Année universitaire 2012-2013 Licence 3 de mathématiques

Algèbre 4 - Examen

Lundi 17 novembre 2012

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.

Questions de cours 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 la 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 intègre admettant ces propriétés est appelé *noethérien*.
   (a)⇒(b) Supposons que A admet un idéal I non engendré par un ensemble fini. On construit la suite croissante des idéaux $I_0 \subseteq I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ de la façon suivante. On choisi $u_0 \in I$ et on pose $I_0 = \langle u_0\rangle$. Puisque I n'est pas engendré par u_0, il existe $u_1 \in I \setminus I_0$. On pose $I_1 = \langle u_0, u_1\rangle$. Puisque I n'est pas engendré par $\{u_0, u_1\}$, il existe $u_2 \in I \setminus I_1$. 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 $u_3 \in I \setminus I_2$. 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 apartient 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 intègre est-il forcement noethérien ?
   Oui, parce que tout idéal est engendré par un seul élément.
4. Supposons que A est noethérien. 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. Utiliser ce théorème pour montrer que les anneau de polynômes $\mathbb{Z}[t_1, \ldots, t_n]$ et $K[t_1, \ldots, t_n]$ (où K est un corps) sont noethériens.
   Puisque $\mathbb{Z}$ est principal, il est noethérien. En utilisant le théorème d'Hilbert, on montre par récurrence sur n que $\mathbb{Z}[t_1, \ldots, t_n]$ est noethérien.

   De même, puisque K est noethérien, on montre par récurrence sur n que $K[t_1, \ldots, t_n]$ est noethérien.

Exercice 1

1. Soient n un nombre naturel, et p un nombre premier. Montrer que le polynôme $f(t) = t^n - p$ est irréductible sur $\mathbb{Q}$.
   Le critère d'Eisenstein implique que $f(t)$ est irréductible sur $\mathbb{Z}$. Par le lemme de Gauss, il est également irréductible sur $\mathbb{Q}$.
2. Rappeler la définition d'un corps de rupture d'un polynôme irréductible sur un corps.
   Soient K un corps et $g(t) \in K[t]$ un polynôme irréductible sur K. Un corps de rupture de g sur K est une extension L de K tel que g admet une racine θ dans L et $L = K(\theta)$. On a $[L : K] = \deg g$.
3. Donner un corps de rupture du polynôme $f(t)$ sur $\mathbb{Q}$. Quel-est son degré sur $\mathbb{Q}$?
   Par exemple $\mathbb{Q}(p^{1/n})$. Son degré sur $\mathbb{Q}$ est $n = \deg f$.

4. En déduire qu'il existe une extension de $\mathbb{Q}$ de degré n pour tout $n \in \mathbb{N}$, $n \geq 1$.

   Ceci découle de la question précédente.

5. Rappeler la définition du corps de décomposition d'un polynôme sur un corps.

   Soient K un corps et $g(t) \in K[t]$. Un corps de décomposition de g sur K est l'extension minimale de K dans laquelle g se décompose en facteurs linéaires.

6. Déterminer le corps de décomposition du polynôme $f(t) = t^4 - 3$. Quel-est son degré sur $\mathbb{Q}$?

   Les racines de f sont $\pm 3^{1/4}, \pm i 3^{1/4}$. Le corps de décomposition est donc $L = \mathbb{Q}(3^{1/4}, i)$. Puisque $i \notin \mathbb{Q}(3^{1/4})$ on a $[L : \mathbb{Q}(3^{1/4})] = 2$, et donc $[L : \mathbb{Q}] = 8$.

Exercice 2 Dans cet exercice on étudie les anneaux finis.

1. Soient A un anneau intègre et a un élément non nul de A. Montrer que l'application

$$\begin{aligned} A &\to A \\ x &\mapsto ax \end{aligned} \tag{1}$$

   est injective.

   C'est un morphisme de groupes additifs. Son noyau est $\{x \in A : ax = 0\}$. Puisque a n'est pas diviseur de 0, le noyau est 0, ce qui démontre que (1) est injective.

2. On suppose en plus que l'anneau A est fini. Montrer que l'application (1) est bijective.

   Tout application injective d'un ensemble fini vers lui même est bijective.

