Université Blaise Pascal,
UFR Sciences et Technologies
Département de Mathématiques et Informatique

jeudi 8 janvier 2009

Licence de Mathématiques, troisième année
U.E. Algèbre et Géométrie,

Durée: trois heures. *L'usage du polycopié du cours est autorisé, à l'exclusion de tout autre document; l'usage des calculatrices, ordinateurs et téléphones portables est interdit durant l'épreuve.*

Premier exercice.

On considère le corps $K = \mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ et l'anneau $A = K[X]$.

1) Donner la liste de tous les polynômes de degré inférieur ou égal à 2 dans A, et indiquer (en justifiant avec précision) lesquels sont irréductibles dans A.

2) On considère dans A le polynôme $P = X^5 + X^2 + \overline{1}$.

a) Montrer que P n'admet pas de diviseur de degré 1 dans A.

b) Montrer que si P est divisible par un polynôme Q de degré 2 dans A, alors Q est irréductible; utiliser la question 1) pour en déduire que Q ne peut alors valoir que $X^2+X+\overline{1}$. Le polynôme P est-il divisible par $X^2 + X + \overline{1}$ dans A ?

c) Conclure que P est irréductible dans A.

Deuxième exercice.

On considère l'anneau $A = \mathbb{Z}[i] = \{a+bi\,;\, a, b \in \mathbb{Z}\}$ des entiers de Gauss. Pour tout $z = a+bi \in A$, on note $N(z) = |z|^2 = a^2 + b^2$, ce qui définit une fonction $N : A \to \mathbb{N}$ multiplicative (c'est-à-dire $N(zz') = N(z)N(z')$ pour tous $z, z' \in A$). On rappelle que A est euclidien, et donc principal.

1) On appelle I l'ensemble des éléments $a + bi$ de A tels que a et b sont de même parité dans $\mathbb{Z}$ (tous les deux pairs, ou tous les deux impairs).

a) Montrer que I est égal à l'idéal principal $(1 + i)A$.

b) Montrer que $1+i$ est irréductible dans A (on pourra utiliser la fonction multiplicative N). Quelle propriété de l'idéal I peut-on en déduire ?

2) On considère dans A les idéaux $J = (3 + i)A$ et $K = (5 + i)A$.

a) Montrer que $J + K = I$. Quels sont tous les pgcd de $3 + i$ et $5 + i$ dans A ?

b) Déterminer c, d dans $\mathbb{Z}$ tels que $J \cap K = (c + di)A$.

c) Montrer que l'idéal J n'est pas premier dans A.

3) On considère dans A l'idéal $L = (3 + 2i)A$. On note $h : \mathbb{Z} \to A/L$ l'application qui, à tout entier $n \in \mathbb{Z}$, associe sa classe $h(n) = \overline{n}$ dans le quotient A/L (ceci a un sens puisque $\mathbb{Z} \subset A$); il est clair que h est un morphisme d'anneaux unitaires de $\mathbb{Z}$ dans A/L.

a) Montrer que, pour tous $a, b \in \mathbb{Z}$, il existe $n \in \mathbb{Z}$ tels que $(a + ib) - n \in L$. En déduire que h est surjective.

b) Montrer que $\operatorname{Ker} h = 13\mathbb{Z}$.

c) Déduire de a) et b) que L est un idéal maximal de A.

Problème

1) Soit A un anneau commutatif unitaire. On note $M_2(A)$ l'ensemble des matrices carrées à deux lignes et deux colonnes à coefficients dans A. Pour toute $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(A)$, on note $\det M = ad - bc$. L'ensemble $M_2(A)$ étant muni du produit matriciel usuel, une matrice M est dite inversible dans $M_2(A)$ lorsqu'il existe une matrice N dans $M_2(A)$ telle que $M \times N = N \times M = I_2$.

- **a)** Montrer qu'une matrice $M \in M_2(A)$ est inversible dans $M_2(A)$ si et seulement si $\det M$ appartient au groupe multiplicatif $U(A)$ des éléments de A inversibles dans A, et calculer alors explicitement son inverse.
- **b)** En déduire que l'ensemble des matrices de $M_2(A)$ qui sont inversibles dans $M_2(A)$ est un groupe, que l'on notera $\mathrm{GL}_2(A)$, et que l'application $\delta : M \mapsto \det M$ définit un morphisme de groupes surjectif de $\mathrm{GL}_2(A)$ dans $U(A)$.
- **c)** On note $\mathrm{SL}_2(A)$ l'ensemble des matrices M dans $M_2(A)$ telles que $\det M = 1_A$. Montrer que $\mathrm{SL}_2(A)$ est un sous-groupe normal de $\mathrm{GL}_2(A)$ et que $\mathrm{GL}_2(A)/\mathrm{SL}_2(A) \simeq U(A)$.

