Devoir à la maison

Partie I Soit $n \geq 1$ et $\chi \in \mathbb{C}$ une racine primitive n-ième de l'unité. Pour un corps K contenant χ et $a \in K$, on considère une racine b de $X^n - a$.

- Montrez que $K[b]$ est une extension galoisienne de K de degré un diviseur d de n avec $b^d \in K$.
- On suppose $n = p$ premier, montrez que $X^p - a$ est soit irréductible soit totalement décomposé. Que se passe-t-il si on ne suppose plus que $\chi \in K$?
- Pour L une extension normale de K dans $\mathbb{C}$ de groupe de Galois G, on note pour $a \in L$, $N_{L/K}(a) = \prod_{\sigma \in G} \sigma(a)$. Montrez que $N_{L/K}(a) \in K$.
- On suppose G cyclique engendré par σ. Montrez que pour $x \in L$, on a l'équivalence (**théorème de Hilbert 90**)
$$N_{L/K}(x) = 1 \Longleftrightarrow \exists y \neq 0 \text{ tel que } x = \frac{y}{\sigma(y)}$$
- Déduire de la question précédente qu'il existe $b \in L$ tel que $L = K[b]$ et $b^n \in K$.
- On se propose de prouver le résultat de la question précédente sans utiliser le théorème de Hilbert 90. Montrez que les valeurs propres de σ sont les racines n-ièmes de l'unité et conclure.

Partie II

- Soit $L = Dec_{\mathbb{F}_p}(X^n - 1)$. Montrer que $\mathrm{Gal}(L/\mathbb{F}_p)$ est isomorphe au sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par l'image de p. Montrer que le n-ième polynôme cyclotomique $\Phi_n(X)$ se décompose sur $\mathbb{F}_p$ en un produit de $\phi(n)/k$ facteurs irréductibles distincts, tous de degré k. Quel est cet entier k? En déduire une version faible du théorème de progression arithmétique, *i.e.* :
pour tout entier n il existe une infinité de nombres premiers p congrus à 1 modulo n.
- En déduire alors que pour G un groupe abélien fini, il existe une extension galoisienne cyclotomique, i.e. contenu dans un $\mathbb{Q}(\zeta_n)$ pour un certain n, K de $\mathbb{Q}$ de groupe de Galois G.

  Remarque: **Le théorème de Kronecker-Weber** affirme que toute extension abélienne est cyclotomique.

Partie III:

- On considère l'équation $x^2+y^2 = z^2$ avec $z \neq 0$. Soit alors $w = \frac{x+iy}{z} \in \mathbb{Q}[i]$. Montrez en utilisant le théorème de Hilbert 90 qu'il existe $(m, n) \in \mathbb{Z}^2$ tel que (x, y, z) est proportionnel à $(m^2 - n^2, 2mn, m^2 + n^2)$.
- On considère désormais l'équation diophantienne $x^2 + Axy + By^2 = z^2$ avec $A, B \in \mathbb{Z}$ tel que le discriminant $A^2 - 4B$ n'est pas un carré. Soit alors $w = \frac{x+ry}{z} \in \mathbb{Q}[r]$ où r est une solution de $r^2 - Ar + B = 0$. Montrez alors que (x, y, z) est proportionnel à $(m^2 - Bn^2, 2mn + An^2, m^2 + Amn, Bn^2)$.
- Soit plus généralement $x^2 + Axy + By^2 = Cz^2$ avec $A, B, C \in \mathbb{Z}$ avec $A^2 - 4B \notin (\mathbb{Q}^\times)^2$. Soit alors $w = \frac{x+ry}{z} \in \mathbb{Q}(r)$. On suppose que l'on connaît une solution (x_0, y_0, z_0) avec $z_0 \neq 0$ et soit $w_0 = \frac{x_0+ry_0}{z_0}$; en considérant w/w_0, trouvez en utilisant le théorème de Hilbert 90, toutes les solutions de cette équation.
- Comparez cette technique à la méthode géométrique.