F' = \operatorname{vect}\{e'_1, \dots, e'_{p'}\}, \qquad G' = \operatorname{vect}\{e'_{p'+1}, \dots, e'_n\}.$$

On a $V = F \oplus G$ et $V = F' \oplus G'$.

Soit $u \in F \cap G'$. Alors, si $u \neq 0$, comme $u \in F$ on a $u = \sum_{i=1}^{p} x_i e_i$ donc $q(u) = \sum_{i=1}^{p} x_i^2 a_i > 0$. D'autre part, puisque $u \in G'$, on a $u = \sum_{i=p'+1}^{n} x_i e'_i$ donc $q(u) = \sum_{i=p'+1}^{r} x_i^2(-a'_i) < 0$: contradiction. Donc $F \cap G' = \{0\}$ et

$$\dim(F + G') = \dim F + \dim G' = p + (n - p')$$

et ceci doit être inférieur à n, donc $p \leqslant p'$.

De même, en considérant F' et G, on montre que $p' \leqslant p$, et donc $p' = p$.

Ainsi p est indépendant du choix de la base, de même que le couple $(p, r-p)$.

De la même façon, on montre que deux formes bilinéaires symétriques équivalentes ont même signature (proposition 7 du chapitre 6) : on choisit pour chaque forme bilinéaire une base comme dans l'énoncé et on fait un raisonnement similaire. ✓

Théorème 4. (Loi d'inertie de Sylvester) Supposons que $K = \mathbb{R}$ et soit $b : V \times V \longrightarrow \mathbb{R}$ une forme bilinéaire symétrique. Il existe une base de V dans laquelle la matrice de b soit diagonale de la forme

$$\begin{pmatrix} I_p & 0 & 0 \\ 0 & -I_{r-p} & 0 \\ 0 & 0 & 0_{n-r} \end{pmatrix}$$

où r est le rang de b et $\text{sign}(b) = (p, r-p)$ est la signature de b, qui ne dépend pas du choix d'une telle base.

En particulier deux formes bilinéaires symétriques sur un $\mathbb{R}$-espace vectoriel V sont équivalentes si et seulement si elles ont même signature.

Démonstration. La première assertion provient du théorème précédent et du fait que dans $\mathbb{R}$ tout réel strictement positif admet une racine carrée dans $\mathbb{R}$. Si b, b' ont même signature, il existe des bases $\mathcal{B}$ et $\mathcal{B}'$ de V dans lesquelles les matrices respectives de b et b' sont les mêmes, donc b et b' sont équivalentes. ✓

On termine le paragraphe en donnant les versions de la loi de Sylvester pour les matrices symétriques et les formes quadratiques.

Théorème 5. (Loi d'inertie de Sylvester, version matricielle) Pour $A \in \text{Sym}_n(\mathbb{R})$, il existe $P \in \text{GL}_n(\mathbb{R})$ telle que ${}^tPAP = D$ est diagonale de la forme

$$\begin{pmatrix} I_s & 0 & 0 \\ 0 & -I_t & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Le couple (s, t) s'appelle la **signature** de A, c'est la signature de la forme bilinéaire symétrique associée à A. Ainsi, toute $A \in \text{Sym}_n(\mathbb{R})$ de signature (s, t) avec $s, t \geqslant 0$ est congruente à la matrice précédente.

En particulier, deux matrices A et A' dans $\text{Sym}_n(\mathbb{R})$ sont congruentes si et seulement si elles ont même signature.

Il y a donc $\frac{(n+1)(n+2)}{2}$ classes de congruence.

Théorème 6. (Loi d'inertie de Sylvester, version formes quadratiques) Soit $q : V \longrightarrow \mathbb{R}$ une forme quadratique de rang r. Alors il existe un entier s avec $0 \leqslant s \leqslant r$ et une base $\{e_1, \ldots, e_n\}$ de V tels que :

$$\forall u = \sum_{i=1}^{n} x_i e_i, \qquad q(u) = x_1^2 + \ldots + x_s^2 - x_{s+1}^2 - \ldots - x_r^2.$$

L'entier s ne dépend pas de la base $\{e_1, \ldots, e_n\}$ choisie.

Le couple $(s, r-s)$ s'appelle la **signature** de q, c'est aussi la signature de la forme bilinéaire symétrique associée à q.

Remarque. Soit V un $\mathbb{R}$-espace vectoriel de dimension n. Une forme bilinéaire symétrique b sur V est un produit scalaire si, et seulement si, sa signature est $(n, 0)$.

- ➢ Supposons que la signature de b soit $(n, 0)$. Soit q la forme quadratique associée à b. Il existe alors une base $\{e_1, \ldots, e_n\}$ telle que pour tout $u = \sum_{i=1}^n x_i e_i$ on ait $q(u) = \sum_{i=1}^n x_i^2$. On a donc $q(u) \geqslant 0$ et si $q(u) = 0$ alors $x_i = 0$ pour tout i et donc $u = 0$. Ainsi, b est un produit scalaire.
- ➢ Supposons que la signature de b soit $(p, r-p) \neq (n, 0)$. Soit q la forme quadratique associée à b. Il existe alors une base $\{e_1, \ldots, e_n\}$ telle que pour tout $u = \sum_{i=1}^n x_i e_i$ on ait $q(u) = \sum_{i=1}^p x_i^2 - \sum_{i=p+1}^r x_i^2$. Si $r < n$, on a $q(e_n) = 0$ avec $e_n \neq 0$. Si $r = n$, alors $p < n$ et on a $q(e_n) < 0$. Dans les deux cas, on en déduit que b n'est pas un produit scalaire.

B. Méthodes pratiques de réduction

Soit q une forme quadratique associée à une forme bilinéaire b (sur un $\mathbb{R}$-espace vectoriel). La loi de Sylvester se traduit en particulier par le fait que $q(u)$ est une combinaison linéaire de carrés.

Comment fait-on dans la pratique pour exprimer $q(u)$ comme une combinaison linéaire de carrés et trouver sa signature ? Une méthode algorithmique est donnée par la

Méthode de Gauss

Soit à réduire la forme quadratique q définie sur V par :

$$q(u) = \sum_{i=1}^{n} a_{ii}x_i^2 + 2\sum_{1\leqslant i<j\leqslant n} a_{ij}x_ix_j, \quad (\text{avec } u = \sum_{i=1}^{n} x_ie_i).$$

On suit alors pas à pas l'algorithme suivant :

① On prend un terme en x_i^2 (avec un coefficient le plus simple possible afin d'alléger les calculs) et on considère tous les termes contenant x_i que l'on écrit comme le début du développement d'un carré. On poursuit cette étape jusqu'à épuisement des termes en x_i^2. Il y a alors deux possibilités : soit le problème est résolu et c'est terminé, soit ce n'est pas le cas et on passe à l'étape ②.

② S'il n'y a pas (ou plus) de termes en x_i^2, on considère un terme «simple» en x_ix_j et on écrit tous les termes contenant x_i ou x_j sous la forme :

$$\lambda x_ix_j + x_iR + x_jS = \lambda \underbrace{(x_i + \frac{S}{\lambda})}_{a}\underbrace{(x_j + \frac{R}{\lambda})}_{b} - \frac{RS}{\lambda}$$

et on utilise le fait que $ab = \frac{1}{4}\left[(a+b)^2 - (a-b)^2\right]$.

