Université d'Ottawa

Département de mathématiques et de statistique

MAT 3543 : Théorie des Anneaux
Professeur : Hadi Salmasian

Examen Final

15 avril, 2014

Nom de famille _____ Prénom _____

Numero d'étudiant(e) # _____

Instructions :

(a) Vous avez 3 heures pour compléter ce test.

(b) Le nombre de points disponibles pour chaque question est indiqué entre crochets.

(c) Vous devez justifier vos réponses pour recevoir le maximum de points. Toutes vos réponses doivent être écrites dans l'espace prévu. Si vous avez besoin d'espace supplémentaire pour répondre à une question particulière, vous devez continuer au verso de la page et l'indiquer **clairement**.

(d) Veuillez écrire votre numéro d'étudiant(e) en en-téte de chaque page dans l'espace prévu.

(e) Vous n'avez le droit de consulter ni vos notes, ni aucun livre. L'usage de téléphones cellulaires et de calculatrices n'est pas autorisé.

(f) Il est strictement conseillé que vous écriviez vos réponse avec un **stylo** (au lieu d'un crayon). write in **pen**, not pencil.

(g) La dernière page de l'examen peut être utilisé comme brouillon.

Bonne chance !

Question	1	2	3	4	5	6	7	8	9	10	11	Total
Maximum	7	6	10	4	7	5	5	7	5	3	3	62
Note												

1. (a) **[2 points]** Soit R un anneau intègre. Donner la définition d'un élément premier de R.

Solution: Un élément $r \in R$ est appelé premier s'il satisfait $r \neq 0$, $r \notin R^*$, et pour tous $a, b \in R$ tels que $r|ab$, on a $r|a$ ou $r|b$.

(b) **[2 points]** Soit R un anneau intègre. Soient $a_1, \ldots, a_n \in R$ des éléments non nuls. Donner la définition de "pgcd" de $a_1, \ldots, a_n$

Solution: Un élément $d \in R$ est appelé un pgcd de $a_1, \ldots, a_n$ s'il satisfait les conditions suivantes :

(a) $d|a_1, \ldots, d|a_n$.

(b) $\forall_{r \in R} : r|a_1, \ldots r|a_n \Rightarrow r|d$.

(c) **[3 points]** Calculer le pgcd de $2x^4 + 2x$ et $x(x^2 + 1)$ comme des éléments de $\mathbb{R}[x]$. Vous devez justifier votre réponse.

Solution:

$$2x^4 + 2x = 2x(x^3 + 1) = 2x(x + 1)(x^2 - x + 1)$$

Puisque $x^2 - x + 1$ et $x^2 + 1$ n'ont aucune racine dans $\mathbb{R}$, ils sont irréductibles dans $\mathbb{R}[x]$. Puisque $R[x]$ est un anneau factoriel, par Proposition 2.74 le pgcd est égal à x.

2. (a) **[4 points]** Soient R et S deux anneaux commutatifs et soit $I \subseteq R \times S$ un idéal principal. Montrer que $I = A \times B$ tel que $A \subseteq R$ et $B \subseteq S$ sont des idéaux principaux.

Solution: Par Propositon 1.89 tout idéal de $R \times S$ est de la forme $A \times B$ où A est un idéal de R et B est un idéal de S.

Soit $A \times B$ un idéal principal de $R \times S$, engendré par $(a, b) \in A \times B$. Montrons que $A = \langle a \rangle$ et $B = \langle b \rangle$. D'abord, nous vérifions que $\langle a \rangle \subseteq A$ et $\langle b \rangle \subseteq B$:

$$\forall_{r \in R} \; : \; (ar, 0) = (a, b)(r, 0) \in A \times B \; \Rightarrow \; ar \in A$$

De même, $br \in B$. Par suite, $\langle a \rangle \subseteq A$ et $\langle b \rangle \subseteq B$. Maintenant nous démontrons que $A \subseteq \langle a \rangle$ et $B \subseteq \langle b \rangle$. Pour tout $x \in A$,

$$(x, 0) \in A \times B \; \Rightarrow \; \exists_{(r,s) \in R \times S} : (x, 0) = (a, b)(r, s) \; \Rightarrow \; x = ar \; \Rightarrow \; x \in \langle a \rangle.$$

(b) **[2 points]** Soit R un anneau intègre. Donner la définition de la condition ACCP.

