

Corps et extensions

I. Caractéristique d'un corps et sous-corps premier

Dans tout le chapitre, un corps est un anneau commutatif K dans lequel $1 \neq 0$ et où tout élément non nul est inversible. Un morphisme de corps est un morphisme d'anneaux unitaires entre deux corps. Son noyau est un idéal de K qui ne contient pas 1 . Or les seuls idéaux d'un corps sont $\{0\}$ et K . Par conséquent, **tout morphisme de corps est injectif**. On identifie donc souvent un corps à son image.

1. Caractéristique

Définition :

Soit K un corps. L'application $\chi: \mathbb{Z} \rightarrow K$, $n \rightarrow n \cdot 1_K$, est un morphisme d'anneaux. Son noyau est un idéal de $\mathbb{Z}$, donc de la forme $p\mathbb{Z}$ avec $p \geq 0$. L'entier p s'appelle la **caractéristique** de K , notée $\text{car}(K)$.

Autrement dit, la caractéristique est nulle si les éléments $n \cdot 1_K$ sont tous distincts. Sinon, c'est le plus petit entier $p \geq 1$ tel que $p \cdot 1_K = 0$.

Proposition :

La caractéristique d'un corps est soit 0 , soit un nombre premier.

Démonstration :

Supposons $p = \text{car}(K) \neq 0$. D'abord, $p \neq 1$ car $1_K \neq 0$. Ensuite, si $p = ab$ avec $1 < a, b < p$, alors $(a \cdot 1_K)(b \cdot 1_K) = p \cdot 1_K = 0$. Comme un corps est intègre, l'un des facteurs est nul. Cela contredit la minimalité de p . Ainsi, p est premier.

2. Sous-corps premier

Définition :

Le **sous-corps premier** de K est l'intersection de tous les sous-corps de K . C'est le plus petit sous-corps de K .

Théorème :

Si $\text{car}(K) = p$ est premier, le sous-corps premier de K est isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Si $\text{car}(K) = 0$, il est isomorphe à $\mathbb{Q}$.

Démonstration :

Tout sous-corps contient 1_K , donc l'image de χ . Si p est premier, le théorème de factorisation donne $\chi(\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$, qui est déjà un corps. Si $p = 0$, χ est injectif. De plus, tout sous-corps contient les quotients $\chi(a)\chi(b)^{-1}$ pour $b \neq 0$. Ainsi, χ se prolonge en un morphisme injectif $\mathbb{Q} \rightarrow K$, $\frac{a}{b} \mapsto \chi(a)\chi(b)^{-1}$, dont l'image est le sous-corps premier.

En conséquence, un corps de caractéristique p est un $\mathbb{F}_p$ -espace vectoriel, et un corps de caractéristique nulle est un $\mathbb{Q}$ -espace vectoriel. Cette remarque simple est à la base de toute la théorie des corps finis.

Propriété :

Si $\text{car}(K) = p$ est premier, l'application $F: x \rightarrow x^p$ est un morphisme de corps de K dans lui-même, appelé **morphisme de Frobenius**. En particulier, $(x + y)^p = x^p + y^p$ pour tous $x, y \in K$.

Démonstration :

Pour $1 \leq k \leq p-1$, on a $k \binom{p}{k} = p \binom{p-1}{k-1}$. Donc p divise $k \binom{p}{k}$. Or p est premier avec k , donc p divise $\binom{p}{k}$ d'après le lemme de Gauss. Par conséquent, dans la formule du binôme, tous les termes intermédiaires sont nuls. La multiplicativité est évidente.

Exemple :

Dans $\mathbb{F}_p$, le Frobenius vaut l'identité : c'est le petit théorème de Fermat $x^p = x$. En revanche, dans le corps des fractions rationnelles $\mathbb{F}_p(T)$, le Frobenius n'est pas surjectif, car T n'est pas une puissance p -ième.

II. Extensions de corps et degré

1. Extensions et degré

Définition :

Une **extension** de K est un corps L qui contient K comme sous-corps. On la note L/K . Alors L est un K -espace vectoriel. Sa dimension, finie ou infinie, s'appelle le **degré** de l'extension et se note $[L : K]$. L'extension est dite finie si ce degré est fini.

Exemple :

On a $[\mathbb{C} : \mathbb{R}] = 2$, de base $(1, i)$. De même, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, de base $(1, \sqrt{2})$. En revanche, $[\mathbb{R} : \mathbb{Q}]$ est infini : en effet, un $\mathbb{Q}$ -espace vectoriel de dimension finie est dénombrable, alors que $\mathbb{R}$ ne l'est pas.

Si L/K est une extension et $A \subset L$, on note $K(A)$ le plus petit sous-corps de L contenant K et A . Par exemple, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est le plus petit sous-corps de $\mathbb{R}$ contenant $\sqrt{2}$ et $\sqrt{3}$. Une extension engendrée par un seul élément est dite **monogène**.