Ensuite, on reprend la méthode à partir de l'étape ①.

Exemples. ➢ Soit $V = \mathbb{R}^4$ de base $\{e_1, e_2, e_3, e_4\}$. Pour $u = x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4$, soit $q(u) = x_1^2 + x_2^2 + x_4^2 + 2x_1x_2 + 2x_2x_3 + 2x_4x_1 - x_3x_4$. On est dans le premier cas, avec le coefficient de x_1^2 non nul. Donc

$$\begin{aligned} q(u) &= x_1^2 + 2x_1(x_2 + x_4) + x_2^2 + x_4^2 + 2x_2x_3 - x_3x_4 \\ &= (x_1 + x_2 + x_4)^2 - (x_2 + x_4)^2 + x_2^2 + x_4^2 + 2x_2x_3 - x_3x_4 \\ &= (x_1 + x_2 + x_4)^2 + 2x_2x_3 - 2x_2x_4 - x_3x_4. \end{aligned}$$

La forme quadratique qui reste ne contient plus de carrés, on passe donc à la deuxième étape :

$$\begin{aligned} q(u) &= (x_1 + x_2 + x_4)^2 - x_3x_4 + x_3(2x_2) - x_4(2x_2) \\ &= (x_1 + x_2 + x_4)^2 + (x_3 + 2x_2)(-x_4 + 2x_2) - 4x_2^2 \\ &= (x_1 + x_2 + x_4)^2 + \tfrac{1}{4}(4x_2 + x_3 - x_4)^2 - \tfrac{1}{4}(x_3 + x_4)^2 - 4x_2^2. \end{aligned}$$

La signature de q est donc $(2, 2)$.

Soit $V = \mathbb{R}^2$ de base $\{e_1, e_2\}$. Pour $u = xe_1 + ye_2$, soit $q(u) = xy$. Alors

$$q(u) = \frac{1}{4}((x+y)^2 - (x-y)^2)$$

et donc la signature de q est $(1, 1)$.

On arrive finalement à une expression de la forme

$$q = \sum_{i=1}^{s} l_i^2 - \sum_{i=s+1}^{r} l_i^2$$

où $l_1, \dots, l_r$ sont des formes linéaires sur V, *linéairement indépendantes*.

La méthode de Gauss fournit une expression sous forme de combinaison linéaire de carrés de formes linéaires linéairement indépendantes. On prendra garde qu'une combinaison linéaire de carrés obtenue autrement qu'à partir de la méthode de Gauss peut contenir des formes linéaires non linéairement indépendantes, et donner des résultats trompeurs pour la signature. Par exemple considérons la forme quadratique sur $\mathbb{R}^3$ définie par

$$q(u) = (x_1 - x_2)^2 + (x_2 - x_3)^2 - (x_1 - x_3)^2$$

On est tenté de conclure que la signature de q est $(2,1)$. Le problème est que les formes linéaires l_1, l_2 et l_3 définies sur $\mathbb{R}^3$ par

$$l_1(u) = x_1 - x_2,\ l_2(u) = x_2 - x_3,\ l_3(u) = x_1 - x_3$$

ne sont pas linéairement indépendantes, car $l_3 = l_1 + l_2$. En fait, en utilisant la méthode de Gauss, on trouve

$$q(u) = \frac{1}{2}(x_1 - 2x_2 + x_3)^2 - \frac{1}{2}(x_1 - x_3)^2$$

et la signature de q est donc $(1,1)$!

Moralité : Si q est donnée comme combinaison linéaire de carrés, on s'assure que les formes linéaires sont linéairement indépendantes. Sinon on développe et on applique la méthode de Gauss.

«Rappel.» Soit V un espace vectoriel de dimension finie sur K. Soit $\mathcal{B} = \{l_1, \dots, l_n\}$ une base de V^*. Alors il existe une base de V dont la base duale est V.

Pour vérifier cela, on considère la base duale $\mathcal{B}^* = \{l_1^*, \dots, l_n^*\}$ de V^{**}. Soit $\varphi : V \to V^{**}$ l'isomorphisme naturel défini par $\varphi(v)(\alpha) = \alpha(v)$ pour tout $v \in V$ et tout $\alpha \in V^*$. On peut considérer la base $\mathcal{C} = \{\varepsilon_1, \dots, \varepsilon_n\}$ de V définie par $\varepsilon_i = \varphi^{-1}(l_i^*)$ pour tout i. Soit $\mathcal{C}^* = \{\varepsilon_1^*, \dots, \varepsilon_n^*\}$ sa base duale (base de V^*).

Rappelons que pour tout $\alpha \in V^*$ on a $\alpha = \sum_{i=1}^n \alpha(\varepsilon_i)\varepsilon_i^*$. Par définition de φ on a donc, pour tout j,

$$l_j = \sum_{i=1}^n l_j(\varepsilon_i)\varepsilon_i^* = \sum_{i=1}^n \varphi(\varepsilon_i)(l_j)\varepsilon_i^* = \sum_{i=1}^n l_i^*(l_j)\varepsilon_i^*.$$

Or $l_i^*(l_j) = \delta_{ij}$, donc $l_j = \varepsilon_j^*$. On a démontré que $\mathcal{B} = \mathcal{C}^*$.

Remarque. Reprenons l'expression

$$q = \sum_{i=1}^s l_i^2 - \sum_{i=s+1}^r l_i^2$$

où $l_1, \dots, l_r$ sont des formes linéaires linéairement indépendantes sur V que l'on complète en une base $\{l_1, \dots, l_n\}$ de V^*. Soit b la forme bilinéaire symétrique associée. Soit $\mathcal{C} = \{\varepsilon_1, \dots, \varepsilon_n\}$ la base de V dont la base duale est $\{l_1, \dots, l_n\}$. Alors $\mathcal{C}$ est une base b-orthogonale de V et pour tout $u = \sum_{i=1}^n x_i\varepsilon_i$ on a $q(u) = \sum_{i=1}^s x_i^2 - \sum_{i=s+1}^r x_i^2$.

- $\rightsquigarrow$ La signature de q est alors le couple $(s, r-s)$.
- $\rightsquigarrow$ On peut aussi déterminer une base b-orthogonale de V à partir de cette expression. Soit $\mathcal{B}$ la base de départ de V. Pour déterminer $\mathcal{C}$ explicitement, on remarque que la matrice de passage de la base $\mathcal{B}$ dans la base $\mathcal{C}$ est
$$P(\mathcal{B}, \mathcal{C}) = {}^tP(\mathcal{B}^*, \mathcal{C}^*)^{-1}.$$
En effet, $P(\mathcal{B}, \mathcal{C}) = M_{\mathcal{C},\mathcal{B}}(\mathrm{id}_V)$ et $P(\mathcal{B}^*, \mathcal{C}^*)^{-1} = P(\mathcal{C}^*, \mathcal{B}^*) = M_{\mathcal{C}^*,\mathcal{B}^*}(\mathrm{id}_{V^*})$. Or id_{V^*} est l'endomorphisme adjoint de id_V, donc les matrices $P(\mathcal{B}, \mathcal{C})$ et $P(\mathcal{B}^*, \mathcal{C}^*)^{-1}$ sont transposées.
Cette méthode oblige en particulier à compléter des bases et à calculer des inverses de matrices. Si on veut éviter cela, on utilisera la méthode alternative suivante.

