Feuille n° 3
jeudi 16 janvier 2020
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 $\cos\left(\frac{2\pi}{17}\right)$

Soit $\zeta = e^{\frac{2i\pi}{17}}$. On note $G = \mathrm{Aut}(\mathbb{Q}(\zeta))$ et θ l'automorphisme $\mathbb{Q}(\zeta) \longrightarrow \mathbb{Q}(\zeta)$

$$\zeta \longmapsto \zeta^3 \, .$$

Si $H \leq G$ est un sous-groupe, on posera

$$\zeta_H = \sum_{h \in H} h(\zeta) \ .$$

On notera H_d l'unique sous-groupe de G d'ordre d si $d|16$.

a) Soit $y = e^{\frac{2i\pi}{5}}$. Vérifier que

$$(X - (y + y^{-1}))(X - (y^2 + y^{-2})) = X^2 + X - 1$$

et en déduire une expression de $\cos\left(\frac{2\pi}{5}\right) = \frac{y+y^{-1}}{2}$ avec des radicaux.

b) Déterminer le polynôme minimal de ζ sur $\mathbb{Q}$. En déduire que θ est bien défini et que c'est un automorphisme.

c) Montrer que $G = \langle\theta\rangle$.

d) Montrer que pour tout $H \leq G$, $\mathbb{Q}(\zeta_H) = \mathbb{Q}(\zeta)^H$ et en déduire que $\theta(\zeta_H) \in \mathbb{Q}(\zeta_H)$.

e) Exprimer ζ_{H_8} et $\theta(\zeta_{H_8})$. *Indication :* $(X - \zeta_{H_8})(X - \theta(\zeta_{H_8})) = X^2 + X - 4$.

f) Exprimer ζ_{H_4} et $\theta^2(\zeta_{H_4})$. *Indication :* $(X - \zeta_{H_4})(X - \theta^2(\zeta_{H_4})) = X^2 - \theta(\zeta_{H_8})X + 1$. En déduire $\theta(\zeta_{H_4})$.

g) Exprimer ζ_{H_2} et $\theta^4(\zeta_{H_2})$. *Indication :* $(X - \zeta_{H_2})(X - \theta^4(\zeta_{H_2})) = X^2 - \zeta_{H_4}X + \theta(\zeta_{H_4})$.

h) Montrer que $\cos\left(\frac{2\pi}{17}\right) =$

$$-\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}} \ .$$

Exercice 3 *Vérifier que les anneaux suivants sont des corps :*

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

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

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

Exercice 4 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) Trouver le polynôme minimal de $\sqrt[3]{2} + j$ sur $\mathbb{Q}$ *(indication : trouver d'abord un polynôme rationnel de degré* 6 *qui annule* $\alpha = \sqrt[3]{2} + j$ *puis montrer que* $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{2}, j)$ *en considérant le pgcd des polynômes* $X^2 + X + 1$ *et* $(\alpha - X)^3 - 2$*).*

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*). *Indications : pour l'existence, procéder par récurrence sur* $\deg P$ *; pour l'unicité, supposons* P *unitaoire et 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 m un idéal maximal de $L_1 \otimes_K L_2$ [†], vérifier alors que $L_1 \simeq \frac{L_1 \otimes_K L_2}{m} \simeq L_2$.

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) *Théorème d'indépendance des caractères d'Artin.* 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.

†. On posera $L_1 \otimes_K L_2 = K[X_1, ..., X_n, Y_1, ..., Y_n]/I_1 + I_2$ où I_1 (*respectivement* I_2) est l'idéal des polynômes qui s'annulent quand on remplace les X_i par les x_i (*respectivement* les Y_i par les y_i)

Indication : supposons que $\lambda_1\sigma_1 + ... + \lambda_n\sigma_n = 0$ pour certains $\lambda_i \in K$; alors comme les σ_i sont des morphismes de groupes, on a :

$$^\forall g \in G,\ \lambda_1\sigma_1(g)\sigma_1 + ... + \lambda_n\sigma_n(g)\sigma_n = 0$$

donc si on choisit g tel que $\sigma_1(g) \neq \sigma_2(g)$, on a :

$$\lambda_2(\sigma_2(g) - \sigma_1(g))\sigma_2 + ... + \lambda_n(\sigma_n(g) - \sigma_1(g))\sigma_n = 0\,...$$

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 $[K : K^G] = |G|$.
Indication : montrer que $[K : K^G] \geq |G|$ grâce à la question précédente puis pour l'autre inégalité, considérer la matrice $(\sigma_i(e_j))_{\substack{1\leq i\leq g\\1\leq j\leq n}}$ si $\{\sigma_1, ..., \sigma_g\} = G$ et si $e_1, ..., e_n$ est une famille d'éléments de K linéairement indépendants sur K^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 ...).*

