UNIVERSITE DU SUD TOULON - VAR

Faculté des Sciences et Techniques

Licence de Mathématiques

Module M53

Durée de l'examen : 180 minutes.
Documents autorisés : résumé manuscrit (5 feuilles A4 r/v max).
Barème : les points attribués à chaque problème sont notés en marge.
Toutes les réponses doivent être justifiées.

Problème 1. On considère le groupe multiplicatif $G = \mathbb{Z}_7^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$.

1. Déterminer la table de multiplication de G. [2]
2. G est-il cyclique ? [1]
3. Déterminer l'ordre de chaque élément de G. [1]
4. Déterminer l'exposant de G. [1]
5. Déterminer les sous-groupes de G. [2]
6. Déterminer la table de multiplication du groupe $K = \mathbb{Z}_7^*/\{\bar{1}, \bar{6}\}$. [2]
7. Montrer que K est cyclique. [1]

Problème 2. Soit $(A, +, \cdot)$ un anneau commutatif et x un élément de A fixé. Dans ce problème on note mutiplicativement la deuxième loi, c'est-à-dire : $\forall a, b \in A$, $ab := a \cdot b$. On définit sur $B := A \times A$ les lois de composition interne suivantes :

$$(a, b) + (c, d) := (a + c, b + d), \quad (a, b)(c, d) := (ac + xbd, ad + bc).$$

(a) Expliquer brièvement pourquoi ces lois sont internes. [0.5]

(b) Démontrer que B muni de ces deux lois est un anneau commutatif. [1.5]

(c) Montrer que B contient un sous-anneau B_1 isomorphe à A. Dans la suite on identifie les éléments de B_1 avec ceux de A. 1.5

(d) Vérifier que x est le carré d'un élément ω de B. 0.5

Cela justifie la terminologie : B est une extension quadratique de A ; elle est notée $B := A[\sqrt{x}]$.

(e) Vérifier que tout élément de B se met sous la forme $a + b\omega$ avec $a, b \in B_1$ et que cette décompostion est unique. [1]

(f) On appelle conjugué de $z := a + b\omega \in B$ l'élément de B noté et défini par $\bar{z} := a - b\omega$. Vérifier les règles de calcul

$$\bar{\omega} = -\omega, \quad \forall z \in A \equiv B_1, \bar{z} = z, \quad \forall z, u \in B, \quad \overline{z + u} = \bar{z} + \bar{u}, \quad \overline{zu} = \bar{z}\bar{u}, \quad \bar{\bar{z}} = z.$$

[0.5]

(g) Pour tout $z \in B$ on appelle norme de z, que l'on note $N(z)$, l'expression

$$N(z) := z\bar{z}.$$

Vérifier que N prend ses valeurs dans $A \equiv B_1$ et que

$$N(1_B) = 1_A, \quad \forall z, u \in B, \quad N(zu) = N(z)N(u), \quad N(z) = N(\bar{z}).$$

1

(h) Démontrer le théorème suivant : pour que $z \in B$ soit inversible (vis-à-vis de la deuxième LCI) il faut et suffit que $N(z)$ soit inversible dans A. 2

(i) On suppose à partir de maintenant que A est un corps. Vérifier que ω est algébrique sur A ; quel est le degré de l'extension B de A ? 0.5

(j) Démontrer le théorème suivant : $A[\sqrt{x}]$ est un corps si et seulement si x n'est pas le carré d'un élément de A. 2

(Session I – 2005)

UNIVERSITE DU SUD TOULON - VAR

Faculté des Sciences et Techniques

Licence de Mathématiques

Module M53

Durée de l'examen : 180 minutes.
Documents autorisés : résumé manuscrit (5 feuilles A4 r/v max).
Barème : les points attribués à chaque problème sont notés en marge.

Problème 1. On considère le groupe multiplicatif $G \equiv \mathbb{Z}_8^*$.

1. Déterminer tous les éléments de G ainsi que sa table de multiplication. [2]
2. Déterminer l'ordre de chaque élément de G. [1.5]
3. Déterminer l'exposant de G. [1.5]
4. On considère l'action de G sur $\mathbb{Z}_8$ donnée par

$$\begin{array}{ccc} G \times \mathbb{Z}_8 & \to & \mathbb{Z}_8 \\ (\bar{n}, \bar{m}) & \mapsto & \overline{nm}. \end{array}$$

   Déterminer les orbites de cette action ainsi que le stabilisateur de chaque élément de $\mathbb{Z}_8$. [2]
5. Pour cette action, déterminer

$$\bigcap_{a \in G} \mathrm{Fix}(a).$$

[1]

Problème 2. Les trois parties sont indépendantes.

Partie A. Soient I_1 et I_2 deux idéaux à gauche d'un anneau A et $J := \{x \in A | xI_1 \subset I_2\}$. Montrer que J est un idéal bilatère de A. [3]

Partie B. Soit $E = \{a, b\}$ un ensemble à deux éléments et $\mathcal{A} := \mathcal{P}(E)$, l'ensemble des parties de E. On admet que $(\mathcal{A}, \Delta, \cap)$ est une structure d'anneau commutatif ; Δ désigne la différence symétrique d'ensembles.

(a) Dresser la liste de tous les idéaux de $\mathcal{A}$. [1]

(b) $\mathcal{A}$ est-il un anneau principal ? [0.5]

(c) Dresser la liste de tous les idéaux maximaux de $\mathcal{A}$. [0.5]

(d) Dresser la liste de tous les idéaux premiers de $\mathcal{A}$. [1]

Partie C. On considère dans $\mathbb{Q}[X]$ le polynôme $m(X) = X^3 - X + 1$.

(1) Montre que m n'a pas de racine dans $\mathbb{Q}$. Puis que m est irréductible sur $\mathbb{Q}$. [1]

(2) Soit α une racine de m dans $\mathbb{C}$. Montrer que m est le polynôme minimal de α sur $\mathbb{Q}$. Puis que si $\gamma \in \mathbb{Q}(\alpha)$ et $\gamma \notin \mathbb{Q}$ alors $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha)$. [1.5]

(3) Soit $\beta := \alpha^2 + \alpha$. Exprimer β^{-1} comme combinaison linéaire de 1, α, α^2. En déduire le polynôme minimal de β sur $\mathbb{Q}$. [1.5]

(Session 2 – 2004)

UNIVERSITE DU SUD TOULON - VAR

Faculté des Sciences et Techniques

Licence de Mathématiques

Module M53

Problème 1. On considère le groupe alterné A_6.