3. En déduire que tout anneau fini intègre est un corps.

   Si $a \neq 0$ alors (1) est bijective. Il existe donc $x \in A$ tel que $ax = 1$. Ceci démontre que tout élément non-nul de A est inversible.

4. Soit p un nombre premier. Est-il vrai que tout anneau à p éléments est un corps ?

   Oui. Soit A un anneau de p éléments. Tout idéal de A est un sous-groupe du groupe additif de A. Puisque ce dernier est d'ordre p, et l'ordre du sous-groupe divise l'ordre du groupe (le « théorème de Lagrange »), il n'existe que 2 sous-groupes : $\{0\}$ et A. Ceci signifie que A n'a que 2 idéaux, ce qui montre que A est un corps.

5. Est-il vrai que tout anneau de p^2 éléments est un corps ?

   Non. Les anneaux $\mathbb{Z}/p^2\mathbb{Z}$ et $\mathbb{F}_p \times \mathbb{F}_p$ ne sont pas intègres (vois la prochaine question).

6. Démontrer que les trois anneaux $\mathbb{F}_{p^2}$, $\mathbb{F}_p \times \mathbb{F}_p$ et $\mathbb{Z}/p^2\mathbb{Z}$ ne sont pas isomorphes deux à deux.

   Les anneau $\mathbb{Z}/p^2\mathbb{Z}$ et $\mathbb{F}_p \times \mathbb{F}_p$ ne sont pas intègres : l'élément p est un diviseur de zéro dans $\mathbb{Z}/p^2\mathbb{Z}$, et $(1, 0)$ est un diviseur de zéro dans $\mathbb{F}_p \times \mathbb{F}_p$. Ceci montre qu'aucun des deux n'est isomorphes à $\mathbb{F}_{p^2}$.

   L'élément p est en fait nilpotent dans $\mathbb{Z}/p^2\mathbb{Z}$, mais $\mathbb{F}_p \times \mathbb{F}_p$ n'a pas de nilpotents. Ceci montre que $\mathbb{Z}/p^2\mathbb{Z}$ et $\mathbb{F}_p \times \mathbb{F}_p$ ne sont pas isomorphes.

Exercice 3

1. Soit p un nombre premier. Parmi les affirmations suivantes, lesquelles sont vraies ?

   (a) Tout polynôme $P(t) \in \mathbb{F}_p[t]$ de degré 2 admet une racine dans $\mathbb{F}_{p^2}$.

   Vrai. Si $P(t)$ est irréductible, alors son corps de rupture est de degré 2 sur $\mathbb{F}_p$, c'est-à-dire, c'est $\mathbb{F}_{p^2}$. Si $P(t)$ est réductible, il admet une racine dans $\mathbb{F}_p$, et donc dans $\mathbb{F}_{p^2}$.

   (b) Tout polynôme $P(t) \in \mathbb{F}_p[t]$ de degré 3 admet une racine dans $\mathbb{F}_{p^3}$.

   Vrai, avec le même argument.

   (c) Tout polynôme $P(t) \in \mathbb{F}_p[t]$ de degré 4 admet une racine dans $\mathbb{F}_{p^4}$.

   Vrai. Si $P(t)$ est irréductible ou s'il admet une racine dans $\mathbb{F}_p$, on utilise le même argument. Sinon, $P(t)$ est produit de deux polynômes irréductibles de degré 2, auquel cas il admet une racine dans $\mathbb{F}_{p^2}$, un sous-corps de $\mathbb{F}_{p^4}$.

(d) Tout polynôme $P(t) \in \mathbb{F}_p[t]$ de degré 5 admet une racine dans $\mathbb{F}_{p^5}$.

Faux. Rappelons que $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ si et seulement si $m \mid n$. En particulier, si ℓ est premier, alors les seules sous-corps de F_{p^ℓ} sont $\mathbb{F}_p$ et $\mathbb{F}_{p^\ell}$. Autrement dit, pour tout $\alpha \in \mathbb{F}_{p^\ell}$ le degré de α sur $\mathbb{F}_p$ est 1 ou ℓ.