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

f) Soit $F \leq E$ une extension galoisienne de groupe G.
Montrer que si $H_1, H_2 \leq G$, alors $E^{H_1} = E^{H_2} \Leftrightarrow H_1 = H_2$.
Montrer que si $F \leq B \leq E$ est un corps intermédiaire alors il existe $H \leq G$ tel que $B = E^H$ *(indication : poser $H = \mathrm{Aut}_B E$ et utiliser que $B^{\sigma_1,..\sigma_r} = F$ pour un système complet de représentants $\{\sigma_1, ..., \sigma_r\}$ de G/H ...)*

g) Démontrer le théorème suivant :
Théorème Soit E/F une extension galoisienne de groupe G.

i) On a deux bijections réciproques :

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

$$H \longmapsto E^H$$

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

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 $\mathrm{Gal}(E/B) \triangleleft G$. Dans ce cas, $\mathrm{Gal}(B/F) \simeq G/\mathrm{Gal}(E/B)$.

h) *Application.* 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) En utilisant qu'un $2-$groupe a toujours un sous-groupe d'indice 2 *(le vérifier)*, conclure.

Exercice 9 Sur les polynômes cyclotomiques

Soit $1 \leq n \in \mathbb{N}$. On pose :

$$\Phi_n(X) = \prod_{\substack{k=1 \\ \mathrm{pgcd}(k,n)=1}}^{n} (X - e^{\frac{2ik\pi}{n}}) = \prod_{\substack{\zeta \in \mathbb{C}^\times \\ \text{d'ordre } n}} (X - \zeta)$$

le $n-$ième polynôme cyclotomique.

a) Vérifier que Φ_n est un polynôme unitaire à coefficients entiers de degré $\varphi(n)$ *Indication : on peut faire une division euclidienne dans* $\mathbb{Z}[X]$ *par un polynôme unitaire ....*

b) Montrer que

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu\left(\frac{n}{d}\right)}$$

où μ est la fonction de Möbius [†]

c) Soit ζ_n une racine primitive $n^{\text{ème}}-$de l'unité. Soit P le polynôme minimal unitaire de P sur $\mathbb{Q}$. Montrer que $P|\Phi_n$ et en déduire que P est à coefficients entiers.

†.

$$\mu(p_1^{a_1}...p_r^{a_r}) = \begin{cases} 0 & \text{si l'un des } a_i \geq 2, \\ (-1)^r & \text{sinon.} \end{cases}$$

d) Si p est un nombre premier, montrer que $P(\zeta_n^p) = 0 \bmod p\mathbb{Z}[\zeta_n]$.

e) Montrer que le discriminant du polynôme $X^n - 1$ est

$$(-1)^{\frac{(n-1)(3n-2)}{2}} n^n \ .$$

f) En déduire que si $P(\zeta_n^p) \neq 0$, alors $p|n$. *Indication : si on note $z_1, ..., z_r$ les racines de p, alors $P(\zeta_n^p) = (\zeta_n^p - z_1)...(\zeta_n^p - z_r)$ qui (si c'est non nul) divise*

$$\prod_{1 \leq k < l \leq n} (\zeta_n^k - \zeta_n^l)^2 \, ,$$

discriminant de $X^n - 1$ dans $\mathbb{Z}[\zeta_n]$.

g) En déduire que si p est premier avec n, alors ζ_n^p est encore une racine de P puis que $\Phi_n = P$ est irréductible sur $\mathbb{Q}$.

h) Montrer que si a est premier avec n alors l'application

$$\theta_a : \begin{cases} \mathbb{Q}[\zeta_n] \longrightarrow \mathbb{Q}[\zeta_n] \\ \\ R(\zeta_n) \longmapsto R(\zeta_n^a) \end{cases}$$

est bien définie et est un automorphisme de corps.

i) Montrer que $(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathrm{Aut}(\mathbb{Q}(\zeta_n))$ est un isomorphisme de groupes.

$$a \longmapsto \theta_a$$

j) *Application.* Soit $\rho : \mathfrak{S}_n \to \mathrm{GL}_N(\mathbb{C})$ un morphisùme de groupes. Soit $\sigma \in \mathfrak{S}_n$ une permutation d'ordre m. Montrer que $\chi_\rho(\sigma) = \mathrm{tr}(\rho(\sigma)) \in \mathbb{Q}(\zeta_m)$ et que c'est un entier algébrique. Montrer que si a est premier à m, alors σ^a etσ sont conjuguées dans $\mathfrak{S}_n$. En déduire que $^\forall a \in (\mathbb{Z}/m\mathbb{Z})^\times$, $\theta_a(\chi_\rho(\sigma)) = \chi_\rho(\sigma)$ puis que la table des caractères de $\mathfrak{S}_n$ est à coefficients entiers.