Algèbre commutative et théorie de Galois **MM002**, 2012-2013.
Université Pierre et Marie Curie

Examen final, deuxième session

Mai 2013

L'utilisation des calculatrices, ordinateurs et téléphones portables est interdite. Le seul document utilisé est le polycopié du cours. Les réponses doivent être soigneusement justifiées. Les quatre exercices sont indépendants. Le barème (sur 100 pts) est indiqué en début de chaque partie.

Exercice 1. (25 pts)
Soient A un anneau, J un idéal de A et $a \in A$. On note $(J : a)$ l'idéal $\{x \in A, ax \in J\}$ de A.
On souhaite montrer qu'un anneau est noethérien si et seulement si tous ses idéaux premiers sont de type fini.

1. (5 pts) Montrer qu'un idéal propre J d'un anneau A n'est pas premier si et seulement si il existe $a \in A$ tel que $J + (a) \neq J$ et $(J : a) \neq J$.

2. (7 pts) Soit J un idéal d'un anneau A et $a \in A$. Montrer que si $J + (a)$ et $(J : a)$ sont des idéaux de type fini de A, alors J est également de type fini.

3. (9 pts) Soit A un anneau non noethérien. Montrer que l'ensemble E des idéaux de A qui ne sont pas de type fini admet un élément maximal pour l'inclusion. Montrer qu'un tel élément maximal de E est un idéal premier de A.

4. (4 pts) Conclure.

Correction

1. Si J n'est pas premier, il existe $a, b \notin J$ tels que $ab \in J$. Alors $a \in J + (a)$, donc $J + (a) \neq J$, et $b \in (J : a)$, donc $(J : a) \neq J$

   Réciproquement, soit $a \in A$ tel que $J + (a) \neq J$ et $(J : a) \neq J$. La première condition revient à dire que $a \notin J$. Comme on a toujours $J \subset (J : a)$, la deuxième condition revient à dire qu'il existe $b \in (J : a)$, et donc $ab \in J$ amis $b \notin J$. Donc $a, b \notin J$ mais $ab \in J$, donc J n'est pas un idéal premier.

2. Soit $x_1, \cdots, x_m$ une famille génératrice finie de $J + (a)$ et $y_1, \cdots, y_n$ une famille génératrice finie de $(J : a)$. Comme $x_i \in J + (a)$, il existe $u_i \in J$ et $v_i \in A$ tels que $x_i = u_i + av_i$. Montrons que la famille $\mathcal{C} = (u_1, \cdots, u_m, ay_1, \cdots, ay_n)$ est une famille génératrice de J ($ay_i \in J$ puisque $y_j \in (J : a)$).

   Soit$z \in J$. Alors, a fortiori, $z \in J + (a)$, donc il existe $(b_i) \in A^m$ tel que

$$z = \sum_i b_i x_i = \sum_i b_i u_i + a \sum_i b_i v_i.$$

Comme $z, \sum_i b_i u_i \in J$, $a\sum_i b_i v_i = z - \sum_i b_i u_i \in J$ et donc $\sum_i b_i v_i \in (J : a)$. Donc il existe $(c_j) \in A^n$ tel que $\sum_i b_i v_i = \sum_j c_j y_j$ et donc $z = \sum_i b_i u_i + \sum_j c_j (a y_j)$, ce qui montre que $\mathcal{C}$ est une famille génératrice de J.

3. Comme A est supposé non noethérien, E est non vide. Pour appliquer le lemme de Zorn à E, il suffit de montrer que si $(I_k)_{k\in K}$ est une famille totalement ordonnée d'idéaux de A qui ne sont pas de type finis, alors cette famille admet un majorant dans E. Montrons que $I = bigcup_k I_k$ est dans E. Supposons par l'absurde que I est de type fini et soit $c_1, \cdots, c_n$ une famille génératrice finie. Alors, pour tout i, il existe $k_i \in K$ tel que $c_i \in I_{k_i}$. Soit $k_0 = \max_i k_i$ (k_0 existe car K est totalement ordonné), alors $c_1, \cdots c_k \in I_{k_0}$ donc $I = I_{k_0} \in E$, ce qui est absurde. On peut donc appliquer le lemme de Zorn à E ce qui montre que E admet un élément maximal.