2. Théorème de la base télescopique

Théorème :

Soient $K \subset L \subset M$ trois corps. Si $(e_i)_{i \in I}$ est une base de L sur K et $(f_j)_{j \in J}$ une base de M sur L , alors $(e_i f_j)_{(i,j) \in I \times J}$ est une base de M sur K . En particulier,

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

Démonstration :

Famille génératrice : soit $x \in M$. On écrit d'abord $x = \sum_j \lambda_j f_j$ avec $\lambda_j \in L$. Ensuite, chaque λ_j s'écrit $\sum_i \mu_{ij} e_i$ avec $\mu_{ij} \in K$. Donc $x = \sum_{i,j} \mu_{ij} e_i f_j$. Famille libre : si $\sum_{i,j} \mu_{ij} e_i f_j = 0$, on regroupe en $\sum_j (\sum_i \mu_{ij} e_i) f_j = 0$. La liberté des f_j sur L donne $\sum_i \mu_{ij} e_i = 0$ pour tout j . Enfin, la liberté des e_i sur K donne $\mu_{ij} = 0$.

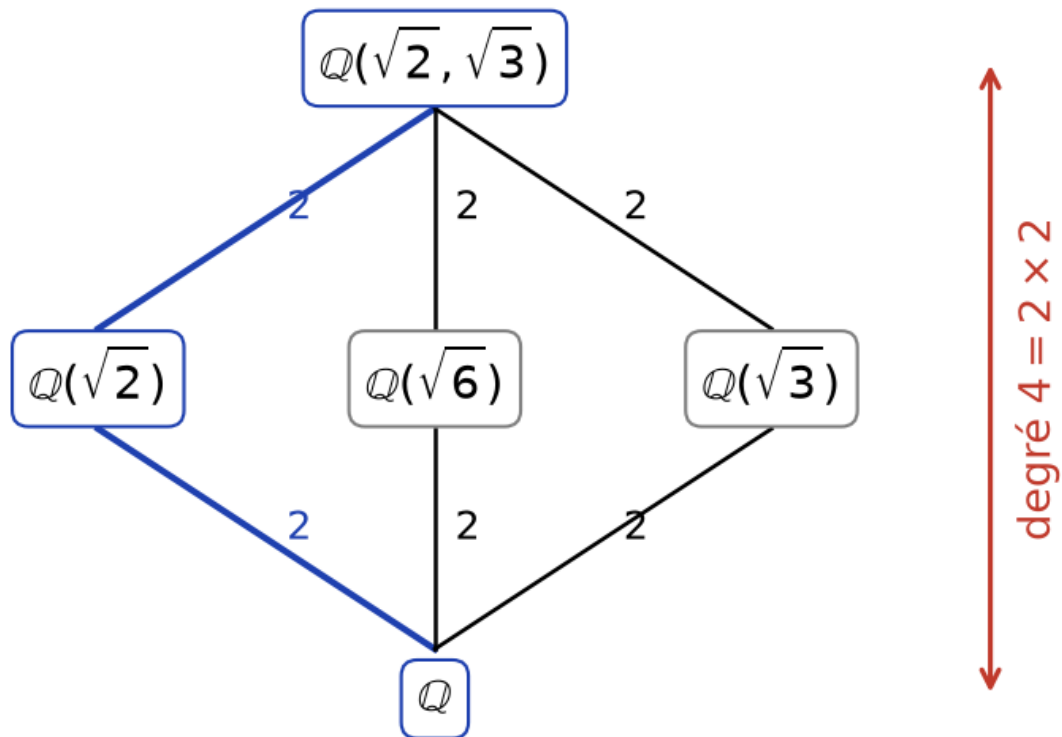
Corollaire :

Si $K \subset L \subset M$ avec M/K finie, alors $[L:K]$ et $[M:L]$ divisent $[M:K]$. En particulier, si $[M:K]$ est premier, il n'y a aucun corps strictement intermédiaire.

Exemple :

On a $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Ensuite, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$: si $\sqrt{3} = a + b\sqrt{2}$ avec a, b rationnels, alors $3 = a^2 + 2b^2 + 2ab\sqrt{2}$, donc $ab = 0$, ce qui mène à $\sqrt{3}$ ou $\sqrt{6}$ rationnel. Ainsi, $X^2 - 3$ n'a pas de racine dans $\mathbb{Q}(\sqrt{2})$, et $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. Par conséquent, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, de base $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$.

La figure ci-dessous représente cette extension et trois de ses sous-corps quadratiques. Chaque segment porte le degré de l'extension correspondante. On lit ainsi la multiplicativité des degrés le long de n'importe quel chemin.



III. Éléments algébriques, transcendants et polynôme minimal

1. Définitions

Définition :

Soit L/K une extension et $\alpha \in L$. On dit que α est **algébrique** sur K s'il existe $P \in K[X]$ non nul tel que $P(\alpha) = 0$. Sinon, α est dit **transcendant** sur K . L'extension L/K est algébrique si tous ses éléments sont algébriques sur K .

Pour étudier α , on considère le morphisme d'évaluation $\text{ev}_\alpha : K[X] \rightarrow L$, $P \mapsto P(\alpha)$. Son image est l'anneau $K[\alpha]$ des expressions polynomiales en α . Son noyau est un idéal de $K[X]$, qui est principal. Tout le chapitre repose sur l'étude de ce noyau.

2. Polynôme minimal

Théorème :

Soit α algébrique sur K . Il existe un unique polynôme unitaire $\mu_\alpha \in K[X]$ tel que $\ker(\text{ev}_\alpha) = (\mu_\alpha)$. On l'appelle le **polynôme minimal** de α sur K . De plus :

- μ_α est irréductible sur K , et c'est l'unique polynôme unitaire irréductible annulant α ;
- $K[\alpha] = K(\alpha)$ et $K(\alpha) \simeq K[X]/(\mu_\alpha)$;
- $[K(\alpha) : K] = \deg \mu_\alpha$, de base $(1, \alpha, \dots, \alpha^{d-1})$ où $d = \deg \mu_\alpha$.

