jeudi 24 janvier 2019
à propos des extensions de corps

Exercice 1 Racines des polynômes de degré 3

Montrer que l'unique racine réelle de $X^3 - X - 1$ est :

$$\sqrt[3]{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{23}{27}}} + \sqrt[3]{\frac{1}{2} - \frac{1}{2}\sqrt{\frac{23}{27}}} \ .$$

Indication : chercher une solution sous la forme $x = u + v$.

Exercice 2 *a) Vérifier que les anneaux suivants sont des corps :*

A) exemple (non commutatif) : le corps gauche des quaternions :

$$\mathbb{H} := \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \ : \ a, b \in \mathbb{C} \right\} \ .$$

B) Exemples commutatifs : $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ *(p premier),* $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(i), \mathbb{C}(X, Y)$.

C) $\mathbb{C}((T)) = \{\sum_{n \geq n_0} a_n T^n \ : \ n_0 \in \mathbb{Z}, {}^\forall n \geq n_0, \ a_n \in \mathbb{C}\}$.

D) $\mathbb{Z}[i]/7, \mathbb{Z}[\sqrt{2}]/3, \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \ : \ b \in \mathbb{F}_5 \right\}$ *sont des corps finis à* $49, 9$ *et* 25 *éléments.*

b) Montrer que si p est un nombre premier impair, alors $\mathbb{Z}[i]/(p)$ est un corps fini à p^2 éléments si $p = -1 \bmod 4$, un anneau isomorphe à $\mathbb{F}_p \times \mathbb{F}_p$ si $p = 1 \bmod 4$. Et si $p = 2$?

Exercice 3 Polynôme minimal

a) Soit $P \in K[X]$. Montrer que $K[X]/(P)$ est un $K-$espace vectoriel de dimension $d = \deg P$ (*une base est donnée par les* $X^k \bmod P$, $0 \leq k < \deg P$).

b) Soit $K \leq E$ une extension de corps. Soit $x \in E$. Montrer que sont équivalentes :

(i) il existe $0 \neq P \in K[X]$ tel que $P(x) = 0$;

(ii) $\dim_K K[x]$ est finie ;

(iii) $K[x] = K(x)$.

Dans ce cas, on dit que x est *algébrique sur* K.

c) Montrer que si $K \leq L$ sont des corps et si $x, y \in L$ sont algébriques sur K, alors $x+y$, xy et x/y aussi (si $y \neq 0$).

d) Montrer que $e^{2i\pi/103}$ est algébrique sur $\mathbb{Q}$, $\cos(2\pi/7)$ aussi, $\sum_{k\geq 0} \frac{1\times\ldots\times(2k-1)}{2\times\ldots\times(2k)} t^k$ est algébrique sur $\mathbb{C}(t)$ (*indication : en effet c'est* $(1-t)^{-1/2}$). Déterminer à chaque fois leur polynôme minimal !

e) Montrer que si $x \in \mathbb{C}$, alors x est entier sur $\mathbb{Z} \Leftrightarrow P_x \in \mathbb{Z}[X]$, où P_x est le polynôme minimal unitaire sur $\mathbb{Q}$.

f) Trouver le polynôme minimal de $\sqrt[3]{2} + j$ sur $\mathbb{Q}$.

Exercice 4 Polynômes irréductibles.

a) Soit $P \in K[X]$. Montrer que P est irréductible $\Leftrightarrow$ $K[X]/(P)$ est un corps.

b) Rappelons que l'anneau $K[X]$ est euclidien, donc principal donc factoriel (donc intégralement clos).

