AGRÉGATION INTERNE, 2013-2014
3 JUILLET 2013
IDÉAUX, ANNEAUX DE POLYNÔMES ET NOMBRES ALGÉBRIQUES
CORRECTION DES QUESTIONS DELICATES

II-7: Le generateur normalise du noyau de ρ est $\prod_{x\in k}(X-x)$.

II-10: Attention on ne peut pas utiliser I-11 car $k[X]_{\leq d-1}$ n'est pas un anneau.

Il suffit de voir que $r_P(Q) = r_P(Q')$ si $Q \sim_{Pk[X]} Q'$.

Supposons $Q \sim_{PK[X]} Q'$ c'est a dire $Q' = Q = PB$.

Mais $Q = AP + r_P(Q)$ donc $Q' = (A+B)P + r_P(Q)$. Par unicité de la division euclidienne $r_P(Q) = r_P(Q')$.

II-11: L'application qui à $x \in k$ associe la classe du polynome constant x modulo P et la composee des morphismes d'anneaux "polynome constant" $k \to k[X]$ et $\pi : k[X]/Pk[X]$. Elle definit un morphisme d'anneau non nul puisqu'aucun polynome constant n'est divisible par P et donc le noyau du morphisme. Comme k est un corps et que tout ideal d'un corps est trivial ce morphisme est injectif et k s'identifie a un sous corps de $k[X]/Pk[X]$ par cette application.

La multiplication dans $k[X]/Pk[X]$ par les elements de k definit la loi externe du k-espace vectoriel $k[X]/Pk[X]$ et la loi de groupe additif est celle de l'anneau $k[X]/Pk[X]$.

La distributivité de la loi externe vis a vis de l'addition et le fait que π est une application lineaire resultent de la distributivité de la multiplication dans $k[X]/Pk[X]$.

On vérifie immédaitement que $\bar{r}_P \circ \pi|_{k[X]_{\leq d-1}} = \mathrm{id}_{k[X]_{\leq d-1}}$. Donc π est injective.

Si $A \in K[X]$ verifie $A = BP + R$ on a $\pi(A) = \pi(R)$ et donc $\pi(A) \in \pi(k[X]_{\leq d-1})$ donc π surjective.

Donc π est un isomorphisme en particulier $\dim_k k[X]/Pk[X] = d$.

III-3 Le morphisme ϕ_X est juste l'inclusion $k[X] \subset k(X)$ de l'anneau intégre $k[X]$ dans son corps de fractions. Donc est injectif.

III-7. Le morphisme $\phi_\alpha : k[X] \to K$ factorise via un morphisme *injectif* $k[X]/\pi_\alpha k[X] \to K$. Son image est un sous anneau de K donc est intègre. Par suite $\pi_\alpha k[X]$ est premier par I-12. Par II-5, π_α est irréductible.

III-8 $(b) \Rightarrow (a)$ Soit n la dimension de l'espace vectoriel sur k engendré par a famille $\{1, \alpha, \alpha^2, \ldots\}$ Nécessairement $\{1, \alpha, \ldots, \alpha^n\}$ est liée puisqu'elle a u $n+1$ elements. Il suit qu'il existe $\alpha_0, \ldots, \alpha_n \in k$, non tous nuls, tels que $\sum_{i=0}^n a_i\alpha^i = 0$. Donc α verifie une equation polynomiale non triviale.

$(c) \Rightarrow (b)$ Cette espace vectoriel est un sous espace vectoriel de L donc est de dimension finie.

$(a) \Rightarrow (c)$ On considere le morphisme d'anneaux $\bar{\phi}_\alpha : k[X]/\pi_\alpha k[X] \to K$. C'est une application k-linéaire. L'image est un sous k-espace vectoriel de dimension plus petite que celle de $k[X]/\pi_\alpha k[X]$ donc finie par II-13. Ce sous espace, noté $k(\alpha)$ est

engendré par $1, \alpha, \ldots, \alpha^{d-1}$ et c'est un anneau comme image du morphisme d'anneaux $\bar{\phi}$ et il est isomorphe à $k[X]/\pi_\alpha k[X]$ puisque $\pi_\alpha k[X] = \ker(\phi_\alpha$.