   Soit J un tel élément maximal de E (J est un idéal propre car A est monogène). Supposons par l'absurde que J n'est pas premier. Alors, d'après la question 1, il existe $a \in A$ tel que $J \subsetneq J + (a)$ et $J \subsetneq (J : a)$. Par maximalité de J dans E, $J + (a)$ et $(J : a)$ ne sont pas dans E, donc sont de type fini. Mais d'après 2, J est donc aussi de type fini, ce qui contredit $J \in E$. Donc J est un idéal premier.

4. Dans 3, on a montré que, si A est un anneau non noethérien, alors A contient un idéal premier qui n'est pas de type fini. Par contraposée, si tous les idéaux premiers de A sont de type fini, A est noethérien. La réciproque est évidente.

Exercice 2. (28 pts)
Soit K un corps de caractéristique différente de 2 et L une extension galoisienne de degré 4 de K telle que $\mathrm{Gal}(L/K)$ soit isomorphe à $\mathbb{Z}/4\mathbb{Z}$. Soit σ un générateur de $\mathrm{Gal}(L/K)$.

1. (5 pts) Montrer qu'il existe $x \in L$ non nul tel que $\sigma^2(x) = -x$. On fixe pour la suite de l'exercice un tel x.

2. (3 pts) Montrer que le stabilisateur de x dans $\mathrm{Gal}(L/K)$ est réduit à $\{\mathrm{Id}_L\}$.

3. (7 pts) Montrer que $L = K(x)$.

4. (5 pts) Montrer que le polynôme minimal de x dans $K[X]$ est de la forme $X^4 + aX^2 + b$ avec $a, b \in K$. On note $d = a^2 - 4b$.

5. (8 pts) Montrer que ni b ni d ne sont des carrés dans K, mais que db^{-1} est un carré dans K (on exprimera b, d et db^{-1} en fonction de x et $\sigma(x)$).

Correction

1. $\sigma^4 = \mathrm{Id}$, donc le polynôme $P(X) = X^2 - 1$ est un polynôme annulateur de l'endomorphisme K-linéaire σ^2 de L. Comme $P = (X-1)(X+1)$ est scindé à racine simple ($1 \neq -1$ car K est de caractéristique différente de 2), L est somme directe des espaces propres de σ^2 pour les valeurs propre 1 et -1. Comme $\sigma^2 \neq \mathrm{Id}$, l'espace propre de valeur propre -1 n'est pas réduit à 0. Il suffit de choisir pour x un tel vecteur propre.

2. Comme $G := \mathrm{Gal}(L/K) \simeq \mathbb{Z}/4\mathbb{Z}$, les seuls sous-groupes de $\mathrm{Gal}(L/K)$ sont $\{Id\}$, $\langle\sigma^2\rangle$ et G. Comme $\sigma^2 \notin Stab(x)$, $Stab(x) = \{Id\}$.

3. Un élément τ de $\mathrm{Gal}(L/K)$ est dans $\mathrm{Gal}(L/K(x))$ seulement si τ fixe x. D'après la question précédente, on obtient donc $\mathrm{Gal}(L/K(x)) = \{\mathrm{Id}\}$. Donc, d'après la correspondance de Galois,

$$K(x) = L^{\mathrm{Gal}(L/K(x))} = L^{\mathrm{Id}} = L.$$

4. Comme $[K(x) : K] = 4$, le polynôme minimal de $x$dans $K[X]$ est de degré 4. Or $P = \prod_{\tau \in \mathrm{Gal}(L/K)}(X - \tau(x))$ est un polynôme annulateur de x à coefficient dans K (ces coefficients sont invariants par $\mathrm{Gal}(L/K)$ et $L^{\mathrm{Gal}(L/K)} = K$ par correspondance de Galois), c'est donc le polynôme minimal. Or

$$P = \prod_{j=0}^{3}(X-\sigma^j(x)) = (X-x)(X-\sigma(x))(X+x)(X+\sigma(x)) = (X^2-x^2)(X^2-\sigma(x^2)) = X^4+aX^2+b$$

avec $a = -x^2 - \sigma(x^2)$ et $b = x^2\sigma(x^2)$.