Dans le cas où A est l'anneau $\mathbb{Z}/n\mathbb{Z}$ pour un entier $n \geq 2$, l'ordre du groupe fini $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ sera noté $j(n)$. Le but du problème est de calculer $j(n) = |\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})|$ en fonction de n.

2) On fixe dans cette question un nombre premier p. On note $\mathbb{K}$ le corps $\mathbb{Z}/p\mathbb{Z}$.

- **a)** Combien y a-t-il d'éléments dans $\mathbb{K}$? Combien y a-t-il de vecteurs (x, y) non-nuls dans $\mathbb{K}^2$? Combien y a-t-il de couples de vecteurs $\big((x, y), (z, t)\big)$ de $\mathbb{K}^2$ qui sont des bases du $\mathbb{K}$-espace vectoriel $\mathbb{K}^2$?
- **b)** En déduire que le groupe $\mathrm{GL}_2(\mathbb{K})$ est fini d'ordre $p(p-1)(p^2-1)$.
- **c)** Utiliser la question 1.c) pour en déduire que $j(p) = p(p^2-1)$.

3) On suppose dans cette question que $n = p^\alpha$ avec p un nombre premier p et $\alpha \geq 2$ un entier. On pose $m = p^{\alpha-1}$ de sorte que $n = pm$.
On considère les deux anneaux $\mathbb{Z}/pm\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots \overline{pm-1}\}$ et $\mathbb{Z}/m\mathbb{Z} = \{\widetilde{0}, \widetilde{1}, \widetilde{2}, \ldots, \widetilde{m-1}\}$.
On introduit l'application $\varphi : \mathbb{Z}/pm\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ définie par $\varphi(\overline{x}) = \widetilde{x}$ pour tout $0 \leq x \leq pm-1$,

ainsi que l'application F: $\left|\begin{array}{ccc} \mathrm{SL}_2(\mathbb{Z}/pm\mathbb{Z}) & \longrightarrow & \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \\ \left(\begin{smallmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{smallmatrix}\right) & \longmapsto & \left(\begin{smallmatrix} \widetilde{a} & \widetilde{b} \\ \widetilde{c} & \widetilde{d} \end{smallmatrix}\right) \end{array}\right.$

- **a)** Montrer que φ est bien définie (c'est-à-dire $\overline{x} = \overline{y}$ implique $\widetilde{x} = \widetilde{y}$ pour tous $0 \leq x, y \leq pm-1$), que c'est un morphisme d'anneaux unitaires, et qu'elle est surjective.

On en déduit (la vérification n'est pas demandée ici) que F est un morphisme de groupes surjectif.

- **b)** Montrer que $\mathrm{Ker}\, F = \left\{ \left(\begin{smallmatrix} \overline{1+mx} & \overline{my} \\ \overline{mz} & \overline{1+mt} \end{smallmatrix}\right) \text{ avec } x, y, z, t \in \mathbb{Z} \text{ tels que : } x + t \equiv 0 \bmod p \right\}$
- **c)** En déduire que le sous-groupe $\mathrm{Ker}\, F$ est d'ordre p^3, puis que $j(pm) = p^3 j(m)$.
- **d)** En déduire par récurrence que $j(p^\alpha) = p^{3(\alpha-1)} j(p)$.

4) On suppose que n est un entier ≥ 2 quelconque. On note $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ sa décomposition en produit de facteurs premiers (avec $p_i \neq p_j$ pour $i \neq j$, et $\alpha_i \geq 1$ pour tout $1 \leq i \leq s$).

- **a)** Montrer que $\mathbb{Z}/n\mathbb{Z} \simeq (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_s^{\alpha_s}\mathbb{Z})$ (isomorphisme d'anneaux).
- **b)** En déduire avec le résultat ($\star$) ci-dessous que $j(n) = j(p_1^{\alpha_1})\, j(p_2^{\alpha_2}) \ldots j(p_s^{\alpha_s})$.
- **c)** Synthétiser les résultats des questions 2) et 3) précédentes pour conclure finalement que:

$$j(n) = n^3 \prod_{i=1}^{s} \big(1 - \frac{1}{{p_i}^2}\big).$$

($\star$) **Question facultative hors-barême.** Montrer que, si A et A' sont deux anneaux commutatifs unitaires, alors le groupe $\mathrm{SL}_2(A \times A')$ est isomorphe au produit direct $\mathrm{SL}_2(A) \times \mathrm{SL}_2(A')$; on explicitera un isomorphisme entre les deux groupes, mais on ne détaillera pas sur la copie les calculs prouvant que c'est un morphisme.

