III. CORPS : THÉORIE ÉLÉMENTAIRE

Sauf dans l'énoncé du théorème de Wedderburn (4.9), les corps seront toujours supposés ***commutatifs***.

1. Les techniques vectorielles.

a) Degré d'une extension. Eléments algébriques.

Définition 1.1.
Soient K, L des corps avec $K \subset L$. On dit que L est une ***extension*** *(sous-entendu : de corps) de K.*

Exemples 1.2.
On a ainsi $\mathbf{R} \subset \mathbf{C}$, $\mathbf{R} \subset \mathbf{R}(T)$, $\mathbf{Q} \subset \mathbf{Q}(i) \ldots$

Remarques 1.3.
1) Si K est un sous-corps de L, L est un K-espace vectoriel.
2) Si $\dim_K L$ est finie, on pose $[L : K] = \dim_K L$ et l'entier $[L : K]$ s'appelle le ***degré*** de L sur K.
3) Si K et L sont des corps finis, on a $|L| = |K|^n$ avec $n = [L : K]$.

Théorème 1.4 (de la base télescopique).
Soient $K \subset L \subset M$ des corps, $(e_i)_{i \in I}$ une base de L sur K, $(f_j)_{j \in J}$ une base de M sur L. Alors la famille $(e_i f_j)_{(i,j) \in I \times J}$ est une base de M sur K.

Corollaire 1.5 (multiplicativité du degré).
Dans la situation de 1.4, si les degrés sont finis, on a $[M : K] = [M : L][L : K]$.

Démonstration (de 1.4)
1) La famille $e_i f_j$ est libre sur K :
En effet, si on a $\sum_{i,j} \lambda_{ij} e_i f_j = 0$, avec $\lambda_{ij} \in K$ on a $\sum_j f_j (\sum_i \lambda_{ij} e_i) = 0$, donc, puisque f_j est une base de M sur L, on a pour tout j, $\sum_i \lambda_{ij} e_i = 0$, et puisque e_i est une base de L sur K, on a bien $\lambda_{ij} = 0$ pour tous i, j.
2) Elle engendre M : soit $x \in M$, on l'écrit $x = \sum_j \mu_j f_j$, $\mu_j \in L$, puis on décompose $\mu_j = \sum_i \lambda_{ij} e_i$ d'où finalement $x = \sum_{i,j} \lambda_{ij} e_i f_j$ avec $\lambda_{ij} \in K$.

Ce théorème très simple est, en fait, un outil très efficace en théorie des corps comme nous le verrons dans la suite.

Définition 1.6.
1) Soit $K \subset L$ une extension et A une partie de L. On dit que A engendre L sur K et on écrit alors $L = K(A)$ si L est le plus petit sous-corps de L contenant K et A. Si A est fini, $A = \{\alpha_1, \ldots, \alpha_n\}$, on note $L = K(\alpha_1, \ldots, \alpha_n)$.
2) L'extension $K \subset L$ est dite ***monogène*** *s'il existe $\alpha \in L$ tel que $L = K(\alpha)$.*

Remarques 1.7.

1) Si on a une extension $K \subset L$ et si $\alpha \in L$ on note $K[\alpha]$ le sous anneau de L engendré par K et α. On a $K[\alpha] \subset K(\alpha)$. ***Attention***, $K[\alpha]$ n'est pas en général isomorphe à l'anneau des polynômes $K[T]$, ni $K(\alpha)$ au corps des fractions rationnelles $K(T)$.

2) On peut décrire ainsi $K[\alpha]$ et $K(\alpha)$:
si $x \in K[\alpha]$, x s'écrit $x = P(\alpha)$ avec $P \in K[T]$ i.e. $x = a_n\alpha^n + \cdots + a_0$, $a_i \in K$,
si $x \in K(\alpha)$, on a $x = \dfrac{P(\alpha)}{Q(\alpha)}$ avec $P, Q \in K[T]$, $Q(\alpha) \neq 0$.
La différence entre $K[\alpha]$ et $K[T]$ (resp. $K(\alpha)$ et $K(T)$) vient du fait qu'on peut avoir $Q(\alpha) = 0$ avec $Q \in K[T]$, $Q \neq 0$. De façon précise, il y a deux types d'éléments de L relativement à K :