Autre méthode (basée sur le théorème 22 du chapitre 6)

➢ Si $q = 0$ n'importe quelle base convient.

➢ Sinon on cherche $\varepsilon_1 \in V$ tel que $q(\varepsilon_1) \neq 0$. On détermine alors $\{\varepsilon_1\}^\perp$. *(On remarque que si* $W_1 := \text{vect}\{\varepsilon_1\}$ *on a* $W_1 \cap W_1^\perp = \{0\}$ *donc* $\dim\{\varepsilon_1\}^\perp = \dim W^\perp = n-1$*.)*
Si $q_{|\{\varepsilon_1\}^\perp} = 0$, on complète ε_1 par une base $\{\varepsilon_2, \dots, \varepsilon_n\}$ de $\{\varepsilon_1\}^\perp$ pour obtenir une base b-orthogonale $\{\varepsilon_1, \dots, \varepsilon_n\}$ de V.

➢ Si $q_{|\{\varepsilon_1\}^\perp} \neq 0$, on cherche $\varepsilon_2 \in \{\varepsilon_1\}^\perp$ tel que $q(\varepsilon_2) \neq 0$. On détermine alors $\{\varepsilon_1, \varepsilon_2\}^\perp$. *(On remarque que si* $W_2 := \text{vect}\{\varepsilon_1, \varepsilon_2\}$ *on a* $W_2 \cap W_2^\perp = \{0\}$ *donc* $\dim\{\varepsilon_1, \varepsilon_2\}^\perp = \dim W_2^\perp = n-2$*.)*
Si $q_{|\{\varepsilon_1, \varepsilon_2\}^\perp} = 0$, on complète $\{\varepsilon_1, \varepsilon_2\}$ par une base $\{\varepsilon_3, \dots, \varepsilon_n\}$ de $\{\varepsilon_1, \varepsilon_2\}^\perp$ pour obtenir une base b-orthogonale $\{\varepsilon_1, \dots, \varepsilon_n\}$ de V.

➢ Si $q_{|\{\varepsilon_1, \varepsilon_2\}^\perp} \neq 0$, on cherche $\varepsilon_3 \in \{\varepsilon_1, \varepsilon_2\}^\perp$ tel que $q(\varepsilon_3) \neq 0$, et on continue le procédé...

On obtient finalement une base b-orthogonale $\{\varepsilon_1, \dots, \varepsilon_n\}$. On détermine la signature de q en comptant le nombre de termes positifs et négatifs dans $\{q(\varepsilon_i) \mid 1 \leqslant i \leqslant n\}$.

Exemple. Soit $V = \mathbb{R}^4$ de base $\{e_1, e_2, e_3, e_4\}$. Pour $u = \sum_{i=1}^4 x_i e_i$ on pose

$$q(u) = x_1^2 + 2x_2^2 - x_4^2 + 2x_1x_2 + 2x_2x_3 - 2x_3x_4.$$

La forme bilinéaire symétrique associée est donnée par

$$b(u,v) = x_1y_1 + 2x_2y_2 - x_4y_4 + x_1y_2 + x_2y_1 + x_2y_3 + x_3y_2 - x_3y_4 - x_4y_3$$

où $v = \sum_{i=1}^4 y_i e_i$.
On pose $\varepsilon_1 = e_1$. On a bien $q(\varepsilon_1) = 1 \neq 0$.
On détermine $\{\varepsilon_1\}^\perp$. On a

$$\{\varepsilon_1\}^\perp = \{u \mid b(u, \varepsilon_1) = 0\} = \{u \mid x_1 + x_2 = 0\}.$$

On pose $\varepsilon_2 = e_4 \in \{\varepsilon_1\}^\perp$. On a bien $q(\varepsilon_2) = -1 \neq 0$.
On détermine $\{\varepsilon_1, \varepsilon_2\}^\perp$.

$$\{\varepsilon_1, \varepsilon_2\}^\perp = \{u \mid b(u, \varepsilon_1) = 0 = b(u, \varepsilon_2)\} = \{u \mid x_1 + x_2 = 0 \text{ et } x_3 + x_4 = 0\}.$$

On pose $\varepsilon_3 = e_1 - e_2 \in \{\varepsilon_1, \varepsilon_2\}^\perp$. On a bien $q(\varepsilon_3) = 1 \neq 0$.
On détermine $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}^\perp$.

$$\begin{aligned}\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}^\perp &= \{u \mid b(u, \varepsilon_1) = 0 = b(u, \varepsilon_2) = b(u, \varepsilon_3)\} \\ &= \{u \mid x_1 + x_2 = 0 \text{ et } x_3 + x_4 = 0 \text{ et } x_2 + x_3 = 0\}.\end{aligned}$$

On pose $\varepsilon_4 = e_1 - e_2 + e_3 - e_4 \in \{\varepsilon_1, \varepsilon_2, \varepsilon_3\}^\perp$.
On a donc obtenu une base b-orthogonale $\{\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4\}$ de V.
De plus, $q(\varepsilon_4) = 0$. La signature est donc $(2,1)$ et le rang est 3.

III Formes bilinéaires symétriques sur un corps fini

On classifie maintenant les formes bilinéaires symétriques non dégénérées sur les corps finis (toujours en caractéristique différente de 2, c'est-à-dire pour des corps dont le cardinal est impair).
On commence par un résultat préliminaire.

Proposition 7. Soit K un corps fini de cardinal impair et $b : V \times V \longrightarrow K$ une forme bilinéaire symétrique non dégénérée sur un espace vectoriel V de dimension supérieure ou égale à 2. Alors la forme quadratique associée $q : V \longrightarrow K$ est surjective.

On aura besoin du lemme suivant.

Lemme 8. Soit K un corps fini de cardinal impair et soient $a, b \in K^*$ et $t \in K$. L'équation $ax^2 + by^2 = t$ a toujours une solution dans $K \times K$.

Démonstration. Soit p le cardinal de K. Vérifions d'abord que l'ensemble $(K^*)^2 = \{x^2 \mid x \in K^*\}$ a $\frac{p-1}{2}$ éléments. L'application $\alpha : K^* \to K^*$, $x \mapsto x^2$ est un morphisme de groupes. Son image est $(K^*)^2$ et son noyau est $\{\pm 1\}$, qui a deux éléments car K est de caractéristique différente de 2. Le théorème d'isomorphisme pour les groupes et le théorème de Lagrange donnent donc le résultat. Soient

$$F = \{ax^2 \mid x \in K\}, \quad G = \{t - by^2 \mid y \in K\}$$

Ces deux ensembles ont donc chacun $1 + \frac{p-1}{2}$ éléments, et donc $\#F + \#G = 1 + p > p$, ainsi $F \cap G \neq \varnothing$, et on a le résultat. ✓

Démonstration de la proposition. Soit maintenant $\mathcal{B} = \{e_1, \dots, e_n\}$ une base b-orthogonale : on a $q(\sum_{i=1}^n x_i e_i) = \sum_{i=1}^n a_i x_i^2$ avec $a_1, \dots, a_n \in K^*$ (b est non-dégénérée, sa matrice dans $\mathcal{B}$ est donc de rang maximal). Alors $q(x_1 e_1 + x_2 e_2) = a_1 x_1^2 + a_2 x_2^2$, et donc le lemme donne le résultat. ✓

Théorème 9. Soit K un corps fini avec $\mathrm{car}(K) \neq 2$ et soit $b : V \times V \longrightarrow K$ une forme bilinéaire symétrique non dégénérée, avec $\dim(V) \geqslant 2$. Il existe une base $\{v_1, \dots, v_n\}$ de V dans laquelle la matrice de b soit diagonale de la forme $\mathrm{diag}(1, \dots, 1, d)$, avec $d \in K^*$.