Université Blaise Pascal,
UFR Sciences et Technologies
Département de Mathématiques et Informatique

Seconde session, 23 juin 2009

Licence de Mathématiques, troisième année
U.E. Algèbre et Géométrie,

Durée: trois heures. *L'usage du polycopié du cours est autorisé, à l'exclusion de tout autre document; l'usage des calculatrices, ordinateurs et téléphones portables est interdit durant l'épreuve. La rigueur des raisonnements, la clarté des justifications et la qualité de la rédaction sont des éléments importants dans l'appréciation de la copie.*

Premier exercice.

On considère un groupe G fini d'ordre $n \geq 1$. Pour tout $x \in G$, on note Ω_x la classe de conjugaison de x et G_x le centralisateur de x. Rappelons que, par définition :

$$\Omega_x = \{gxg^{-1}\,;\, g \in G\} = \{y \in G \mid \exists\, g \in G,\ y = gxg^{-1}\} \quad \text{et} \quad G_x = \{g \in G \mid gx = xg\}.$$

1) Montrer que l'ensemble des classes de conjugaison des éléments de G forme une partition de G.

2) On note v_x le nombre d'éléments de Ω_x et a_x le nombre d'éléments de G_x. Quelle relation a-t-on, pour tout $x \in G$, entre v_x, a_x et n ?

3) On appelle N le nombre de classes de conjugaison distinctes dans G.

- **a)** Montrer que $1 \leq N \leq n$.
- **b)** Que peut-on dire de G lorsque $N = 1$? Que peut-on dire de G lorsque $N = n$?
- **c)** Montrer que $N = 2$ si et seulement si G est le groupe cyclique d'ordre 2.

4) On cherche à déterminer dans cette question tous les groupes finis G tels que $N = 3$.

- **a)** On suppose que $N = 3$. Montrer qu'il existe deux diviseurs $a \geq b \geq 2$ de n tels que: $\dfrac{1}{n} + \dfrac{1}{a} + \dfrac{1}{b} = 1$. Montrer que, si $b \geq 3$, alors on a $a = n = 3$. Montrer que, si $b = 2$, alors on a, soit $n = 6$ et $a = 3$, soit $n = a = 4$; vérifier qu'aucun groupe fini ne correspond au second cas.
- **b)** En déduire que les groupes finis G tels que $N = 3$ sont le groupe cyclique d'ordre 3 et le groupe symétrique S_3.

5) Dans cette question, G est le groupe alterné A_4.

- **a)** Combien vaut n ?
- **b)** Soient $\gamma = [i, j, k]$ un 3-cycle dans G, et $\sigma \in G$ quelconque ; que vaut $\sigma\gamma\sigma^{-1}$?
- **c)** Montrer que si $\tau = [i, j][k, \ell]$ est un produit de deux transpositions disjointes dans G, alors $\sigma\tau\sigma^{-1} = [\sigma(i), \sigma(j)][\sigma(k), \sigma(\ell)]$ pour tout $\sigma \in G$.
- **d)** Déterminer les classes de conjugaison de G. Combien vaut N ?

Deuxième exercice

1) On considère dans $\mathbb{Z}[X]$ un polynôme $P = u_n X^n + u_{n-1}X^{n-1} + \cdots + u_1 X + u_0$ de degré égal à $n \geq 1$; on a donc $u_i \in \mathbb{Z}$ pour tout $0 \leq i \leq n$ et $u_n \neq 0$.

- **a)** On se donne un nombre rationnel non-nul $y = \frac{a}{b}$, avec a, b des entiers premiers entre eux, $b \neq 0$. Montrer que si y est un zéro de P dans $\mathbb{Q}$, alors a divise u_0 et b divise u_n dans $\mathbb{Z}$ (indication: on pourra montrer d'abord que a divise $u_0 b^n$ et b divise $u_n a^n$).
- **b)** En déduire que, si P est unitaire et vérifie $u_0 = \pm 1$, alors les seuls zéros possibles de P dans $\mathbb{Q}$ sont 1 et -1.

2) En déduire que tout polynôme P de la forme $P = X^2 + uX \pm 1$ ou $P = X^3 + uX^2 + vX \pm 1$, avec $u, v \in \mathbb{Z}$, qui vérifie $P(1) \neq 0$ et $P(-1) \neq 0$, est irréductible dans $\mathbb{Q}[X]$.