Définition 1.8.
Soit $K \subset L$ une extension et soit $\alpha \in L$. Soit $\varphi : K[T] \longrightarrow L$ l'homomorphisme défini par $\varphi|_K = \mathrm{id}_K$ et $\varphi(T) = \alpha$.
1) Si φ est injectif, on dit que α est ***transcendant sur*** *K,*
2) sinon, on dit que α est ***algébrique sur*** *K. Ceci signifie qu'il existe un polynôme $P(T)$, non nul, tel que $P(\alpha) = 0$. Plus précisément, si $I = \mathrm{Ker}\ \varphi$, I est un idéal principal non nul (cf. II, 3.29 et 3.32), et on a donc $I = (P)$, avec $P \neq 0$ et on peut supposer P unitaire. Le polynôme P est, par définition, le* ***polynôme minimal*** *de α sur K.*

Exemples 1.9.

1) On peut montrer que e et π sont transcendants sur $\mathbf{Q}$ (mais pas sur $\mathbf{R}$, bien entendu). Dans $K(T)$, l'élément T est transcendant sur K.

2) Les nombres $\sqrt{2}$, i, $\sqrt[3]{2}, \cdots$ sont algébriques sur $\mathbf{Q}$, de polynômes minimaux respectifs $X^2 - 2$, $X^2 + 1$, $X^3 - 2, \cdots$.

On peut alors préciser la structure de $K(\alpha)$ selon les deux cas de 1.8 :

Proposition 1.10.
Si α est transcendant, on a $K[\alpha] \simeq K[T]$ et $K(\alpha) \simeq K(T)$ (et donc $K(\alpha)$ est distinct de $K[\alpha]$).

Démonstration. C'est clair, car l'homomorphisme $\varphi : K[T] \to L$ est injectif et d'image $K[\alpha]$.

Théorème 1.11.
Soit $K \subset L$ une extension et soit $\alpha \in L$. Les propriétés suivantes sont équivalentes :
1) α est algébrique sur K,
2) on a $K[\alpha] = K(\alpha)$,
3) on a $\dim_K K[\alpha] < +\infty$.

Précisément, si P est le polynôme minimal de α, P est irréductible et on a $\dim_K K[\alpha] = [K[\alpha] : K] = d^\circ P$. Cet entier s'appelle le **degré** *de α.*

Démonstration. Prouvons 1) $\Longrightarrow$ 2). Supposons α algébrique de polynôme minimal P. D'après II § 0, on a un isomorphisme :

$$\overline{\varphi} = K[T]/(P) \longrightarrow K[\alpha].$$

Comme l'anneau $K[\alpha]$ est inclus dans L, il est intègre, de sorte que l'idéal (P) est premier, donc P est irréductible dans l'anneau principal $K[T]$, donc (P) est maximal (cf. II, 3.22). Il en résulte que $K[\alpha]$ est un corps d'où $K[\alpha] = K(\alpha)$.
On a aussi 2) $\Longrightarrow$ 1) (par 1.10) et 3) $\Longrightarrow$ 1) est clair également car si α est transcendant on a $K[\alpha] \simeq K[T]$ par 1.10, et cet espace vectoriel est de dimension infinie sur K. Enfin 1) $\Longrightarrow$ 3) et la remarque sur la dimension résultent de l'isomorphisme $K[T]/(P) \longrightarrow K[\alpha]$, car si P est de degré n, on montre par division euclidienne, cf. II, 3.31, que $1, \alpha, \ldots, \alpha^{n-1}$ est une base de $K[\alpha]$ sur K .

On se reportera aux exercices pour d'autres démonstrations.

Définition 1.12.
1) Une extension $K \subset L$ est dite **finie** *si on a $\dim_K L (= [L : K]) < +\infty$.*
2) Une extension $K \subset L$ est dite **algébrique** *si pour tout $\alpha \in L$, α est algébrique sur K.*

Remarque 1.13. Le théorème 1.11 montre que toute extension finie est algébrique. Nous verrons plus loin que la réciproque est fausse.

Théorème 1.14.
Soit $K \subset L$ une extension et posons

$$M = \{x \in L \mid x \text{ est algébrique sur } K\}.$$

Alors M est un sous-corps de L.