Démonstration. On procède par récurrence sur $n = \dim(V)$, de manière très similaire à la preuve du Théorème 22 du chapitre 6.

Supposons que $n = 2$. La proposition précédente assure qu'il existe $v \in V$ tel que $q(v) = b(v, v) = 1$. On a alors $\mathrm{vect}\{v\} \cap \mathrm{vect}\{v\}^\perp = \{0\}$ donc $\dim \mathrm{vect}\{v\}^\perp = 1$. Soit donc $w \in \mathrm{vect}\{v\}^\perp$ un vecteur non nul, alors $\{v, w\}$ est une base de V qui est b-orthogonale. De plus, $d = q(w) = b(w, w) \neq 0$ car b est non-dégénérée.

Supposons maintenant que $n > 2$ et le résultat montré au rang $< n$. Soit $v \in V$ tel que $q(v) = b(v, v) = 1$. Le raisonnement de la preuve du théorème 22 du chapitre 6 s'applique à l'identique à l'espace $W = \mathrm{vect}\{v\}$, et fournit la base demandée. ✓

Théorème 10. Soit K un corps fini avec $\mathrm{car}(K) \neq 2$. Soient $b_1, b_2 : V \times V \longrightarrow K$ des formes bilinéaires symétriques non dégénérées. Alors b_1 et b_2 sont équivalentes si et seulement si $\mathrm{discr}(b_1) = \mathrm{discr}(b_2)$. Ainsi, à équivalence près, il y a exactement deux formes bilinéaires symétriques non dégénérées sur V.

Démonstration. Si b_1 et b_2 sont équivalentes, alors elles ont même discriminant d'après la Définition-Proposition 10 du chapitre 6.

Réciproquement, supposons que $\mathrm{discr}(b_1) = \mathrm{discr}(b_2)$. D'après le théorème précédent, il existe des bases $\mathcal{B}_1$ et $\mathcal{B}_2$ de V dans lesquelles les matices respectives de b_1 et b_2 sont

$$A_1 = M_{\mathcal{B}_1}(b_1) = \mathrm{diag}(1, \dots, 1, d_1), \quad A_2 = M_{\mathcal{B}_2}(b_2) = \mathrm{diag}(1, \dots, 1, d_2).$$

Puisque $\mathrm{discr}(b_1) = \mathrm{discr}(b_2)$, il existe $\alpha \in K^*$ tel que $d_2 = \alpha^2 d_1$. Soit $\mathcal{B}_2' =$

Si $\mathcal{B}_2 = \{e_1, \dots, e_n\}$, soit $\mathcal{B}_2' = \{e_1, \dots, \alpha^{-1} e_n\}$, c'est toujours une base b_2-orthogonale. De plus, $b_2(\alpha^{-1} e_n, \alpha^{-1} e_n) = d_1$. La matrice de b_2 dans la base $\mathcal{B}_2'$ est donc A_1, et b_1 et b_2 sont bien équivalentes.

La dernière assertion provient du fait que $(K^*)^2$ a $\frac{p-1}{2}$ éléments (voir la preuve du lemme 8), et donc $K^*/(K^*)^2$ a 2 éléments. ✓

Exemple. Si $K = \mathbb{F}_5$, on peut choisir $\begin{pmatrix} I_{n-1} & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} I_{n-1} & 0 \\ 0 & 2 \end{pmatrix}$ comme représentants des classes de congruence de matrices symétriques inversibles. Notons que $\begin{pmatrix} I_{n-1} & 0 \\ 0 & -1 \end{pmatrix}$ est congruente à I_n et que $\begin{pmatrix} I_{n-1} & 0 \\ 0 & 2 \end{pmatrix}$ est congruente à $\begin{pmatrix} I_{n-1} & 0 \\ 0 & -2 \end{pmatrix}$.

Si $K = \mathbb{F}_7$, on peut choisir $\begin{pmatrix} I_{n-1} & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} I_{n-1} & 0 \\ 0 & -1 \end{pmatrix}$.

La suite n'est pas au programme.

Définition 11. *On se place dans un espace euclidien de dimension n, et on fixe une base orthonormée. On peut donc supposer qu'il s'agit de $\mathbb{R}^n$ muni de sa base canonique.*

On appelle ***hypersurface du second degré*** *l'ensemble $\mathcal{H}$ des points $u \in \mathbb{R}^n$ vérifiant :*

$$F(u) := q(u) + \ell(u) + c = 0$$

où q est une forme quadratique non nulle, ℓ est une forme linéaire, et c est une constante (réelle).

Lorsque $n = 2$, une hypersurface de degré 2 s'appelle une ***conique****; lorsque $n = 3$ une hypersurface de degré 2 s'appelle une* ***quadrique****.*

On cherche à déterminer la forme de l'hypersurface. Nous commencerons dans le cas général, puis déterminerons la classification complète dans le cas des coniques et des quadriques.

Rappel. **(Théorème spectral pour les endomorphismes symétriques.)** Soit E un espace euclidien. On note f son produit scalaire. Soit ψ un endomorphisme symétrique de E. Alors ψ est diagonalisable dans une base f-orthonormale : il existe une base f-orthonormale de E formée de vecteurs propres pour ψ.

Nous allons déterminer une *équation réduite* pour $\mathcal{H}$.

① La première étape est de réduire la forme quadratique q dans une base f-orthonormale.
Soit A la matrice associée à q, et soit ψ l'endomorphisme de $\mathbb{R}^n$ dont la matrice dans la base canonique est A. La matrice A est symétrique.
Si $u \in \mathbb{R}^n$, soit U le vecteur colonne associé ; alors

$$q(u) = {}^tUAU = {}^t(AU)U = \langle \psi(u), u \rangle.$$

Comme ψ est symétrique, on peut lui appliquer le théorème spectral : il existe donc une base f-orthonormale $\{\varepsilon_1, \dots, \varepsilon_n\}$ de E formée de vecteurs propres pour ψ. Soit λ_i la valeur propre associée au vecteur propre ε_i.
Notons $u = \sum_{i=1}^{n} x_i \varepsilon_i$. Alors $q(u) = \langle \psi(u), u \rangle = \sum_{i=1}^{n} \lambda_i x_i^2$, donc $F(u) = \sum_{i=1}^{n} \lambda_i x_i^2 - \sum_{i=1}^{n} \tau_i x_i + c$.

② La deuxième étape est de réduire F. Pour cela on «complète les carrés», c'est-à-dire que l'on écrit, lorsque $\lambda_i \neq 0$,

$$\lambda_i x_i^2 - \tau_i x_i = \lambda_i (x_i^2 - \frac{\tau_i}{\lambda_i} x_i) = \lambda_i \left(x_i - \frac{\tau_i}{2\lambda_i} \right)^2 - \frac{\tau_i^2}{4\lambda_i}.$$

L'équation devient donc

$$\sum_{i=1}^{r} \lambda_i x_i'^2 = \sum_{r+1}^{n} \tau_i x_i + c'. \qquad (\dagger)$$

Ceci revient à faire un changement d'origine (si $\lambda_1, \dots, \lambda_r$ sont non nuls et $\lambda_{r+1} = \cdots = \lambda_n = 0$, la nouvelle origine est $\Omega = \left(\frac{\tau_1}{2\lambda_1}, \dots, \frac{\tau_r}{2\lambda_r}, 0, \dots, 0 \right)$ – on a fait une translation dans $\mathbb{R}^n$).
Notons que si l'un des τ_i est non nul, par exemple τ_n, alors on peut faire un nouveau changement d'origine pour que l'équation ne contienne plus de constante ($\Omega' = \Omega + (0, \dots, 0, -\frac{c'}{\tau_n})$).