Démonstration :

Le noyau est non nul car α est algébrique. Comme $K[X]$ est principal, il est engendré par un unique polynôme unitaire μ_α . Ensuite, $K[X]/(\mu_\alpha) \simeq K[\alpha]$ est un sous-anneau du corps L , donc intègre. Par conséquent, (μ_α) est premier, donc μ_α est irréductible. Or, dans un anneau principal, un idéal premier non nul est maximal. Ainsi, $K[\alpha]$ est un corps, donc $K[\alpha] = K(\alpha)$. Enfin, la division euclidienne par μ_α montre que $(1, \alpha, \dots, \alpha^{d-1})$ est une base. Si Q est unitaire, irréductible et annule α , alors μ_α divise Q , donc $Q = \mu_\alpha$.

Méthode :

Pour déterminer le polynôme minimal d'un nombre α :

- trouver un polynôme unitaire P annulant α , en éliminant les radicaux par élévations successives au carré ou au cube ;
- prouver que P est irréductible (absence de racine en degré 2 ou 3, critère d'Eisenstein,

réduction modulo un premier) ;

- ou bien prouver que $\deg P = [K(\alpha) : K]$, en calculant ce degré par le théorème de la base télescopique.

Exemple :

Soit $\alpha = \sqrt{1 + \sqrt{2}}$. On a $\alpha^2 - 1 = \sqrt{2}$, donc $(\alpha^2 - 1)^2 = 2$, puis $\alpha^4 - 2\alpha^2 - 1 = 0$. Le polynôme $P = X^4 - 2X^2 - 1$ n'a pas de racine rationnelle, car $P(\pm 1) = -2$. S'il se factorisait en $(X^2 + aX + b)(X^2 - aX + c)$ sur $\mathbb{Q}$, on aurait $a(c - b) = 0$ et $bc = -1$. Le cas $a = 0$ impose $b + c = -2$, donc b et c racines de $t^2 + 2t - 1$, qui valent $-1 \pm \sqrt{2}$: impossible. Le cas $b = c$ donne $b^2 = -1$: impossible. Donc $\mu_\alpha = X^4 - 2X^2 - 1$ et $[K(\alpha) : K] = 4$.

3. Éléments transcendants et extensions algébriques

Proposition :

Si α est transcendant sur K , alors ev_α est injectif. Ainsi, $K[\alpha] \simeq K[X]$ et $K(\alpha) \simeq K(X)$, corps des fractions rationnelles. En particulier, $[K(\alpha) : K]$ est infini.

On admet que e et π sont transcendants sur $\mathbb{Q}$. Cependant, l'existence de nombres transcendants s'obtient à peu de frais : l'ensemble des nombres algébriques sur $\mathbb{Q}$ est dénombrable, alors que $\mathbb{C}$ ne l'est pas.

Théorème :

Soit L/K une extension.

- Si L/K est finie, elle est algébrique, et le degré de tout $\alpha \in L$ divise $[L : K]$.
- Si $\alpha_1, \dots, \alpha_n$ sont algébriques sur K , alors $K(\alpha_1, \dots, \alpha_n)/K$ est finie.
- Les éléments de L algébriques sur K forment un sous-corps de L .

Démonstration :

Si $[L : K] = n$, la famille $(1, \alpha, \dots, \alpha^n)$ a $n + 1$ éléments, donc elle est liée : une relation de liaison fournit un polynôme non nul annulant α . De plus, $K \subset K(\alpha) \subset L$, donc $\deg \mu_\alpha = [K(\alpha) : K]$ divise $[L : K]$. Pour le deuxième point, on raisonne par récurrence : α_{k+1} est algébrique sur $K(\alpha_1, \dots, \alpha_k)$, et la base télescopique multiplie des degrés finis. Enfin, si α et β sont algébriques, $K(\alpha, \beta)$ est finie, donc $\alpha + \beta$, $\alpha\beta$ et α^{-1} sont algébriques.

IV. Corps de rupture et corps de décomposition

Jusqu'ici, les éléments algébriques vivaient dans un corps donné à l'avance, par exemple $\mathbb{C}$. L'angle du chapitre est inverse : on part d'un polynôme et l'on **fabrique** un corps où il a une racine, grâce au quotient $K[X]/(P)$.

1. Corps de rupture

Définition :

Soit $P \in K[X]$ irréductible. Un **corps de rupture** de P sur K est une extension L de K de la forme $L = K(\alpha)$ avec $P(\alpha) = 0$.

Théorème :

Soit $P \in K[X]$ irréductible de degré n . Alors $L = K[X]/(P)$ est un corps de rupture de P , avec $\alpha = \overline{X}$, et $[L : K] = n$. De plus, deux corps de rupture $K(\alpha)$ et $K(\beta)$ de P sont isomorphes par un unique isomorphisme qui fixe K et envoie α sur β .

Démonstration :

L'idéal (P) est maximal car P est irréductible dans l'anneau principal $K[X]$. Donc L est un corps. Il contient une copie de K (les classes des constantes), et $P(\overline{X}) = \overline{P} = 0$. Ensuite, $L = K[\overline{X}]$. Pour l'unicité, P est le polynôme minimal de α et de β à un scalaire près. Donc $K(\alpha) \simeq K[X]/(P) \simeq K(\beta)$, la composée envoyant α sur β .