Comme π_α est irreductible non nul $\pi_\alpha k[X]$ est maximal. Donc $k[X]/\pi_\alpha k[X]$ est un corps et $k(\alpha)$ qui lui est isomorphe aussi . On a $\dim_k k(\alpha) = d$.

III-9. Un espace vectoriel E sur L est necessairement un espace vectoriel sur k et si $e_1, \ldots, e_d$ est une base de E sur L et $x_1, \ldots, x_p$ une base de L sur k E a une base sur k de la forme $x_i e_j$. Donc $dim_k(E) = \dim_k(L) \dim_L(E)$.

En appliquant ceci a $E = L(\alpha)$ qui est de dimension finie sur k on peut appliquer III-8-(c) pour conclure. Comme $k(\alpha) \subset L(\alpha)$ $\deg_k(\alpha) = \dim_k(k(\alpha)) \leq \dim_k(L(\alpha)) = \dim_k(k(\alpha)) \dim_L(L(\alpha)$.

III-10 Posons $L = k(\alpha)$, qui est de dimension finie sur k. Comme α est alg sur k il l'est sur L a fortiori. Donc $L(\beta)$ est de dim finie sur L donc sur k.

Or $\alpha + \beta$ et $\alpha\beta$ sont dans $L(\beta)$! Donc par $III - 8 - (c)$ ils sont algebriques.

III-11. C'est un anneau par la question precedente. Reste a voir que si α est algebriquesα^{-1} l'est aussi. Mais c'est clair car multipliant par α^{-n} la relation $\sum a_i \alpha^i = 0$ on obtient l'equation polynomiale $\sum_{a_{n-i}} \alpha^{-i} = 0$ pour α^{-1}.

Soit $\alpha \in K$ tel que α est algebrique sur k_K^{alg}. Soit $\sum_{i=0}^n a_i \alpha^i = 0$ une equation polynomiale a coeff dans k_K^{alg}.

Par recurrence sur i on montre que le corps L_i defini par $L_0 = k$ $L_{i+1} = L_i(a_{i+1})$ est de dimension finie sur k (car a_{i+1} est algebrique sur k a fortiori sur L_i. Donc L_n est de dimension finie sur k.

Mais α est algebrique sur L_n donc $L_n(\alpha)$ est de dimension finie sur L_n. Donc α est dans un sous corps de dimension finie sur k, donc est algebrique sur k.

IV-1. Tout polynome a coefficients dans $\bar{\mathbb{Q}}$ a une racine dans $\mathbb{C}$ puisque $\mathbb{C}$ est alg clos. Par III-11, cette racine est dans $\bar{\mathbb{Q}}$.

IV-2 l'ensemble des polynomes a coefficients dans Q est denombrable car $\mathbb{Q}$ est denombrable. Donc comme chaque polynome n'a qu'un nombre fini de racines l'ensemble des paires (P, α) ou $P \in \mathbb{Q}[X]^*$ et $P(\alpha) = 0$ est denombrable.

$\bar{\mathbb{Q}}$ etant l'image de l'application $(P, \alpha) \mapsto \alpha$, il est denombrable.

IV-5 (a) $\deg(P_n) = n$, $cd(P_n) = 2^n$, $P_{n+2}(0) = -P_n(0)$ donc $P_n(0) = 0$ pour n impair et $P_{2k}(0) = (-1)^k$. La parite de P_n est celle de n.

(d) Si $A \in \mathbb{Z}[X]$ a coeff dominant 1 tout $\alpha \in \mathbb{Q}$ qui est racine de A est entier.