1. Déterminer toutes ses classes de conjugaison ainsi que leurcardinalité. [3]
2. Calculer $\mathrm{Exp}(A_6)$. [1]
3. Déterminer le centre de A_6. [1]
4. Soient a, b, c, d, e, f des éléments distincts de $\{1, 2, 3, 4, 5, 6\}$. Démontrer les identités suivantes [1.5]

$$\begin{aligned}(abc)(bcd) &= (ab)(cd),\\ (abc)(cde) &= (abcde),\\ (abc)(cde)(def) &= (abcd)(ef).\end{aligned}$$

5. Montrer que tout élément de A_6 peut s'écrire comme produitde 3-cycles. [1.5]

Problème 2. Soit $(G, +)$ un groupe abélien et $f : G \to \mathrm{End}(G)$ un morphisme de-groupes abéliens. On convient de noter multiplicativement l'action des éléments de $\mathrm{End}(G)$ surG : pour tout$\varphi \in \mathrm{End}(G)$ et $g \in G$, $\varphi x := \varphi(x)$. On considère la loi decomposition interne $\star$ sur G définie par :$a \star b := f(a)b$.

Vérifier que $(G, +, \star)$ n'est pas en général un anneau. (Indication : penser à utilise-run contre-exemple) [2]

Problème 3. Soit A un anneau commutatif et J un idéal de A. Démontrer que J est premier si et seulement si [2]

$$(ab \in J \quad \text{et} \quad b \notin J) \quad \Longrightarrow \quad a \in J.$$

Problème 4. Soit K corps commutatif, L un sous-corps de K et $0 \neq \alpha \in K$ algébrique sur L. Onrappelle que $L(\alpha)$ désigne l'extension de L par α.

1. (a) Montrer que $L(\alpha^2) \subset L(\alpha)$. [1]

(b) Montrer que l'inclusion réciproque n'est pas vraie en général. [1]

On étudie maintenant un cas où $L(\alpha) = L(\alpha^2)$. Soit m_α le polynôme minimal de α sur L. On supposel'un au moins des monômes non nuls de m_α a un exposant impair. Soit p la somme des monômesde m_α d'exposants pairs et i la somme des monômes de m_α d'exposants impairs.

2. Montrer que p et i sont des polynômes non nuls et que $i(\alpha) \neq 0$. [2]

3. (a) Montrer qu'il existe deux polynômes f et g à coefficients dans L tels que [1]

$$\alpha = \frac{f(\alpha^2)}{g(\alpha^2)}.$$

(b) En déduire que $L(\alpha^2) = L(\alpha)$. [/]

4. (a) Pour $K = \mathbb{R}$ et $L = \mathbb{Q}$ trouver un exemple d'élément $\alpha \in \mathbb{R}$ tel que $\alpha \notin \mathbb{Q}$,α algébrique sur $\mathbb{Q}$ et $L(\alpha^2) = L(\alpha)$. [/]

(b) Expliciter m_α, p, i, f, g dans cetexemple. [/]

(Session 1 – 2005)

Faculté des Sciences et Techniques — Mardi 10 janvier 2006
Université du Sud Toulon-Var — salle Y013, 09h 12h

Corrigé de l'examen d'Algèbre
Première session
Licence de Mathématiques, troisième année, module M53

Problème 1. Voir C.-A. Pillet.

Problème 2. Soit $(G,+) = (\mathbb{Z}^2,+)$ et $f : \mathbb{Z}^2 \to \mathrm{End}\,(\mathbb{Z}^2)$ définie par

$$f(n) = \begin{pmatrix} 0 & n_1 \\ n_2 & 0 \end{pmatrix}, \quad \text{c'est-à-dire} \quad f(n)a = \begin{pmatrix} n_1 a_2 \\ n_2 a_1 \end{pmatrix}.$$

IL est élémentaire de vérifier que $f(n) \in \mathrm{End}\,(\mathbb{Z}^2)$ pour tout $n \in \mathbb{Z}^2$ et que f est un morphisme entre les groupes $(\mathbb{Z}^2,+)$ et $(\mathrm{End}\,(\mathbb{Z}^2),+)$. On montre alors que $\star$ n'a pas d'élément neutre. En effet soit x celui-ci, alors pour tout $a \in \mathbb{Z}^\star \times \{0\}$ on aurait $x \star a = a$ c'est-à-dire

$$\begin{pmatrix} x_1 a_2 \\ x_2 a_1 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \quad \text{soit en particulier} \quad 0 = a_1$$

ce qui contredit le choix de a.

Problème 3. ($\Rightarrow$) Soit $ab \in J$ et $b \notin J$. En notant $p : A \to A/J$ le morphisme (d'anneaux) surjectif qui a tout x de A associe la classe d'équalence de x modulo J on a

$$ab \in J \Rightarrow p(ab) = 0 \quad \Rightarrow \quad p(a)p(b) = 0.$$

Comme $p(b) \neq 0$ car $b \notin J$ et que A/J est intégre alors $p(a) = 0$ et donc $a \in J$.

($\Leftarrow$) Soit α, β and A/J tels que $\alpha\beta = 0$ et $\beta \neq 0$. Soit alors $a \in \alpha$, $b \in \beta$. Comme $\alpha\beta = 0$ et $\beta \neq 0$ on a $ab \in J$ et $b \notin J$ d'où $a \in J$ et donc $\alpha = 0$, ce qui monttre que A/J est intègre.

Problème 4. 1. (a) Comme $\alpha \in L(\alpha)$, on a aussi $\alpha^2 \in L(\alpha)$ puisque $L(\alpha)$ est un corps. Et comme $L(\alpha^2)$ est le plus petit corps contenant α^2 nécessairement $L(\alpha^2) \subset L(\alpha)$.

(b) Soit $L = \mathbb{R}$, $K = \mathbb{C}$ et $\alpha = i$, alors $i^2 = -1 \in L$ et donc $L(i) = \mathbb{C}$ tandis que $L(\alpha^2) = \mathbb{R} \neq \mathbb{C}$.