Méthode :

Pour calculer dans $L = K[X]/(P)$ avec $\alpha = \overline{X}$:

- tout élément s'écrit de façon unique $a_0 + a_1 \alpha + \dots + a_{n-1} \alpha^{n-1}$;
- un produit se réduit grâce à la relation $P(\alpha) = 0$, c'est-à-dire en prenant le reste de la division euclidienne par P ;
- l'inverse de $Q(\alpha) \neq 0$ s'obtient par une relation de Bézout $UQ + VP = 1$: alors $Q(\alpha)^{-1} = U(\alpha)$.

Exemple :

Dans $\mathbb{Q}[X]/(X^3 - 2)$, on a $\alpha^3 = 2$. Comme $(\alpha + 1)(\alpha^2 - \alpha + 1) = \alpha^3 + 1 = 3$, on obtient directement $(1 + \alpha)^{-1} = \frac{1}{3}(\alpha^2 - \alpha + 1)$.

2. Corps de décomposition

Définition :

Soit $P \in K[X]$ de degré $n \geq 1$. Un **corps de décomposition** de P sur K est une extension L dans laquelle $P = c(X - \alpha_1) \dots (X - \alpha_n)$, et telle que $L = K(\alpha_1, \dots, \alpha_n)$.

Théorème :

Tout polynôme $P \in K[X]$ de degré $n \geq 1$ admet un corps de décomposition L , et $[L : K] \leq n!$. De plus, deux corps de décomposition de P sur K sont isomorphes par un isomorphisme qui fixe K .

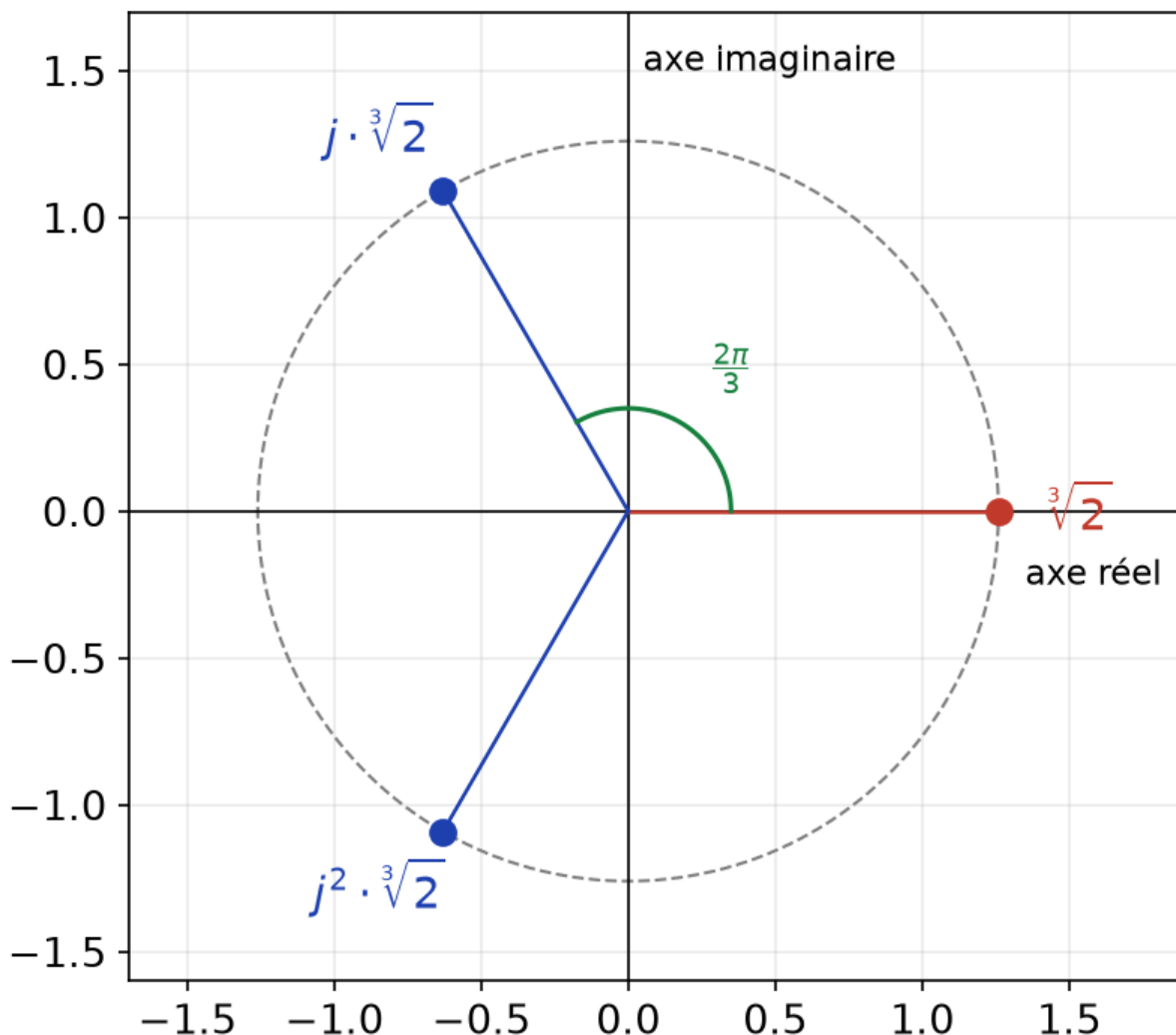
Démonstration :

Existence, par récurrence sur n . On choisit un facteur irréductible Q de P et un corps de rupture $K_1 = K(\alpha_1)$ de Q . Alors $[K_1 : K] \leq n$, et $P = (X - \alpha_1)P_1$ dans $K_1[X]$ avec $\deg P_1 = n - 1$. L'hypothèse de récurrence fournit un corps de décomposition de P_1 sur K_1 , de degré au plus $(n-1)!$. La base télescopique conclut. L'unicité se démontre de même, en prolongeant pas à pas un isomorphisme grâce à l'unicité des corps de rupture ; nous l'admettons ici.