Démonstration. Soient $\alpha, \alpha' \in M$. Considérons le sous-anneau $K[\alpha, \alpha']$ engendré par α et α'. On a $K[\alpha, \alpha'] = K[\alpha][\alpha']$ et donc comme α' est algébrique sur K, donc *a fortiori* sur $K[\alpha]$, le théorème 1.11 montre que $K[\alpha]$ et $K[\alpha, \alpha']$ sont des corps. De plus le théorème 1.11 et la multiplicativité des degrés donnent $[K[\alpha, \alpha'] : K] < +\infty$. Mais alors, comme $K[\alpha + \alpha']$ et $K[\alpha\alpha']$ sont inclus dans $K[\alpha, \alpha']$, ils sont eux aussi de dimension finie sur K et donc, cf. 1.11, $\alpha + \alpha'$ et $\alpha\alpha'$ sont algébriques donc sont dans M.

Remarque 1.15. Sans les techniques vectorielles, ce théorème n'est pas évident. On s'en convaincra aisément en cherchant un polynôme de $\mathbf{Q}[T]$ qui s'annule en $\sqrt[7]{5} + \sqrt[3]{7}\ \sqrt[5]{3}$.

Exemple 1.16. Soit $A = \{\alpha \in \mathbf{C} \mid \alpha \text{ algébrique sur } \mathbf{Q}\}$, A est un corps, algébrique sur $\mathbf{Q}$, mais l'extension $\mathbf{Q} \subset A$ n'est pas finie car il existe des éléments de A de degré arbitrairement grand, par exemple $\sqrt[n]{2}$, qui est de degré n car le polynôme $X^n - 2$ est irréductible sur $\mathbf{Q}$ (en vertu du critère d'Eisenstein, cf. ci-dessous 3.2).

Définition 1.17.
Un corps K est dit **algébriquement clos** *s'il vérifie l'une quelconque des propriétés équivalentes suivantes :*
1) tout polynôme $P \in K[X]$ de degré ≥ 1 admet une racine dans K,

2) tout polynôme $P \in K[X]$ est produit de polynômes de degré 1,
3) les éléments irréductibles de $K[X]$ sont les $X - a$, $a \in K$,
4) si une extension $K \subset L$ est algébrique, on a $L = K$.

Exemples 1.18.

1) Le corps $\mathbf{C}$ est algébriquement clos, (théorème de D'Alembert-Gauss).

2) Le corps A défini en 1.16 ci-dessus est lui aussi algébriquement clos. C'est même la clôture algébrique de $\mathbf{Q}$ (cf. ci-dessous 1.33). On montre aisément que A est dénombrable, ce qui, puisque $\mathbf{R}$ ne l'est pas, prouve l'existence dans $\mathbf{R}$ de nombres transcendants sur $\mathbf{Q}$, cf. Exercice 3.

b) Application : constructions à la règle et au compas.

Nous allons résoudre par la négative deux problèmes de construction posés par les grecs : la duplication du cube et la trisection de l'angle. On se rendra compte, là encore, de l'efficacité des méthodes vectorielles. Pour des détails, notamment historiques, on consultera l'excellent livre de J.-C. Carréga, cf. [Ca].

On considère le plan euclidien $\mathbf{R}^2$ muni de deux points $O = (0,0)$ et $I = (1,0)$. On cherche à construire de nouveaux points « à la règle et au compas ». Précisément, soit A une partie de $\mathbf{R}^2$, on considère trois types de figures construites à partir de A :

a) les ***droites affines*** $< P, Q >$ pour $P, Q \in A$, $P \neq Q$,

b) les ***cercles*** centrés en un point $P \in A$, passant par un point $Q \in A$, avec $P \neq Q$,

b') les ***cercles*** centrés en $P \in A$, de rayon $||QR||$, avec $Q, R \in A$, $Q \neq R$.

Définition 1.19.

1) Soit A une partie de $\mathbf{R}^2$ et soit $M \in \mathbf{R}^2$. On dit que M est constructible (sous-entendu, à la règle et au compas), en un pas, à partir de A s'il existe deux éléments distincts, droites ou cercles, de type a) ou b) ([1]) ci-dessus, dont M soit un point d'intersection.