2. $i \neq 0$ par hypothèse; si $p = 0$ alors m_α n'a pas de terme de degré zéro d'où X divise m ce qui est impossible car m_α est irréductible dans $L[X]$. Enfin si $i(\alpha) = 0$ alors en désignant par $2m+1$ le degré de i et $\{i_{2k+1}\}_k$ ses coefficients on aurait

$$0 = \sum_{k=1}^{m} i_{2k+1}\alpha^{2k+1} = \alpha\left(\sum_{k=i}^{m} i_{2k+1}\alpha^{2k}\right)$$

Comme $\alpha \neq 0$ par hypothèse on trouverait ainsi un polynôme

$$j := \sum_{k=i}^{m} i_{2k+1}X^{2k}$$

qui serait annulé par α; or le degré de ce polynôme est strictement inférieur à celui de i et donc de m_α ce qui est impossible d'après les propriétés du polynôme minimal de α sur L.

3. (a) De $m_\alpha(\alpha) = 0$ et avec les notations de la question 2) on tire $p(\alpha) + \alpha j(\alpha) = 0$; or si $2n$ est le degré de p on a

$$p = \sum_{k=0}^{2n} p_{2k}X^{2k} \quad \text{et donc} \quad p(\alpha) = f(\alpha^2) \quad \text{avec} \quad f = \sum_{k=0}^{2n} p_{2k}X^{k}.$$

De même en posant

$$g = \sum_{k=i}^{m} i_{2k+1}X^{k} \quad \text{on a} \quad g(\alpha^2) = j(\alpha).$$

Enfin comme on a vu que $j(\alpha) \neq 0$ on a aussi $g(\alpha^2) \neq 0$ ce qui permet de conclure que

$$\alpha = \frac{f(\alpha^2)}{g(\alpha^2)}.$$

(b) Du résultat précédent il suit que $\alpha \in L(\alpha^2)$ et donc que $L(\alpha) \subset L(\alpha^2)$ et finalement que $L(\alpha) = L(\alpha^2)$ puisque l'inclusion inverse a été démontrée dans la question 1).

4. (a) Soit $\alpha = 1 + \sqrt{2}$; on a $\alpha \notin \mathbb{Q}$ puisque $\alpha \in \mathbb{Q}$ ssi $\alpha - 1 = \sqrt{2} \in \mathbb{Q}$; or $\sqrt{2} \notin \mathbb{Q}$ est un résultat bien connu dont la preuve a été vu au cours de l'année. Puis $\alpha^2 = 3 + \sqrt{2} = 2 + \alpha$ ce qui montre que $\alpha \in L(\alpha^2)$.

(b) Ici le polynôme minimal est $m_\alpha = (X-1)^2 + 2$, et par conséquent $p = X^2 + 3$, $i = -2X$, $f = X + 3$, $g = -2$.

UNIVERSITE DU SUD TOULON - VAR

Faculté des Sciences et Techniques

Licence de Mathématiques

Module M53

Durée de l'examen : 180 minutes.
Documents autorisés : résumé manuscrit (5 feuilles A4 r/v max).
Barème : les points attribués à chaque problème sont notés en marge.
Toutes les réponses doivent être justifiées.

Problème 1. On considère le groupe multiplicatif $G = \mathbb{Z}_7^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$.

1. Déterminer la table de multiplication de G. [2]
2. G est-il cyclique ? [1]
3. Déterminer l'ordre de chaque élément de G. [1]
4. Déterminer l'exposant de G. [1]
5. Déterminer les sous-groupes de G. [2]
6. Déterminer la table de multiplication du groupe $K = \mathbb{Z}_7^*/\{\bar{1}, \bar{6}\}$. [2]
7. Montrer que K est cyclique. [1]

Problème 2. Soit $(A, +, \cdot)$ un anneau commutatif et x un élément de A fixé. Dans ce problème on note mutiplicativement la deuxième loi, c'est-à-dire : $\forall a, b \in A$, $ab := a \cdot b$. On définit sur $B := A \times A$ les lois de composition interne suivantes :

$$(a, b) + (c, d) := (a + c, b + d), \quad (a, b)(c, d) := (ac + xbd, ad + bc).$$

(a) Expliquer brièvement pourquoi ces lois sont internes. [0.5]

(b) Démontrer que B muni de ces deux lois est un anneau commutatif. [1.5]

(c) Montrer que B contient un sous-anneau B_1 isomorphe à A. Dans la suite on identifie les éléments de B_1 avec ceux de A. 1.5

(d) Vérifier que x est le carré d'un élément ω de B. 0.5

Cela justifie la terminologie : B est une extension quadratique de A ; elle est notée $B := A[\sqrt{x}]$.

(e) Vérifier que tout élément de B se met sous la forme $a + b\omega$ avec $a, b \in B_1$ et que cette décompostion est unique. [1]

(f) On appelle conjugué de $z := a + b\omega \in B$ l'élément de B noté et défini par $\bar{z} := a - b\omega$. Vérifier les règles de calcul

$$\bar{\omega} = -\omega, \quad \forall z \in A \equiv B_1, \bar{z} = z, \quad \forall z, u \in B, \quad \overline{z + u} = \bar{z} + \bar{u}, \quad \overline{zu} = \bar{z}\bar{u}, \quad \bar{\bar{z}} = z.$$

[0.5]

(g) Pour tout $z \in B$ on appelle norme de z, que l'on note $N(z)$, l'expression

$$N(z) := z\bar{z}.$$

Vérifier que N prend ses valeurs dans $A \equiv B_1$ et que

$$N(1_B) = 1_A, \quad \forall z, u \in B, \quad N(zu) = N(z)N(u), \quad N(z) = N(\bar{z}).$$

1

(h) Démontrer le théorème suivant : pour que $z \in B$ soit inversible (vis-à-vis de la deuxième LCI) il faut et suffit que $N(z)$ soit inversible dans A. 2

(i) On suppose à partir de maintenant que A est un corps. Vérifier que ω est algébrique sur A ; quel est le degré de l'extension B de A ? 0.5

(j) Démontrer le théorème suivant : $A[\sqrt{x}]$ est un corps si et seulement si x n'est pas le carré d'un élément de A. 2

(Session 2 – 2005)

UNIVERSITE DU SUD TOULON - VAR

Faculté des Sciences et Techniques

Licence de Mathématiques

Module M53

Durée de l'examen : 180 minutes.
Documents autorisés : résumé manuscrit (2 feuilles A4 r/v max).
Barème : les points attribués à chaque problème sont notés en marge.

Problème 1. Dans ce problème tous les groupes sont notés multiplicativement et on dénote par $C_n = \{z \in \mathbb{C} \mid z^n = 1\}$ le groupe cyclique d'ordre n des racines n-èmes de l'unité.

