# Corps commutatif.

## I Définition.

Définition 1

Un anneau commutatif (unitaire) $(A, +, \times)$ est appelé un *corps (commutatif)* si et seulement si tout élément non élément non nul de $A$ est inversible dans $A$ pour la loi $\times$.

Remarques.

1. Le terme commutatif, le plus souvent est omis. Lorsqu'il s'avère nécessaire de distinguer on parle de corps commutatif et de corps gauche (ou d'anneau de division).
2. Autrement dit $(A \setminus \{0\}, \times)$ est un groupe abélien.

Exemples.

1. $(\mathbb{Z}, + \times)$ est un anneau mais n'est pas un corps.
2. $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des corps.
3. $(\mathbb{H}, +, \times)$ le corps des quaternions est un corps non commutatif, c'est un corps gauche.
4. $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ avec $p \in \mathbb{N}$ premier est un corps commutatif fini.
5. Si $\mathbb{K}$ est un anneau commutatif, $(\mathbb{K}(X), +, \times)$, c'est-à-dire l'ensemble des fractions rationnels, est un corps.

## II Corps des fractions d'anneau intègre.

## III La localisation.

Il s'agit d'un procédé généralisant la démarche de construction du corps des fractions.

## IV Extension engendrée.

Proposition 1

Soient :
. $K$ un corps,
. $L$ une extension de $K$,
. $A \subset L$.

Il existe une extension de $K$, que nous noterons $K(A)$, contenant $A$ et minimum pour la relation d'inclusion entre extensions de $K$ contenues dans $L$.
De plus $K(A)$ est l'ensemble des éléments de $L$ de la forme $F(a_1,\dots,a_k)$ où $k \in \mathbb{N}$, $F \in K(X_1,\dots,X_k)$ dont le dénominateur ne s'annule pas en $(a_1,\dots,a_k)$.

Remarques.

1. L'extension $K(A)$ est appelée *l'extension engendrée par $A$*.
2. Dans le cas $A = \{a_1,\dots,a_n\}$ fini, plutôt que $K(A)$ nous écrirons $K(a_1,\dots,a_n)$.

Proposition 2

Soient :
. $K$ un corps,
. $L$ une extension de $K$,
. $A \subset L$,
. $B \subset L$.

$$K(A \cup B) = K(A)(B).$$

Exercice 1

Exrcice 10 $LM$ est le compositum c'est-à-dire le plus petit sur-corps contenant $M \cup L$.

Correction exercice 1

1. Montrons que si $t$ est fini alors, $m$ et $l$ le sont.

   Supposons donc $t$ fini.

   Puisque $K \subset L \subset LM$, $[L : K] \leqslant [LM : K]$. Autrement dit : $l \leqslant t$.
   De même : $m \leqslant t$.
   $l$ et $m$ sont donc fini.

   Si $t$ est fini, alors $l$ et $m$ le sont.

Démontrons que si $l$ et $m$ sont fini, alors forcément $t$ l'est aussi.

Supposons que $m$ et $l$ et sont finis et démontrons alors que $t$ l'est.

Par récurrence forte sur $m$. L'hypothèse de récurrence c'est l'implication elle même.

2. Arithmétique.
3. Utiliser la questin 1 pour avoir une inégalité.
4. Là encore avec l'inégalité de la question 1.
   Contre exemple : $M = \mathbb{Q}(\sqrt[3]{2})$ et $L = \mathbb{Q}(j\sqrt[3]{2})$.
   On a : $[M : \mathbb{Q}] = 3$ et $[L : \mathbb{Q}] = 3$ et pourtant $[ML : \mathbb{Q}] = 6$ car $[ML : M] = 2$.

# V Extension algébrique.

## Nombre algébrique.

Définition 2

Soient :
. $K$ un corps,
. $L$ une extension de $K$.

Un élément $a \in L$ est dit *algébrique* si et seulement si : $\exists P \in K[X]$, $P(a) = 0$.

Exemples.

1. $\sqrt{2}$, $\sqrt[3]{2}$ et $e^{\frac{2i\pi}{n}}$ sont des nombres complexes algébriques sur $\mathbb{Q}$.

