Nombres algébriques

AI 2015-2016

Exercice 1 :
Soit E un espace vectoriel de dimension finie n sur $\mathbb{F}_p$.
Que peut-on dire du cardinal de E.

Exercice 2 :
Soit $\mathbb{K} \subset \mathbb{L}$ deux corps. On dit que $\mathbb{L}$ est une extension finie de $\mathbb{K}$ si $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel de dimension finie. On dira alors que le degré de l'extension, notée $[\mathbb{L} : \mathbb{K}]$ est la dimension de cet espace vectoriel. Dans le cas contraire, on parle d'extension inifinie.
Donnez plusieurs exemples d'extension de degré 2. De degré infini.

Exercice 3 :
On suppose que

1. $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$,
2. $[\mathbb{M} : \mathbb{L}] < \infty$,
3. $[\mathbb{L} : \mathbb{K}] < \infty$.

Montrer alors que $[\mathbb{M} : \mathbb{K}] < \infty$.

Exercice 4 Soit $\mathbb{K} \subset \mathbb{L}$ deux corps, et soit α un élément de $\mathbb{L}$. On dit que α est algébrique sur $\mathbb{K}$ s'il existe $P \in \mathbb{K}[X]$ tel que P considéré comme élément de $\mathbb{L}[X]$ admette α comme racine.
On dit que $P \in \mathbb{K}[X]$ est un polynôme annulateur de α si α est racine de P considéré comme polynôme de $\mathbb{L}[X]$.
On notera $\mathbb{K}[\alpha] := \{\tilde{P}(\alpha)/P \in \mathbb{K}[X] \subset \mathbb{L}[X]\}$ où $\tilde{P}$ est la fonction polynôme de P considéré comme élément de $\mathbb{L}[X]$.

1. Donnez l'exemple d'un élément algébrique sur $\mathbb{R}[X]$.
2. Donnez l'exemple d'un nombre algébrique sur $\mathbb{R}$ mais non sur $\mathbb{Q}$.
3. Montrer que si α est un élément algébrique sur $\mathbb{K}$, il existe un unique polynôme annulateur unitaire μ_α de $\mathbb{K}[X]$ tel que P est un polynôme annulateur de α si et seulement si P est un multiple de μ_α.
4. Donnez le polynôme minimal de $i\sqrt{2}$ sur $\mathbb{R}$. Sur $\mathbb{C}$. Sur $\mathbb{Q}$.
5. Soit α un élément algébrique sur $\mathbb{K}$. Que peut-on dire de l'anneau $\mathbb{K}[X]/(\mu_\alpha(X))$?
6. On appelle $\mathbb{K}(\alpha)$ le plus petit corps contenant $\mathbb{K}$ et α. Montrer que $\mathbb{K}(\alpha) = \mathbb{K}[\alpha]$.
7. Montrer que $\mathbb{K}(\alpha)$ est un extension finie de $\mathbb{K}$, et que $[\mathbb{K}(\alpha) : \mathbb{K}] = deg(\mu_\alpha(X))$.
8. Exhiber une base de $\mathbb{K}(\alpha)$ considéré comme $\mathbb{K}$-espace-vectoriel.

Exercice 5 :
Montrer que $\mathbb{R}[X]/(X^2 + 1)$ est isomorphe à $\mathbb{C}$.

Exercice 6 :
Soit $\mathbb{F}$ un corps commutatif quelconque. Soit $m(X)$ un polynôme irréductible unitaire et non constant de $\mathbb{F}(X]$.
Montrer qu'il existe $\gamma \in \mathbb{F}[X]/(m(X))$, algébrique sur $\mathbb{F}$, et dont le polynôme minimal est $m(X)$.

Exercice 7 :
Si $\mathbb{K}$ est un sous-corps de $\mathbb{L}$, on dit que $\mathbb{L}$ est une extension algébrique de $\mathbb{K}$ si tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.
Montrer que si $\mathbb{L}$ est un extension de degré fini sur $\mathbb{K}$, alors c'est une extension algébrique.
La réciproque est-elle vraie ?

Exercice 8 :
Soit $\mathbb{F}$ un corps commutatif, et $P(X)$ un polynôme sur $\mathbb{F}$. On dit que $\mathbb{K}$ un sur-corps de $\mathbb{F}$ est un corps de rupture de $P(X)$ sur $\mathbb{F}$ si $P(X)$ a au moins une racine dans $\mathbb{K}$.
Montrer que, si $P(X)$ est un polynôme non constant quelconque sur $\mathbb{F}$ corps commutatif, il existe un corps de rupture de $P(X)$ sur $\mathbb{F}$.