Si G est un groupe abélien fini d'exposant $m = \mathrm{Exp}(G)$ on dénote par $G^* = \mathrm{Hom}(G, C_m)$ l'ensemble des morphismes de G dans le groupe cyclique C_m.

1. Montrer que $(f \cdot g)(x) = f(x)g(x)$ définit une loi de composition interne sur G^*. [2]
2. Montrer que G^* est un groupe abélien. On l'appelle groupe dual du groupe G. [1]
3. Montrer que si G et H sont des groupes abéliens finis isomorphes alors $G^* \simeq H^*$. [1]
4. On considère maintenant le cas particulier des groupes cycliques, c'est-à-dire $G = C_m$. On pose $\xi = e^{2\pi i/m}$. Montrer que l'application

$$\begin{array}{ccc} G & \to & G^* \\ \xi^k & \mapsto & f_k, \end{array}$$

définie par $f_k(z) = z^k$ est un isomorphisme. [3]

5. On admettra le théorème suivant : Si G et H sont des groupes abéliens finis alors $(G \times H)^* \simeq G^* \times H^*$. En déduire que tout groupe abélien fini est isomorphe à son dual. [3]

Problème 2. Soit $(X, \star)$ un magma associatif, c'est-à-dire un ensemble X muni d'une loi de composition interne associative notée $\star$; on ne suppose pas que $\star$ est commutative. Soit $(A, +, \times)$ un anneau et B le sous-ensemble des applications de X dans A telles que

$$B \ni f \iff \mathrm{card}\{x \in X \mid f(x) \neq 0\} < \infty.$$

On munit B des lois suivantes (la multiplication de A est notée dans la suite $a \times b = ab$) :

$$\begin{array}{rcl} (f,g) \in B \times B & \mapsto & f + g \in B, \\ (f,g) \in B \times B & \mapsto & fg := f \times g \in B, \end{array} \qquad \begin{array}{rcl} (f+g)(x) & := & f(x) + g(x), \\ (fg)(x) & := & \sum_{y \star z = x} f(y)g(z). \end{array}$$

a) Vérifier que ces deux lois sont des lois de composition interne sur B. [2]

b) Démontrer que ces deux lois font de B un anneau. [2]

c) On suppose A commutatif. Comment s'appelle B lorsque $(X, \star) = (\mathbb{N}, +)$ c'est-à-dire le magma associatif constitué des nombres entiers naturels muni de l'addition. [1]

Problème 3. Soit i la racine carrée complexe usuelle de -1 et $\mathbb{C} \supset L := \mathbb{Q}(\sqrt{2}, i)$ l'extension de $\mathbb{Q}$ par $\sqrt{2}$ et i. Le but de ce problème est de déterminer $[L : \mathbb{Q}]$, le degré de L comme extension de $\mathbb{Q}$ et de donner une base de L comme $\mathbb{Q}$-espace

vectoriel. On admet que le degré de $\mathbb{Q}(\sqrt{2})$ comme extension de $\mathbb{Q}$ est 2. Le candidat a le choix de la méthode. Il peut s'il le désire suivre la méthode suivante.

a) Soit $\alpha := \sqrt{2} + \mathrm{i}$. Vérifier que α est algébrique sur $\mathbb{Q}$ et que $\mathbb{Q}(\alpha) \subset \mathrm{L}$. [1]

b) Calculer $\sqrt{2}$ et i en fonction de α et α^{-1}. En déduire que $\mathrm{L} = \mathbb{Q}(\alpha)$. [1]

c) En considérant la tour $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathrm{L}$ vérifier que $[\mathrm{L} : \mathbb{Q}]$ est pair. [0.5]

d) Vérifier que $\{1, \sqrt{2}, \mathrm{i}\}$ est libre dans le $\mathbb{Q}$-espace vectoriel $\mathbb{C}$. En déduire que [1]

$$[\mathrm{L} : \mathbb{Q}] \geqslant 4.$$

e) Montrer que le polynôme minimal de α sur $\mathbb{Q}$ est de degré 4. [1]

f) Conclure. [0.5]

(Session 1 – 2006)

Faculté des Sciences et Techniques — Lundi 08 janvier 2007
Université du Sud Toulon-Var — salle Amphi 400, 09h 12h

Examen d'Algèbre
Première session
Licence de Mathématiques, troisième année, module M53

Problème 1.

Problème 2. Soit $(X, \star)$ un magma associatif, c'est-à-dire un ensemble X muni d'une loi de composition interne associative notée $\star$; on ne suppose pas que $\star$ est commutative. Soit $(A, +, \times)$ un anneau et B le sous-ensemble des applications de E dans A telles que

$$B \ni f \iff \text{card}\,\{x \in X, f(x) \neq 0\} < \infty.$$

On munit B des lois suivantes (la multiplication de A est notée dans la suite $a \times b =: ab$):

$$\begin{aligned} (f,g) \in B \times B \to f+g \in B, \qquad & (f+g)(x) := f(x) + g(x), \\ (f,g) \in B \times B \to fg := f \times g \in B, \qquad & (fg)(x) := \sum_{y \star z = x} f(y)g(z). \end{aligned}$$

a) Vérifier que ces deux lois sont des lois de composition interne sur B. [2]

b) Démontrer que ces deux lois font de B un anneau. [2]

c) On suppose A commutatif. Comment s'appelle B lorsque $(X, \star) = (\mathbb{N}, +)$ c'est-à-dire le magma associatif constitué des nombres entiers naturels muni de l'addition. [1]

Problème 3. Soit i la racine carré complexe usuelle de -1 et $\mathbb{C} \supset L := \mathbb{Q}(\sqrt{2}, i)$ l'extension de $\mathbb{Q}$ par $\sqrt{2}$ et i. Le but de ce problème est de déterminer: $[L : \mathbb{Q}]$, le degré de L comme extension de $\mathbb{Q}$ et de donner une base de L comme $\mathbb{Q}$-e.v.. On admet que le degré de $\mathbb{Q}(\sqrt{2})$ comme extension de $\mathbb{Q}$ est 2. Le candidat a le choix de la méthode. Il peut s'il le désire suivre la méthode suivante.