3) Le résultat de la question 1) reste-t-il vrai si l'on remplace $\mathbb{Z}$ par un anneau principal quelconque A ? Par quoi faut-il alors remplacer $\mathbb{Q}$?

... suite au verso →

Troisième exercice

On note A l'anneau (commutatif et unitaire) $\mathcal{F}(\mathbb{R},\mathbb{R})$ des applications de $\mathbb{R}$ dans $\mathbb{R}$. Rappelons que les lois $+$ et $.$ sont l'addition et la multiplication ordinaires des fonctions, définies par:

$$(f+g)(x) = f(x)+g(x) \quad \text{et} \quad (f.g)(x) = f(x)g(x) \quad \text{pour tous } f,g \in A,\ x \in \mathbb{R}.$$

1) Rappeler comment sont définies les applications 0_A et 1_A, éléments neutres pour l'addition et la multiplication dans A respectivement.

2) Donner un exemple de deux applications f et g dans A distinctes de 0_A telles que $f.g = 0_A$. Que peut-on en déduire pour l'anneau A ?

3) Donner une condition nécessaire et suffisante pour qu'une application $f \in A$ appartienne au groupe $U(A)$ des éléments de A inversibles dans A.

4) Montrer que l'ensemble $B = \{f \in A \mid f(0) = f(1)\}$ est un sous-anneau unitaire de A.

5) On note $I = \{f \in A \mid f(0) = f(1) = 0\}$.

- **a)** Montrer que I est un idéal de A et un idéal de B.
- **b)** Donner un exemple de deux applications f et g dans A n'appartenant pas à I et telles que $f.g \in I$. Que peut-on en déduire pour l'idéal I de A ?
- **c)** Montrer que l'application $\varphi : B \to \mathbb{R}$ définie par $\varphi(f) = f(0)$ pour tout $f \in B$ est un morphisme d'anneaux unitaires, surjectif ; vérifier que l'anneau quotient B/I est isomorphe à $\mathbb{R}$. Que peut-on en déduire pour l'idéal I de B ?
- **d)** En résumé, I est-il un idéal premier de A ? de B ?
- **e)** Montrer que I est l'intersection de deux idéaux maximaux de A (que l'on déterminera naturellement à partir de la définition de I).
- **f)** Montrer que I est un idéal principal de A (on explicitera une application $f \in A$ telle que $fA = Af = I$).

Quatrième exercice.

On se place dans le plan affine euclidien orienté $\mathcal{E}$.

1) Soit $\mathcal{X}$ l'ensemble de points formé par la réunion de deux droites perpendiculaires D et D' dans $\mathcal{E}$.

- **a)** Déterminer le groupe $G_{\mathcal{X}}^{+}$ des isométries affines directes laissant globalement invariant l'ensemble $\mathcal{X}$.
- **b)** Déterminer le groupe $G_{\mathcal{X}}$ des isométries affines laissant globalement invariant l'ensemble $\mathcal{X}$. Le groupe $G_{\mathcal{X}}$ est-il un groupe fini ?

2) Soit $\mathcal{Y}$ l'ensemble de points formé par la réunion de deux droites strictement parallèles Δ et Δ' dans $\mathcal{E}$.

- **a)** Déterminer le groupe $G_{\mathcal{Y}}^{+}$ des isométries affines directes laissant globalement invariant l'ensemble $\mathcal{Y}$.
- **b)** Déterminer une isométrie indirecte de $\mathcal{E}$ laissant globalement invariant l'ensemble $\mathcal{Y}$. Ceci suffit-il pour déterminer le groupe $G_{\mathcal{Y}}$ de toutes isométries affines laissant globalement invariant l'ensemble $\mathcal{Y}$? Le groupe $G_{\mathcal{Y}}$ est-il un groupe fini ?

Université Blaise Pascal,
UFR Sciences et Technologies
Département de Mathématiques et Informatique

jeudi 7 janvier 2010

LICENCE DE MATHÉMATIQUES, TROISIÈME ANNÉE
U.E. Algèbre et Géométrie

Durée: trois heures. *L'usage du polycopié du cours est autorisé, à l'exclusion de tout autre document; l'usage des calculatrices, ordinateurs et téléphones portables est interdit durant l'épreuve.*

EXERCICE I.

On considère dans $\mathbb{Q}$ le sous-ensemble des nombres dyadiques $B = \{\frac{a}{2^n}\,;\, a \in \mathbb{Z}, n \in \mathbb{N}\}$.

