Année universitaire 2013-2014 Licence 3 de mathématiques

Algèbre 4 - Examen

Lundi 16 décembre 2013

Tout anneau ci-dessous est commutatif. Si a et b sont des éléments d'un anneau A, on note par $\langle a, b\rangle$ l'idéal engendré par a et b. On note $\mathbb{F}_q$ le corps fini à q éléments.

Questions de cours 1 Soit A un anneau.

1. Rappeler la définition de l'idéal engendré par un ensemble $S \subset A$.

   L'idéal engendré par S (noté $\langle S\rangle$ est le plus petit idéal de A contenant S. De façon équivalente,

   $$\langle S\rangle = \{a_1u_1 + \cdots + a_mu_m : a_1, \ldots a_m \in A, u_1, \ldots, u_m \in S\}.$$

2. Démontrer que les deux propriétés suivantes sont équivalentes.

   (a) Toute suite croissante $I_0 \subseteq I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ d'idéaux de A est stationnaire. (C'est-à-dire, il existe $n \in \mathbb{N}$ tel que $I_n = I_{n+1} = I_{n+2} = \ldots$)

   (b) Tout idéal de A est engendré par un ensemble fini.

   On rappelle qu'un anneau admettant ces propriétés est appelé *noethérien*.

   (a)⇒(b) Supposons que A admette un idéal I non engendré par un ensemble fini. On construit la suite croissante d'idéaux $I_0 \subseteq I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ de la façon suivante. On choisit $u_0 \in I$ et on pose $I_0 = \langle u_0\rangle$. Puisque I n'est pas engendré par u_0, il existe $u_1 \in I \smallsetminus I_0$. On pose $I_1 = \langle u_0, u_1\rangle$. Puisque I n'est pas engendré par $\{u_0, u_1\}$, il existe $u_2 \in I \smallsetminus I_1$. On pose $I_2 = \langle u_0, u_1, u_2\rangle = \langle I_1, u_2\rangle$. Puisque I n'est pas engendré par $\{u_0, u_1, u_2\}$, il existe $u_3 \in I \smallsetminus I_2$. On pose $I_3 = \langle u_0, u_1, u_2, u_3\rangle = \langle I_2, u_3\rangle$, etc. On obtient une suite infinie strictement croissante $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \ldots$, ce qui contredit (a).

   (b)⇒(a) Soit $I_0 \subseteq I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ une suite croissante d'idéaux. Posons $I = \cup_{n=0}^{\infty} I_n$. Une vérification immédiate montre que I est un idéal de A. Par l'hypothèse (b) il est engendré par un ensemble fini : $I = \langle u_1, \ldots, u_s\rangle$. Tout u_k appartient à un certain I_{n_k} ; si on pose $n = \max\{n_1, \ldots, n_s\}$ alors $u_1, \ldots, u_s \in I_n$, ce qui implique que $I_n \supset I$. Or d'autre part $I_n \subseteq I_{n+1} \subseteq I_{n+2} \subseteq \ldots \subseteq I$, ce qui montre que

   $$I_n = I_{n+1} = I_{n+2} = \ldots = I.$$

3. Un anneau principal est-il forcément noethérien ?

   Oui, parce que tout idéal d'un anneau principal est engendré par un seul élément.

4. Supposons que A soit noethérien.

   (a) Soit $f : A \to B$ un morphisme d'anneau surjectif. L'anneau B, est-il forcément noethérien ?

   Oui. Si I est un idéal de B alors $f^{-1}(I)$ est un idéal de A. Puisque A est noethérien, $f^{-1}(I)$ est engendré par un ensemble fini S. Alors I est engendré par l'ensemble fini $f(S)$.

   (b) Qu'est-ce qu'on peut dire de l'anneau de polynômes $A[t]$? Énoncer le théorème correspondant sans le démontrer.

   Le théorème d'Hilbert affirme que l'anneau de polynômes $A[t]$ est noethérien si A l'est.

5. L'anneau $\mathbb{Z}[\sqrt{2013}] = \{a + b\sqrt{2013} : a, b \in \mathbb{Z}\}$ est-il noethérien ?

   Oui : l'anneau $\mathbb{Z}[t]$ est noethérien par le théorème d'Hilbert, et le morphisme $\mathbb{Z}[t] \to \mathbb{Z}[\sqrt{2013}]$ défini par $P(t) \mapsto P(\sqrt{2013})$ est surjectif.