Rappels sur les anneaux :

Définition 1 Soit A un anneau intègre.
On dit que A est *euclidien* s'il existe une fonction $q : A \setminus \{0\} \to \mathbb{N}$ telle que :

$$^{\forall} a, b \in A,\ b \neq 0, {}^{\exists} q, r \in A,\ a = bq + r$$

$$\text{avec } r = 0 \text{ ou } r \neq 0 \text{ et } q(r) < q(b).$$

On dit que A est *principal* si tout idéal de A peut être engendré par un élément.
On dit que $0 \neq a \in A$ est irréductible si a n'est pas inversible et si $bc = a, b,\ c \in A \Rightarrow b$ ou c inversible.
On dit que A est *factoriel* si tout $a \neq 0$ dans A s'écrit :

$$a = up_1....p_s$$

avec u inversibles et les p_i irréductibles et si cette écriture est unique au sens suivant :

$$a = up_1...p_s = vp'_1...p'_{s'}$$

$\Rightarrow s = s'$ et il existe $\sigma \in \mathfrak{S}$ tel que $p'_i = u_i p_{\sigma(i)}$ pour un certain u_i inversible

$$\text{euclidien} \Longrightarrow \text{principal} \Longrightarrow \text{factoriel} \Longrightarrow \text{intégralement clos}$$

$$\mathbb{R}[X,Y]/(X^2+Y^2+1) \xleftarrow[\times\times]{} \mathbb{R}[X,Y] \xleftarrow[\times\times]{} \mathbb{Z}[i\sqrt{5}]$$

c) Montrer que si A est factoriel, alors l'anneau $A[X]$ aussi. Plus précisément les irréductibles de $A[X]$ sont les $a \in A$ irréductibles et les $P \in A[X]$ de degré > 0, tels que $c(P) \sim 1$ et P est irréductible dans $K[X]$ où $c(P)$ est le pgcd des coefficients de P (*défini à multiplication par un inversible près*). *Indication : montrer d'abord que* $c(PQ) = c(P)c(Q)$).

Par exemple : si $P \in \mathbb{Z}[X]$, alors P irréductible sur $\mathbb{Z} \Rightarrow P$ irréductible sur $\mathbb{Q}$.

d) **Technique de la réduction mod p.** Montrer que $X^4 - X - 1$ est irréductible sur $\mathbb{Q}$ en réduisant $\bmod 2$. Mais montrer que $X^4 + 1$ est irréductible sur $\mathbb{Q}$ alors qu'il est réductible $\bmod p$ pour tout p.

e) Montrer que le déterminant vu comme polynôme dans

$$K[X_{ij} \ : \ 1 \leq i, j \leq n]$$

est irréductible.

f) Montrer que le polynôme $X^3 + Y^3 - 1$ est irréductible dans $\mathbb{C}[X, Y]$.

Exercice 5 Corps de rupture, corps de décomposition

a) Soit K corps et soit $P \in K[X]$ irréductible. Justifier l'existence et l'unicité *(à isomorphisme près)* d'un *corps de rupture* pour P.

b) Soit $0 \neq P \in K[X]$. On suppose que $E \geq K$ est un corps où P est scindé : $P = c(X - x_1)...(X - x_n)$, $c \in K^\times$. On dit que $K(x_1, ..., x_n)$ est le *corps de décomposition* de P dans E. Montrer qu'un corps de décomposition pour un polynôme $P \in K[X]$ existe toujours et est unique (*à isomorphisme près*). *Pour l'existence, procéder par récurrence sur* $\deg P$. *Pour l'unicité :*

supposons $P = X^n - a_1 X^{n-1} + ... + (-1)^n a_n \in K[X]$. *Supposons aussi qu'il existe* L_1, L_2 *des corps contenant* K, $x_1, .., x_n \in L_1$, $y_1, ..., y_n \in L_2$ *tels que* $P = (X - x_1)...(X - x_n)$ *dans* $L_1[X]$ *et* $P = (X - y_1)...(X - y_n)$ *dans* $L_2[X]$ *et* $L_1 = K(x_1, ..., x_n)$ *et* $L_2 = K(y_1, ..., y_n)$.