5. $b = (x\sigma(x))^2$, donc les deux racines carrées de b dans L sont $x\sigma(x)$ et $-x\sigma(x)$. Or $\sigma(x\sigma(x)) = \sigma(x)\sigma^2(x) = -x\sigma(x) \neq x\sigma(x)$ (car $x\sigma(x) \neq 0$ et la caractéristique de L est différente de 2). Donc $x\sigma(x) \notin L^\sigma = K$ et donc b n'est pas un carré dans K

   De même $d = x^4 - 2x^2\sigma(x)^2 + \sigma(x)^4 = (x^2 - \sigma(x^2))^2$, donc les deux racines de d dans L sont $x^2-\sigma(x^2)$ et $-x^2+\sigma(x^2)$. On a $x^2-\sigma(x^2) \neq 0$ car sinon $x^2 \in L^\sigma = K$, ce qui contredit que x est de degré 4 sur K. Or $\sigma(x^2 - \sigma(x^2)) = \sigma(x)^2 - \sigma^2(x)^2 = \sigma(x)^2 - x^2 \neq x^2 - \sigma(x^2)$. Donc $x^2 - \sigma(x^2) \notin L^\sigma = K$, donc d n'est pas un carré dans K

   $db^{-1} = (\frac{x}{\sigma(x)} - \frac{\sigma(x)}{x})^2$.

   Or

$$\sigma(\frac{x}{\sigma(x)} - \frac{\sigma(x)}{x}) = \frac{\sigma(x)}{\sigma^2(x)} - \frac{\sigma^2(x)}{\sigma(x)} = \frac{x}{\sigma(x)} - \frac{\sigma(x)}{x},$$

   donc $\frac{x}{\sigma(x)} - \frac{\sigma(x)}{x} \in L^\sigma = K$ et db^{-1} est un carré dans K.

Exercice 3. (22 pts)
Soient K un corps et $P, Q \in K[X]$ deux polynômes non constants. On note n le degré de P et m le degré de Q. Soit L un corps de décomposition de $P \circ Q = P(Q(X))$. On suppose de plus que L/K est une extension séparable.

1. (4 pts) Montrer que L/K est une extension galoisienne.

2. (6 pts) On note K_0 le sous-corps de L engendré par K et les racines de P contenues dans L. Montrer que K_0/K est une extension galoisienne.

3. (6 pts) Montrer que $P \circ Q = \prod_{i=1}^{n} R_i$ où $R_1, \cdots, R_n \in K_0[X]$ sont des polynômes de degré m.

4. (6 pts) En déduire que $[L : K]$ divise $n!(m!)^n$.

Correction

1. L/K est une extension de décomposition, c'est donc une extension normale. Comme elle est de plus supposée séparable, elle est galoisienne.

2. Soit $\sigma \in \mathrm{Gal}(L/K)$, et x une racine de P dans L, alors $\sigma(x)$ est aussi une racine de P donc $\sigma(x) \in K_0$. On en déduit donc que K_0 est stable par $\mathrm{Gal}(L/K)$, donc K_0/K est une extension galoisienne.

3. Si $P = P_1P_2$ avec $P_1, P_2 \in K[X]$ et $deg(P_1 \geq 1)$. Le polynôme $P_1 \circ Q$ divise $P \circ Q$ donc a une racine α dans L. Alors $Q(\alpha)$ est une racine de P_1 dans L. On a donc montré que tout facteur non constant de P admettait une racine dans L. Comme L/K est galoisienne, P est donc scindé sur L et donc aussi sur K_0. Donc $P = \prod_{i=1}^{n}(X - \beta_i)$ dans $K_0[X]$.