Questions de cours 2

1. Soient A un anneau, $a, b \in A$. Rappeler la définition du $\mathrm{pgcd}(a, b)$.

   On appelle $d \in A$ le $\mathrm{pgcd}(a, b)$ si d est diviseur commun de a et b (c'est à dire, $d \mid a$ et $d \mid b$) et tout autre diviseur commun de a et b divise d. Le $\mathrm{pgcd}(a, b)$ est bien défini à l'équivalence arithmétique près.

   Supposons que l'anneau A soit factoriel.

2. Montrer l'existence du $\mathrm{pgcd}(a,b)$ pour tout $a,b \in A$.

   Supposons que $a,b \neq 0$. Soit $\{p_1,\dots,p_s\}$ l'ensemble de tous (à équivalence près) les diviseurs irréductibles de ab. Alors on factorise a et b comme $a = p_1^{\alpha_1}\cdots p_s^{\alpha_s}$ et $b = p_1^{\beta_1}\cdots p_s^{\beta_s}$, ou $\alpha_i, \beta_i \in \mathbb{Z}_{\geq 0}$. Alors $p_1^{\min\{\alpha_1,\beta_1\}}\cdots p_s^{\min\{\alpha_s,\beta_s\}} = \mathrm{pgcd}(a,b)$.

   Si, disons, $a = 0$ alors $\mathrm{pgcd}(a,b) = b$.

3. Quel lien y a-t-il entre $\mathrm{pgcd}(a,b)$ et l'idéal $\langle a,b\rangle$?

   On a $\langle a,b\rangle \subset \langle \mathrm{pgcd}(a,b)\rangle$, et $\langle a,b\rangle = \langle \mathrm{pgcd}(a,b)\rangle$ si l'anneau A est principal. Si A n'est pas principal, il est possible que $\langle a,b\rangle \subsetneq \langle \mathrm{pgcd}(a,b)\rangle$: par exemple, dans l'anneau $A = \mathbb{C}[t,u]$ on a $\mathrm{pgcd}(t,u) = 1$ mais $\langle t,u\rangle \neq \langle 1\rangle = A$.

4. Rappeler la définition du *contenu* d'un polynôme $P(t) \in A[t]$, et la définition d'un *polynôme primitif*.

   Le *contenu* d'un polynôme est le pgcd des ses coefficients. Un polynôme est dit *primitif* si son contenu est 1. Si d est le contenu du polynôme P alors $P = d\widetilde{P}$ où $\widetilde{P}$ est un polynôme primitif.

5. Quel lien y a-t-il entre les contenus de $P(t)$, de $Q(t)$ et de $P(t)Q(t)$? Démontrer cette propriété.

   Le « Lemme de Gauss » affirme que $\mathrm{cont}(PQ) = \mathrm{cont}(P)\,\mathrm{cont}(Q)$. Considérons d'abord le cas particulier où P et Q sont primitifs. Il faut montrer que PQ est primitif. Pour ceci, il suffit de montrer qu'aucun p irréductible ne divise tous les coefficients de PQ. Fixons un tel p et écrivons

   $$P(t) = a_0 + a_1t + \dots, \quad Q(t) = b_0 + b_1t + \dots, \quad P(t)Q(t) = c_0 + c_1t + \dots,$$

   Puisque P est primitif il existe i tel que $p \nmid a_i$. Soit k le plus petit i avec ce propriété. De même, soit ℓ le plus petit j tel que $p \nmid b_j$. On a

   $$p \nmid a_k, \quad p \mid a_i \quad (i = 0,\dots,k-1); \qquad p \nmid b_\ell, \quad p \mid b_j \quad (j = 0,\dots,\ell-1).$$

   En écrivant

   $$c_{k+\ell} = \sum_{i=0}^{k-1} a_i b_{k+\ell-i} + a_k b_\ell + \sum_{i=k+1}^{k+\ell} a_i b_{k+\ell-i} = \sum_{i=0}^{k-1} a_i b_j + a_k b_\ell + \sum_{j=0}^{\ell-1} a_{k+\ell-j} b_j$$

   on observe que les deux sommes sont divisibles par p mais le terme $a_k b_\ell$ ne l'est pas. Ceci montre que $p \nmid c_{k+\ell}$, ce qui achève la démonstration du lemme de Gauss pour les polynômes primitifs.
   Pour démontrer le cas général du lemme de Gauss on écrit $P = d\widetilde{P}$ et $Q = e\widetilde{Q}$, où $d = \mathrm{cont}(P)$, $e = \mathrm{cont}(Q)$ et $\widetilde{P}, \widetilde{Q}$ sont primitifs. Alors $PQ = de\widetilde{P}\widetilde{Q}$, où $\widetilde{P}\widetilde{Q}$ est primitif par ce qui précède, ce qui montre que $\mathrm{cont}(PQ) = de$.

