Contrôle continu du 13 octobre.

Documents, calculatrices, téléphones portables interdits. Durée 2 heures

Exercice 1 :

Soit A un anneau commutatif et x et y des éléments de A. On note $\overline{y}$ la classe de y dans l'anneau quotient $B = A/(x)$. Etablir un isomorphisme entre les anneaux quotients $A/(x, y)$ et $B/(\overline{y})$.

Exercice 2 :

On considère le sous-anneau A de $\mathbb{Z}[X]$ formé des polynômes dont le coefficient du terme de degré 1 est divisible par 3.

1. Pourquoi l'anneau A est-il intègre ?
2. Quels sont les éléments inversibles de A ?
3. Montrer que $3X$ est un polynôme irréductible de A.
4. En considérant le polynôme $9X^2$, montrer que l'idéal de A engendré par $3X$ n'est pas un idéal premier de A. L'anneau A est-il factoriel ?
5. Soit I l'idéal de A engendré par $3X$ et X^2. L'idéal I est-il premier ?
6. Donner deux idéaux maximaux de A qui contiennent I.
7. Les polynômes $3X$ et X^2 ont-ils un pgcd dans A ?
8. Les polynômes $3X$ et X^2 ont-ils un ppcm dans A ?

Exercice 3 :

On considère le morphisme de $\mathbb{C}$-algèbres $\phi : \mathbb{C}[X, Y] \to \mathbb{C}[T]$ défini par $\phi(X) = T^2$ et $\phi(Y) = T^3$.

1. Le morphisme ϕ est-il surjectif ?
2. Montrer que le noyau de ϕ est l'idéal de $\mathbb{C}[X, Y]$ engendré par $Y^2 - X^3$.
3. L'anneau quotient $A = \mathbb{C}[X, Y]/(Y^2 - X^3)$ est-il intègre ?
4. Montrer que l'élément $\overline{X}$ de A est un irréductible de A.
5. L'anneau quotient $\mathbb{C}[X, Y]/(Y^2 - X^3)$ est-il factoriel ?

Exercice 4 :

Soit A un anneau factoriel et $z \in A$.

1. Montrer l'équivalence :
   (a) L'anneau quotient $A[X]/(X^2 - z)$ est intègre.
   (b) z n'est pas le carré d'un élément de A.
2. Soit P un polynôme de $A[X]$ et $a \in A \setminus \{0\}$. Montrer que si le polynôme $aP - 1$ est divisible par $X^2 - z$ alors a est inversible dans A.
3. Montrer l'équivalence :
   (a) L'anneau quotient $A[X]/(X^2 - z)$ est un corps.
   (b) L'anneau A est un corps et z n'est pas le carré d'un élément de A.
4. On suppose que z n'est ni inversible ni nul. Montrer que l'idéal de l'anneau quotient $A[X]/(X^2 - z)$ engendré par $\overline{X}$ est premier si et seulement si z est irréductible dans A.

Contrôle continu 2

Exercice 1 :

On considère le sous-corps L du corps $\mathbb{C}$ qui est le corps de décomposition du polynôme X^4+12 de $\mathbb{Q}[X]$.