Solution: On dit qu'un anneau commutatif R vérifie la condition ACCP si toute suite croissante d'idéaux principaux est stationnaire. Autrement dit, pour toute suite des idéaux

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \cdots$$

il existe un nombre $n \in \mathbb{Z}^+$ tel que $\langle a_n \rangle = \langle a_{n+1} \rangle = \cdots$.

3. Vrai ou faux ? Vous devez justifier vos réponses.

(a) **[2 points]** $\mathbb{Z}_6[x]$ est un anneau factoriel.

Solution: Faux. Par la définition, tout anneau factoriel et un anneau intègre, mais $\mathbb{Z}_6[x]$ n'est pas un anneau intègre car $2 \cdot 3 = 0$.

(b) **[2 points]** $x^3 - 3x + 1$ est un polynôme irréductible de $\mathbb{Q}[x]$.

Solution: Vrai. les racine rationelle de $x^3 - 3x + 1$ sont entre $\{\pm 1\}$ (Thm 2.17). Il suit que $x^3 - 3x + 1$ n'a aucune racine dans $\mathbb{Q}$. Puisque $\deg(x^3 - 3x + 1) = 3$, il est irréductible.

(c) **[2 points]** L'application

$$\sigma : \mathrm{GF}(32) \to \mathrm{GF}(32) \ , \ \sigma(x) = x^4$$

est un automorphisme de $\mathrm{GF}(32)$.

Solution: Vrai. En fait $\sigma = \tau \circ \tau$ où $\tau(x) = x^2$ est l'homomorphisme de Frobenius (Exemple 1.81), alors σ est un homomorphisme d'anneaux, donc σ est un automorphisme car $\mathrm{GF}(32)$ est un corps.

(d) **[2 points]** $\pi^2 + \pi$ est algébrique sur $\mathbb{Q}$. ($\pi = 3.1415\cdots$).

Solution: Faux. Supposons au contraire que $\pi^2 + \pi$ est algébrique. Alors, il existe $d \geq 1$ et $a_0, \cdots, a_{d-1} \in \mathbb{Q}$ tels que

$$a_0 + a_1(\pi^2 + \pi) + \cdots + a_{d-1}(\pi^2 + \pi)^{d-1} + (\pi^2 + \pi)^d = 0.$$

Considerons le polynôme $p(x) = a_0 + a_1(x^2 + x) + \cdots + a_{d-1}(x^2 + x)^{d-1} + (x^2 + x)^d$. Donc $p(x)$ est monique, $\deg(p(x)) = 2d > 0$, et $p(\pi) = 0$. C'est une contradiction, parce que π n'est pas algébrique sur $\mathbb{R}$ (Thm 3.7).

(e) **[2 points]** L'anneau $\mathbb{Z}[x]$ avec

$$\delta : \mathbb{Z}[x] \to \mathbb{N} \quad , \quad \delta(f(x)) = \deg(f(x))$$

est un anneau euclidien.

Solution: Faux. Tout anneau euclidien est un anneau principal, mais $\mathbb{Z}[x]$ n'est pas un anneau principal (voir Ex. 2.81) parce que l'idéal $\langle 2, x\rangle$ n'est pas principal.

En fait, si $\langle 2, x\rangle = \langle h(x)\rangle$, alor $2 = h(x)q(x)$ et donc $h(x)$ est un polynôme constant, à savoir $h(x) = c \in \mathbb{Z}$. Pourtant, $x = h(x)q(x) = c \cdot q(x)$ implique que $c = \pm 1$, alors $1 \in \langle 2, x\rangle$ d'où la contradiction.