6. Déterminer le contenu du polynôme

   $$P(t) = (2t-1)(3t-2)\cdots(2014t-2013) \in \mathbb{Z}[t].$$

   Le polynôme $(n+1)t - n$ est primitif : son contenu divise $n+1-n = 1$. Le polynôme $P(t)$ est donc primitif en tant que produit de polynômes primitifs.

Exercice 1

1. Quelle-est la structure du groupe multiplicatif $\mathbb{F}_{27}^\times$?

   C'est un groupe cyclique d'ordre 26.

2. Montrer que pour $\theta \in \mathbb{F}_{27}^\times$ on a $\theta^{13} \in \{1,-1\}$.

   On a $(\theta^{13})^2 = \theta^8 = 1$, d'où θ^{13} est une racine du polynôme $t^2 - 1$, c'est-à-dire $\theta^{13} \in \{1,-1\}$.

3. Supposons que $\theta^{13} = -1$ mais $\theta \neq -1$. Montrer que θ engendre le groupe $\mathbb{F}_{27}^\times$. Est-ce que la réciproque est vraie ?

   Un élément θ engendre $\mathbb{F}_{27}^\times$ si et seulement si l'ordre de θ dans $\mathbb{F}_{27}^\times$ est 26. Puisque cet ordre divise 26, il est égal à 26 si et seulement s'il ne divise ni 13 ni 2, c'est-à-dire si et seulement si $\theta^{13} \neq 1$ et $\theta^2 \neq 1$, ce qui est équivalent à notre hypothèse $\theta^{13} = -1$ et $\theta \neq -1$. Ceci démontre aussi l'énoncé réciproque.

4. Considérons le polynôme $P(t) = t^3 - t - 1 \in \mathbb{F}_3[t]$. Est-il irréductible sur $\mathbb{F}_3$?

   Un polynôme de degré 3 est irréductible sur un corps si et seulement si il n'a pas de racines dans ce corps. Puisque $t^3 - t - 1$ n'a pas de racines dans F_3, il est irréductible.

5. Montrer que $P(t)$ admet une racine dans $\mathbb{F}_{27}$. Soit θ une telle racine. Exprimer θ^{-1}, θ^4, θ^8 et θ^{12} comme $a+b\theta+c\theta^2$ avec $a,b,c\in\mathbb{F}_3$.
Le polynôme $P(t)$ admet une racine θ dans son corps de rupture, qui est $\mathbb{F}_{27}$. On a $-\theta+\theta^3=1$ et $\theta^3=1+\theta$, ce qui implique
$$\begin{aligned}\theta^{-1} &= \theta^{-1}(-\theta+\theta^3) = -1+\theta^2;\\ \theta^4 &= \theta\cdot\theta^3 = \theta(1+\theta) = \theta+\theta^2;\\ \theta^8 &= (\theta^4)^2 = (\theta+\theta^2)^2 = \theta^2+2\theta^3+\theta^4 = \theta^2+2(1+\theta)+\theta+\theta^2 = -1-\theta^2;\\ \theta^{12} &= \theta^4\cdot\theta^8 = (\theta+\theta^2)(-1-\theta^2) = -\theta-\theta^2-\theta^3-\theta^4 = -\theta-\theta^2-(1+\theta)-(\theta+\theta^2) = -1+\theta^2\end{aligned}$$

6. Est-il vrai que θ engendre le groupe $\mathbb{F}_{27}^{\times}$? Même question sur $-\theta$.
Puisque $\theta^{12}=-1+\theta^2=\theta^{-1}$, on a $\theta^{13}=1$, ce qui montre que θ n'engendre pas $\mathbb{F}_{27}^{\times}$. Par contre,
$$(-\theta)^{13} = (-1)^{13}\theta^{13} = -1,$$
ce qui montre que $-\theta$ l'engendre.