Exemple :

Le polynôme $X^3 - 2$ est irréductible sur $\mathbb{Q}$ par le critère d'Eisenstein en 2 . Ses racines complexes sont $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$, avec $j = e^{2i\pi/3}$. Le corps $\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture, de degré 3. Cependant, il est inclus dans $\mathbb{R}$, donc il ne contient pas les deux racines non réelles. Le corps de décomposition est $\mathbb{Q}(\sqrt[3]{2}, j)$, de degré $3 \times 2 = 6$.

Comme le montre la figure ci-dessous, les trois racines forment un triangle équilatéral dans le plan complexe. Une seule d'entre elles est réelle. C'est pourquoi un corps de rupture n'est pas toujours un corps de décomposition.



V. Constructions à la règle et au compas

1. Nombres constructibles

Définition :

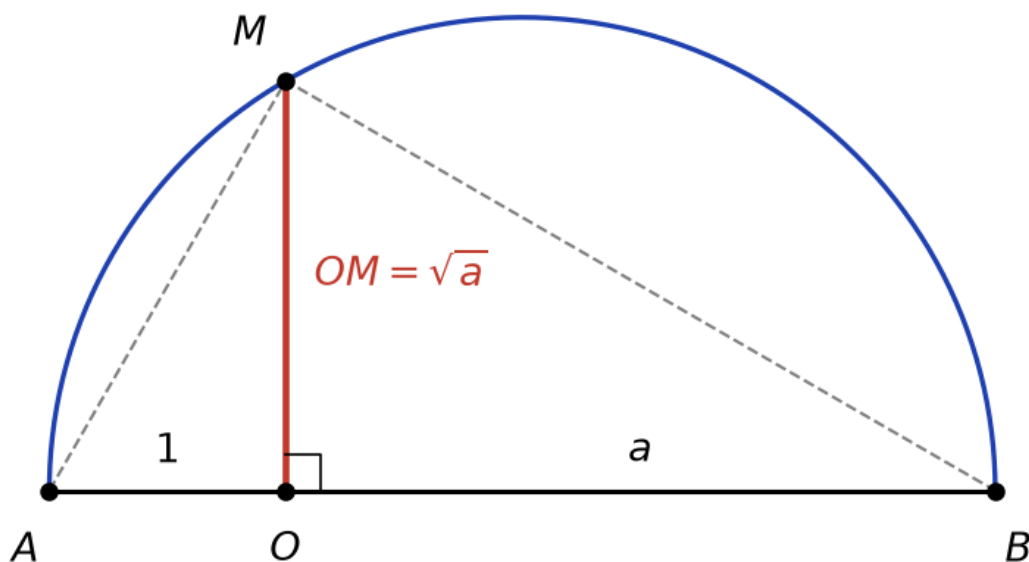
On part des points $O = (0, 0)$ et $I = (1, 0)$ du plan. On s'autorise à tracer la droite passant

par deux points déjà construits et le cercle de centre un point construit passant par un autre point construit. Les intersections de ces droites et cercles sont de nouveaux points construits. Un réel est dit **constructible** s'il est une coordonnée d'un point constructible.

Proposition :

L'ensemble des réels constructibles est un sous-corps de $\mathbb{R}$. De plus, si $a > 0$ est constructible, alors $\sqrt{a}$ l'est aussi.

Les opérations de corps s'obtiennent par le théorème de Thalès. Pour la racine carrée, on trace le demi-cercle de diamètre $[AB]$, où $AO = 1$ et $OB = a$. La perpendiculaire en O coupe le demi-cercle en M . En effet, le triangle AMB est rectangle en M , donc $OM^2 = OA \times OB = a$. La figure ci-dessous montre cette construction.



2. Le théorème des tours quadratiques

Théorème :

Un réel x est constructible si et seulement s'il existe une suite de sous-corps

$\mathbb{Q} = K_0 \subset K_1 \subset \dots \subset K_r \subset \mathbb{R}$ telle que $[K_{i+1} : K_i] = 2$ pour tout i et $x \in K_r$. En particulier, si x est constructible, alors x est algébrique sur $\mathbb{Q}$ et $[\mathbb{Q}(x) : \mathbb{Q}]$ est une puissance de 2.

Démonstration :

Supposons que tous les points déjà construits aient leurs coordonnées dans un corps K . Une droite passant par deux tels points a une équation à coefficients dans K . Un cercle aussi. L'intersection de deux droites s'obtient en résolvant un système linéaire : elle reste dans K . Ensuite, l'intersection d'une droite et d'un cercle conduit à une équation du second degré sur K . Enfin, deux cercles se ramènent au cas précédent en soustrayant leurs équations. Chaque nouveau point a donc ses coordonnées dans K ou dans $K(\sqrt{\delta})$ avec $\delta \in K$, extension de degré 1 ou 2. On obtient ainsi la tour. Par la base télescopique, $[K_r : \mathbb{Q}] = 2^r$, et $[\mathbb{Q}(x) : \mathbb{Q}]$ divise 2^r . La réciproque découle de la proposition précédente.