1) Montrer que B est un sous-anneau de $\mathbb{Q}$ contenant $\mathbb{Z}$, et qui n'est pas un corps.

2) Soit s le morphisme d'anneau unitaire $\mathbb{Z}[X] \to \mathbb{Q}$ défini par $s(X) = \frac{1}{2}$. L'image par s d'un polynôme quelconque $P = \sum_{i=0}^{m} a_i X^i$ de $\mathbb{Z}[X]$ est donc le rationnel $s(P) = \sum_{i=0}^{m} \frac{a_i}{2^i}$.
Déterminer $\operatorname{Im} s$. Montrer que $\operatorname{Ker} s$ est égal à l'idéal principal $I = (1-2X)\mathbb{Z}[X]$ engendré par $(1-2X)$. Conclure que $B \simeq \mathbb{Z}[X]/I$.

3) Déduire des questions précédentes que I est un idéal premier non maximal de $\mathbb{Z}[X]$. Que peut-on en déduire pour l'anneau $\mathbb{Z}[X]$?

EXERCICE II.

On fixe dans cet exercice G un groupe abélien. On note $T(G)$ le sous-ensemble formé des éléments de G qui sont d'ordre fini dans G. La loi du groupe G étant a priori notée multiplicativement, un élément $x \in G$ appartient donc à $T(G)$ si et seulement s'il existe un entier $n \geq 1$ tel que $x^n = e$.
On dit que G est un groupe sans torsion si $T(G) = \{e\}$, que G est un groupe de torsion si $T(G) = G$, et que G est mixte si $\{e\} \neq T(G) \neq G$.

1) Donner un exemple de groupe G qui est de torsion. Donner un exemple de groupe G qui est sans torsion. Montrer que $\mathbb{C}^*$ est mixte.

2) Montrer que $T(G)$ est un sous-groupe de G, et que le groupe quotient $G/T(G)$ est un groupe abélien sans torsion.

3) On prend dans cette question le groupe $G = \mathbb{Q}/\mathbb{Z}$, muni de l'addition. On note $q : x \mapsto q(x) = \overline{x}$ la surjection canonique $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$.

- **a)** Réécrire comment se traduit ici, en notation additive, le fait qu'un élément $\overline{x} \in \mathbb{Q}/\mathbb{Z}$ (avec $x \in \mathbb{Q}$) appartienne à $T(G)$.
- **b)** Montrer que $G = \mathbb{Q}/\mathbb{Z}$ est un groupe de torsion et qu'il est infini. Est-il vrai que tout groupe abélien fini est de torsion ? (justifier votre réponse).
- **c)** Pour tout entier $n \geq 1$, on note H_n le sous-groupe cyclique engendré par $q(\frac{1}{n})$ dans $\mathbb{Q}/\mathbb{Z}$. Montrer que H_n est d'ordre n.
- **d)** Réciproquement, soit K un sous-groupe de $\mathbb{Q}/\mathbb{Z}$ quelconque. Soit $n \geq 1$ l'ordre de K. Montrer que $K = H_n$. [*Indication:* vérifier que, pour tout $x = q(\frac{a}{b}) \in K$ avec a, b entiers premiers entre eux, on a b qui divise na, et en déduire que $x \in H_n$].
- **e)** Conclure que, pour tout entier $n \geq 1$, il existe un et un seul sous-groupe d'ordre n dans $\mathbb{Q}/\mathbb{Z}$.
- **f)** Citer (sans rappeler la démonstration) un type de groupe abélien fini admettant un et un seul sous-groupe d'ordre n pour tout entier $n \geq 1$ divisant l'ordre de ce groupe.

Exercice III

1) On pose $\omega = \dfrac{1+\sqrt{5}}{2} \in \mathbb{R}$. On considère dans $\mathbb{R}$ le sous-ensemble $B = \{a + b\omega\,;\, a \in \mathbb{Z}, b \in \mathbb{Z}\}$.

a) Vérifier que $\omega^2 = \omega + 1$.

b) Montrer que B est un sous-anneau de $\mathbb{R}$ contenant $\mathbb{Z}$.

c) Soit l'application $\sigma : B \to B$ qui, à tout $x = a + b\omega$ avec $a, b \in \mathbb{Z}$, associe $\sigma(x) = (a+b) - b\omega$. Montrer que σ est une bijection telle que $\sigma^{-1} = \sigma$, et que c'est un automorphisme d'anneau unitaire de B.

d) En déduire que l'application $N : B \to \mathbb{Z}$ qui, à tout $x = a + b\omega$ avec $a, b \in \mathbb{Z}$, associe $N(x) = x\sigma(x) = a(a+b) - b^2$ est multiplicative (c'est-à-dire que $N(xy) = N(x)N(y)$ pour tous $x, y \in B$).