Soit $g_2(t), g_3(t) \in \mathbb{F}_p[t]$ des polynômes irréductibles de degré 2 et 3, respectivement. (De tels polynômes existent : on peut prendre par exemple les polynômes minimaux d'un élément de $\mathbb{F}_{p^2} \smallsetminus \mathbb{F}_p$ et d'un élément de $\mathbb{F}_{p^3} \smallsetminus \mathbb{F}_p$.) Alors toute racine de $f(t) = g_2(t)g_3(t)$ est de degré 2 ou 3 ; en particulier, aucune racine n'appartient à $\mathbb{F}_{p^5}$.

Justifier vos réponses.

2. Quelle-est la structure du groupe multiplicatif $\mathbb{F}_9^\times$?

   C'est un groupe cyclique d'ordre 8.

3. Montrer que pour $\theta \in \mathbb{F}_9^\times$ on a $\theta^4 \in \{1, -1\}$. Montrer que $\theta^4 = -1$ si et seulement si θ engendre le groupe $\mathbb{F}_9^\times$.

   On a $(\theta^4)^2 = \theta^8 = 1$, d'où θ^4 est une racine du polynôme $t^2 - 1$, c'est-à-dire $\theta^4 \in \{1, -1\}$.

   Puis, θ engendre $\mathbb{F}_9^\times$ si et seulement si l'ordre de θ dans $\mathbb{F}_9^\times$ est 8. Puisque cet ordre divise 8, il est égale à 8 si et seulement si il ne divise pas 4, c'est-à-dire si et seulement si $\theta^4 \neq 1$.

4. Considérons le polynôme $P(t) = t^2 + t - 1 \in \mathbb{F}_3[t]$. Est-il irréductible sur $\mathbb{F}_3$?

   Oui, parce qu'il n'a pas de racine dans $\mathbb{F}_3$.

5. Montrer que $P(t)$ admet une racine dans $\mathbb{F}_9$. Soit θ une telle racine. Déterminer θ^4.

   $P(t)$ admet une racine θ dans son corps de rupture, qui est $\mathbb{F}_9$. On a $\theta^2 = 1 - \theta$ ce qui implique
   $$\theta^4 = (1-\theta)^2 = 1 - 2\theta + \theta^2 = 1 + \theta + (1 - \theta) = 2 = -1.$$

6. Est-il vrai que θ engendre le groupe $\mathbb{F}_9^\times$?

   Oui, voir la question 3.

7. Donner un exemple d'un polynôme $Q(t) \in \mathbb{F}_3[t]$ de degré 2, irréductible sur $\mathbb{F}_3$ et admettant la propriété suivante : aucune racine de $Q(t)$ n'engendre $\mathbb{F}_9^\times$.

   On peut prendre $Q(t) = t^2 + 1$. C'est un polynôme irréductible sur $\mathbb{F}_3$, et sa racine η vérifie $\eta^2 = -1$ et $\eta^4 = 1$, ce qui montre qu'elle n'engendre pas $\mathbb{F}_9$, voir la question 3.

Exercice 4

1. Rappeler les définitions d'un polynôme symétrique en n variables, des polynômes symétriques élémentaires en n variables, et l'énoncé du théorème des polynômes symétriques.

   Soit A un anneau. On dit que $P(x_1, \dots, x_n) \in A[x_1, \dots, x_n]$ est symétrique si pour toute permutation τ de l'ensemble $\{1, \dots, n\}$ on a
   $$P(x_{\tau(1)}, \dots, x_{\tau(n)}) = P(x_1, \dots, x_n).$$
   Les polynômes symétriques élémentaires sont
   $$\begin{aligned}
   \sigma_1(x_1, \dots, x_n) &= x_1 + \cdots + x_n, \\
   \sigma_2(x_1, \dots, x_n) &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n = \sum_{1 \le i < j \le n} x_ix_j, \\
   \sigma_3(x_1, \dots, x_n) &= x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n = \sum_{1 \le i < j < k \le n} x_ix_jx_k, \\
   &\vdots \\
   \sigma_m(x_1, \dots, x_n) &= \sum_{1 \le i_1 < i_2 < \dots < i_m \le n} x_{i_1}x_{i_2}\cdots x_{i_m}, \\
   &\vdots \\
   \sigma_n(x_1, \dots, x_n) &= x_1 \cdots x_n.
   \end{aligned}$$
   Le théorème affirme que pour tout polynôme symétrique $P(x_1, \dots, x_n) \in A[x_1, \dots, x_n]$ il existe un polynôme $Q(y_1, \dots, y_n) \in A[y_1, \dots, y_n]$ tel que
   $$P(x_1, \dots, x_n) = Q\big(\sigma_1(x_1, \dots, x_n), \dots, \sigma_n(x_1, \dots, x_n)\big).$$