③ Pour étudier l'hypersurface $\mathcal{H}$, on se placera dans le repère orthonormal privilégié $(\Omega \mid \varepsilon_1, \dots, \varepsilon_n)$ dans lequel l'équation a l'expression réduite (†).

A. Classification des coniques

Soit $\mathcal{C}$ une conique (c'est-à-dire une hypersurface de degré 2 dans un espace euclidien de dimension 2). Notons $\begin{pmatrix} x \\ y \end{pmatrix}$ les coordonnées d'un point dans le repère privilégié $(\Omega \mid \varepsilon_1, \varepsilon_2)$, et λ, μ les valeurs propres de ψ.

➢ Si q est de rang 2, i.e. les valeurs propres sont non nulles, l'équation réduite de $\mathcal{C}$ est $\lambda x^2 + \mu y^2 = \delta$. Notons que quitte à diviser par $|\delta|$, on peut supposer que $\delta = 1, 0$ ou -1. On peut également, quitte à tout multiplier par -1 ou à échanger les rôles de x et y, supposer que $\lambda = \frac{1}{\alpha^2} > 0$. On obtient alors :

Equation réduite	*Nature de la conique*
$\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} = 1$	Ellipse
$\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} = 0$	Point Ω
$\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} = -1$	Vide
$\frac{x^2}{\alpha^2} - \frac{y^2}{\beta^2} = 0$	Réunion de deux droites sécantes d'équations $y = \pm\frac{\beta}{\alpha}x$
$\frac{x^2}{\alpha^2} - \frac{y^2}{\beta^2} = 1$	Hyperbole

➢ Si q est de rang 1, i.e. si l'une des valeurs propres est nulle, par exemple μ, l'équation réduite de $\mathcal{C}$ est $\lambda x^2 + \tau y = \rho$. Comme auparavant, nous pouvons supposer que $\lambda = \frac{1}{\alpha^2} > 0$ et $\rho = 0, 1$ ou -1, et même que $\rho = 0$ lorsque $\tau \neq 0$. On obtient alors :

Equation réduite	*Nature de la conique*
$\frac{x^2}{\alpha^2} = 1$	Réunion de deux droites parallèles d'équations $x = \pm\alpha$
$\frac{x^2}{\alpha^2} = 0$	Droite d'équation $x = 0$
$\frac{x^2}{\alpha^2} = -1$	Vide
$\frac{x^2}{\alpha^2} - \frac{y}{\beta} = 0$	Parabole

Exemple. Considérons la conique $\mathcal{C}$ d'équation $x^2 + 10\sqrt{3}xy + 11y^2 - 16 = 0$. Nous voulons déterminer sa nature.

La forme quadratique est $x^2 + 10\sqrt{3}xy + 11y^2$. La matrice de ψ dans la base canonique est donc

$$A = \begin{pmatrix} 1 & 5\sqrt{3} \\ 5\sqrt{3} & 11 \end{pmatrix}.$$

Nous voulons trouver ses valeurs propres et ses vecteurs propres.

Le polynôme caractéristique est

$$\begin{vmatrix} 1-\lambda & 5\sqrt{3} \\ 5\sqrt{3} & 11-\lambda \end{vmatrix} = \lambda^2 - 12\lambda - 64 = (\lambda - 16)(\lambda + 4)$$

donc les valeurs propres sont 16 et -4, non nulles.

Le noyau de $A + 4I = 5\begin{pmatrix} 1 & \sqrt{3} \\ \sqrt{3} & 3 \end{pmatrix}$ est engendré par $\begin{pmatrix} 3 \\ -\sqrt{3} \end{pmatrix}$ et le noyau de $A - 16I = 5\begin{pmatrix} -3 & \sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix}$ est engendré par $\begin{pmatrix} 1 \\ \sqrt{3} \end{pmatrix}$. Donc nous obtenons un repère orthonormal en normalisant ces vecteurs :

$$\left(O \mid \begin{pmatrix} \frac{\sqrt{3}}{2} \\ -\frac{1}{2} \end{pmatrix}; \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix}\right).$$

Dans ce repère, $\mathcal{C}$ a pour équation $16X^2 - 4Y^2 = 16$, ou

$$X^2 - \frac{Y^2}{4} = 1.$$

Il s'agit donc d'une hyperbole.

B. Classification des quadriques

Soit $\mathcal{Q}$ une quadrique (c'est-à-dire une hypersurface de degré 2 dans un espace euclidien de dimension 3). Notons x, y, z les coordonnées dans le repère privilégié $(\Omega \mid \varepsilon_1, \varepsilon_2, \varepsilon_3)$ et λ, μ, ν les valeurs propres de ψ.

➢ Si q est de rang 3, i.e. si les valeurs propres sont toutes non nulles, alors l'équation réduite de $\mathcal{Q}$ est $\lambda x^2 + \mu y^2 + \nu z^2 = \delta$. Comme dans le cas des coniques, on peut supposer que $\lambda = \frac{1}{\alpha^2} > 0$ et $\mu = \frac{1}{\beta^2} > 0$, et que $\delta = 0, 1$ ou -1. On obtient alors :

Equation réduite	*Nature de la quadrique*
$\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} + \frac{z^2}{\gamma^2} = 1$	Ellipsoïde
$\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} - \frac{z^2}{\gamma^2} = 1$	Hyperboloïde à une nappe
$\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} - \frac{z^2}{\gamma^2} = -1$	Hyperboloïde à deux nappes
$\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} - \frac{z^2}{\gamma^2} = 0$	Cône du second degré à base elliptique
$\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} + \frac{z^2}{\gamma^2} = 0$	Point Ω
$\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} + \frac{z^2}{\gamma^2} = -1$	Vide

➢ Si q est de rang 2, i.e. si exactement une des valeurs propres, par exemple ν, est nulle, l'équation réduite de $\mathcal{Q}$ est $\lambda x^2 + \mu y^2 = \tau z + \delta$. Quitte à changer z en $-z$, on peut supposer que $\tau \geqslant 0$. Lorsque $\tau \neq 0$, on peut supposer que $\delta = 0$. Donc on suppose que $\tau = 1$ et $\delta = 0$ ou que $\tau = 0$ et que $\delta = 0, 1$ ou -1. On obtient alors :

Equation réduite	*Nature de la quadrique*
$\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} = z$	Paraboloïde elliptique
$\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} = 1$	Cylindre à base elliptique
$\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} = 0$	Droite d'équations $x = 0;\ y = 0$
$\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} = -1$	Vide
$\frac{x^2}{\alpha^2} - \frac{y^2}{\beta^2} = z$	Paraboloïde hyperbolique
$\frac{x^2}{\alpha^2} - \frac{y^2}{\beta^2} = 1$	Cylindre à base hyperbolique
$\frac{x^2}{\alpha^2} - \frac{y^2}{\beta^2} = 0$	Réunion de deux plans d'équations $y = \pm\frac{\beta}{\alpha}x$