Soit I_1 *l'idéal des polynômes* $P \in K[X_1, ..., X_n]$ *tels que* $P(x_1, ..., x_n) = 0$ *dans* L_1. *Soit* I_2 *l'idéal des polynômes* $P \in K[Y_1, ..., Y_n]$ *tels que* $P(y_1, ..., y_n) = 0$ *dans* L_2. *Soit* M *un idéal maximal de l'anneau*

$$K[X_1, ..., X_n, Y_1, ..., Y_n]$$

qui contient $I_1 + I_2$ *(aucun problème car* $1 \notin I_1 + I_2$ [*] *et car* $K[X, Y]/I_1 + I_2$ *est de dimension finie, il suffit donc de choisir* $M \geq I_1 + I_2$ *tel que* $\dim_K K[X, Y]/M$ *est minimal* ≥ 1*).*

---

[*]. en effet, si $\phi_1 : K[X_1, ..., X_n] \to K$ est une forme linéaire de noyau contenant I_1 (idem pour ϕ_2), alors on pose $\phi : K[X_1, ..., X_n, Y_1, ..., Y_n] \to K$, $cX^a Y^b \to c\phi_1(X^a)\phi_2(Y^b)$. On vérifie facilement que $\phi(A(X)B(Y)) = \phi_1(A(X))\phi_2(B(Y))$ et que $I_1 + I_2$ est dans le noyau de ϕ. Si $\phi_1, \phi_2 \neq 0$, il est clair que $\phi \neq 0$ donc $I_1 + I_2 \neq k[X, Y]$ ...

Alors $L_1 \simeq K[X]/I_1 \xrightarrow{\varphi} K[X,Y]/M$, $P \bmod I_1 \mapsto P \bmod M$ *est un morphisme* $K-$*linéaire de corps donc injectif. Or* $L = K[X,Y]/M$ *est engendré par les* $\overline{X_i}$ *et les* $\overline{Y_j}$, *classes des* $X_i, Y_j \bmod M$.
Dans $L_1[X]$, *on a* $(X-x_1)...(X-x_n) = X^n + \sum_{k=1}^n \sigma_k(x_1,...,x_n)(-1)^k X^{n-k} = P(X)$
Donc $\sigma_k(x_1,...,x_n) = a_k \Rightarrow \sigma_k(X_1,...,X_n) = a_k \bmod M$i.e. $\sigma_k(\overline{X_1},...,\overline{X_n}) = a_k$ *dans* L. *De même,* $\sigma_k(\overline{Y_1},...,\overline{Y_n}) = a_k$ *dans* L *et donc*

$$\prod_i (X - \overline{X_i}) = \prod_i (X - \overline{Y_i})$$

dans $L[X]$ *et donc* $\{\overline{X_i} \,:\, 1 \leq i \leq n\} = \{\overline{Y_i} \,:\, 1 \leq i \leq n\}$. *Or* $\overline{X_i} \in \operatorname{Im}\varphi$. *Donc* $\overline{Y_i}$ *aussi et* φ *est un isomorphisme. De même, on a un isomorphisme* $L_2 \simeq K[X,Y]/M$.

Exercice 6 Automorphismes de corps.

a) Montrer que si K est de caractéristique p, $x \mapsto x^p$ est un endomorphisme du corps K.

b) Montrer :
- $\mathrm{Aut}(\mathbb{R}) = 1$,
- $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \{\mathrm{Id}, a + b\sqrt{2} \mapsto a - b\sqrt{2}\}$,
- $\mathrm{Aut}\mathbb{C}(t) \simeq \mathrm{PGL}_2(\mathbb{C})$ *(indication : considérer les automorphismes* $t \mapsto \frac{at+b}{ct+d}$ *lorsque* $ad - bc \neq 0$*)* ,
- $\mathrm{Aut}\mathbb{Q}(\sqrt[3]{2}) = \{\mathrm{Id}\}$,
- $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, j) = \langle s, t\rangle \simeq \mathfrak{S}_3$, où s est le $\mathbb{Q}(j)$-automorphisme qui envoie $\sqrt[3]{2}$ sur $j\sqrt[3]{2}$ et t la conjugaison complexe.

c) Soit $K \leq L$ une extension algébrique i.e. *tous les éléments de* L *sont algébriques sur* K. Montrer que si f est un endomorphisme $K-$linéaire du corps L, alors f est un automorphisme de corps !