2. Parmi les polynômes suivants en variables $x_1, \ldots, x_n$, lesquels sont symétriques ?

$$\begin{aligned} P_1(x_1, x_2) &= x_1^3 x_2^2 + x_2^3 x_1^2 && (n = 2); \\ P_2(x_1, x_2, x_3) &= x_1^3 x_2^2 + x_2^3 x_3^2 + x_3^3 x_1^2 && (n = 3); \\ P_3(x_1, x_2, x_3) &= x_1^2 x_2^2 + x_2^2 x_3^2 + x_3^2 x_1^2 + x_1 x_2 x_3 && (n = 3). \end{aligned}$$

Les polynômes P_1 et P_3 sont symétriques. Le polynôme P_2 n'est pas symétrique, parce que

$$P_2(x_2, x_1, x_3) \neq P_2(x_1, x_2, x_3)$$

3. Exprimer le polynôme $P_3(x_1, x_2, x_3)$ en forme $Q(\sigma_1, \sigma_2, \sigma_3)$, où Q est un polynôme et $\sigma_1, \sigma_2, \sigma_3$ sont les polynômes symétriques élémentaires en 3 variables.

$$\begin{aligned} P_3(x_1, x_2, x_3) &= \sigma_2(x_1, x_2, x_3)^2 - 2x_1^2 x_2 x_3 - 2x_1 x_2^2 x_3 - 2x_1 x_2 x_3^2 + x_1 x_2 x_3 \\ &= \sigma_2(x_1, x_2, x_3)^2 - 2\sigma_1(x_1, x_2, x_3)\sigma_3(x_1, x_2, x_3) + \sigma_3(x_1, x_2, x_3). \end{aligned} \tag{2}$$

4. Soit a un nombre complexe. Déterminer le discriminant du polynôme

$$f(t) = t^3 - 3at^2 + 4 \in \mathbb{C}[t]$$

en fonction du paramètre a.
On a $f'(t) = 3t^2 - 6at$. Les racines de f' sont 0 et $2a$. Puisque f est un polynôme unitaire, son discriminant est

$$D_f = R(f, f') = 3^3 f(0) f(2a) = -432(a^3 - 1).$$

5. Déterminer l'ensemble S des valeurs de a pour lesquelles le polynôme $f(t)$ admet 3 racines complexes distinctes.

Le polynôme $f(t)$ admet une racine multiple si et seulement si $D_f = 0$, c'est-à-dire $a^3 = 1$. L'ensemble des racines de cette équation est $\{1, \frac{-1-i\sqrt{3}}{2}, \frac{-1+i\sqrt{3}}{2}\}$. On a donc $S = \mathbb{C} \setminus \{1, \frac{-1-i\sqrt{3}}{2}, \frac{-1+i\sqrt{3}}{2}\}$.

6. Soient $a \in S$ et $\alpha_1, \alpha_2, \alpha_3$ les racines complexes de $f(t)$. Déterminer $P_3(\alpha_1, \alpha_2, \alpha_3)$.
On a $\sigma_1(\alpha_1, \alpha_2, \alpha_3) = 3a$, $\sigma_2(\alpha_1, \alpha_2, \alpha_3) = 0$ et $\sigma_3(\alpha_1, \alpha_2, \alpha_3) = -4$. En utilisant (2) on trouve

$$P_3(\alpha_1, \alpha_2, \alpha_3) = 0^2 - 2 \cdot 3a \cdot (-4) + (-4) = 24a - 4.$$