Méthode :

Pour montrer qu'un réel x n'est pas constructible :

- trouver un polynôme unitaire $P \in \mathbb{Q}[X]$ annulant x ;
- prouver que P est irréductible sur $\mathbb{Q}$, donc que $P = \mu_x$;
- constater que $\deg P$ n'est pas une puissance de 2 (typiquement $\deg P = 3$).

Exemple :

La duplication du cube demande de construire $\sqrt[3]{2}$. Or $X^3 - 2$ est irréductible sur $\mathbb{Q}$, donc $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, qui n'est pas une puissance de 2. Par conséquent, **la duplication du cube est impossible** à la règle et au compas. De même, $\cos 20^\circ$ est racine de $8X^3 - 6X - 1$, irréductible : l'angle de 60° ne peut pas être partagé en trois.

Attention :

La condition « degré puissance de 2 » est nécessaire mais pas suffisante en général. Pour prouver qu'un nombre est constructible, il faut exhiber la tour d'extensions quadratiques, ou bien une construction explicite.

VI. Corps finis

1. Cardinal d'un corps fini

Proposition :

Un corps fini K a une caractéristique première p , et son cardinal est de la forme p^n avec $n = [K : \mathbb{F}_p]$.

Démonstration :

Le morphisme $\chi : \mathbb{Z} \rightarrow K$ ne peut pas être injectif, donc $\text{car}(K) = p$ est premier. Ensuite, K est un $\mathbb{F}_p$ -espace vectoriel de dimension finie n . Il est donc en bijection avec $\mathbb{F}_p^n$, qui a p^n éléments.

2. Existence et unicité

Théorème :

Pour tout nombre premier p et tout entier $n \geq 1$, posons $q = p^n$. Il existe un corps à q éléments, et il est unique à isomorphisme près : c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. On le note $\mathbb{F}_q$. Ses éléments sont exactement les racines de $X^q - X$.

Démonstration :

Soit L un corps de décomposition de $P = X^q - X$ sur $\mathbb{F}_p$. Sa dérivée vaut $qX^{q-1} - 1 = -1$, donc P est premier avec P' : ses racines sont simples. L'ensemble R de ses racines a donc q éléments. Ensuite, $R = \left\{ x \in L, \begin{matrix} F^n(x) = x \end{matrix} \right\}$ où F est le Frobenius. Comme F^n est un morphisme de corps, R est un sous-corps de L . Il contient toutes les racines de P , donc $R = L$ et $|L| = q$. Réciproquement, si $|K| = q$, le groupe K^* a $q - 1$ éléments. Le théorème de Lagrange donne $x^{q-1} = 1$ pour $x \neq 0$, donc $x^q = x$ pour tout x . Ainsi, K est un corps de décomposition de $X^q - X$, et l'unicité des corps de décomposition conclut.

Méthode :

Pour construire $\mathbb{F}_{p^n}$ concrètement, on cherche un polynôme $P \in \mathbb{F}_p[X]$ irréductible de degré n . Alors $\mathbb{F}_p[X]/(P)$ est un corps à p^n éléments. En degré 2 ou 3, il suffit de vérifier que P n'a pas de racine dans $\mathbb{F}_p$. En degré 4, il faut en plus exclure un produit de deux facteurs irréductibles de degré 2.

Exemple :

Le polynôme $X^3 + X + 1$ n'a pas de racine dans $\mathbb{F}_2$, car il vaut 1 en 0 et en 1. Il est

donc irréductible, et $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3 + X + 1)$. En notant $\beta = \overline{X}$, on a $\beta^3 = \beta + 1$. Les huit éléments sont les $a + b\beta + c\beta^2$ avec $a, b, c \in \{0, 1\}$.

3. Cyclicité du groupe multiplicatif

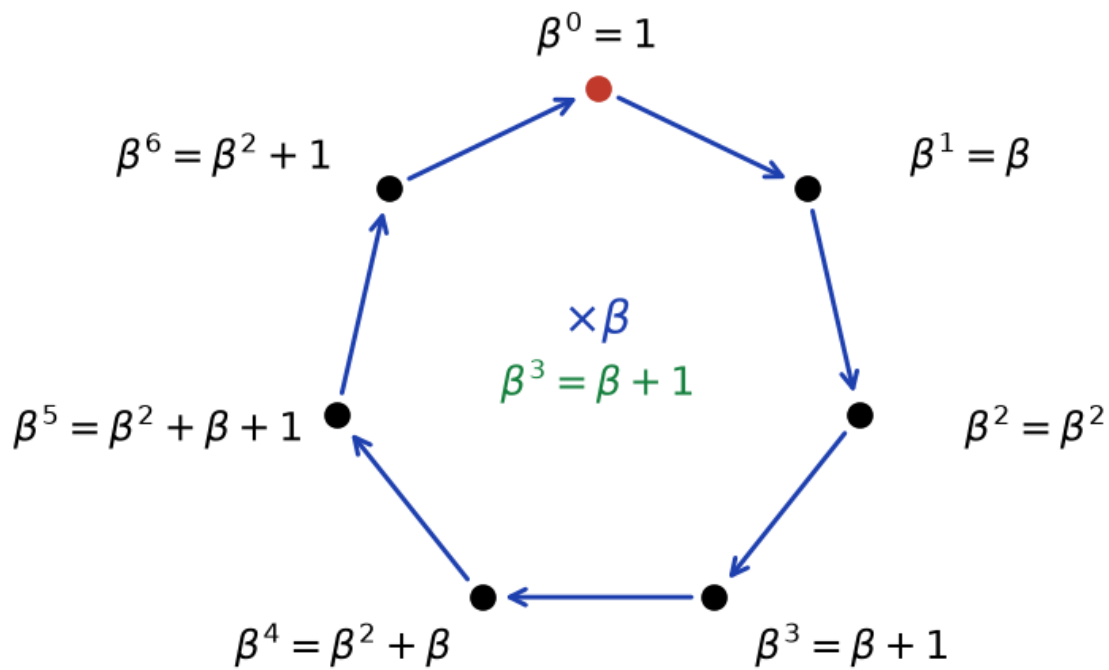
Théorème :