2) On considère dans $\mathbb{R}$ le sous-ensemble $K = \{\alpha + \beta\omega\,;\, \alpha \in \mathbb{Q}, \beta \in \mathbb{Q}\}$.

a) Montrer que, pour tout élément $z \in \mathbb{R}$, on a $z \in K$ si et seulement s'il existe $x, y \in B$ avec $y \neq 0$ tels que $z = \frac{x}{y}$. Il en résulte que K est égal au corps des fractions de B (on ne demande pas de rédiger ici une justification de ce point).

b) On prolonge σ à K en posant $\sigma(\frac{x}{y}) = \frac{\sigma(x)}{\sigma(y)}$ pour $x, y \in B$, $y \neq 0$. Montrer que l'on a encore $\sigma(z) = (\alpha + \beta) - \beta\omega$ pour tout $z = \alpha + \beta\omega \in K$, avec $\alpha, \beta \in \mathbb{Q}$.

c) En déduire que N se prolonge en l'application multiplicative $N : K \to \mathbb{Q}$ qui, à tout $z = \alpha + \beta\omega$ avec $\alpha, \beta \in \mathbb{Q}$, associe $N(z) = z\sigma(z) = \alpha(\alpha + \beta) - \beta^2$.

d) Montrer que, pour tous $x, y \in B$ avec $y \neq 0$, il existe un élément $q \in B$ tel que $|N(\frac{x}{y} - q)| < 1$. [*Indication:* on pourra utiliser le fait que, pour tout $\alpha \in \mathbb{Q}$, il existe $e \in \mathbb{Z}$ tel que $|\alpha - e| \leq \frac{1}{2}$].

e) En déduire que B est euclidien (préciser le stathme).

3) On considère dans $\mathbb{R}$ le sous-ensemble $A = \{u + v\sqrt{5}\,;\, u \in \mathbb{Z}, v \in \mathbb{Z}\}$.

a) Montrer que A est inclus dans B, puis que A est un sous-anneau de B contenant $\mathbb{Z}$.

b) Montrer que la restriction de N à A est définie par $N(u + v\sqrt{5}) = u^2 - 5v^2$ pour tous $u, v \in \mathbb{Z}$. Montrer que le groupe $U(A)$ des éléments inversibles dans A est égal à l'ensemble des $x \in A$ tels que $N(x) = \pm 1$, et que c'est un ensemble infini.

c) Vérifier que les trois éléments $1 + \sqrt{5}$, $1 - \sqrt{5}$ et 2 sont irréductibles dans A. [*Indication:* on pourra vérifier au préalable qu'il n'existe pas d'entiers u, v tels que $u^2 - 5v^2 = \pm 2$]. En déduire deux décompositions distinctes de l'élément 4 de A en produit de facteurs irréductibles non associés dans A.

d) En déduire que A n'est pas principal.

4) Il résulte des questions précédentes que $\mathbb{Z} \subset A \subset B$, avec B euclidien (donc principal) et A non principal. Donner l'unique décomposition de l'élément 4 en produit de facteurs irréductibles dans B. Comparer au résultat de la question 3.c et expliquer, par un commentaire pertinent et argumenté, pourquoi l'apparente contradition n'en est pas une.

Université Blaise Pascal,
UFR Sciences et Technologies
Département de Mathématiques et Informatique

jeudi 24 juin 2010

LICENCE DE MATHÉMATIQUES, TROISIÈME ANNÉE
U.E. Algèbre et Géométrie

Durée: trois heures. *L'usage du polycopié du cours est autorisé, à l'exclusion de tout autre document; l'usage des calculatrices, ordinateurs et téléphones portables est interdit durant l'épreuve.*

EXERCICE I.

Soit G un groupe noté multiplicativement. On désigne par e son élément neutre. On suppose que G est abélien. Pour tout entier $n \geq 1$ fixé, on désigne par K_n le sous-ensemble de G formé des éléments x tels que $x^n = e$, et par H_n le sous-ensemble des éléments de G qui sont une puissance n-ième d'un élément de G. En d'autres termes:

$$H_n = \{y \in G\,;\, \exists\, x \in G, y = x^n\} = \{x^n\,;\, x \in G\} \quad \text{et} \quad K_n = \{x \in G\,;\, x^n = e\}.$$

1) Montrer que H_n et K_n sont des sous-groupes de G.

