TD n°12 : Théorie de Galois

Exercice 1. [Théorème de d'Alembert-Gauss] Le but de cet exercice est de montrer que tout polynôme non constant à coefficients dans $\mathbf{C}$ admet une racine dans $\mathbf{C}$, en utilisant comme seul résultat d'analyse le fait que tout polynôme réel de degré impair admet une racine réelle.

Soit $P \in \mathbf{C}[X]$ non constant.

1. Montrer qu'on peut supposer que P est à coefficients réels.

   On note maintenant $d = 2^n(2m+1)$ le degré de P, et on va raisonner par récurrence sur n. On écrit $P = \ell \cdot \prod_{i=1}^{d}(X - x_i)$ dans un corps de décomposition de P et on pose, pour $i < j$ et pour $\lambda \in \mathbf{R}$, $f_{ij}(\lambda) = x_i + x_j + \lambda x_i x_j$.
2. Montrer qu'on peut appliquer l'hypothèse de récurrence au polynôme
$$Q_\lambda = \prod_{i<j}(X - f_{ij}(\lambda)).$$
3. En déduire qu'il existe $i < j$ tels que x_i et x_j sont dans $\mathbf{C}$.
4. Conclure.

Exercice 2. [Discriminant et résultant] Soient $P = a_0X^n + \cdots + a_n \in k_n[X]$ et $Q = b_0X^m + \cdots + b_m \in k_m[X]$ deux polynômes de degrés respectifs n et m. On définit $\mathrm{Res}(P,Q)$ comme le déterminant de l'application linéaire $\varphi : \begin{array}{ccc} k_{m-1}[X] \times k_{n-1}[X] & \longrightarrow & k_{n+m-1}[X] \\ (U,V) & \longmapsto & UP+VQ \end{array}$ calculé dans les bases respectives
$$((X^{n-1},0),(X^{n-2},0),\cdots,(X,0),(1,0),(0,X^{m-1}),\cdots,(0,1))$$
et $(X^{n+m-1},\cdots,X,1)$.

1. À quelle condition sur (P,Q) l'application φ est-elle bijective ?
2. Si $P \in k[X]$, on note $D(P) = \mathrm{Res}(P,P')$. Calculer $D(P)$ pour P de degré 2 et 3. Qu'observe-t-on ?
3. Soient $\underline{\alpha} = (\alpha_1,\cdots,\alpha_n)$ et $\underline{\beta} = (\beta_1,\cdots,\beta_m)$ et u_0, v_0 des indéterminées, et soient $P = u_0(X-\alpha_1)\cdots(X-\alpha_n), Q = v_0(X-\beta_1)\cdots(X-\beta_m)$. On note $\mathrm{Res}(P,Q) = R(u_0,v_0,\underline{\alpha},\underline{\beta}) \in \mathbf{Z}[u_0,v_0,\underline{\alpha},\underline{\beta}]$.
   (a) Montrer que $\alpha_1 - \beta_1$ divise R.
   (b) En déduire que $R = F\prod_{i,j}(\alpha_i - \beta_j)$, avec $F \in \mathbf{Z}[u_0,v_0,\underline{\alpha},\underline{\beta}]$.
   (c) En comparant la partie homogène de plus haut degré en les indéterminées $\beta_1,\cdots,\beta_m$ de R et du produit $\prod_{i,j}(\alpha_i - \beta_j)$, en déduire que $F = u_0^m v_0^n$.
4. En déduire une façon de calculer le discriminant d'un polynôme $P \in k[X]$ sans avoir besoin de calculer ses racines.

Exercice 3. [Sous-corps d'un corps algébriquement clos] Soit Ω un corps algébriquement clos de caractéristique 0. Soit K un sous-corps de Ω tel que Ω/K est de degré fini. Le but de cet exercice est de montrer que $\Omega = K(\sqrt{-1})$.

1. Rappeler pourquoi Ω/K est galoisienne.

   On note i une racine de X^2+1 dans Ω et on pose $G = \mathrm{Gal}(\Omega/K(i))$. On suppose que G n'est pas trivial, et on fixe p un nombre premier qui divise l'ordre de G.

2. Montrer qu'il existe un sous-corps L de Ω, contenant $K(i)$, tel que Ω/L est galoisienne de degré p.
3. Montrer qu'il existe $a \in L$ tel que $P = X^p - a$ est irréductible dans $L[X]$ et que $\Omega = L[X]/(P)$.
4. On suppose ici que $p \neq 2$. Soit $\alpha \in \Omega$ une racine de P. Calculer $\prod_{\sigma \in \mathrm{Gal}(\Omega/L)} \sigma(\alpha)$ et exhiber une contradiction en prenant β une racine p-ième de α.
5. Conclure.
6. Montrer qu'un élément non trivial de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ d'ordre fini est nécessairement d'ordre 2.

Exercice 4. [Extensions monogènes] Dans un premier temps, on va montrer qu'une extension finie L/K de corps infinis est monogène (c'est-à-dire qu'il existe $\alpha \in L$ tel que $L = K[\alpha]$) si et seulement si elle ne possède qu'un nombre fini d'extensions intermédiaires.

1. On suppose que L/K est monogène, $L = K[\alpha]$. Si P est le polynôme minimal de α sur K, montrer qu'on a une application injective de l'ensemble des extensions intermédiaires de L/K dans l'ensemble des diviseurs unitaires de P dans $L[X]$.
2. Réciproquement, si L/K ne possède qu'un nombre fini d'extensions intermédiaires, en considérant $\alpha, \beta \in L$, montrer que $K(\alpha, \beta)$ est monogène (on pourra considérer les extensions de la forme $K(\alpha + t\beta)$ pour $t \in K$). En déduire que L est monogène.

   On va maintenant exhiber une extension finie L/K de corps infinis non monogène.
3. Soit K un corps de caractéristique $p > 0$. Expliquer pourquoi $P(X) = X^p + T$ est irréductible sur $K(T)$. Montrer qu'un corps de rupture de P en est aussi un corps de décomposition.
4. Soit $K = \mathrm{Frac}(\mathbb{F}_p[T, U])$ et L un corps de décomposition de $P(X) = (X^p - T)(X^p - U)$.
   (a) Montrer que $[L : K] = p^2$.
   (b) Montrer que si $x \in L$, alors $x^p \in K$.
   (c) En déduire que L/K n'est pas monogène.