Si K est un corps, tout sous-groupe fini de K^* est cyclique. En particulier, le groupe $\mathbb{F}_q^*$ est cyclique d'ordre $q - 1$. Un générateur de ce groupe s'appelle un **élément primitif**, et il y en a exactement $\varphi(q - 1)$.

Démonstration :

Soit G un sous-groupe fini de K^* , d'ordre n . Pour $d \mid n$, notons $N(d)$ le nombre d'éléments d'ordre d . Si $N(d) \neq 0$, soit x d'ordre d . Les d éléments $1, x, \dots, x^{d-1}$ sont racines de $X^d - 1$. Or ce polynôme a au plus d racines dans le corps K . Donc tout élément d'ordre d est une puissance de x , et il y en a $\varphi(d)$. Ainsi, $N(d) \leq \varphi(d)$ pour tout d . De plus, $\sum_{d \mid n} N(d) = n = \sum_{d \mid n} \varphi(d)$. Par conséquent, $N(d) = \varphi(d)$ pour tout d . En particulier, $N(n) = \varphi(n) \geq 1$: le groupe est cyclique.

Dans l'exemple de $\mathbb{F}_8$, le groupe $\mathbb{F}_8^*$ a 7 éléments. Comme 7 est premier, tout élément différent de 1 est un générateur. La figure ci-dessous parcourt les puissances successives de β : on obtient bien les sept éléments non nuls.



Méthode :

Pour trouver un générateur de $\mathbb{F}_q^*$, on factorise $q - 1 = \ell_1^{a_1} \dots \ell_r^{a_r}$. Un élément $g \neq 0$ est un générateur si et seulement si $g^{(q-1)/\ell_i} \neq 1$ pour tout i . On teste alors des candidats simples, en commençant par 2, 3 ou $\overline{X}$.

Exemple :

Dans $\mathbb{F}_{11}$, on a $q - 1 = 10 = 2 \times 5$. Or $2^5 = 32 = 10 \neq 1$ et $2^2 = 4 \neq 1$. Donc 2 engendre $\mathbb{F}_{11}^*$, et les générateurs sont les 2^k avec k premier à 10, soit 2, 8, 7, 6.

4. Sous-corps d'un corps fini

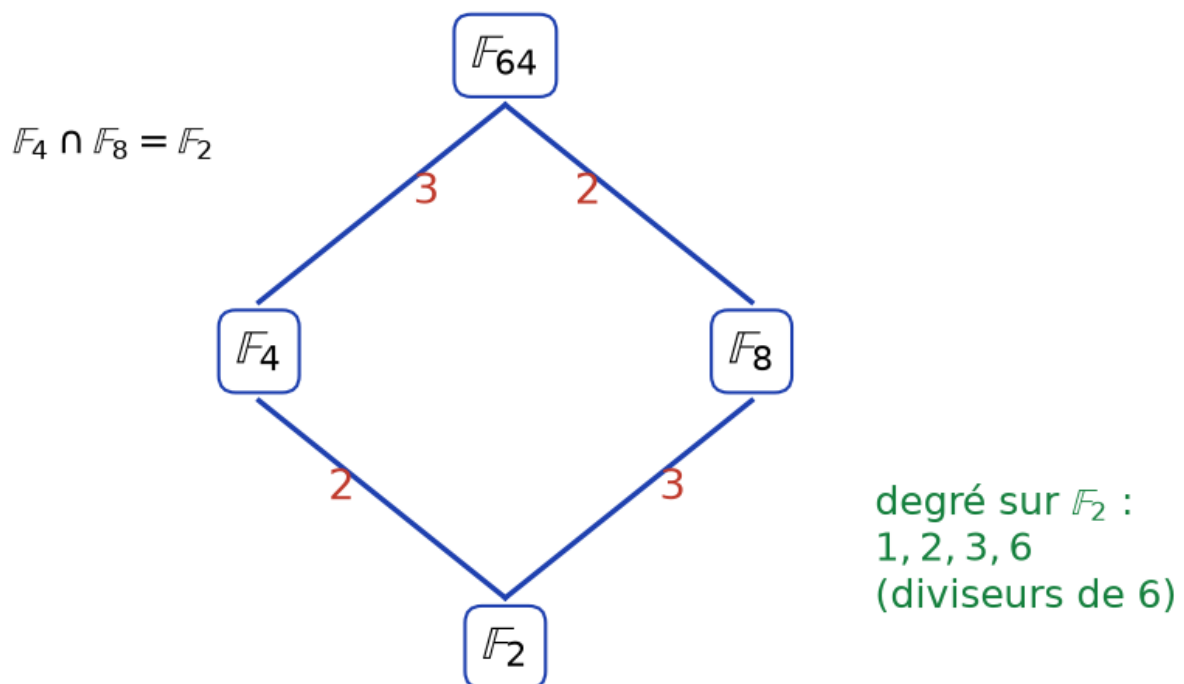
Théorème :