➢ Si q est de rang 1, i.e. si exactement deux valeurs propres sont nulles, disons μ et ν, l'équation réduite est $\frac{x^2}{\alpha^2} = \tau y + \sigma z + \omega$. Comme auparavant, on peut supposer que lorsque τ ou σ est non nul alors $\omega = 0$, et que $\omega = 0, 1$ ou -1 sinon. De plus, lorsque $\tau \neq 0$ et $\sigma \neq 0$, on peut changer la variable y pour mettre l'équation sous la forme $\lambda x^2 + \tau y' = 0$ avec $y' = (y + \frac{\sigma}{\tau} z)$ (en supposant déjà que $\omega = 0$). On obtient :

Equation réduite	*Nature de la quadrique*
$x^2 = 2py$	Cylindre à base parabolique
$\frac{x^2}{\alpha^2} = 1$	Réunion de deux plans parallèles distincts d'équations $x = \pm\alpha$
$\frac{x^2}{\alpha^2} = 0$	Plan d'équation $x = 0$
$\frac{x^2}{\alpha^2} = -1$	Vide

Exemple. Considérons une quadrique $\mathcal{Q}$ d'équation $-7x^2+25y^2+7z^2+48xz+5x-k=0$.

La matrice associée à la forme quadratique est $A=\begin{pmatrix}-7&0&24\\0&25&0\\24&0&7\end{pmatrix}$. Ses valeurs propres sont -25 (simple) et 25 (double). On choisit une base orthonormale du plan $\mathrm{Ker}(A-25I)$ et on complète avec un vecteur normal ε_3 de la droite $\mathrm{Ker}(A+25I)$. On obtient donc un nouveau repère orthonormal $(0,\varepsilon_1=\begin{pmatrix}\frac{3}{5}\\0\\\frac{4}{5}\end{pmatrix};\varepsilon_2=\begin{pmatrix}0\\1\\0\end{pmatrix};\varepsilon_3=\begin{pmatrix}\frac{4}{5}\\0\\-\frac{3}{5}\end{pmatrix})$ par exemple. L'équation de $\mathcal{Q}$ devient $25X^2+25Y^2-25Z^2+3X+4Z=k$, soit

$$25X'^2+25Y'^2-25Z'^2=k-\frac{7}{100}$$

en posant $X'=X+\frac{3}{50}$, $Y'=Y$ et $Z'=Z-\frac{4}{50}$, c'est-à-dire que l'on a pris $\Omega=\left(-\frac{3}{50};0;\frac{2}{25}\right)$ dans le repère $(O\mid\varepsilon_1,\varepsilon_2,\varepsilon_3)$.

Donc,

➢ si $k>\frac{7}{100}$, alors $\mathcal{Q}$ est un hyperboloïde à une nappe ;

➢ si $k<\frac{7}{100}$, alors $\mathcal{Q}$ est un hyperboloïde à deux nappes ;

➢ si $k=\frac{7}{100}$, alors $\mathcal{Q}$ est un cône à base circulaire (les coefficients de X' et Y' sont égaux).

V Démonstration du théorème spectral pour les endomorphismes symétriques

Soit E un espace euclidien.

Proposition 12. Supposons que ψ soit un endomorphisme symétrique de E. Alors le polynôme caractéristique de f est scindé dans $\mathbb{R}[X]$ (ses valeurs propres sont réelles).

Démonstration. Le polynôme caractéristique de ψ est scindé dans $\mathbb{C}[X]$, il suffit donc de démontrer que toutes les valeurs propres de ψ sont réelles. Soit donc $\lambda\in\mathbb{C}$ une valeur propre de ψ.
Soit A la matrice de ψ dans une base orthonormale. Alors ${}^tA=A$. On peut voir A comme une matrice de $\mathcal{M}_n(\mathbb{C})$. Il existe $V\in\mathcal{M}_{n,1}(\mathbb{C})$ non nul tel que $AV=\lambda V$. On conjugue cette relation coefficient à coefficient. Puisque les coefficients de A sont réels, on obtient : $\overline{\lambda}\,\overline{V}=\overline{AV}=A\overline{V}$. On multiplie à gauche par ${}^tV$, ce qui donne ${}^tV(A\overline{V})=\overline{\lambda}\,{}^tV\overline{V}$. D'autre part, puisque A est symétrique, on a

$${}^tVA={}^tV{}^tA={}^t(AV)={}^t(\lambda V)=\lambda\,{}^tV$$

donc ${}^tVA\overline{V}=\lambda\,{}^tV\overline{V}$. De plus, si $V={}^t(v_1\ \cdots\ v_n)$, on a ${}^tV\overline{V}=|v_1|^2+\cdots+|v_n|^2>0$. Puisque $\lambda\,{}^tV\overline{V}={}^tVA\overline{V}=\overline{\lambda}\,{}^tV\overline{V}$, on en déduit donc que $\lambda=\overline{\lambda}$ et donc que $\lambda\in\mathbb{R}$. ✓

Proposition 13. Soit ψ un endomorphisme symétrique de E et soit V un sous-espace vectoriel de E stable par ψ. Alors $V^\perp$ est stable par ψ.

Démonstration. Soit $u\in V^\perp$. On doit vérifier que $\psi(u)\in V^\perp$. Soit donc $v\in V$. On a

$$\langle\psi(u),v\rangle=\langle u,\psi(v)\rangle=0$$

car $\psi(v)\in V$ par hypothèse. Donc $\psi(u)\in V^\perp$. ✓

Théorème 14. (Théorème spectral des endomorphismes symétriques) Soit $(E,\langle,\rangle)$ un espace euclidien et soit ψ un endomorphisme symétrique. Alors ψ est diagonalisable dans une base **orthonormale**. Autrement dit, il existe une base orthonormale de E formée de vecteurs propres de ψ.

Démonstration. Nous allons démontrer le théorème par récurrence sur $n = \dim E$.
Si $n = 1$, alors il n'y a rien à démontrer.
Soit $n \geqslant 2$ tel que le résultat soit vrai pour les endomorphismes symétriques d'un espace euclidien de dimension $n-1$. Nous savons d'après la proposition 12 qu'il existe une valeur propre réelle, λ. Soit v_1 un vecteur propre associé à la valeur propre λ ci-dessus. Quitte à le diviser par sa norme, nous pouvons supposer que $\|v_1\| = 1$. Nous avons une décomposition orthogonale $E = \text{vect}\{v_1\} \oplus \text{vect}\{v_1\}^\perp$ qui est stable par ψ. Nous pouvons donc restreindre ψ à $\text{vect}\{v_1\}^\perp$ pour obtenir un endomorphisme symétrique $\tilde{\psi} : \text{vect}\{v_1\}^\perp \to \text{vect}\{v_1\}^\perp$. Ce sous-espace est de dimension $n-1$, donc par hypothèse de récurrence, il existe une base orthonormale $\{v_2, \ldots, v_n\}$ de $\text{vect}\{v_1\}^\perp$ formée de vecteurs propres pour $\tilde{\psi}$ et donc pour ψ. Donc $\{v_1, \ldots, v_n\}$ est une base orthonormale de E formée de vecteurs propres pour ψ. ✓

Du théorème précédent, on déduit :

Corollaire 15. (Théorème spectral pour les matrices symétriques) Soit $A \in \mathcal{M}_n(\mathbb{R})$ une matrice symétrique. Alors il existe une matrice orthogonale P telle que ${}^tPAP$ soit diagonale.