a) Soit $\alpha := \sqrt{2} + i$. Vérifier que α est algébrique sur $\mathbb{Q}$ et que $\mathbb{Q}(\alpha) \subset L$. [1]

b) Calculer $\sqrt{2}$ et i en fonction de α et α^{-1}. En déduire que $L = \mathbb{Q}(\alpha)$. [1]

c) En considérant la tour $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2} \subset L$ vérifier que $[L : \mathbb{Q}]$ est pair. [0.5]

d) Vérifier que $\{1, \sqrt{2}, i\}$ est libre dans le $\mathbb{Q}$-espace vectoriel $\mathbb{C}$. En déduire que $[L : \mathbb{Q}] \geq 4$. [1]

e) Montrer que le polynôme minimal de α sur $\mathbb{Q}$ est de degré 4. [1]

f) Conclure. [0.5]

Université du Sud Toulon-Var salle Amphi 400, 09h 12h

Corrigé de l'examen d'Algèbre
Première session
Licence de Mathématiques, troisième année, module M53

Problème 2. a) Soit $f \in B$, on désigne par $\operatorname{supp} f$ l'ensemble des $x \in X$ pour lesquels $f(x) \neq 0$. Par définition $\operatorname{supp} f$ est fini pour tout $f \in B$. On commence par vérifier que $f+g$ est bien définie. D'une part $f+g$ est bien une application de X dans A, car $f(x)+g(x) \in A$ pour tout $x \in X$ puisque A est un anneau. D'autre part on a (évidemment)

$$\operatorname{supp} f+g \subset \operatorname{supp} f \cup \operatorname{supp} g$$

et donc le support de $f+g$ est aussi fini. Donc $f+g \in B$. On passe maintenant à la deuxième loi. On a

$$\{(y,z) \in X \times X,\ f(y) \neq 0 \text{ et } g(z) \neq 0\} = \operatorname{supp} f \times \operatorname{supp} g$$

qui est fini puisque les deux facteurs $\operatorname{supp} f$ et $\operatorname{supp} g$ sont finis. Donc pour tout $x \in X$, $\sum_{y \star z = x} f(y)g(z)$ est une somme finie de produits d'élément de A, c'est donc un élément de A puisque ce dernier est un anneau. Cela montre que $(fg)(x)$ est bien défini pour tout $x \in X$. Reste à prouver que $\operatorname{supp} fg$ est fini. On va établir que

$$\operatorname{supp} fg \subset \operatorname{supp} f \star \operatorname{supp} g$$

ce qui suffit pour prouver que $\operatorname{card} \operatorname{supp} fg < \infty$ car: $\operatorname{supp} f$ et $\operatorname{supp} g$ fini impliquent bien sur que $\operatorname{supp} f \star \operatorname{supp} g$ est fini. On a

$$x \notin \operatorname{supp} fg \quad \Longleftarrow \quad (y \star z = x \Rightarrow f(y)g(z) = 0)$$

et donc en prenant la négation

$$\begin{aligned} x \in \operatorname{supp} fg \quad &\Longrightarrow \quad (\exists y,z \in X,\ y \star z = x \text{ et } f(y)g(z) \neq 0) \\ &\Longrightarrow \quad (\exists y,z \in X,\ y \star z = x \text{ et } y \in \operatorname{supp} f \text{ et } z \in \operatorname{supp} g) \end{aligned}$$

ce qui prouve l'inclusion annoncée.

b) α) $(B,+)$ est un groupe abélien. En effet

$$\begin{aligned} &+ \text{ est associative} \\ \text{déf. de l'assoc.} \iff\ &\forall f,g,h \in B, \quad f+(g+h) = (f+g)+h \\ \text{déf. de l'égalité des appl.} \iff\ &\forall f,g,h \in B, x \in X, \quad (f+(g+h)(x) = ((f+g)+h)(x) \\ \text{déf. de + sur B} \iff\ &\forall f,g,h \in B, x \in X, \quad f(x)+(g+h)(x) = (f+g)(x)+h(x) \\ \text{déf. de + sur B} \iff\ &\forall f,g,h \in B, x \in X, \quad f(x)+(g(x)+h(x)) = (f(x)+g(x))+h(x) \\ \text{car + est associative sur } A \iff\ &\text{VRAI} \end{aligned}$$

La preuve de la commutativité de + se conduit comme au-dessus, en plus simple. + possède un élément neutre, il s'agit de l'application: $0_B : X \to A$, définie par:

$$\forall x \in X, \quad 0_B(x) := 0_A.$$

On remarque que comme $\operatorname{supp} 0_B = \emptyset$, il est fini. Enfin tout élément $f \in B$ possède un symétrique:

$$-f : X \to A; \quad \forall x \in X,\ (-f)(x) := -f(x).$$

La vérification de ces deux dernières affirmations est évidente.

β) On montre maintenant que $(B, \times)$ est un monoïde. D'abord x est associative. On calcule pour tout f, g, h dans B

$$\begin{aligned}(f(gh))(x) &= \sum_{y\star z=x} f(y)(gh)(z) = \sum_{y\star z=x} f(y) \sum_{u*v=z} g(u)h(v) \\ &= \sum_{\substack{y\star z=x \\ u*v=z}} f(y)g(u)h(v) \quad \text{car } \times \text{ est dist. sur } + \text{ dans } A \\ &= \sum_{y\star u\star v=x} f(y)g(u)h(v)\end{aligned}$$

car on a égalité des deux ensembles suivants (élémentaire à vérifier)

$$\{(y,u,v) \in X^3,\ \exists z \in X,\ y \star z = x \text{ et } u \star v = z\} = \{(y,u,v) \in X^3,\ y \star u \star v = x\}.$$

De même

$$(f(gh))(x) = \sum_{\substack{y\star z=x \\ u*v=y}} f(u)g(v)h(z) = \sum_{u\star v\star z=x} f(u)g(v)h(z)$$

en procédant dans cette dernière expression aux changements de variables muettes

$$u \to y, \quad v \to u, \quad z \to v$$

on établit l'égalité $(f(gh))(x) = (f(gh))(x)$ et ceci pour tout x ce qui montre l'associativité de la deuxième LCI.

L'application $I_B : X \to A$ définie par $1_B(x) = 1_A$ est l'élément neutre de cette deuxième LCI.