Les sous-corps de $\mathbb{F}_{p^n}$ sont exactement les $\left\{x, x^{p^d} = x\right\}$, pour d diviseur de n . Chacun a p^d éléments, et il existe un unique sous-corps de cardinal p^d pour chaque $d \mid n$.

Démonstration :

Si K est un sous-corps à p^d éléments, la base télescopique donne $n = [\mathbb{F}_{p^n} : K] \times d$, donc $d \mid n$. De plus, K est formé des racines de $X^{p^d} - X$, qui a au plus p^d racines : il est donc unique. Réciproquement, si $d \mid n$, alors $p^d - 1$ divise $p^n - 1$, donc $X^{p^d} - X$ divise $X^{p^n} - X$. Il a donc p^d racines distinctes dans $\mathbb{F}_{p^n}$, qui forment un sous-corps.

La figure ci-dessous représente les sous-corps de $\mathbb{F}_{64}$. Les diviseurs de 6 sont 1, 2, 3, 6, d'où quatre sous-corps. Ainsi, $\mathbb{F}_4$ n'est pas inclus dans $\mathbb{F}_8$, puisque 2 ne divise pas 3.



VII. Ce qu'il faut retenir

- Un morphisme de corps est injectif. La caractéristique vaut 0 ou un premier p , et le sous-corps premier est $\mathbb{Q}$ ou $\mathbb{F}_p$.
- En caractéristique p , le Frobenius $x \rightarrow x^p$ est un morphisme : $(x + y)^p = x^p + y^p$.
- Base télescopique : $[M : K] = [M : L][L : K]$. Le degré d'un élément divise le degré de toute extension finie qui le contient.
- Le polynôme minimal est l'unique polynôme unitaire irréductible annulant α , et $[K(\alpha) : K] = \deg \mu_\alpha$.
- Les nombres algébriques forment un corps. Un élément transcendant engendre une extension de degré infini.
- Si P est irréductible, $K[X]/(P)$ est un corps de rupture de degré $\deg P$. Le corps de décomposition existe et a un degré au plus $n!$.
- Un réel constructible a un degré puissance de 2 : duplication du cube et trisection de l'angle sont impossibles.
- Un corps fini a p^n éléments. Pour chaque $q = p^n$, il existe un unique corps $\mathbb{F}_q$: le corps de décomposition de $X^q - X$, réalisé comme $\mathbb{F}_p[X]/(P)$ avec P irréductible de degré n .
- Le groupe $\mathbb{F}_q^*$ est cyclique et possède $\varphi(q-1)$ générateurs. On les détecte en testant $g^{(q-1)/\ell} \neq 1$.
- Les sous-corps de $\mathbb{F}_{p^n}$ sont les $\mathbb{F}_{p^d}$ pour $d \mid n$.

Questions fréquentes sur corps et extensions

Comment calculer le degré d'une extension comme $\mathbb{Q}(\sqrt{2}, \sqrt{3})$?

On empile les extensions et l'on applique le théorème de la base télescopique : les degrés se multiplient. Ici, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, puis $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, donc le second étage est aussi de degré 2. Le degré total vaut donc 4.

Quelle différence entre corps de rupture et corps de décomposition ?

Un corps de rupture de P irréductible est engendré par une seule racine de P , et il est isomorphe à $K[X]/(P)$. Un corps de décomposition contient toutes les racines de P . Pour $X^3 - 2$, le corps $\mathbb{Q}(\sqrt[3]{2})$ est de rupture, de degré 3, mais le corps de décomposition est de degré 6.

Pourquoi ne peut-on pas dupliquer le cube à la règle et au compas ?

Un réel constructible a un degré sur $\mathbb{Q}$ égal à une puissance de 2, car chaque construction ajoute au plus une racine carrée. Or $\sqrt[3]{2}$ a pour polynôme minimal $X^3 - 2$, de degré 3. Il n'est donc pas constructible.

Comment trouver un générateur du groupe multiplicatif d'un corps fini ?

On factorise $q - 1$ en produit de nombres premiers ℓ . Un élément g non nul engendre $\mathbb{F}_q^*$ si et seulement si $g^{(q-1)/\ell} \neq 1$ pour chaque ℓ . On teste alors de petits candidats, comme 2 ou la classe de X .

Pour aller plus loin en L3

- Les énoncés : [exercices de maths en L3 sur corps et extensions](#)
- À maîtriser avant : [Anneaux, idéaux et arithmétique](#)
- Chapitre précédent : [Anneaux, idéaux et arithmétique](#)
- Chapitre suivant : [Réduction de Jordan et décomposition de Dunford](#)
- Tester vos connaissances : [QCM de maths en L3 par chapitre](#)
- Le sommaire : [tous les chapitres de maths de L3](#) et la [licence de maths de L1 à L3](#)