4. **[4 points]** Montrer que $2 - 3\sqrt{-1}$ est un élément irréductible de $\mathbb{Z}[\sqrt{-1}]$, où

$$\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \ : \ a, b \in \mathbb{Z}\}.$$

Solution: Posons $N(a + b\sqrt{-1}) = a^2 + b^2$. Supposons que $2 - 3\sqrt{-1} = xy$, tel que $x, y \in \mathbb{Z}[\sqrt{-1}]$. Alors,

$$N(2 - 3\sqrt{-1}) = N(x)N(y) \ \Rightarrow \ 13 = N(x)N(y) \ \Rightarrow \ N(x) = 1 \text{ ou } N(y) = 1.$$

De plus,

$$a, b \in \mathbb{Z} \text{ et } N(a + b\sqrt{-1}) = 1 \ \Rightarrow \ a^2 + b^2 = 1 \ \Rightarrow \ a = \pm 1, b = 0 \text{ ou } a = 0, b = \pm 1.$$

Conséquemment, $2 - 3\sqrt{-1}$ est irréductible.

5. **[7 points]** Déterminer tous les idéaux $I \subseteq \mathbb{Z}_3[x]$ tels que $\mathbb{Z}_3[x]/I \cong \mathrm{GF}(9)$. Vous devez justifier votre réponse.

(Puisque $\mathbb{Z}_3[x]$ est un anneau principal, vous pouvez décrire chaque idéal par son generateur.)

Solution: Pusique $\mathbb{Z}_3[x]/I$ est un corps, l'idéal I doit être maximal. Alors, I est engendré par un polynôme irréductible $f(x)$. Par Thm, $2 = [\mathrm{GF}(9) : \mathbb{Z}_3] = \deg(f(x))$. Conséquemment, il faut trouver tout polynôme irréductible $f(x) = x^2 + ax + b \in \mathbb{Z}_3[x]$. Par Thm , $f(x)$ est irréductible si et seulement si $f(x)$ n'a aucune racine dans $\mathbb{Z}_3$. Il y a 9 polynômes $f(x) = x^2 + ax + b \in \mathbb{Z}_3[x]$, parmi lesquelle 3 sont de la forme $(x - r_1)(x - r_2)$ et 3 sont de la forme $(x - r)^2$. Alors, on obtient les idéaux :

$$\langle x^2 + 1 \rangle \quad , \quad \langle x^2 + x + 2 \rangle \quad , \quad \langle x^2 + 2x + 2 \rangle.$$

6. (a) **[2 points]** Soient $\mathbb{F}$ un corps et $f(x) \in \mathbb{F}[x]$. Donner la définition de corps de décomposition de $f(x)$.

Solution: Une extension $\mathbb{F} \subseteq \mathbb{K}$ est appelée un corps de décomposition de $f(x)$ si $f(x)$ se décompose en facteurs linéaires dans $\mathbb{K}[x]$ comme

$$f(x) = c(x - r_1) \cdots (x - r_n)$$

et $\mathbb{K} = \mathbb{F}(r_1, \ldots, r_n)$.

(b) **[3 points]** Soient p un nombre premier, et $n \in \mathbb{Z}^+$. Montrer que $\mathrm{GF}(p^n)$ est le corps de décomposition de $f(x) = x^{p^n-2} + x^{p^n-3} + \cdots + x^2 + x + 1 \in \mathbb{Z}_p[x]$.

Solution: $\mathrm{GF}(p^n)$ est le corps de décomposition de $x^{p^n} - x$. Remarquons que

$$x^{p^n} - x = x(x^{p^n-1} - 1) = x(x-1)(x^{p^n-2} + \cdots + x + 1).$$

Alors $x^{p^n-2} + \cdots + x + 1$ se décompose en facteurs linéaires, e.g.,

$$x^{p^n-2} + \cdots + x + 1 = (x - r_1) \cdots (x - r_{p^n-2}) \quad , \quad r_1, \ldots, r_{p^n-2} \in \mathrm{GF}(p^n)$$

et $\mathrm{GF}(p^n) = \mathbb{Z}_p(0, 1, r_1, \ldots, r_{p^n-2}) = \mathbb{Z}_p(r_1, \ldots, r_{p^n-2})$. Conséquemment, $\mathrm{GF}(p^n)$ est le corps de décomposition de $x^{p^n-2} + \cdots + x + 1$.