1. Montrer que le polynôme X^4+12 admet 4 racines distinctes α_1, α_2, $\alpha_3=-\alpha_1$ et $\alpha_4=-\alpha_2$ dans $\mathbb{C}$ et déterminer α_1 et α_2.
2. Montrer que $L=\mathbb{Q}(\alpha_1,\alpha_2)=\mathbb{Q}(i,\alpha_1)$.
3. On rappelle que le sous-anneau $\mathbb{Z}[i]$ de $\mathbb{C}$ est un anneau factoriel et que 3 est un élément irréductible de $\mathbb{Z}[i]$. En déduire que X^4+12 est irréductible dans $\mathbb{Q}(i)[X]$.
4. Montrer que $[L:\mathbb{Q}]=8$.
5. Quel est le polynôme minimal de α_2 sur $\mathbb{Q}(\alpha_1)$?
6. Montrer que le corps L contient les sous-corps $\mathbb{Q}(\sqrt[4]{3})$ et $\mathbb{Q}(\sqrt{3})$.
7. Montrer qu'il existe un automorphisme δ du corps $\mathbb{Q}(\sqrt{3})$ tel que $\delta(\sqrt{3})=-\sqrt{3}$.
8. Peut-on prolonger δ en un automorphisme de $\mathbb{Q}(\sqrt[4]{3})$?
9. Montrer qu'on peut prolonger les automorphismes γ_0 et γ_1 de $\mathbb{Q}(i)$ tels que $\gamma_0(i)=i$ et $\gamma_1(i)=-i$ en des automorphismes $\phi_{k,l}$ du corps L vérifiant pour $k\in\{0,1\}$ et $l\in\{1,2,3,4\}$, $\phi_{k,l}(\alpha_1)=\alpha_l$ et $\phi_{k,l}(i)=(-1)^k i$.
10. Montrer que les automorphismes $\phi_{k,l}$ sont les seuls automorphismes du corps L.
11. Quelles sont les images de $\alpha_1+\alpha_2$ par les 8 automorphismes de L ?
12. Soit $\beta\in L$. Montrer que si $L=\mathbb{Q}(\beta)$ alors β possède 8 images distinctes par les différents automorphismes de L.
13. En déduire la valeur de $[\mathbb{Q}(\alpha_1+\alpha_2):\mathbb{Q}]$.
14. Quel est le polynôme minimal de $\alpha_1+\alpha_2$ sur $\mathbb{Q}$?

Exercice 2 :

Soit p un entier premier et r un entier strictement positif. On pose $q=p^r$.

1. Soit L un corps de décomposition de X^q-X sur $\mathbb{F}_p$. Que vaut $[L:\mathbb{F}_p]$?
2. L'écriture de X^q-X en produit d'irréductibles de $\mathbb{F}_p[X]$ contient-elle des polynômes irréductibles de degré strictement supérieur à r ?
3. Soit Q un facteur irréductible de X^q-X dans $\mathbb{F}_p[X]$. Notons d son degré. Montrer que le polynôme Q possède exactement d racines dans L ?
4. Deux racines de Q ont-elles nécessairement le même ordre dans $L^\times$?

Contrôle du 26/10/2016

Exercice 1 :
Soit k un corps. On considère le morphisme d'anneaux

$$\varphi \,:\, k[Y,T] \;\to\; k[X] \tag{1}$$

défini par $\varphi(P(Y,T)) = P(X^2, X^3)$. Notons A l'image de φ.

1. A est-il intègre ?
2. Donner une expression explicite des éléments de A et en déduire que $A \neq k[X]$;
3. Calculer les inversibles de A ;
4. Montrer que X^2 et X^3 sont irréductibles dans A ;
5. En déduire que A n'est pas factoriel.

Exercice 2 :

1. Montrer que le polynôme $X^3 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$;
2. Montrer que le polynôme $X^4 + X^3 + X - 1$ n'a pas de racines dans $\mathbb{F}_3$;
3. Déduire des points précédents que $P = X^4 + 4X^3 + 3X^2 + 7X - 4 \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$.

Exercice 3 :
Soit A l'anneau $A = \mathbb{Z}[i\sqrt{3}]$, dont les éléments sont les réels qui s'écrivent (forcement de manière unique) comme $a + bi\sqrt{3}$, avec $a, b \in \mathbb{Z}$.

Notons également par B l'anneau $B = Z[j]$ où j est la racine cubique complexe primitive de l'unité $j = \frac{-1+i\sqrt{3}}{2}$. Les éléments de B s'écrivent de manière unique comme $a + bj$, avec $a, b \in \mathbb{Z}$.

Nous allons accepter le fait que B est Euclidien.

1. Montrer que j est racine de $X^2 + X + 1$.
2. Montrer que si $p \neq 2, 3$ s'écrit sous la forme $p = a^2 + 3b^2$, avec $a, b \in \mathbb{Z}$, alors $p \equiv 1 \pmod 3$. p premier

On suppose désormais que $p \neq 2, 3$ et que $p \equiv 1 \pmod 3$. Nous rappelons que le groupe $\mathbb{F}_p^\times$ des inversibles du corps $\mathbb{F}_p$ est cyclique (isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$). **T.S.V.P.**