Remarques.

1. Un nombre qui n'est pas algébrique est dit *transcendant*.

Exercice 2

*Nombre de Liouville.*

1. Soit $a$ un élément algébrique sur $\mathbb{Q}$ de degré $n \geqslant 1$, montrer qu'il existe $c(a) \in \mathbb{R}_+^*$ vérifiant
$$\forall \frac{p}{q} \in \mathbb{Q}, q > 0,\ a \neq \frac{p}{q} \Leftrightarrow \left| a - \frac{p}{q} \right| \geqslant \frac{c(a)}{q^n}.$$
2. En déduire la transcendance de $a = \sum_{n>0} \frac{a_n}{10^{n!}}$ pour toute suite $(a_n)$ d'entiers naturels compris entre 1 et 9.

Correction exercice 2

1. Utilise entre autre le théorème des accroissements finis.
2. Raisonnement par l'absurde : on suppose et $a$ algébrique et il faut faire apparaître une contradiction : on majore $c(a)$ par une suite convergeant vers 0.

**Polynôme minimal d'un élément algébrique.**

Définition 3

Soient :

. $K$ un corps,

. $L$ une extension de $K$,

. $a \in L$ un élément algébrique sur $K$.

L'unique polynôme unitaire de degré minimum s'annulant en $a$ est appelé *le polynôme minimal de a sur K*.
Le degré du polynôme minimal de $a$ sur $K$ est appelé *le degré de a sur K*.

Exemples.

1. $X^2 - 2$ est le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$. De plus $\sqrt{2}$ est de degré deux sur $\mathbb{Q}$.

Remarques.

1. L'ensemble des polynômes annulateurs de $a$ forme un idéal de $K[X]$. Or $K[X]$ est un anneau principal donc l'idéal des polynômes annulateurs de $a$ est engendré par un polynôme de degré minimum qu'il est possible de rendre unitaire.
2. Le polynôme minimal d'un élément $a \in K$ est $X - a$.
3. Le polynôme minimal dépend du corps $K$. $X^6 - 2$ est le polynôme minimal de $\sqrt[6]{2}$ sur $\mathbb{Q}$ mais $X^3 - \sqrt{2}$ est le polynôme minimal de $\sqrt[6]{2}$ sur $\mathbb{Q}[\sqrt{2}]$.

Proposition 3 - propriétés du polynôme minimal d'un élément algébrique.

Soient :

. $K$ un corps,

. $L$ une extension de $K$,

. $a \in L$ un élément algébrique sur $K$,

. $\mu$ le polynôme minimal de $a$ sur $K$.

(*i*) Tout polynôme de $K[X]$ s'annulant en $a$ est divisible par $\mu$.

(*ii*) $\mu$ est irréductible sur $K$ (il n'est pas le produit de deux éléments non constants de $K[X]$).

(*iii*) Toute racine de $\mu$ dans $L$ admet $\mu$ pour polynôme minimal sur $K$.

(*iv*) Si $L$ est un corps de caractéristique 0, alors $a$ est une racine simple de sont polynôme minimal.

**Extension engendrée par un élément algébrique.**

## VI Clôture algébrique.

Proposition 4

Soit $K$ un corps.
les assertions suivantes sont équivalentes.

1. Tout élément de $k[X]$ qui n'est pas dans $k$ admet au moins une racine dans $K$.
2. Les polynômes irréductibles de $K[X]$ sont ceux de degré 1.
3. Toute extension algébrique de $K$ est triviale.

Démonstration 1

* $1 \Leftrightarrow 2$.
* $2 \Leftrightarrow 3$.
  Soit $L|K$ une extension.et $x \in L$ démontrons que $x \in K$. $x$ algébrique sur $K$ puisque les polynômes irréductibles sont de degré 1 nécessairement $[K(x) : K] = 1$. Autrement dit $K = K(x)$.
* $3 \Leftrightarrow 1$.
  Soient $P \in K[x]$. $L$ un corps de rupture de $P$. alors il existe $x \in K$ tel que $L = K(x)$ et $[L : K] = deg(P)$.
  $L|K$ extension algébrique donc : $L = K$.

