Test 4 (Polynômes, extensions de corps; 4h)

D. Harari

Agrégation

Tous les corps sont par définition commutatifs. Rappelons qu'un corps L est une *extension* d'un corps K s'il existe un morphisme de corps i (qui est nécessairement injectif) de K dans L, ce qui équivaut à dire qu'on peut identifier K au sous-corps $i(K)$ de L.

1. Soit L une extension d'un corps K. On rappelle qu'un élément $x \in L$ est *algébrique sur* K s'il existe un polynôme unitaire $P \in K[X]$ tel que $P(x) = 0$.

a) Montrer que x est algébrique sur K si et seulement si le sous K-ev $K[x]$ de L engendré par $(x^n)_{n \in \mathbf{N}}$ est de dimension finie.

b) Montrer que si $x \in L$ est algébrique sur K, alors $K[x]$ est un sous-corps de L. La réciproque est-elle vraie ?

c) Montrer que l'ensemble E des éléments de L algébriques sur K est un sous-corps de L.

d) Soit $P = X^n + a_{n-1}X^{n-1} + ... + a_0$ un polynôme unitaire à coefficients dans E. Montrer que le corps $K(a_0, a_1, ..., a_{n-1})$ (défini comme le sous-corps de E engendré par K et les a_i) est un K-ev de dimension finie.

e) On suppose que L est algébriquement clos. Montrer alors que E est algébriquement clos.

f) On prend $K = \mathbf{Q}$ et $L = \mathbf{C}$. Montrer que le corps E est alors dénombrable.

2. Soit K un corps fini de cardinal q et de caractéristique p. On rappelle que q est une puissance de p et que pour tout entier strictement positif m, il existe un corps de cardinal p^m, unique à isomorphisme près, qui est le corps de décomposition sur $\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$ du polynôme $X^{p^m} - X$. Soit $d > 0$ un entier.

a) Montrer qu'il existe une extension de corps L de K de degré d, unique à isomorphisme près.

b) On rappelle que le groupe multiplicatif L^* est cyclique. Soit α un générateur de ce groupe. Montrer que $L = K[\alpha]$.

c) En déduire qu'il existe un polynôme irréductible P dans $K[X]$, avec $\deg P = d$.

d) Soit maintenant réciproquement $R \in K[X]$ un polynôme irréductible de degré d. Soit $L = K[a]$ un corps de rupture de R. Montrer que l'application $F : x \mapsto x^q$ est un automorphisme du corps L qui induit l'identité sur K.

e) On note $F^m = F \circ F \circ ... \circ F$ le m-ième itéré de F. Montrer que d est le plus petit entier $m > 0$ tel que $F^m(a) = a$ (raisonner par l'absurde, en montrant que si on avait $m < d$, alors a appartiendrait à une extension de corps de K strictement incluse dans L), puis en déduire que L est aussi un corps de décomposition de R.

f) On considère les corps $\mathbf{F}_4$ et $\mathbf{F}_{16}$, corps respectivement à 4 et à 16 éléments. Montrer que $\mathbf{F}_{16}$ est une extension de degré 2 de $\mathbf{F}_4$ qui peut s'écrire $\mathbf{F}_{16} = \mathbf{F}_4[\beta]$, où β est un élément d'ordre 5 de $\mathbf{F}_{16}^*$ (ici β n'est donc pas un générateur de $\mathbf{F}_{16}^*$).

3. a) Soit K un corps de caractéristique zéro. Montrer que si $P \in K[X]$ est irréductible dans $K[X]$ et si L est une extension de corps de K, alors toute racine de P dans L est simple.

b) Un corps K de caractéristique $p > 0$ est dit *parfait* si le morphisme de corps $x \mapsto x^p$ de K dans K est bijectif. Donner un exemple de corps parfait et un exemple de corps imparfait.

c) Montrer que a) reste vrai si K est un corps parfait de caractéristique p, et qu'il est faux si K est un corps imparfait.

4. Soit K un corps. Soit $\sigma : K \to K$ un automorphisme de K. Soit L un K-espace vectoriel.

a) Montrer que $(L, +)$, muni de la loi externe $(\alpha, x) \mapsto \sigma(\alpha).x$ est aussi un K-espace vectoriel, que l'on notera L'.

b) Montrer que si L est de dimension finie d, alors L' est aussi de dimension d.

c) On rappelle (cf. exercice 3) qu'un corps K de caractéristique $p > 0$ est dit *parfait* si le morphisme de corps $x \mapsto x^p$ de K dans K est bijectif. Déduire de b) que si K est un corps parfait de caractéristique $p > 0$, toute extension L de K telle que L soit de dimension finie sur K est un corps parfait.

d) Le résultat de c) reste-t-il vrai pour une extension algébrique (pas forcément finie), c'est-à-dire pour une extension L de K vérifiant : tout élément de L est algébrique sur K (cf. exercice 1) ?