*Un point $M \in \mathbf{R}^2$ est dit **constructible** s'il existe une suite $A_0 \subset \ldots \subset A_n$ de parties de $\mathbf{R}^2$ avec :*

a) $A_0 = \{O, I\}$, b) $M \in A_n$, c) $A_i = A_{i-1} \cup \{M_i\}$ où M_i est constructible en un pas à partir de A_{i-1}.

Un nombre réel x est dit constructible si et seulement si $(x, 0)$ l'est.

Proposition 1.20.

Les points suivants de $\mathbf{R}^2$ sont constructibles :
1) les $(n, 0)$ pour $n \in \mathbf{N}$,
2) les $(0, n)$ pour $n \in \mathbf{N}$,
3) les $(x, 0)$ pour $x \in \mathbf{Q}$.
Si le réel $x > 0$ est constructible, il en est de même de $\sqrt{x}$.

Démonstration.

L'assertion 1) est claire et 2) aussi car on construit l'axe des ordonnées comme médiatrice des points $1, -1$ de l'axe des abscisses. Pour 3) on montre d'abord que si on a trois points $P, Q, R \in \mathbf{R}^2$, distincts, on sait construire à la règle et au compas la parallèle à $< P, Q >$ passant par R.

([1]) *Le lecteur vérifiera que l'on peut remplacer les cercles de type b) par ceux de type b') sans changer, en définitive, les points constructibles.*

On construit alors $\frac{p}{q} \in \mathbf{Q}$ en menant la parallèle au segment $< (p,0);(0;q) >$ passant par $(0,1)$ (c'est le théorème de Thalès !).
Enfin, pour le dernier point, on pose $a = \frac{x-1}{2}$, $b = a+1 = \frac{x+1}{2}$. On a $(b-a)(b+a) = b+a = b^2 - a^2 = x$, donc $b^2 = a^2 + c^2$ avec $c^2 = x$. On construit alors à partir de x les points $(0,a)$ et $(b,0)$ et on construit $(c,0)$ comme troisième sommet d'un triangle rectangle de sommets O et $(0,a)$ et dont l'hypothénuse a pour longueur b (c'est le théorème de Pythagore !).

Théorème 1.21.
Soit x un réel constructible. Alors x est algébrique sur $\mathbf{Q}$ et son degré $[\mathbf{Q}[x] : \mathbf{Q}]$ est une puissance de 2.

Remarque 1.22. Attention, la réciproque est fausse, par exemple il existe des x de degré 4 non constructibles. La condition suffisante est que la clôture normale de $\mathbf{Q}(x)$ soit de degré 2^n (cf. par exemple [St]).
Démonstration (de 1.21) Par hypothèse, on a une suite $A_0 \subset A_1 \subset \ldots \subset A_n$ comme en 1.19, avec $(x,0) \in A_n$. Soit K_i le sous-corps de $\mathbf{R}$ engendré sur $\mathbf{Q}$ par les coordonnées des points de A_i. On a donc $K_0 = \mathbf{Q}$ et $x \in K_n$.

Lemme 1.23.
On a $[K_i : K_{i-1}] = 1$, 2 ou 4.

Admettons un instant ce lemme, alors une récurrence immédiate montre que $[K_n : \mathbf{Q}]$ est une puissance de 2 en vertu de la multiplicativité des degrés (cf. 1.5) et comme $\mathbf{Q}[x]$ est un sous-corps de K_n, $[\mathbf{Q}[x] : Q]$ divise $[K_n : \mathbf{Q}]$ (toujours par 1.5) d'où le résultat. (2)
Démonstration (de 1.23) On a $A_i = A_{i-1} \cup \{M_i\}$ avec $M_i = (x_i, y_i)$, donc $K_i = K_{i-1}(x_i, y_i)$.
Par définition M_i est intersection de droites ou de cercles, dont les équations sont dans $K_{i-1}[X,Y]$ de sorte que x_i et y_i vérifient des équations de degré ≤ 2 sur K_{i-1}. On a donc $[K_{i-1}(x_i) : K_{i-1}] \leq 2$ et $[K_{i-1}(x_i, y_i) : K_{i-1}(x_i)] \leq 2$ d'où le résultat.

En fait, une étude plus attentive montre que $[K_i : K_{i-1}] = 1$ ou 2 car l'intersection de deux cercles se ramène toujours à une intersection d'un cercle (l'un des deux) et d'une droite (l'axe radical).