Théorème 1

Soient $K$ un corps.
$K$ possède au moins une clôture algébrique et deux clôture algébrique sur $K$ sont $K$-isomorphes.

## VII Corps de rupture.

Définition 4

Soient :

. $K$ un corps,

. $P \in K[X]$,

. $L$ une extension de $K$.

L'extension $L$ de $K$ est appelée *corps de rupture de $P$ sur $K$* si

$$\begin{cases} \exists x \in L,\ P(x) = 0 \\ L = K[x] \end{cases}$$

Remarques.

1. $\mathbb{Q}[\sqrt[3]{2}]$ et $\mathbb{Q}[j\sqrt[3]{2}]$ sont des corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$.

Proposition 5

Soient :

. $K$ un corps,

. $P \in K[X]$ un polynôme irréductible de degré $n \in \mathbb{N}$.

L'anneau quotient $L = \frac{K[X]}{(P)}$ est un corps de rupture de $P$, extension de degré $n$ de $K$ contenant la classe $x$ de $X$ comme racine de $P$.
$P$ est le polynôme minimal de $x$ sur $K$.

## VIII Corps de décomposition.

Définition 5

Soient :
. $K$ un sous-corps de $\mathbb{C}$,
. $P \in K[X]$.

Nous appellerons *corps de décomposition de $P$ sur $K$* le corps $K\left(P^{-1}(\{0\})\right)$.

Remarques.
1.

## Exercice 3

Déterminez les corps de décomposition des polynômes suivants sur $\mathbb{Q}$. Vous déterminerez aussi le degré de l'extension.

1. $X^3 - 1$.
2. $X^6 - 1$.
3. $X^4 - 7$.
4. $X^6 - 10X^4 + 31X^2 - 30$.
5. $X^4 + 1$.

Correction exercice 3

1. $P(X) = (X-1)(X-j)(X-j^2)$. Donc le corps de décomposition de $P$ sur $\mathbb{Q}$ est $\mathbb{Q}(1,j,j^2) = \mathbb{Q}(j)$.
   De plus : $[\mathbb{Q}(j) : \mathbb{Q}] = 2$ car $P$ est un polynôme irréductible de $j$ sur $\mathbb{Q}$.
2. $P(X) = (X-1)(X+1)(X^2+X+1)(X^2-X+1)$.
   Donc la corps de décomposition de $P$ sur $\mathbb{Q}$ est $\mathbb{Q}(j)$. D'après la question précédente il s'agit donc d'une extension de degré deux.
3. $P(X) = (X - \sqrt[4]{7})(X + \sqrt[4]{7})(X - i\sqrt[4]{7})(X + i\sqrt[4]{7})$.
   D'où le corps de décomposition de $P$ sur $\mathbb{Q}$ : $\mathbb{Q}(\sqrt[4]{7},i)$.
   On remarque que le corps de rupture de $\sqrt[4]{7}$ sur $\mathbb{Q}$ est une extension de degré 4 de $\mathbb{Q}$ puisque $P$, de degré 4, est irréductible.
   De plus $X^2+1$ est un polynôme irréductible sur $\mathbb{Q}(\sqrt[4]{7})$ car ses racines sont imaginaires pures. Comme $X^2+1$ est annulateur de $i$, finalement $[\mathbb{Q}(\sqrt[4]{7})(i) : \mathbb{Q}(\sqrt[4]{7})] = 2$.
   Par multiplicativité du degré dans la tour d'extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{7}) \subset \mathbb{Q}(\sqrt[4]{7})(i)$ :

$$\begin{aligned}[\mathbb{Q}(\sqrt[4]{7},i) : \mathbb{Q}] &= [\mathbb{Q}(\sqrt[4]{7})(i) : \mathbb{Q}(\sqrt[4]{7})] \cdot [\mathbb{Q}(\sqrt[4]{7}) : \mathbb{Q}] \\ &= 2 \times 4 \\ &= 8\end{aligned}$$

4. $P(X) = (X-\sqrt{2})(X+\sqrt{2})(X-\sqrt{3})(X+\sqrt{3})(X-\sqrt{5})(X+\sqrt{5})$.
   À faire : le degré de cette extension est de degré 8.