En effet, $A = X^n + a_{n-1}X^{n-1} + \ldots$ et $\alpha = p/q$ $p, q > 0$ entiers premiers entre eux implique $(p/q)^n + a_{n-1}(p/q)^{n-1} + \ldots = 0$ d'ou:

$$p^n = -q(p^{n-1}a_{n-1} + p^{n-2}qa_{n-1} + \ldots$$

et q divise p^n. Comme p, q premiers entre eux $q = 1$ et $\alpha \in Z$.

Puisque Q est pair ou impair il suffit de montrer que $Q_n(k) \neq 0$ pour $k \geq 2$.

Mais puisque $Q_{n+2}(k) = hQ_{n+1}(k) - Q_n(k)$ et $Q_1(k) \geq Q_0(k) = 1 > 0$ une recurrence immediate donne $Q_{n+1}(k) \geq Q_n(k) > 0$.

IV-6. Comme l'eq caracteristique de la relation de recurrecne est $X^2 - 2\cos(\theta)X + 1$ de racines $e^{\pm i\theta}$ on a $u_n = a\cos(n\theta) + b\sin(n\theta)$ (si $\theta \neq 0, \pi$).

$P_n(\cos(\theta)) = \sin((n+1)\theta)/\sin(\theta)$ (si $\theta \neq 0, \pi$).

Les racines sont les $x_{k,n} = \cos(k\pi/(n+1))$ $k = 1, \ldots, n$ deux a deux distincts.

IV-7 Ce sont des racines de P_4, P_6. P_4 n'est pas irreductible. Il a une factorisation de la forme $P = Q(X)Q(-X)$ avec $Q = X^2 + X/2 - 1/4$. Le polynome minimal de $\cos(\frac{2\pi}{5})$ est $X^2 + X/2 - 1/4$.

V-1.

$(-1, 0)$ est l'intersection du cercle C de centre $(0, 0)$ et de rayon 1 et de la droite joignant les deux points $(0, 0)$ et $(0, 1)$.

Si on a deux points constructibles distincts la mediatrice du segment qu'ils delimitent est constructible car c 'est la droite joignant intersections des cercles centres en ces points et de rayon la longueur du segment .

Donc l'axe des ordonnées est constructible comme mediatrice de $[(-1, 0), (1, 0)]$.

$(0, 1)$ est constructible puisque c'est l'intersection de l'axe des ordonnées et de C.

$(0, 2)$ est constructible comme intersection du cercle centre en $(0, 1)$ de rayon 1 et de l'axe des ordonnées. La droite horizontale via $(0, 1)$ est la mediatrice de $[(0, 0); (0, 2)]$ est donc constructible. De même la verticale via $(1, 0)$ et ces deux droites s'intersectent en $(1, 1)$.

En itérant ces construction on voit que les points a coordonnees entieres sont constructibles.

V-2 La droite d equation $x = y$ est constructible puisqu'elle joint $(0, 0)$ et $(1, 1)$.

Si P est un point constructible et D une droite constructible on peut toujours trouver $n \in \mathbb{N}$ avec $n > dist(P, D)$. La mediatrice du segment delimite par l'intersection avec D du cercle centre en P de rayon n est constructible.

Ainsi la projection P' de P sur D est constructible, ainsi que le symetrique de P vis a vis de D comme l'autre point d'intersection de la droite (PP') avec le cercle centre en P' de rayon PP'.

V-3 La perpendiculaire a une droite constructible passant par un point constructible est constructible. La perpendiculaire a la perpendiculaire passant toutes deux par P a une droite constructible est la parallele a D passant par P, donc la parallele a une droite constructible par un point constructible est constructible. V-3 en resulte immediatement.

V-4 (a) Pour les cercles, l'equation est $(x - x_0)^2 + (y - y_0)^2 = d^2$ ou $x_0, x_1, d^2 \in L$. Elle est donc de la forme $x^2 + y^2 + ax + by + c = 0$, $a, b, c \in L$.