d) **Extensions galoisiennes.**
Soit K un corps. Si $G \leq \mathrm{Aut}K$ est un sous-groupe on note K^G les éléments de K fixés par G.
Une extension galoisienne finie est une extension de corps de la forme :

$$K^G \leq K$$

où $G \leq \mathrm{Aut}K$ est un sous-groupe fini.
Montrer que les extensions suivantes sont galoisiennes :
$\mathbb{F}_{q^n}/\mathbb{F}_q$ (*indication : dans ce cas,* $G = \langle f\rangle$ *où* $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, $x \mapsto x^q$),
$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$, $\mathbb{C}(t)/\mathbb{C}(t + t^{-1})$.
Montrer que $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ et $\mathbb{F}_p(X)/\mathbb{F}_p(X^p)$ ne le sont pas.

Exercice 7 Correspondance de Galois

a) Si G est un groupe, si $\sigma_1, ..., \sigma_n : G \to K^\times$ sont des morphismes de groupes deux à deux distincts, alors montrer que les σ_i sont $K-$linéairement indépendantes comme fonctions de G dans K. *Théorème d'indépendance des caractères d'Artin.*

b) Montrer que si $s_1, ..., s_m : K \to K'$ sont m morphismes de corps distincts, alors si $K_0 := K^{\{s_1,...,s_m\}} = \{x \in K \ : \ s_1(x) = ... = s_m(x)\}$, on a :

$$[K : K_0] \geq m \ .$$

Indication : si $e_1, ..., e_n$ est une famile génératrice de K comme K_0-ev, considérer la matrice $(s_i(e_j))_{\substack{1\leq i\leq m \\ 1\leq j\leq n}}$.

c) Montrer que si $G \leq \mathrm{Aut}(K)$ est un sous-groupe fini, alors $[K : K^G] = |G|$.

d) Soit $K' \leq K$ une extension finie. Montrer que $|\mathrm{Aut}_{K'}K| \leq [K : K']$ avec égalité si et seulement si l'extension K/K' est galoisienne *(indication : $K' \leq K^{\mathrm{Aut}_{K'}K} \leq K$ et comparer les degrés ...)*.

Montrer que $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ n'est pas galoisienne.

e) Démontrer le théorème suivant :

Théorème Soit E/F une extension galoisienne de groupe G.

i) On a deux bijections réciproques :

$$\{\text{sous-groupes } H \leq G\} \overset{1:1}{\longleftrightarrow} \{\text{corps intermédiaires } F \leq B \leq E\}$$

$$H \longmapsto E^H$$

$$\mathrm{Gal}(E/B) \longmapsto B \ .$$

ii) L'extension E/B est galoisienne et $[E : B] = |\mathrm{Gal}(E/B)|$;

iii) $[B : F] = |G/\mathrm{Gal}(E/B)|$;

iv) l'extension B/F est galoisienne si et seulement si $\mathrm{Gal}(E/B) \lhd G$. Dans ce cas, $\mathrm{Gal}(B/F) \simeq G/\mathrm{Gal}(E/B)$.

v) Déterminer les sous-corps de $\mathbb{Q}(j, \sqrt[3]{2})$.

Exercice 8 le corps $\mathbb{C}$ est algébriquement clos.

Soit Q un polynôme irréductible sur $\mathbb{R}$. Soit K un corps de décomposition de Q sur $\mathbb{C}$ *c-à-d* $Q = (X - x_1)...(X - x_n)$ et $K = \mathbb{C}(x_1, ..., x_n)$.

a) Monter que l'extension $K/\mathbb{R}$ est galoisienne. Notons G son groupe.

b) Soit P un $2-$Sylow de G. Montrer que $K^P = \mathbb{R}$ *(Indication :* $[K^P : \mathbb{R}]$ *est impair)* et que G est un $2-$groupe.

c) Supposons qu'il existe $H \leq \mathrm{Gal}(K/\mathbb{C})$ d'indice 2. Montrer qu'alors $K^H/\mathbb{C}$ est de degré 2 *absurde ...*

d) Conclure.