Démonstration. La matrice A représente un endomorphisme symétrique dans la base canonique (orthonormale) de $\mathbb{R}^n$. Donc d'après le théorème spectral ci-dessus, il existe une matrice $P \in \mathcal{M}_n(\mathbb{R})$ inversible telle que $P^{-1}AP$ soit diagonale. De plus, toujours d'après le théorème spectral, cette matrice est la matrice de passage d'une base orthonormale à une autre base orthonormale. Elle est donc bien orthogonale, et $P^{-1} = {}^tP$. ✓

Annexe : théorèmes spectraux pour les endomorphismes d'un espace hermitien

Soit $(H, \langle , \rangle)$ un espace hermitien de dimension n.

I Endomorphismes hermitiens ou auto-adjoints

Définition-Proposition 16. *Soit M une matrice dans $\mathcal{M}_n(\mathbb{C})$. On appelle **adjointe** de M la matrice $M^* = {}^t\overline{M}$. On dit que M est **hermitienne** ou **auto-adjointe** si $M^* = M$.*

*Un endomorphisme ψ de H est dit **hermitien** ou **auto-adjoint** si $\psi^* = \psi$. Cela équivaut à dire que la matrice de ψ dans une (ou toute) base orthonormale est auto-adjointe.*

Démonstration. Analogue au cas réel. ✓

Proposition 17. Soit ψ un endomorphisme hermitien. Alors ses valeurs propres sont réelles.

Démonstration. Soit λ une valeur propre pour ψ, et soit z un vecteur propre associé. Alors d'une part $\langle \psi(z), z\rangle = \langle \lambda z, z\rangle = \lambda \|z\|^2$ et d'autre part, puisque ψ est hermitien, $\langle \psi(z), z\rangle = \langle z, \psi^*(z)\rangle = \langle z, \psi(z)\rangle = \langle z, \lambda z\rangle = \overline{\lambda}\|z\|^2$. Comme $z \neq 0$ (c'est un vecteur propre), on a $\|z\| \neq 0$ et donc $\lambda = \overline{\lambda}$. ✓

II Isométries ou endomorphismes unitaires

Soient $(H, \langle , \rangle)$ et $(H', \langle , \rangle')$ deux espaces hermitiens. Notons $\|\cdot\|$ et $\|\cdot\|'$ les normes associées.

Définition 18. *Une **isométrie** de $(H, \langle , \rangle)$ vers $(H', \langle , \rangle')$ est une application linéaire $\Phi : H \to H'$ qui préserve la norme, c'est-à-dire que $\|\Phi(z)\|' = \|z\|$ pour tout $z \in H$. Si $H = H'$, on dit aussi que Φ est un **endomorphisme unitaire**.*

Les résultats suivants se démontrent comme dans le cas euclidien.

Propriété 19. Une application linéaire $\Phi : H \to H'$ est une isométrie si et seulement si elle préserve le produit hermitien.

Proposition 20. Si Φ est une isométrie de H dans H', alors Φ est injective. De plus, si $\Phi : H \to H$ est un endomorphisme unitaire, alors Φ est un isomorphisme.

Théorème 21. Tout espace hermitien de dimension n est isométrique à l'espace hermitien canonique $\mathbb{C}^n$ (c'est-à-dire qu'il existe une isométrie bijective entre les deux).

Propriétés 22. Soit $(H, \langle , \rangle)$ un espace hermitien.

(i) Soit Φ une isométrie de H. Alors Φ^{-1} est une isométrie de H.

(ii) Si Φ et Ψ sont des isométries de H alors $\Psi \circ \Phi$ est une isométrie de H.

(iii) id_H est une isométrie de H.

Définition-Proposition 23. *L'ensemble des isométries de l'espace hermitien $(H, \langle , \rangle_H)$ est un sous-groupe de $\mathrm{GL}(H)$. On l'appelle le* ***groupe unitaire*** *et on le note $\mathrm{U}(H)$.*

L'ensemble des isométries de H dont le déterminant est égal à 1 est également un sous-groupe de $\mathrm{GL}(H)$. On l'appelle le ***groupe spécial unitaire*** *et on le note $\mathrm{SU}(H)$. C'est le noyau de l'application déterminant sur $\mathrm{U}(H)$.*

Si $H = \mathbb{C}^n$ est muni de sa structure canonique d'espace hermitien, on note $\mathrm{U}(H) = \mathrm{U}_n(\mathbb{C})$ et $\mathrm{SU}(H) = \mathrm{SU}_n(\mathbb{C})$.

Proposition 24. Soit $(H, \langle , \rangle)$ un espace hermitien et soit $\Phi : H \to H$ une application linéaire. Alors les assertions suivantes sont équivalentes :

(i) Φ est une isométrie.

(ii) $\Phi^* = \Phi^{-1}$.

(iii) Si $\mathcal{B}$ est une base orthonormale de H et si M est la matrice de Φ dans la base $\mathcal{B}$, alors ${}^t\overline{M}M = I_n = M{}^t\overline{M}$.

(iv) Si $\mathcal{B}$ est une base orthonormale de H et si M est la matrice de Φ dans la base $\mathcal{B}$, alors M est inversible et $M^{-1} = {}^t\overline{M}$.

(v) Si $\mathcal{B}$ est une base orthonormale de H et si M est la matrice de Φ dans la base $\mathcal{B}$, alors les vecteurs colonne de M forment une base orthonormale de $\mathbb{C}^n$ avec sa structure hermitienne canonique.

(vi) Si $\mathcal{B}$ est une base orthonormale de H, alors $\Phi(\mathcal{B})$ est une base orthonormale de H.

Lorsque les conditions équivalentes (iii)-(v) ci-dessus sont vérifiées pour une matrice M, on dit que M est une **matrice unitaire.**

Proposition 25. Soit Φ une isométrie. Alors

(i) les valeurs propres de Φ sont de module 1 ;

(ii) $|\det \Phi| = 1$.

Démonstration. (i) Soit λ une valeur propre pour Φ et soit z un vecteur propre ($z \neq 0$) associé. Alors, puisque Φ est une isométrie, $\|z\| = \|\Phi(z)\| = \|\lambda z\| = |\lambda|\|z\|$, donc $|\lambda| = 1$.

(ii) Soit M la matrice de Φ dans une base orthonormale. Alors $M{}^t\overline{M} = I_n$, donc

$$1 = \det(I_n) = \det(M{}^t\overline{M}) = \det(M)\det({}^t\overline{M}) = \det(M)\overline{\det(M)} = |\det(M)|^2 = |\det(\Phi)|^2,$$

donc $|\det(\Phi)| = 1$. ✓

III Endomorphismes normaux

Définition 26. *Un endomorphisme χ de H est dit* ***normal*** *s'il commute avec son adjoint, i.e. $\chi \circ \chi^* = \chi^* \circ \chi$.*

Une matrice A est dite ***normale*** *si $A^*A = AA^*$.*

Remarque. Un endomorphisme χ est normal si et seulement si sa matrice dans une (toute) base **orthonormale** est normale.