Exercice 2 Soit A un anneau. On considère le morphisme d'anneaux $f : A[x,y]\to A[t]$ vérifiant $f(a)=a$ pour tout $a\in A$ et
$$f(x)=t^2, \quad f(y)=t^2+t.$$

1. Montrer que $\ker f = I$, où $I=\langle x-(y-x)^2\rangle$.
On note $P(x,y)=x-(y-x)^2$. Alors
$$f(P) = t^2-(t^2+t-t^2)^2 = 0,$$
ce qui montre que $\langle P\rangle\subset I$.
Montrons que $I\subset\langle P\rangle$. Soit $G(x,y)\in I$. En effectuant la division euclidienne par rapport à y, on trouve $G(x,y)=P(x,y)Q(x,y)+R(x,y)$ avec $\deg_y R\leq 1$. Montrons que R est le polynôme nul : ceci impliquera que $G=PQ\in I$.
Pour ceci on écrit $R(x,y)=R_1(x)y+R_0(x)$. Alors
$$0=f(G)=f(P)f(Q)+f(R_1)f(y)+f(R_0)=R_1(t^2)(t^2+t)+R_0(t^2),$$
d'où
$$tR_1(t^2) = -R_1(t^2)-R_0(t^2). \tag{1}$$
Si le polynôme R_1 était non-nul alors à gauche de (1) on aurait un polynôme de degré impair et à droite de degré pair, ce qui est impossible. Ceci montre que $R_1=0$, ce qui implique aussi que $R_0=0$, et donc $R=0$, ce qui achève la démonstration de l'inclusion $I\subset\langle P\rangle$.

2. Établir que $A[x,y]/I\cong A[t]$.
Puisque f est surjectif, on a $A[t]\cong A[x,y]/\ker f$.

3. À quelle condition l'idéal I est-il premier ?
Il est premier si et seulement si $A[t]$ est intègre, ce qui est équivalent à dire que A est intègre.

4. Trouver un idéal maximal contenant I quand $A=\mathbb{Q}$, $A=\mathbb{Z}$.
Il suffit de trouver un idéal J de $A[t]$ tel que $A[t]/J$ est corps. Dans ce cas $I'=f^{-1}(J)$ est le noyau du morphisme composé $A[x,y]\xrightarrow{f}A[t]\to A[t]/J$; il est donc idéal maximal contenant I.
Si $A=\mathbb{Q}$ on peut prendre, par exemple, $J=\langle t\rangle$. On a $\mathbb{Q}[t]/J=\mathbb{Q}$ et $I'=\langle x-(y-x)^2, x-y\rangle=\langle x,y\rangle$.
Si $A=\mathbb{Z}$ on peut prendre, par exemple, $J=\langle t,2\rangle$. On a $\mathbb{Z}[t]/J=\mathbb{F}_2$ et $I'=\langle x-(y-x)^2,x-y,2\rangle=\langle x,y,2\rangle$.

Exercice 3

1. On note a,b,c les racines dans $\mathbb{C}$ du polynôme $t^3+t+3\in\mathbb{Q}[t]$. Expliciter le polynôme unitaire $P(t)\in\mathbb{C}[t]$ de degré 3 dont les racines sont $a+b, b+c, c+a$.
Posons $A=b+c$, $B=a+c$, $C=a+b$. On a
$$\begin{aligned}\sigma_1(A,B,C) &= 2\sigma_1(a,b,c)=0,\\ \sigma_2(A,B,C) &= (b+c)(a+c)+(b+c)(a+b)+(a+c)(a+b) = a^2+b^2+c^2+3ab+3ac+3bc\\ &= \sigma_1(a,b,c)^2+\sigma_2(a,b,c)=1,\\ \sigma_3(A,B,C) &= (b+c)(a+c)(a+b) = a^2b+a^2c+b^2a+b^2c+c^2a+c^2b+2abc\\ &= \sigma_1(a,b,c)\sigma_2(a,b,c)-\sigma_3(a,b,c)=-3.\end{aligned}$$

D'où $P(t) = t^3 + t - 3$.
On peut aussi remarquer que, puisque $a + b + c = 0$, on a $A = -a$, $B = -b$ et $C = -c$, d'où

$$\sigma_k(A, B, C) = (-1)^k \sigma_k(a, b, c).$$

2. Résoudre dans $\mathbb{F}_5$ le système d'équations algébriques

$$x + y + z = 2, \quad \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = -2, \quad x^2 + y^2 + z^2 = 1.$$

On peut re-écrire notre système comme

$$\sigma_1 = 2, \quad \frac{\sigma_2}{\sigma_3} = -2, \quad \sigma_1^2 - 2\sigma_2 = 1$$

(on écrit σ_k au lieu de $\sigma_k(x, y, z)$). En résolvant ce système, on trouve $\sigma_1 = 2$, $\sigma_2 = -1$, $\sigma_3 = -2$. Ceci implique que x, y, z sont les racines du polynôme $t^3 - 2t^2 - t + 2$. Par inspection, on trouve que les racines sont $2, 1, -1$. Ceci montre que (x, y, z) est une permutation de $(2, 1, -1)$.