γ) Enfin $\times$ est distributive sur $+$. On calcule

$$\begin{aligned}((f+g)h)(x) &= \sum_{y\star z=x} (f+g)(y)h(z) \quad (\text{déf. de } \times \text{ sur } B) \\ &= \sum_{y\star z=x} (f(y)+g(y))h(z) \quad (\text{déf. de } + \text{ sur } B) \\ &= \sum_{y\star z=x} (f(y)h(z)+g(y)h(z)) \quad (\text{dist. de } \times \text{ sur } + \text{ dans } A) \\ &= \left(\sum_{y\star z=x} f(y)h(z)\right) + \left(\sum_{y\star z=x} g(y)h(z))\right) \quad (\text{ass. de } + \text{ dans } A) \\ &= (fh)(x) + (gh)(x) \quad (\text{déf. de } \times \text{ sur } B)\end{aligned}$$

ce qui montre que $(f+g)h = fh + gh$ et ceci pour tout $f, g, h \in B$. La preuve de $f(g+h) = fg + fh$ est analogue.

c) Il s'agit de l'anneau des polynômes à coefficients dans A. En effet soit $f : \mathbb{N} \to A$ telle que $\operatorname{supp} f < \infty$, f définit un polynôme à coefficients dans A puisque l'image de f est une suite finie de coefficients dans A:

$$\{f(0), f(1), \ldots, f(m), 0, \ldots\}$$

si m est le plus grand élément de $\operatorname{supp} f$. Il est alors évident de vérifier que la loi $+$ de B est bien l'addition des polynômes; de même pour la deuxième LCI on a

$$(fg)(k) = \sum_{i+j=k} f(i)g(j)$$

qui est bien la multiplication des polynômes.

Problème 3. a) On calcule successivement $\alpha^2 = 1 + 2\sqrt{2}i$ puis $(\alpha^2 - 1)^2 = -8$ et donc α est racine du polynôme $P \in \mathbb{Q}[X]$:

$$P = X^4 - 2X^2 + 9$$

ce qui montre que α est algébrique sur $\mathbb{Q}$. Comme α est une expression polynomiale à coefficients dans $\mathbb{Q}$ de $\sqrt{2}$ et i, on a $\alpha \in L$ et par définition de $\mathbb{Q}(\alpha)$ on a $\mathbb{Q}(\alpha) \subset L$.
b) Comme $\alpha^{-1} = \sqrt{2} - i$ on a $\sqrt{2} = (\alpha + \alpha^{-1})/2$ et $i = (\alpha - \alpha^{-1})/2$ et en particulier $\{\sqrt{2}, i\} \subset \mathbb{Q}(\alpha)$ puisque ces derniers sont des expressions rationnelles à coefficients dans $\mathbb{Q}$ en α et α^{-1}. Il suit d'après la définition de L que $L \subset \mathbb{Q}(\alpha)$ et finalement $L = \mathbb{Q}(\alpha)$ d'après la question précédente.
c) On sait que $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}), \mathbb{Q}]$. Comme il a été rappelé dans l'énoncé que $[\mathbb{Q}(\sqrt{2}), \mathbb{Q}] = 2$, il suit que $[L : \mathbb{Q}]$ est pair.
d) Soit α, β, γ dans $\mathbb{Q}$ tels que $\alpha 1 + \beta\sqrt{2} + \gamma i = 0$. Il suit que $\alpha + \beta\sqrt{2} = \gamma = 0$ puisque ce sont respectivement les parties réelles et imaginaire d'un nombre complexe nul. Comme cela a été rappelé dans l'énoncé, $\{1, \sqrt{2}\}$ est un système de rang 2 dans le $\mathbb{Q}$ e.v. $\mathbb{C}$ (puisque $[\mathbb{Q}(\sqrt{2}, \mathbb{Q}] = 2$) et donc on a aussi $\alpha = \beta = 0$. On a trouvé un système de trois vecteurs linéairement indépendants dans le $\mathbb{Q}$ e.v. L, ce dernier a donc pour dimension au moins 3. Or comme on a vu que cette dimension est paire, on a obtenu

$$[L : \mathbb{Q}] \geq 4.$$

e) Soit m_α le polynôme minimal de α sur $\mathbb{Q}$. Comme le polynôme P obtenu au a) s'annule en α on sait que m_α divise P, ce qui montre que $\deg m_\alpha \leq \deg P = 4$. Or d'après la question précédente $\deg m_\alpha = [L : \mathbb{Q}] \geq 4$. Il suit que $\deg m_\alpha = 4$.
f) On a donc obtenu que $[L : \mathbb{Q}] = \deg m_\alpha = 4$; et au passage que $m_\alpha = P$ puisque P est normé. Enfin une base de L est

$$\{1, \alpha, \alpha^2, \alpha^3\} = \{1, \sqrt{2} + i, 1 + 2\sqrt{2}i, 5i - \sqrt{2}\}.$$

UNIVERSITE DU SUD TOULON - VAR

FACULTÉ DES SCIENCES ET TECHNIQUES

Licence de Mathématiques

Module M53

Durée de l'examen : 180 minutes.
Documents autorisés : aucun.
Barème : les points attribués à chaque problème sont notés en marge.
Toutes les réponses doivent être justifiées.

Problème 1. Soit G le sous-groupe du groupe symétrique S_4 engendré par les deux permutations

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

1. Montrer que G est abélien d'ordre 4. [2]
2. Déterminer l'ordre de chaque élément de G. [1]
3. Déterminer l'exposant de G. [1]
4. Soient H_σ et H_τ les sous-groupes de G engendrés par σ et τ. Montrer que $G = H_\sigma \otimes H_\tau$. [2]
5. Qu'elle est la stucture de G ? (décomposition en produit direct de sous-groupes cycliques). [1]
6. On considère l'action naturelle du groupe G sur l'ensemble $X = \{1, 2, 3, 4\}$. Déterminer les orbites de cette action. [1]
7. Pour chaque $x \in X$ déterminer le stabilisateur G_x ainsi que son indice $[G : G_x]$. [1]
8. Déterminer l'ensemble $\mathrm{Fix}\, g$ des points fixes de chaque élément $g \in G$. [1]
9. Vérifier l'identité

$$\sum_{x \in X} (1 - \frac{1}{|G_x|}) = \frac{1}{|G|} \sum_{g \in G \setminus \{Id\}} |\mathrm{Fix}\, g|.$$

Sur quoi porte la somme du membre de gauche de cette identité ? [2]

Problème 2. On considère sur $\mathbb{R}^2$ les deux lois de composition interne suivantes

$$\begin{aligned} (a, b) + (a', b') &:= (a + a', b + b') \\ (a, b) \times (a', b') &:= (aa' + bb', ab' + a'b)). \end{aligned}$$

1. Démontrer que $(\mathbb{R}^2, +, \times)$ est un anneau commutatif. [3]
2. Est-il intègre ? [2]

Problème 3. Soit $\omega := \sqrt{5} + 2i\sqrt{3}$ dans $\mathbb{C}$, où $i^2 = -1$.