2) Que valent H_n et K_n lorsque $n = 1$?

3) Déterminer H_n et K_n dans chacun des cas suivants:

a) $G = \mathbb{R}^*$ et $n = 2$,

b) $G = \mathbb{C}^*$ et $n = 2$,

c) $G = \{1, i, -1, -i\} \subset \mathbb{C}^*$ pour $n = 2$, puis pour $n = 3$, puis pour $n = 4$.

4) Montrer que le groupe quotient G/K_n est isomorphe à H_n.

5) On prend dans cette question $G = \langle a \rangle = \{e, a, a^2, \ldots, a^{p-1}\}$ cyclique d'ordre p (avec $p \geq 2$). Soit n un entier tel que $1 \leq n \leq p$. Déterminer les sous-groupes H_n et K_n, en précisant leur ordre (on pourra faire intervenir le pgcd d de n et p).

EXERCICE II.

On note G le groupe $\mathrm{GL}(2, \mathbb{R})$ et on considère dans G les matrices suivantes:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad C = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

1) On note H l'ensemble $\{I, -I, A, -A, B, -B, C, -C\}$.

a) Montrer que $AB = C,\ A^2 = -I,\ AB = -BA$.

On admettra sans écrire les vérifications que l'on a de même:

$$BC = A,\ B^2 = -I,\ BC = -CB,\ CA = B,\ C^2 = -I,\ CA = -AC.$$

b) Montrer que H est un sous-groupe de G.

c) Déterminer tous les sous-groupes de H et montrer qu'ils sont normaux dans H.

d) Préciser le centre $Z(H)$.

2) On note D le sous-groupe de G engendré par R et S.

a) Ecrire tous les éléments de D. Quel est l'ordre de D ? A quel groupe classique D est-il isomorphe ?

b) Déterminer tous les sous-groupes de D.

c) Pour tout point $M(x,y)$ du plan affine euclidien $\mathcal{E}$ rapporté à un repère orthonormé $\mathcal{R}$ et toute matrice $T = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in D$, on note $T.M$ le point $M'(x',y')$ tel que $x' = \alpha x + \beta y,\ y' = \gamma x + \delta y$. Montrer que le groupe D opère sur l'ensemble $\mathcal{E}$ par $(T,M) \mapsto T.M$. Décrire explicitement l'orbite d'un point M quelconque sous cette action, en distinguant suivant que les coordonnées (x,y) de M vérifient: $xy = 0$, ou $xy \neq 0$ et $|x| = |y|$, ou $xy \neq 0$ et $|x| \neq |y|$; (on fera des dessins correspondant à chaque situation).

d) Montrer que les groupes H et D ne sont pas isomorphes.

3) Pour tout n, on considère la matrice $\Gamma_n = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}$, et on note C_n le sous-groupe engendré par Γ_n dans G.

a) Montrer que C_n est cyclique d'ordre n.

b) Démontrer que les groupes C_8, $C_4 \times C_2$ et $C_2 \times C_2 \times C_2$ ne sont pas deux à deux isomorphes.

c) Démontrer que ni H ni D ne sont isomorphes à aucun des trois groupes de la question précédente.

Exercice III.

On cherche à trouver tous les couples d'entiers $(y,z) \in \mathbb{Z}^2$ solutions de l'équation:

$$y^2 + 4 = z^3 \qquad (\star)$$

1) Vérifier que $(11,5)$ et $(2,2)$ sont des solutions; en déduire deux autres couples solutions.

2) Supposons que (y,z) est une solution de $(\star)$ avec y impair.

a) Montrer que l'on a, dans l'anneau $\mathbb{Z}[i]$ des entiers de Gauss, l'égalité $(y+2i)(y-2i) = z^3$

b) Considérons $a+ib$, avec $a,b \in \mathbb{Z}$, un diviseur commun de $y+2i$ et $y-2i$ dans l'anneau $\mathbb{Z}[i]$. Montrer que $a+ib$ divise $2y$ et $4i$. En déduire que a^2+b^2 divise 4 dans $\mathbb{Z}$. Quelles sont alors les valeurs possibles pour $a+ib$? Vérifier que certaines d'entre elles contredisent l'imparité de y. Conclure que $y+2i$ et $y-2i$ sont premiers entre eux dans $\mathbb{Z}[i]$.

c) Déduire des questions a) et b) que $y+2i$ est un cube dans $\mathbb{Z}[i]$, en précisant quelles propriétés arithmétiques de l'anneau $\mathbb{Z}[i]$ sont utilisées.

d) En écrivant $y+2i = (a+ib)^3$ avec $a,b \in \mathbb{Z}$, trouver les valeurs possibles de y puis de z.