3. Montrer que $\mathbb{F}_p^\times$ admet un élément d'ordre 3.
4. Utiliser l'élément d'ordre 3 de $\mathbb{F}_p^\times$ pour montrer que le polynôme $X^2 + X + 1$ admet une racine dans $\mathbb{F}_p$.
5. Montrer que A est contenu dans B, et montrer qu'un élément $\alpha = x + jy$ de B est dans A si et seulement si y est pair.
6. Montrer que si α est dans B alors au moins un élément dans l'ensemble $\{\alpha, j\alpha, j^2\alpha\}$ est dans A.
7. Montrer que p est la norme d'un élément de A si et seulement si c'est la norme d'un élément de B.[1]
8. Montrer que A n'est pas factoriel en écrivant deux factorisations de 4.
9. Montrer que B est intègre.
10. Montrer que les anneaux quotients $\mathbb{F}_p[X]/(X^2+X+1)$ et $B/(p)$ sont isomorphes.
11. En déduire que p est réductible dans B.
12. Montrer que p est de la forme $p = N(x)$, avec $x \in B$.
13. Montrer que p s'écrit donc sous la forme $p = a^2 + 3b^2$ avec $a, b \in \mathbb{Z}$.

1. Comme d'habitude, on définit la norme d'un nombre complexe comme $N(a+ib) = a^2+b^2$. C'est aussi donné par $N(a+ib) = (a+ib)(a-ib)$.

Contrôle du 9/12/2016

Exercice 1 :
Soit $i \in \mathbb{C}$ l'unité imaginaire complexe. Est-ce qu'il existe un polynôme $f(x) \in \mathbb{Q}[X]$ de degré 3, ayant pour racines $\sqrt{2}$, $\sqrt{2}+i$, $\sqrt{2}-i$?

Exercice 2 :
Question de cours : Soit K un corps de caractéristique nulle et L/K un corps de décomposition d'une famille de polynômes de $K[x]$. Démontrer que si $A(x) \in K[x]$ est un polynôme irréductible, et si A possède une racine dans L alors toutes les racines de A sont dans L.

Soit p un nombre premier. Soient $v = \sqrt[3]{p}$ et $u = \sqrt[3]{p} + \sqrt[3]{p^2}$.

1. Calculer le polynôme minimal $P(X)$ de u sur $\mathbb{Q}$;
2. Calculer les degrés $[\mathbb{Q}(u) : \mathbb{Q}]$ et $[\mathbb{Q}(v) : \mathbb{Q}]$;
3. Est-ce que $\mathbb{Q}(u) = \mathbb{Q}(v)$?
4. Calculer $(v-1)^{-1}$ dans la base $\{1, v, v^2, \ldots\}$ de $\mathbb{Q}(v)$ sur $\mathbb{Q}$.
5. Justifier que l'extension $\mathbb{Q}(u)$ ne peut pas être un corps de décomposition.
6. Soient $L(P)$ et $L(Q)$ les corps de décomposition de P et Q respectivement sur $\mathbb{Q}$. Montrer que $L(P) = L(Q)$. (Utiliser la question de cours). Q = polynôme minimal de v sur K $K = \mathbb{Q}$
7. Calculer le corps des racines $L(P)$ du polynôme P.
8. Quel est le degré $[L(P) : K]$?
9. Montrer qu'un $\mathbb{Q}$-automorphisme $\sigma : L(P) \xrightarrow{\sim} L(P)$ stabilise u si et seulement si il stabilise v ;
10. Calculer le groupe des K-automorphismes de $L(P)$; $K = \mathbb{Q}$
11. Trouver toutes les extensions intermédiaires $\mathbb{Q} \subsetneq F \subsetneq \mathbb{Q}(u)$.

Exercice 3 :
Soit p un nombre premier et soient k et k' deux corps finis de cardinaux p^n et p^m respectivement. Donner une condition nécessaire et suffisante pour qu'il existe un plongement $k \subseteq k'$?

Exercice 4 :
Soit k un corps fini. Montrer que tout élément $a \in k$ admet une racine p-ème $a^{1/p}$ dans k. Plus généralement quelles sont les racines du polynôme $X^p - a$ dans k ? $p = \mathrm{car}(k)$.