   Alors $P \circ Q = \prod_{i=1}^{n}(Q(X) - \beta_i)$ dans $K_0[X]$. Il suffit de poser $R_i = Q(X) - \beta_i$.

4. On a $[L : K] = [L : K_0][K_0 : K]$. Comme K_0 est engendré par des racines de P qui est de degré n, $[K_0 : K]$ divise $n!$. Comme L est le corps de décomposition de $\prod_{i=1}^{n} R_i$ sur K_0, où chaque R_i est de degré m, $[L : K_0]$ divise $(m!)^n$.

   D'où le résultat.

Exercice 4. (25 pts)
Soit $P = X^4 + 8X + 12 \in \mathbb{Q}[X]$.

1. (7 pts) Montrer que P est un polynôme irréductible de $\mathbb{Q}[X]$ (on pourra par exemple réduire modulo 5).

2. (11 pts) Montrer que le groupe de Galois de P est isomorphe à A_4.

3. (7 pts) Soit L le corps de décomposition de P. Montrer qu'il n'existe pas d'extension K de $\mathbb{Q}$ dans L telle que $[K : \mathbb{Q}] = 2$.

Correction

1. En réduisant modulo 5, on obtient $\bar{P} = X^4 - 2X + 2$, qui a -1 comme racine évidente. Donc $\bar{P} = (X + 1)(X^3 - X^2 + X + 2)$. Comme $X^3 - X^2 + X + 2$ est un polynôme de degré 3 sans racine dans $\mathbb{F}_5$, il est irréductible.

   Si $P = RQ$ dans $\mathbb{Q}[X]$ avec $\deg R, Q \geq 1$, quitte a multiplier R et Q par leur contenu et changer de signe, on peut supposer $R, Q \in \mathbb{Z}[X]$ unitaires. Alors en réduisant modulo 5, on doit tomber sur l'unique décomposition non trivial de $\bar{P}$, donc P doit avoir une racine congrue à -1 modulo 5. Or une racine entière de P doit diviser $P(0) = 12$, donc les seules possibilités sont -6, -1 et 4, et aucun n'est racine de P.

2. L'action de $\mathrm{Gal}(P/\mathbb{Q})$ sur l'ensemble des racines de P dans $\mathbb{C}$ induit (en numérotant les racines) un morphisme injectif $\mathrm{Gal}(P/\mathbb{Q}) \to S_4$. Comme P est irréductible $4|\,\mathrm{Gal}(P/\mathbb{Q})$. De plus, puisque P a un facteur irréductible de degré 3 modulo 5, on a aussi $3|\,\mathrm{Gal}(P/\mathbb{Q})$ (pour prouver que $3|\,\mathrm{Gal}(P/\mathbb{Q})$, on peut aussi montrer que le polynôme résolvant de P est irréductible, cf. § 20.12.3). Donc $12|\,\mathrm{Gal}(P/Q)$.

On calcule le discriminant de P à l'aide de la formule du poly (proposition 20.26). On trouve $\Delta = ((-3)^3 \cdot 8^4 + 4^4 \cdot 12^3) = 2^1 2 \cdot 3^3 \cdot (-1+4) = (2^6 \cdot 3^2)^2$. Le discriminant est un carré dans $\mathbb{Q}$ donc $\mathrm{Gal}(P\mathbb{Q})$ est un sous-groupe de A_4, or comme $12 | \mathrm{Gal}(P/Q)$, $\mathrm{Gal}(P\mathbb{Q})$ est isomorphe à A_4.

3. Si K est une telle extension, $\mathrm{Gal}(L/K)$ est un sous-groupe d'indice 2 de $\mathrm{Gal}(L/\mathbb{Q}) \simeq A_4$. Or A_4 n'a pas de sous-groupe d'indice 2. En effet, comme les 3-cycles sont d'ordre 3 dans A_4, un tel sous-groupe d'indice 2 devrait contenir les 3-cycles, mais les 3-cycles engendrent A_4, d'où une contradiction.