7. **[5 points]** Calculer $[\mathbb{Q}(\sqrt[3]{1-\sqrt{3}}) : \mathbb{Q}]$, et donner une base de $\mathbb{Q}(\sqrt[3]{1-\sqrt{3}})$ comme espace vectoriel sur $\mathbb{Q}$. Vous devez justifier votre réponse.

Solution:

$$x = \sqrt[3]{1-\sqrt{3}} \Rightarrow x^3 - 1 = -\sqrt{3} \Rightarrow (x^3-1)^2 = 3 \Rightarrow x^6 - 2x^3 - 2 = 0.$$

Par le critère d'Eisenstein pour $p = 2$, le polynôme $x^6 - 2x^3 - 2$ est irréductible dans $\mathbb{Q}[x]$, et donc, par Thm 3.16(iii), il est le polynôme minimal de $\sqrt[3]{1-\sqrt{3}}$ sur $\mathbb{Q}$. Conséquemment, Thm 3.19(ii) implique que $[\mathbb{Q}(\sqrt[3]{1-\sqrt{3}}) : \mathbb{Q}] = \deg(\sqrt[3]{1-\sqrt{3}}) = 6$, et une base de $\mathbb{Q}(\sqrt[3]{1-\sqrt{3}})$ sur $\mathbb{Q}$ est l'ensemble

$$\left\{1, \sqrt[3]{1-\sqrt{3}}, \left(\sqrt[3]{1-\sqrt{3}}\right)^2, \left(\sqrt[3]{1-\sqrt{3}}\right)^3, \left(\sqrt[3]{1-\sqrt{3}}\right)^4, \left(\sqrt[3]{1-\sqrt{3}}\right)^5\right\}$$

8. Soit $\mathbb{F}$ le corps de décomposition de $f(x) = (x^2+3)(x^2+3x+1) \in \mathbb{Q}[x]$.

(a) **[3 points]** Trouver $m, n \in \mathbb{Z}$ tels que $\mathbb{F} = \mathbb{Q}(\sqrt{m}, \sqrt{n})$.

Solution: les racines de x^2+3x+1 sont $x = \frac{1}{2}(-3 \pm \sqrt{5})$, et les racines de x^2+3 sont $\pm\sqrt{-3}$. Donc le corps de décomposition de $f(x)$ est

$$\mathbb{Q}(\sqrt{-3}, -\sqrt{-3}, \frac{1}{2}(-3+\sqrt{5}), \frac{1}{2}(-3-\sqrt{5})) = \mathbb{Q}(\sqrt{-3}, \sqrt{5}).$$

(b) **[4 points]** Donner une base de $\mathbb{F}$ (comme un espace vectoriel sur $\mathbb{Q}$).

Vous devez justifiez que les vecteurs dans la base sont linéairement independents.

Solution: Nous montrons que $\{1, \sqrt{-3}, \sqrt{5}, \sqrt{-15}\}$ est une base de $\mathbb{F}$. Remarquons que

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\sqrt{5})(\sqrt{-3}) = \mathbb{F}$$

Par Thm 3.19(ii), $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$ et $\{1, \sqrt{5}\}$ est une base de $\mathbb{Q}(\sqrt{5})$ sur $\mathbb{Q}$. De plus, $\mathbb{Q}(\sqrt{5}) \subsetneq \mathbb{Q}(\sqrt{5})(\sqrt{-3})$ car $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{R}$. Alors $[\mathbb{F} : \mathbb{Q}(\sqrt{5})] \geq 2$. Puisque $\sqrt{-3}$ est une racine de $x^2+3 \in \mathbb{Q}(\sqrt{5})[x]$, Thm 3.19(ii) implique que $[\mathbb{F} : \mathbb{Q}(\sqrt{5})] \leq 2$. Par suite, $[\mathbb{F} : \mathbb{Q}(\sqrt{5})] = 2$, et donc $\{1, \sqrt{-3}\}$ est une base de $\mathbb{F}$ sur $\mathbb{Q}(\sqrt{5})$. Conséquemment, Thm 3.21(i) implique que $\{1, \sqrt{-3}, \sqrt{5}, \sqrt{-15}\}$ est une base de $\mathbb{F}$.

