

THÉORIE DE GALOIS

PARTIEL DU 10 MARS 2025. DURÉE 2H00.

Pas de documents autorisés.

Exercice 1. Questions de cours.

- i. Soit k un corps et n un entier d'image non nulle dans k . On note k_n le corps de décomposition du polynôme $X^n - 1$.
 - (a) Montrer que k_n/k est Galoisienne et construire un morphisme de groupes injectif $\chi_{n,k} : \text{Gal}(k_n/k) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$.
 - (b) Décrire $\chi_{n,\mathbb{R}}$ et $\chi_{n,\mathbb{F}_p}$, où p est un nombre premier.
 - (c) Montrer que $\chi_{n,k}$ est un isomorphisme si et seulement si le polynôme cyclotomique $\Phi_n \in \mathbb{Z}[X]$ est irréductible dans $k[X]$.
- ii. Montrer que pour tout groupe fini G , il existe une extension de corps K/k Galoisienne telle que $\text{Gal}(K/k) \simeq G$.

Exercice 2. Soit K un corps algébriquement clos de caractéristique 0, et soit $k \subset K$ un sous-corps tel que $[K : k]$ soit fini.

- i. Montrer que K/k est Galoisienne.

L'extension est séparable puisqu'on est en caractéristique 0. Elle est normale puisque K est algébriquement clos (tout polynôme minimal f_α est en particulier scindé dans $K[X]$).
- ii. Soit p un diviseur premier de $[K : k]$.
 - (a) Montrer qu'il existe une sous-extension $k \subset L \subset K$ telle que $[K : L] = p$.

L'ordre du groupe $\text{Gal}(K/k)$ est divisible par p , donc ce groupe contient un élément σ d'ordre p . Il suffit de poser $L = K^\sigma$ (pts fixes). Un théorème du cours implique que K/L est Galoisienne de groupe $\langle \sigma \rangle = \mathbb{Z}/p\mathbb{Z}$.
 - (b) Montrer que L contient les racines p -èmes de 1, et en déduire que $K = L(\alpha)$ avec $\alpha^p \in L$. On pose alors $a := \alpha^p$.

Soit ζ une racine p -ème primitive de 1 dans K . Le polynôme minimal de ζ divise $\Phi_p(X) = X^{p-1} + \dots + 1$, donc est de degré d premier à p . Comme $d = [L(\zeta) : L]$ divise $[K : L] = p$, il s'ensuit que $d = 1$ et donc $L(\zeta) = L$.

Comme K/L est une extension cyclique de degré p , on peut appliquer un théorème du cours qui dit que, puisque L contient les racines p -èmes de 1, alors K est de la forme $L(\alpha)$ comme voulu.

- (c) Notons $N_{K/L}(\alpha)$ le déterminant de la multiplication par α , vue comme endomorphisme L -linéaire de K . Montrer que $N_{K/L}(\alpha) = (-1)^{p-1}a$

On sait que la famille $1, \alpha, \dots, \alpha^{p-1}$ est une L -base de K . La multiplication par α dans cette base est la matrice “permutation” $(b_{ij})_{i,j}$ telle que $b_{21} = b_{32} = \dots = b_{p,p-1} = 1$ et $b_{1p} = a$. Son déterminant est $(-1)^p a$.

- (d) Montrer qu’il existe $\beta \in K$ tel que $\beta^p = \alpha$. De l’égalité $N_{K/L}(\beta)^p = (-1)^{p-1}a$, déduire que $p = 2$ et $a \in -(L^\times)^2$.

L’existence de β découle du fait que K est algébriquement clos. $N_{L/K}$ est une application multiplicative $K^\times \rightarrow L^\times$ (par multiplicativité du déterminant), donc on a bien $N_{K/L}(\beta)^p = N_{K/L}(\beta^p) = (-1)^{p-1}a$. Puisque a n’a pas de racine p -ème dans L , on doit avoir $(-1)^{p-1} = -1$, donc $p = 2$, ce qui implique alors $a = -N_{K/L}(\beta)^2 \in -(L^\times)^2$.

- iii. En conclure que $K = k$ ou $K = k(\sqrt{-1})$.

Supposons $k \neq K$. On peut alors appliquer les questions précédentes qui montrent l’existence d’une extension $k \subset L \subsetneq K$ telle que $K = L(\sqrt{-1})$. En particulier, on a $\sqrt{-1} \notin k$. On a donc l’équivalence $k \neq K \Leftrightarrow \sqrt{-1} \notin k$. Celle-ci, appliquée à $k(\sqrt{-1})$, montre que $K = k(\sqrt{-1})$.