M1 Année 2016/2017

JUSTIFIER TOUTES VOS REPONSES

Question du cours :

1. Donner le critère d'Eisenstein pour qu'un polynôme à coefficients dans un anneau A factoriel soit irréductible.

   donner une démonstration du critère d'Eisenstein pour $A = \mathbb{Z}$ et p un nombre premier en considèrant le morphisme de réduction modulo p, $\mathbb{Z}[X] \to (\mathbb{Z}/(p))[X]$,

2. Soit p un nombre premier montrer que

$$X^{p-1} + X^{p-2} + \ldots + X + 1 \in \mathbb{Z}[X],$$

   est irreductible. [Indication : on pourra poser $X = Y + 1$]

3. Montrer que $X^4 + 1$ est irreductible dans $\mathbb{Z}[X]$.

Exercice 1

1. (a) Donner un exemple d'un anneau intègre qui n'est pas factoriel.
   (b) Donner un exemple d'un anneau factoriel qui n'est pas principal.

2. Donner un exemple d'un anneau A avec un idéal premier $I \subset A$ qui n'est pas maximal.

3. (a) Soient A, B des anneaux commutatifs et $\phi : A \to B$ un morphisme d'anneaux commutatifs (tel que $\phi(1_A) = 1_B$). Montrer que si $I \subset B$ est un idéal premier alors $\phi^{-1}(I) \subset A$ est un idéal premier.
   (b) Determiner les idéaux maximaux de $\mathbb{R}[X]/(X^2)$.
   [Indication : On pourra considerer le morphisme de réduction $\mathbb{R}[X] \to \mathbb{R}[X]/(X^2)$.]

4. (a) Montrer que $X^2 + X + 1$ est irréductible dans $\mathbb{R}[X]$.
   (b) Determiner les idéaux maximaux de $\mathbb{R}[X]/(X^2 + X + 1)$.

Exercice 2

1. Soient K un corps, L une extension finie de K et M, $K \subset M \subset L$ un corps intermediare. Décrire la relation entre les degrés $[L : K], [M, K]$ et $[L : M]$.

2. Soient L un corps, $K \subset L$ un sous corps et $\alpha \in L$. Montrer que $K(\alpha)$, l'intersection de tous les sous corps de L qui contiennent K et α, est un corps.

3. On suppose que $[L : K]$ est fini.
   (a) Montrer que le morphisme d'évaluation $\mathrm{spe}_\alpha : K[X] \to L$ n'est pas injectif.
   (b) Donner la définition :
      i. du degré de α sur K.
      ii. du degré de $K(\alpha)$ sur K.
   (c) Montrer que $K(\alpha) = K[\alpha]$ et en déduire que le degré de α sur K est égal au degré de $K(\alpha)$ sur K.
   (d) Soient $\alpha, \beta \in L$ avec le degré de α sur K égal à m et le degré de β sur K égal à n. Montrer que $\alpha + \beta$ est algebrique sur K de degré au plus mn.

4. (a) Soient K un corps et $f \in K[X]$ un polynôme unitaire de degré 3. Montrer que le degré du corps de décomposition de f sur K est un diviseur de 6.
   (b) Soit $\mathbb{F}_3$ le corps de cardinal 3 et $f = X^3 + X^2 + 1 \in \mathbb{F}_3[X]$.
      i. Est-ce que le polynôme f est irréductible sur $\mathbb{F}_3$?
      ii. Determiner le corps de décomposition de f.

Exercice 3

On considère la matrice

$$M = \begin{pmatrix} 9 & 15 & 21 \\ 15 & 9 & 6 \\ 21 & 6 & 9 \end{pmatrix}$$

1. Calculer :
   (a) le PGCD des coefficients de M.
   (b) le déterminant de M.
   (c) le produit

$$\begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 9 & 15 & 21 \\ 15 & 9 & 6 \\ 21 & 6 & 9 \end{pmatrix}$$

2. (a) Trouver une matrice équivalente à M de la forme

$$M = \begin{pmatrix} 3 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}$$

où $a, b, c, d \in \mathbb{Z}$ sont à determiner.

(b) Préciser le PGCD de quatre entiers a, b, c, d.

3. Trouver la matrice réduite équivalente à M :

$$\begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_2 & b \\ 0 & c & a_3 \end{pmatrix}$$

avec $a_i \in \mathbb{Z}$.

4. Soit N le sous-module de $\mathbb{Z}^3$ engendré par les vecteurs colonne de la matrice M. Trouver une base de $\mathbb{Z}^3$ adaptée à N.

5. Décrire la classe d'isomorphisme du groupe $\mathbb{Z}^3/N$.