9. (a) **[1 point]** Donner un exemple d'un isomorphisme d'anneaux $\sigma : \mathbb{C}[x] \to \mathbb{C}[x]$ tel que

$$\exists_{f(x)\in\mathbb{C}[x]} : \sigma(f(x)) \neq f(x).$$

Solution: Par exemple $\sigma(a_0 + \cdots + a_n x^n) = \overline{a_0} + \cdots + \overline{a_n} x^n$.

(b) **[4 points]** Soient $\mathbb{F}$ un corps et $\sigma : \mathbb{F}[x] \to \mathbb{F}[x]$ un homomorphisme d'anneaux. Supposons que σ est surjectif. Montrer que σ est un isomorphisme.

Solution: Il suffit de démontrer que $\ker(\sigma) = \{0\}$. Puisque $\mathbb{F}[x]$ est un anneau principal, il existe $f(x) \in \mathbb{F}[x]$ tel que $\ker(\sigma) = \langle f(x) \rangle$. Supposons, au contraire, que $f(x) \neq 0$. Puisque $\mathbb{F}[x]/\ker(\sigma) \cong \mathrm{im}(\sigma) = \mathbb{F}[x]$, l'anneau $\mathbb{F}[x]/\ker(\sigma)$ est un anneau intègre et donc $\ker(\sigma)$ est un idéal premier. Tout idéal premier et non nul de $\mathbb{F}[x]$ est un idéal maximal (Thm 2.53), alors $\ker(\sigma)$ est maximal et donc $\mathbb{F}[x]/\ker(\sigma) \cong \mathbb{F}[x]$ doit être un corps. Contradiction.

10. **[3 points]** Donner la démonstration du théorème suivant :

Soient $\mathbb{F} \subseteq \mathbb{K}$ une extension de corps, et $u \in \mathbb{K}$ algébrique sur $\mathbb{F}$. Soit $m(x) \in \mathbb{F}[x]$ le polynôme minimal de u sur $\mathbb{F}$. Alors, $m(x)$ est irréductible.

Solution: Supposons que $m(x) = p(x)q(x)$ tel que $0 < \deg(p(x)), \deg(q(x)) < \deg(m(x))$. Nous pouvons supposer, sans perte de généralité, que $p(x)$ et $q(x)$ sont moniques. Puisque $m(u) = 0$, on obtient $p(u) = 0$ ou $q(u) = 0$. Conséquemment, $m(x)$ n'est pas le polynôme minimal de u. Contradiction.

11. **[3 points]** Donner la démonstration du théorème de Kronecker :

Soient $\mathbb{F}$ un corps et $f(x) \in \mathbb{F}[x]$ un polynôme non constant. Alors, il existe une extension de corps $\mathbb{F} \subseteq \mathbb{K}$ tel que

$$f(x) = (x-a)g(x) \text{ où } a \in \mathbb{K} \text{ et } g(x) \in \mathbb{K}[x].$$

Solution: Soit $p(x) \in \mathbb{F}[x]$ un polynôme irréductible tel que $p(x)|f(x)$. Puisque $p(x)$ est irréductible, l'idéal $\langle p(x)\rangle$ est maximal et donc $\mathbb{F}[x]/\langle p(x)\rangle$ est un corps. Posons $\mathbb{K} := \mathbb{F}[x]/\langle p(x)\rangle$. Il est clair que $\mathbb{F} \subseteq \mathbb{K}$. Posons $a := \langle p(x)\rangle + x \in \mathbb{K}$. Il est clair que $f(a) = \langle p(x)\rangle + f(x) = \langle p(x)\rangle + 0$ dans $\mathbb{K}$.