5. $P(X) = \left(X - \sqrt{i}\right)\left(X + \sqrt{i}\right)\left(X - \sqrt{-i}\right)\left(X + \sqrt{-i}\right)$ avec $\sqrt{i} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$ et $\sqrt{-i} = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$.
   Le corps de décomposition de $P$ sur $\mathbb{Q}$ est $\mathbb{Q}(\sqrt{2},i) = \mathbb{Q}(\sqrt{2})(i)$. Il s'agit d'une extension de degré 4.

## Exercice 4

Soit $L$ un corps de décomposition de $P \in K[X]$ sur $K$.
Montrez que

1. $[L : K] \leqslant \deg(P)!$,
2. $[L : K] | \deg(P)!$.

Correction exercice 4

Notons $n = \deg(P)$, $(x_1, \ldots, x_n) \in L^n$ les racines deux à deux distinctes ou non de $P$ dans $L$.

1. Notons, pour tout $n \in \mathbb{N}^*$, $\mathscr{P}(n)$ : « $\forall P \in K_n[X]$, $[L_P : K] \leqslant \deg(P)!$ » où $L_P$ désigne le corps de rupture de $P$ sur $K$.

   Démontrons par une récurrence forte que $\mathscr{P}(n)$ est vraie pour tout $n \in \mathbb{N}^*$.

   * Démontrons que $\mathscr{P}(1)$ est vraie.
     Si $P$ est une constante ($\deg(P) < 1$), alors son corps de rupture peut être vu comme $K$ lui-même donc $[L_P : K] = 1 \leqslant n!$.
     Si $\deg(P) = 1$, alors : $\exists(\alpha,\beta) \in K^2$, $P(X) = \alpha(X - \beta)$. Dans ce cas nécessairement $\beta \in K$ donc $L_P = K$ et à nouveau $[L_P : K] = 1 \leqslant n!$.
     Dans tous les cas $\mathscr{P}(1)$ est vraie.
   * Soit $n \in \mathbb{N}^*$. Supposons que $\mathscr{P}(k)$ est vraie pour tout $k \in [\![1,n]\!]$ et démontrons qu'alors nécessairement $\mathscr{P}(n+1)$ est vraie.
     Soit $P \in K_{n+1}[X]$.

     Si $P \in K_n[X]$, alors d'après l'hypothèse de récurrence : $[L_P : K] \leqslant n!$. Et donc, *a fortiori*, $[L_P : K] \leqslant (n+1)!$.

     Supposons donc dorénavant que $\deg(P) = n+1$.
     Notons $a_1, \ldots, a_{n+1}$ les racines de $P$ répétées autant de fois que l'indique leur ordre de multiplicité.
     Nous avons la tour d'extension suivante : $K \subset K(a_1, \ldots, a_n) \subset L_P$.
     Or $K(a_1, \ldots, a_n)$ est le corps de décomposition de $\frac{P}{X - a_{n+1}}$ (qui est de degré $n$) sur $K$, donc, d'après l'hypothèse de récurrence, $[K(a_1, \ldots, a_n) : K] \leqslant n!$.
     D'autre part $P$ est polynôme annulateur de $a_{n+1}$ sur $K$ donc $K(a_{n+1})$ est de degré au plus $n+1$ sur $K$ donc sur $K(a_1, \ldots, a_n)$. Ainsi $[L_P : K(a_1, \ldots, a_n)] \leqslant n+1$.

Finalement par multiplicativité des degrés pour la tour d'extension précédemment considérée : $[L_P : K] = [L_P : K(a_1,\dots,a_n)] \cdot [K(a_1,\dots,a_n) : K] \leqslant (n+1) \times n!$.
Autrement dit $\mathscr{P}(n+1)$ est vraie.

Nous avons démontré par récurrence sur $n \in \mathbb{N}^*$ que
$\forall P \in K_n[X]$, $[L_P : K] \leqslant \deg(P)!$.

Exemple de polynôme pour lequel il y a égalité : $P(X) = X^3 - 1$.