(b) Traitons l'intersection de deux cercles de centres distincts. On a les equations:

$$x^2 + y^2 + a_1x + b_1y + c = 0,\ x^2 + y^2 + a_2x + b_2y + c = 0$$

avec $(a_1, b_1) \neq (a_2, b_2)$ puisque ces parametres sont -2 fois les coordonnées des centres. Ceci donne une relation lineaire non triviale $(a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2)$ qui permet d'ecrire $y = ax + b$ ou $x = ay + b$ $a, b \in L$. Inserant ceci dans $x^2 + y^2 + a_1x + b_1y + c = 0$ une equation quadratique $(1 + a^2)x^2 + cx + d$ (ou similaire en y) s'ensuit.

V-7 Soient x, y des reels constructibles. La parallele via $(y, 0)$ a la droite joignant $(1, 0)$ a $(0, x)$ coupe l'axe des ordonnees en $(0, xy)$.

Menelaus peut etre aussi utilise.

V-8 Il reste a voir que l'inverse d'un constructible non nul est constructible.

La parallele via $(1,0)$ a la droite joignant $(x,0)$ a $(0,1)$ coupe l'axe des ordonnees en $(0,1/x)$.

V-9 Ce cercle rencontre l'axe des ordonnees en $(0,\sqrt{\alpha})$.

V-10 Ceci resulte de $V-9$ car K_{p+1} etant une extension quadratique de K_p on a $K_{p+1}=K_p(\sqrt{\alpha_p})$ avec $\alpha_p \in K_p \cap \mathbb{R}_{>0}$.

V-14 (a) Les racines rationnelles de P sont entieres par le resultat etabli en IV-5(d). On dresse le tableau de variation de P et on conclut facilement qu'il n a pas de racines entieres.

V-14 (b). C'est la question vraiment difficile du problème.

Soient r_1, r_2, r_3, r_4 les 4 racines distinctes de P. r_3 et r_4 sont complexes conjugués non réels.

$t = r_1r_2 + r_3r_4$. Introduisons $s = r_1r_3 + r_2r_4$ et $ur_1r_4 + r_2r_3$. Le groupe des permutations de r_1, r_2, r_3, r_4 agit par permutations de s, t, u.

Par suite $stu, st+tu+su, s+t+u$ sont des fonctions symetriques de r_1, r_2, r_3, r_4 qui s'expriment donc polynomialement en fonction de $r_1+r_2+r_3+r_4 = 0, \ldots, r_1r_2r_3r_4 = 2$.

Un calcul volumineux donne $s+t+u = 0$ $st+tu+us = 8$ $stu = 16$. t est racine de $(X-t)(X-s)(X-u)$ donc $t^3+8t-16 = 0$.

V-14 (c). Comme $(x \mapsto x^3+8x-16)$ est croissante ce polynome a t comme unique racine reelle. Elle n 'est pas rationnelle car elle serait entiere par le resultat etabli en IV-5(d) et les entiers possibles s eliminent aisement. Donc ce polynome de degre 3 ne peut pas etre produit de deux polynomes a coefficients dans Q de degres 1 et 2 puisque le facteur de degre 1 fournirait une racine. Donc il est irreductible. Ceci implique qu'il est le polynome minimal de t qui est de degre 3.

V-14 (d) P n a pas de facteur de degre 1 car il n a pas de racine rationnelle. Si P est produit de deux facteurs de degre 2 ce sont necessairement $(X^2+aX+b) = (X-r_3)(X-\bar{r}_3)$ et $X^2+cX+d = (X-r_1)(X-r_2)$ qui sont a coefficients rationnels. Mais alors t serait rationnel. Donc P est irreductible dans $\mathbb{Q}[X]$. Il suit que r_i est de degre 4 sur $\mathbb{Q}$.

V-15 (e) sinon $c = -r_1 - r_2$, $d = r_1r_2$ seraient constructibles. Calculant a, b par $bd = 2$ et $a+c = 0$ on deduit que a, b constructibles. Donc $t = b + r_1r_2$ constructible ce qui n'est pas puisque 3 n est pas puissance de 2.