1. Montrer que ω est algébrique sur $\mathbb{Q}$ (les nombres rationnels). [1.5]
2. Vérifier que $\bar{\omega}$, le conjugué complexe de ω, appartient à $\mathbb{Q}(\omega)$. On rappelle que $\mathbb{Q}(\omega)$ désigne l'extension de $\mathbb{Q}$ par ω. [0.5]
3. (Facultative) Démontrer que si $n \neq 0$ est un entier naturel premier alors $\sqrt{n}$ n'est pas rationnel. [1]
4. Déterminer le polynôme minimal de ω sur $\mathbb{Q}$, la dimension de $\mathbb{Q}(\omega)$ sur $\mathbb{Q}$ et une base de $\mathbb{Q}(\omega)$ sur $\mathbb{Q}$. [3]

(Session 2 – 2006)

UNIVERSITE DU SUD TOULON - VAR

Faculté des Sciences et Techniques

Licence de Mathématiques

Module M53

Durée de l'examen : 180 minutes.
Documents autorisés : aucun.
Barème : les points attribués à chaque problème sont notés en marge.

Toutes les réponses doivent être justifiées !

Problème 1. Soit $\mathrm{GL}(2,\mathbb{R})$ le groupe des automorphismes du plan vectoriel $\mathbb{R}^2$:

$$\mathrm{GL}(2,\mathbb{R}) = \left\{ g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} | a,b,c,d \in \mathbb{R}, \det g = ad - bc \neq 0 \right\}.$$

(a) Déterminer le sous-groupe $G \subset \mathrm{GL}(2,\mathbb{R})$ des endomorphismes laissant invariant le sous-ensemble $\mathbb{Z}^2 \subset \mathbb{R}^2$, c'est-à-dire

$$G = \{g \in \mathrm{GL}(2,\mathbb{R}) | g\mathbb{Z}^2 \subset \mathbb{Z}^2\}.$$

[2]

(b) Montrer que $\mathbb{Z}$ est l'image de G par le morphisme $g \mapsto \det g$. [2]

(c) Montrer que tout $g \in G$ est une bijection de $\mathbb{Z}^2$ dans $\mathbb{Z}^2$. [2]

(d) En considérant $\mathbb{Z}^2$ comme un sous-groupe du groupe additif $\mathbb{R}^2$, montrer que pour tout $g \in G$

$$\begin{array}{rccc} \hat{g}: & \mathbb{R}^2/\mathbb{Z}^2 & \to & \mathbb{R}^2/\mathbb{Z}^2 \\ & x+\mathbb{Z}^2 & \mapsto & gx+\mathbb{Z}^2 \end{array}$$

définit un endomorphisme $\hat{g}$ du groupe quotient $\mathbb{R}^2/\mathbb{Z}^2$. [2]

(e) Montrer que $\hat{g}$ est bijectif et que $\phi : G \to \mathrm{Aut}(\mathbb{R}^2/\mathbb{Z}^2)$, définit par $\phi(g) = \hat{g}$ est un morphisme injectif. [2]

Problème 2. Soit A un anneau commutatif et $f : A \to \mathbb{R}_+$ une application réelle positive définie sur A qui vérifie : (i) $f(x) = 0$ si et seulement si $x = 0$, (ii) $\forall x,y \in A$, $f(xy) = f(x)f(y)$, (iii) $\forall x,y \in A$, $f(x+y) \leqslant \max\{f(x), f(y)\}$.

(a) Démontrer que $F := \{x \in A | f(x) \leqslant 1\}$ est un sous-anneau de A. [2]

(b) Démontrer que $U := \{x \in A | f(x) < 1\}$ est un idéal de F. [1]

Problème 3. Soit A un anneau commutatif. Pour tout idéal I de A on définit $R[I] := \{x \in A | \exists n \in \mathbb{N}^*, x^n \in I\}$.

(a) Montrer que $R[I]$ est un idéal de A qui contient I. [1]

(b) Montrer que $R[R[I]] = R[I]$. [1]

(c) Montrer que $R[I \cap J] = R[I] \cap R[J]$. [1]

(d) Facultative. Comment s'appellent les éléments de $R[\{0\}]$? [0.5]

Problème 4. Soit $u := \sqrt{2} + i\sqrt{3}$ un élément de $\mathbb{C}$, l'ensemble des nombres complexes, avec $i^2 = -1$. On admet que $\sqrt{2}$ et $\sqrt{3}$ sont deux éléments algébriques sur $\mathbb{Q}$, le corps des nombres rationnels et que leurs polynômes minimaux sur $\mathbb{Q}$ sont tous deux de degré 2. On rappelle que $\mathbb{Q}(a)$ avec $a \in \mathbb{C}$ désigne le plus petit sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$ et a.

(1) Montrer que u est algébrique sur $\mathbb{Q}$. [1]

(2) (a) Calculer $\sqrt{2}$ et $i\sqrt{3}$ en fonction de u et u^{-1}. [0.5]

(b) En déduire que $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(u)$.

(c) Montrer que le degré de $\mathbb{Q}(u)$ sur $\mathbb{Q}$ est pair. [1]

(d) Montrer que $\mathbb{Q}(u)$ est différent de $\mathbb{Q}(\sqrt{2})$. [0.5]

(3) (a) Déterminer le polynôme minimal de u sur $\mathbb{Q}$. [1]

(b) Décrire les éléments de $\mathbb{Q}(u)$ au moyen de puissances de u.