2. Même méthode de récurrence. L'idée pour l'hérédité. Il faut prendre une racine de $P$ et distinguer est dans $L$ ou n'est pas dans $L$. On considère dans ce second cas la tour d'extension : $\mathbb{Q} \subset \mathbb{Q}(a) \subset L$. Puis on considère $\mu$ polynôme minimal de $a$ sur $\mathbb{Q}$ et on utilise l'hypothèse de récurrence.

# IX Extension normale.

Définition 6

On dit qu'une extension $L|K$ de corps est normale si pour tout polynôme irréductible de $K[X]$, s'il admet une racine dans $L$ alors $P$ est scindé dans $L$.

Théorème 2

Soit $L|K$ une extension de corps.
Les assertions suivantes sont équivalentes.

1. $L|K$ est un extension finie et normale.
2. $L$ est le corps de décomposition d'un polynome sur $K$.

Démonstration 2

1. $\Leftarrow$.
   Soient $(x_1,\dots,x_n)$ une $K$-base de $L$.
   Notons $P_i = \mu_{x_i,K}$ comme $x_i \in L$ et $L|K$ normale, toutes les racines de $P_i$ sont dans $L$.
   $L = K(x_1,\dots,x_n)$ et donc $L$ sera le corps de décomposition de $P_1 \dots P_n$.
2. $\Rightarrow$ Soit $P \in K[X]$ et $L$ le corps de décomposition de $P$ sur $K$.
   $x_1,\dots,x_n$ les racines de $P$ alors $L = K(x_1,\dots,x_n)$ est une extension finie.

Soit $Q \in K[X]$ irréductible et $y_1$ et $y_2$ deux racines avec $y_1$ dans $L$. Démontrons qu'alors $y_2 \in L$.

$K(y_1$ et $K(y_2$ sont deux corps de rupture de $Q$ sur $K$ donc ils ont $K$-isomorphes.

De plus $L(y_1)$ est le corps de décomposition de $P$ sur $K(y_1)$. De même avec indice 2.

Puisque $K(y_1) \sim K(y_2)$ $L(y_1)$ est un corps de décomposition de $P$ sur $K(y_2)$.

Du fait de l'unicité des corps de décompositions $L(y_1) \sim L(y_2)$ alors ils sont uniques.

On en déduit $[L(y_2) : L] = 1$. et donc $y_2 \in L$.

Définition 7

Fermeture normale d'une extension.

# X $K$-morphismes.

### Éléments conjugués.

Définition 8

Proposition 6

$K$-morphismes et nombres conjugués.

### Plongements.

Définition 9

En particuliers si $L$ est une extension de $K$ alors les $K$-morphismes de $L$ dans $\Omega$ sont des plongements de $L$ dans $\Omega$.

Proposition 7 - nombre de plongements.

Exercice 5

Exo 14.

Correction exercice 5

Soit $x \in L$ extension de $K$ et $x \notin K$.
$x$ existe car extension de degré deux.
Soit $P$ irréductible de $x$ sur $K$. . Nécessairement $degP = 2$ car sinon $x \in K$
Notons $P = X^2 + ax + b$.
L'autre racine est alors dans $L$ puisque la somme des racines égale $a$.

## Exercice 6

17

Correction exercice 6

1. Soit $\sigma$ $\mathbb{Q}$-morphisme.

   (a) $\sigma(7+3i) = 7+3\sigma(i)$. $\sigma(i)$ est un conjugué de $i$ donc $\pm i$. Comme $-i \in \mathbb{Q}(7+3i)$ il y a deux $\mathbb{Q}$-morphismes possibles : $\sigma(i) = i$ ou $\sigma(i) = -i$.

   (b) $X^4 - 2 = (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X - i\sqrt[4]{2})(X + i\sqrt[4]{2})$.
   Donc (évidemment $\sigma(1) = 1$) et $\sigma(\sqrt[4]{2}) \in \{\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}\}$.
   On obtient donc 4 $\mathbb{Q}$-morphismes mais seuls deux d'entre eux sont des automorphismes (c'est-à-dire des endomorphismes).