Exercice 9 :
Soit $\mathbb{F}$ un corps commutatif quelconque et $P(X)$ un polynôme sur $\mathbb{F}$. On dit qu'un sur-corps $\mathbb{M}$ de $\mathbb{F}$ est un corps de décomposition de $P(X)$ sur $\mathbb{F}$ si $P(X)$ est scindé dans $\mathbb{M}[X]$.
On remarque donc qu'un corps de décomposition est un corps de rupture.
Montrer que si $P(X)$ est un polynôme non constant quelconque sur un corps $\mathbb{F}$, alors il existe un corps de décomposition de $P(X)$ sur $\mathbb{F}$.

Petit complément sur les corps finis.

Définition 0.1

Un corps fini est un corps de cardinal fini.

Proposition 0.1

Soit p un nombre premier et $m(X)$ un polynôme de degré n sur $\mathbb{F}_p$, irréductible.
Alors $\mathbb{F}_p[X]/(m(X))$ est un corps fini de cardinal p^n.

Théorème 0.2 (WEDDERBURN)

Tout corps fini est commutatif.

Proposition 0.3

1. *La caractéristique d'un corps fini est un nombre premier.*
2. *Tout sous-corps d'un corps fini de caractéristique p contient $\mathbb{F}_p$ (sous-corps premier).*
3. *Un corps fini est algébrique sur tous ses sous-corps.*

Conséquence : Si $\mathbb{K}$ est un corps fini de caractéristique p, alors c'est nécessairement une extension de degré fini r. Et donc $|\mathbb{K}| = p^r$. De plus, $\forall x \in \mathbb{K}$, $x^{p^r} = x$.
Rappel : on a vu que pour un corps fini $\mathbb{K}$, $(\mathbb{K}^*, \times)$ est un groupe cyclique (isomorphe à $(\mathbb{Z}/(p^r - 1)\mathbb{Z}, +)$).

Définition 0.2

Une racine primitive d'un corps fini est un générateur de son groupe multiplicatif.

Dans ce cas, $\mathbb{K} = \{0, 1, \alpha, \ldots, \alpha^{p^r-2}\}$.

Théorème 0.4

Soit $\mathbb{K}$ un corps fini de caractéristique p et de cardinal p^r. Soit α une racine primitive de $\mathbb{K}$, et soit $\mu_\alpha(X)$ son polynôme minimal sur $\mathbb{F}_p$,

1. $\mathbb{K} = \mathbb{F}_p(\alpha) = \mathbb{F}_p[\alpha]$.
2. $deg(\mu_\alpha) = r$.
3. $1, \alpha, \ldots, \alpha^{r-1}$ *forment une base de* $\mathbb{K}$ *sur* $\mathbb{F}_p$.
4. $\mathbb{K}$ *est isomorphe à* $\mathbb{F}_p[X]/(\mu_\alpha(X))$.

Théorème 0.5

Soit $\mathbb{K}$ un corps fini de cardinal p^r.

1. *Tout sous-corps de $\mathbb{K}$ a pour cardinal p^t, avec t diviseur de r,*
2. *pour tout entier positif t diviseur de r, il existe un unique sous-corps de $\mathbb{K}$ dont le cardinal est p^t,*
3. *pour tout entier t diviseur de r, le sous-corps de $\mathbb{K}$ de cardinal p^t est l'ensemble des racines de $X^{p^t} - X$.*

Par conséquent, si α est un élément d'un corps fini de cardinal p^r, alors le dergré du polynôme minimal de α sur $\mathbb{F}_p$ est un diviseur de r.
Enfin, si $\mathbb{K}$ est un corps fini de cardinal p^r, si t est un diviseur de r et si $\mathbb{L}$ est l'unique sous-corps de $\mathbb{K}$ de cardinal p^t,

1. *su α est une racine primitive de $\mathbb{L}$, alors le degré de son polynôme minimal sur $\mathbb{F}_p$ est égal à t,*
2. *si β est un élément de $\mathbb{K}$ dont le degré du polynôme minimal sur $\mathbb{F}_p$ est égal à t, alors $\mathbb{F}_p(\beta) = \mathbb{L}$.*

Bon, un petit dernier.

Théorème 0.6

Si p est un entier premier, et si r est un entier strictement positif, alors il existe un corps fini de cardinal p^r.
Si p est un entier premier, et si r est un entier strictement positif, alors il existe un polynôme de degré r sur $\mathbb{F}_p$ qui est irréductible sur $\mathbb{F}_p$.
Deux corps finis de même cardinal sont isomorphes.
Si p est un entier premier, et si r est un entier strictement positif. Soit $m(X)$ un polynôme de degré r sur $\mathbb{F}_p$, irréductible sur $\mathbb{F}_p$. Tout corps fini de cardinal p^r est isomorphe à $\mathbb{F}_p[X]/(m(X))$.