Exemples. (i) Tout endomorphisme hermitien est normal.

(ii) Tout endomorphisme unitaire (isométrie) est normal.

(iii) $A = \begin{pmatrix} i & -1 \\ 1 & i \end{pmatrix}$: alors $A^* = \begin{pmatrix} -i & 1 \\ -1 & -i \end{pmatrix}$. Donc A n'est ni hermitienne, ni unitaire. Cependant, A est normale car

$$AA^* = \begin{pmatrix} 2 & 2i \\ -2i & 2 \end{pmatrix} = A^*A.$$

IV Théorèmes spectraux

Théorème 27. (Théorème spectral des endomorphismes normaux) Soit H un espace *hermitien*. Un endomorphisme χ de H est normal si et seulement s'il est diagonalisable dans une base orthonormale de H.

Démonstration. Supposons d'abord que χ soit diagonalisable dans une base orthonormale, c'est-à-dire qu'il existe une base orthonormale $\mathcal{B}$ telle que la matrice D de χ dans $\mathcal{B}$ soit diagonale. Alors la matrice de χ^* est égale à $\overline{D}$. Or $D\overline{D} = \overline{D}D$, donc $\chi^* \circ \chi = \chi \circ \chi^*$, c'est-à-dire que χ est normal. On notera que les valeurs propres de χ sont des nombres complexes arbitraires.

On montre la réciproque par récurrence sur $n = \dim H$.

Le cas $n = 1$ est évident.

Supposons donc que $n \geqslant 2$ et que le résultat soit vrai pour un espace hermitien de dimension $n-1$. Soit χ un endomorphisme normal de H, où H est un espace hermitien de dimension n. Comme H est un espace vectoriel complexe, il existe une valeur propre λ pour χ. Soit z un vecteur propre associé. Posons $e_1 = \frac{z}{\|z\|}$: alors e_1 est un vecteur propre de norme 1 associé à la valeur propre λ.

Nous voulons montrer que $\text{vect}\{e_1\}^\perp$ est stable par χ. Montrons d'abord que $\chi^*(e_1) = \overline{\lambda}e_1$. Pour cela, posons $w = \chi^*(e_1) - \overline{\lambda}e_1$, et calculons

$$\begin{aligned}
\langle w, w\rangle &= \langle \chi^*(e_1), \chi^*(e_1)\rangle - \langle \chi^*(e_1), \overline{\lambda}e_1\rangle - \langle \overline{\lambda}e_1, \chi^*(e_1)\rangle + \langle \overline{\lambda}e_1, \overline{\lambda}e_1\rangle \\
&= \langle e_1, \chi \circ \chi^*(e_1)\rangle - \lambda\langle e_1, \chi(e_1)\rangle - \overline{\lambda}\langle \chi(e_1), e_1\rangle + |\lambda|^2\|e_1\|^2 \\
&= \langle e_1, \chi^* \circ \chi(e_1)\rangle - \lambda\langle e_1, \lambda e_1\rangle - \overline{\lambda}\langle \lambda e_1, e_1\rangle + |\lambda|^2 \\
&= \langle \chi(e_1), \chi(e_1)\rangle - |\lambda|^2 - |\lambda|^2 + |\lambda|^2 \\
&= \langle \lambda e_1, \lambda e_1\rangle - |\lambda|^2 \\
&= |\lambda|^2\|e_1\|^2 - |\lambda|^2 \\
&= 0,
\end{aligned}$$

D'où $w = 0$ et donc $\chi^*(e_1) = \overline{\lambda}e_1$.

Soit $F = \text{vect}\{e_1\}^\perp$ et soit $z' \in F$. Alors $\langle \chi(z'), e_1\rangle = \langle z', \chi^*(e_1)\rangle = \langle z', \overline{\lambda}e_1\rangle = \lambda\langle z', e_1\rangle = 0$ donc $\chi(z') \in F$. Ainsi la restriction de χ à F définit un endomorphisme $\chi_{|F}$ de F. C'est encore un endomorphisme normal (car on voit facilement que $(\chi_{|F})^* = (\chi^*)_{|F}$). L'hypothèse de récurrence montre qu'il existe une base orthonormale $\{e_2, \ldots, e_n\}$ de F formée de vecteurs propres pour $\chi_{|F}$ et donc pour χ. Alors $\{e_1, e_2, \ldots, e_n\}$ est une base orthonormale de H formée de vecteurs propres pour χ. ✓

De la même façon que dans le cas réel, on déduit la version matricielle :

Corollaire 28. (Théorème spectral pour les matrices normales) Soit $A \in \mathcal{M}_n(\mathbb{C})$. Alors A est une matrice normale si et seulement s'il existe une matrice unitaire P telle que P^*AP soit diagonale.

Remarque. Attention, il n'y a pas de théorème spectral pour les endomorphismes normaux d'un espace euclidien (ou pour les matrices normales de $\mathcal{M}_n(\mathbb{R})$).

Corollaire 29. (Théorème spectral des endomorphismes hermitiens) Soit H un espace hermitien. Soit ψ un endomorphisme hermitien. Alors les valeurs propres de ψ sont réelles. De plus, ψ est diagonalisable dans une base orthonormale, c'est-à-dire qu'il existe une base orthonormale de H formée de vecteurs propres pour ψ.

Démonstration. Si ψ est hermitien, alors $\psi^* = \psi$ et donc ψ est normal. On peut donc appliquer le théorème spectral pour les endomorphismes normaux et la proposition 17. ✓

Corollaire 30. (Théorème spectral des endormorphismes unitaires) Soit $(H, \langle , \rangle)$ un espace hermitien et soit Φ une isométrie de H. Alors les valeurs propres de Φ sont de module 1. De plus, Φ est diagonalisable dans une base orthonormale de H.

Démonstration. Si Φ est unitaire, alors $\Phi^* = \Phi^{-1}$ donc Φ est normal. On peut donc appliquer le théorème spectral pour les endomorphismes normaux et la proposition 25. ✓

Corollaire 31. (Caractérisation des endomorphismes hermitiens et unitaires) Soit χ un endomorphisme normal de H. Pour que χ soit hermitien (*resp.* unitaire), il faut et il suffit que ses valeurs propres soient réelles (*resp.* de module 1).

Démonstration. Les conditions nécessaires ont déjà été prouvées (propositions 17 et 25).

Réciproquement, d'après le théorème spectral pour les endomorphismes normaux, il existe une base orthonormale $\mathcal{B}$ dans laquelle la matrice de χ est diagonale, notons-la D.

Si les coefficients diagonaux sont réels, il est clair que ${}^t\overline{D} = D$, donc χ est hermitien.

Si les coefficients diagonaux sont des complexes de module 1, il est clair que ${}^t\overline{D} = \overline{D} = D^{-1}$, donc χ est unitaire. ✓

Remarque. Nous pouvons maintenant également démontrer la proposition 12 du Chapitre 7 et par conséquent le théorème spectral pour les endomorphismes symétriques d'un espace euclidien en utilisant ce qui précède.

En effet, soit ψ un endomorphisme symétrique d'un espace euclidien E. Soit A la matrice de ψ dans une base orthonormale. Alors ${}^tA = A$. Le polynôme caractéristique c de A est scindé dans $\mathbb{C}[X]$. De plus, A est hermitienne, donc ses valeurs propres sont réelles, donc c est scindé dans $\mathbb{R}[X]$.