Applications : où l'on surpasse les grecs.

i) Impossibilité de la duplication du cube.

Le problème (dit de Délos) est de construire à la règle et au compas un nombre a tel que le cube d'arête a ait un volume double du cube unité. Autrement dit, on a $a^3 = 2$ et il s'agit donc de construire $a = \sqrt[3]{2}$.

Proposition 1.24.
Le nombre $\sqrt[3]{2}$ n'est pas constructible.

Démonstration. En effet le polynôme $X^3 - 2$ est irréductible sur $\mathbf{Q}$ (car il n'a pas de racines dans $\mathbf{Q}$, voir aussi 3.2) donc c'est le polynôme minimal de $\sqrt[3]{2}$ et donc on a (cf. 1.11) $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$ qui n'est pas une puissance de 2.

(2) Simple, mais efficace, n'est-ce-pas ?

ii) Impossibilité de la trisection de l'angle.

On cherche à « trisecter » l'angle $\pi/3$, donc, à construire $x = \cos \pi/9$. La formule $\cos 3\theta = 4\cos^3 \theta - 3\cos\theta$ montre que x vérifie $8x^3 - 6x - 1 = 0$ et, ce polynôme étant irréductible sur $\mathbf{Q}$, on a encore $[\mathbf{Q}(x) : \mathbf{Q}] = 3$.

iii) Impossibilité de la quadrature du cercle.

On cherche cette fois un carré de côté a dont l'aire soit celle du cercle unité i.e. on cherche a vérifiant $a^2 = \pi$, donc $a = \sqrt{\pi}$. Mais on a le théorème suivant :

Théorème 1.25 (Lindemann).
Le nombre π (donc aussi $\sqrt{\pi}$) est transcendant sur $\mathbf{Q}$, donc non constructible (cf. 1.21).

Le théorème de Lindemann est beaucoup moins élémentaire que ce qui précède et utilise des techniques d'analyse. On se reportera à [St] Chapitre VI pour une démonstration.

c) Corps de rupture, corps de décomposition.

Nous allons résoudre maintenant les deux problèmes suivants :

1) Étant donné $P \in K[X]$, irréductible de degré $d > 1$, construire une extension dans laquelle P admet une racine a (donc est divisible par $X - a$ et, en particulier, n'est plus irréductible).

2) Étant donné $P \in K[X]$, construire une extension dans laquelle P soit décomposé en produit de facteurs de degré 1.

Définition 1.26.
Soit K un corps, $P \in K[X]$ un polynôme ***irréductible****. Une extension $L \supset K$ est appelée un* ***corps de rupture*** *de P sur K si L est une extension monogène $L = K(\alpha)$ avec $P(\alpha) = 0$.*

Théorème 1.27.
Soit $P \in K[X]$, irréductible. Il existe un corps de rupture de P sur K, unique à isomorphisme près.

Démonstration.

a) *Existence.*

On prend $L = K[X]/(P)$, c'est un corps (cf. II, 3.22), dans lequel K s'injecte et si x est l'image de X dans L, on a bien $P(x) = 0$ et $L = K(x)$.

Ainsi, par exemple, $\mathbf{C} = \mathbf{R}[X]/(X^2 + 1)$ est un corps de rupture de $X^2 + 1$, $\mathbf{Q}(\sqrt[3]{2}) = \mathbf{Q}[X]/(X^3 - 2)$ est un corps de rupture de $X^3 - 2$, etc.

b) *Unicité.*

Plus précisément, on a le lemme suivant :

Lemme 1.28.
Soient K, K' deux corps, $i : K \longrightarrow K'$ un isomorphisme que l'on étend de manière évidente en un isomorphisme, noté encore i, de $K[X]$ sur $K'[X]$ en envoyant X sur X. Soit $P \in K[X]$ un polynôme irréductible et soit $P' = i(P)$. Soit L (resp. L') un corps de rupture de P sur K (resp. de P' sur K') engendré par une racine x de P (resp. x' de P'). Alors il existe un unique isomorphisme φ de L sur L', prolongeant i, et vérifiant $\varphi(x) = x'$.

Démonstration. On a un morphisme $u : K[X]/(P) \longrightarrow L$ défini par $u(\overline{X}) = x$, (où $\overline{X}$ désigne l'image de X dans le quotient). C'est un isomorphisme (il est