(Session 1 – 2007)

M53 – Seconde session 2008

Problème 1. (a) Les éléments de $G = \mathbb{Z}_{15}^*$ sont les classes de congruences modulo 15 des entiers premiers à 15, c'est à dire $1, 2, 4, 7, 8, 11, 13, 14$. G est d'ordre 8, sa table de multiplication est

	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{7}$	$\bar{8}$	$\overline{11}$	$\overline{13}$	$\overline{14}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{7}$	$\bar{8}$	$\overline{11}$	$\overline{13}$	$\overline{14}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{8}$	$\overline{14}$	$\bar{1}$	$\bar{7}$	$\overline{11}$	$\overline{13}$
$\bar{4}$	$\bar{4}$	$\bar{8}$	$\bar{1}$	$\overline{13}$	$\bar{2}$	$\overline{14}$	$\bar{7}$	$\overline{11}$
$\bar{7}$	$\bar{7}$	$\overline{14}$	$\overline{13}$	$\bar{4}$	$\overline{11}$	$\bar{2}$	$\bar{1}$	$\bar{8}$
$\bar{8}$	$\bar{8}$	$\bar{1}$	$\bar{2}$	$\overline{11}$	$\bar{4}$	$\overline{13}$	$\overline{14}$	$\bar{7}$
$\overline{11}$	$\overline{11}$	$\bar{7}$	$\overline{14}$	$\bar{2}$	$\overline{13}$	$\bar{1}$	$\bar{8}$	$\bar{4}$
$\overline{13}$	$\overline{13}$	$\overline{11}$	$\bar{7}$	$\bar{1}$	$\overline{14}$	$\bar{8}$	$\bar{4}$	$\bar{2}$
$\overline{14}$	$\overline{14}$	$\overline{13}$	$\overline{11}$	$\bar{8}$	$\bar{7}$	$\bar{4}$	$\bar{2}$	$\bar{1}$

(b) Les ordres des éléments sont

a	$\omega(a)$
$\bar{1}$	1
$\bar{2}$	4
$\bar{4}$	2
$\bar{7}$	4
$\bar{8}$	4
$\overline{11}$	2
$\overline{13}$	4
$\overline{14}$	2

(c) G n'admet aucun élément d'ordre $|G| = 8$, il n'est donc pas cyclique.

(d) G étant abélien, son exposant est donné par $\mathrm{Exp}(G) = \mathrm{ppcm}\{\omega(a) | a \in G\} = 4$.

(e) Les sous-groupes de G sont d'ordre $1, 2, 4$ ou 8 (les diviseurs de $|G| = 8$).

- 1. Il n'y a qu'un sous-groupe d'ordre 1, c'est $\{\bar{1}\}$.
- 2. Les sous-groupes d'ordre 2 sont cycliques. Ils sont donc formés de l'élément neutre et d'un élément d'ordre 2: $\{\bar{1}, \bar{4}\}$, $\{\bar{1}, \overline{11}\}$, $\{\bar{1}, \overline{14}\}$.
- 4. Les sous-groupes d'ordre 4 sont soit cycliques, soit isomorphes au petit groupe de Klein ($\simeq C_2 \times C_2$). Dans le premier cas, il sont engendrés par un élémént d'ordre 4:

  $$\{\bar{1}, \bar{2}, \bar{4}, \bar{8}\},\ \{\bar{1}, \bar{4}, \bar{7}, \overline{13}\}.$$

  Dans le second cas, ils sont formés de l'élément neutre et de trois éléments d'ordre 2:

  $$\{\bar{1}, \bar{4}, \overline{11}, \overline{14}\}$$

- 8. Le seul sous-groupe d'ordre 8 est G lui même.

(f) On a $|G| = 8 = 2^3$. Les partitions de 3 sont $1+1+1$, $1+2$ et 3. Les structures possibles sont donc $C_2 \times C_2 \times C_2$, $C_2 \times C_4$ et C_8. La dernière possibilité est exclue par le fait que G n'est pas cyclique (question (c)). La première possibilité exclut tout élément d'ordre 4. On en conclut que

$$G \simeq C_2 \times C_4.$$

UNIVERSITE DU SUD TOULON - VAR

Faculté des Sciences et Techniques

Licence de Mathématiques

Module M53

Durée de l'examen : 180 minutes.
Documents autorisés : aucun.
Barème : les points attribués à chaque problème sont notés en marge.

Toutes les réponses doivent être justifiées !

Problème 1. On considère le groupe (multiplicatif) $G \equiv \mathbb{Z}_{15}^*$.

(a) Ecrire la table de multiplication de G. [2]

(b) Déterminer l'ordre de chaque élément de G. [2]

(c) G est-il cyclique ? Si oui, en donner un générateur. [1]

(d) Quel est l'exposant de G ? [1]

(e) Déterminer tous les sous-groupes de G. [2]

(f) Déterminer la structure de G. [2]

Problème 2. Soit A un anneau commutatif et $f : A \to \mathbb{R}_+$ une application réelle positive définie sur A qui vérifie : (i) $f(x) = 0$ si et seulement si $x = 0$, (ii) $\forall x, y \in A$, $f(xy) = f(x)f(y)$, (iii) $\forall x, y \in A$, $f(x+y) \leqslant \max\{f(x), f(y)\}$.

(a) Démontrer que $F := \{x \in A | f(x) \leqslant 1\}$ est un sous-anneau de A. [2]

(b) Démontrer que $U := \{x \in A | f(x) < 1\}$ est un idéal de F. [1]

Problème 3. Soit A un anneau commutatif. Pour tout idéal I de A on définit $R[I] := \{x \in A | \exists n \in \mathbb{N}^*, x^n \in I\}$.

(a) Montrer que $R[I]$ est un idéal de A qui contient I. [1]

(b) Montrer que $R[R[I]] = R[I]$. [1]

(c) Montrer que $R[I \cap J] = R[I] \cap R[J]$. [1]

(d) Facultative. Comment s'appellent les éléments de $R[\{0\}]$? [0.5]

Problème 4. Soit $u := \sqrt{2} + i\sqrt{3}$ un élément de $\mathbb{C}$, l'ensemble des nombres complexes, avec $i^2 = -1$. On admet que $\sqrt{2}$ et $\sqrt{3}$ sont deux éléments algébriques sur $\mathbb{Q}$, le corps des nombres rationnels et que leurs polynômes minimaux sur $\mathbb{Q}$ sont tous deux de degré 2. On rappelle que $\mathbb{Q}(a)$ avec $a \in \mathbb{C}$ désigne le plus petit sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$ et a.

(1) Montrer que u est algébrique sur $\mathbb{Q}$. [1]

(2) (a) Calculer $\sqrt{2}$ et $i\sqrt{3}$ en fonction de u et u^{-1}. [0.5]

(b) En déduire que $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(u)$.

(c) Montrer que le degré de $\mathbb{Q}(u)$ sur $\mathbb{Q}$ est pair. [1]

(d) Montrer que $\mathbb{Q}(u)$ est différent de $\mathbb{Q}(\sqrt{2})$. [0.5]

(3) (a) Déterminer le polynôme minimal de u sur $\mathbb{Q}$. [1]

(b) Décrire les éléments de $\mathbb{Q}(u)$ au moyen de puissances de u.

(Session 2 – 2007)