EXAMEN

ALGÈBRE L3

Les notes de cours sont autorisées. La bonne présentation de la copie compte dans la note. Tous les anneaux sont commutatifs.

1. Un théorème de Galois

Le but de ce problème est de démontrer ce résultat de Galois :

> Théorème. Pour qu'une équation irréductible de degré premier soit soluble par radicaux, il faut et il suffit que deux quelconques des racines étant connues, les autres s'en déduisent rationnellement.

On voit $\mathfrak{S}_n$ comme le groupe des bijections de $\mathbf{Z}/n\mathbf{Z}$. Soit Aff_n l'ensemble des éléments de $\mathfrak{S}_n$ qui sont de la forme $x \mapsto ax + b$ avec $a, b \in \mathbf{Z}/n\mathbf{Z}$ et Trans_n ceux qui sont de la forme $\tau_b : x \mapsto x + b$ avec $b \in \mathbf{Z}/n\mathbf{Z}$.

1.1. Quel est le cardinal de Aff_n?

1.2. Montrer que Aff_n est un sous-groupe transitif de $\mathfrak{S}_n$.

1.3. Montrer que si $g \in \mathrm{Aff}_n$ fixe deux éléments distincts de $\mathbf{Z}/n\mathbf{Z}$, alors $g = \mathrm{Id}$.

1.4. Montrer que Aff_n est un groupe résoluble.

1.5. Montrer que le normalisateur de Trans_n dans $\mathfrak{S}_n$ est Aff_n (rappel : le normalisateur d'un sous-groupe H d'un groupe G est l'ensemble des $g \in G$ tels que $gHg^{-1} = H$).

On pourra montrer que si $g\tau_1 g^{-1} = \tau_b$, alors $g(x) = bx + g(0)$.

Soit K un corps et $P \in K[X]$ un polynôme irréductible et séparable de degré p premier. Soit F un corps de décomposition de P et $G = \mathrm{Gal}(F/K)$.

1.6. On suppose que $F = K(x)$ où x est une racine de P. Montrer que $G = \mathbf{Z}/p\mathbf{Z}$.

1.7. On suppose maintenant que $F = K(x, y)$ où x et y sont deux racines distinctes de P. Montrer que $[F : K] \leq p(p-1)$.

1.8. Montrer que G, vu comme sous-groupe de $\mathfrak{S}_p$, contient un cycle d'ordre p.

Date: 10 mai.

1.9. Soient σ et τ deux cycles d'ordre p contenus dans G. Montrer (en utilisant par exemple la question 1.7) qu'ils engendrent le même sous-groupe de G, et en déduire que ce sous-groupe est normal dans G.

1.10. Montrer que G est résoluble.

Montrons à présent la réciproque. Pour cela, on admet le résultat suivant dû à Galois : si p est un nombre premier et si G est un sous-groupe résoluble et transitif de $\mathfrak{S}_p$, alors G est conjugué à un sous-groupe de Aff_p.

1.11. Montrer que si G est résoluble, alors $F = K(x, y)$ quelles que soient les racines (distinctes) x et y de P.

2. Morphismes d'anneaux

2.1. Soit A un anneau noethérien et $f : A \to A$ un morphisme d'anneaux. Montrer que si f est surjectif, alors il est injectif.

On pourra considérer $I_n = \ker(f^{\circ n})$ où $f^{\circ n} = f \circ \cdots \circ f$, n fois.

2.2. Donner un contre-exemple si on ne suppose plus A noethérien.

3. Unités

3.1. Soit A un anneau intègre et noethérien et I un idéal non nul de A.

Montrer que si $x \in A$ vérifie $I = xI$, alors x est une unité de A.

3.2. Donner un contre-exemple si on ne suppose plus A intègre et noethérien.

4. Corps finis et polynômes

Cet exercice demande un peu plus de travail que les autres questions de l'examen.

4.1. Trouver tous les polynômes $P(X) \in \mathbf{F}_q[X]$ tels que $P : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$ est une bijection pour tout $n \geq 1$.