3) Supposons que (y,z) est une solution de $(\star)$ avec y pair.

a) Montrer que z est pair. En posant $y = 2u$ et $z = 2v$, montrer que l'on est ramené à la résolution de $u^2 + 1 = 2v^3$, avec u impair.

b) En raisonnant comme dans la question 2), montrer qu'un pgcd de $u+i$ et $u-i$ est $1+i$. Quels sont les autres pgcd ?

c) En déduire qu'il existe deux éléments $a+ib$ et $c+id$ premiers entre eux dans $\mathbb{Z}[i]$, avec $a,b,c,d \in \mathbb{Z}$, tels que $u+i = (1+i)(a+ib)$ et $u-i = (1-i)(c+id)$.

d) Déduire des questions a) et c) que $a+ib$ est un cube dans $\mathbb{Z}[i]$. En notant $a+ib = (s+it)^3$ avec $s,t \in \mathbb{Z}$, expliciter la partie imaginaire de $(1+i)(a+ib)$ et vérifier qu'elle est divisible par $s-t$ dans $\mathbb{Z}$. Quelles sont les valeurs possibles de s et t ?

e) En déduire les valeurs possibles de u, puis de v ; en déduire y et z.

4) Conclure en donnant l'ensemble des solutions de $(\star)$ dans $\mathbb{Z}^2$.

Université Blaise Pascal,
UFR Sciences et Technologies
Département de Mathématiques et Informatique

vendredi 7 janvier 2011

LICENCE DE MATHÉMATIQUES, TROISIÈME ANNÉE
U.E. Algèbre et Géométrie

Durée: trois heures. *L'usage du polycopié du cours est autorisé, à l'exclusion de tout autre document ; l'usage des calculatrices, ordinateurs et téléphones portables est interdit durant l'épreuve.*

Le sujet comprend deux parties, représentant chacune environ la moitié de la note d'ensemble de l'épreuve.

PARTIE I.

Cette partie est composée d'une série de questions brèves, indépendantes les unes des autres. On attend pour chacune de ces questions une preuve courte et rigoureuse.

Question 1. Montrer que, dans le groupe symétrique S_5, il n'existe pas d'élément d'ordre 14, et qu'il n'existe pas non plus d'élément d'ordre 15.

Question 2. On note G le groupe multiplicatif $U(\mathbb{Z}/20\mathbb{Z})$ formé des éléments inversibles dans l'anneau $\mathbb{Z}/20\mathbb{Z}$, et H le sous-groupe de G engendré par l'élément $\overline{9}$. Déterminer G et H, et reconnaître à isomorphisme près le groupe quotient G/H.

Question 3. On considère le groupe $G = \mathrm{GL}_2(\mathbb{R})$. Le sous-groupe H formé des matrices diagonales sans zéro sur la diagonale est-il normal dans G ?

Question 4. On se place dans le plan affine euclidien $\mathcal{E}$ rapporté à un repère orthonormé et on appelle $\mathcal{X}$ l'ensemble de tous les points de $\mathcal{E}$ de coordonnés $(n, 0)$ où n décrit $\mathbb{Z}$. Déterminer le groupe $G_{\mathcal{X}}^{+}$ des isométries directes de $\mathcal{E}$ qui laissent $\mathcal{X}$ globalement invariant. Déterminer le groupe $G_{\mathcal{X}}$ de toutes les isométries de $\mathcal{E}$ qui laissent $\mathcal{X}$ globalement invariant.

Question 5. Déterminer le plus petit sous-anneau unitaire de $\mathbb{Q}$ contenant $\frac{1}{5}$.

Question 6. Soient A un anneau commutatif unitaire et P un idéal de A distinct de A. Montrer que P est un idéal premier de A si et seulement s'il satisfait la propriété $(\star)$ suivante :

quels que soient des idéaux I et J de A, si $IJ \subseteq P$, alors $I \subseteq P$ ou $J \subseteq P$.

Question 7. On considère le corps $K = \mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$. Déterminer tous les polynômes irréductibles dans $K[X]$ de degré inférieur ou égal à 3.

.../...

Partie II.

Cette partie est un court problème ; on pourra admettre le résultat d'une question pour l'utiliser si nécessaire dans une question suivante.

1) Soit A un anneau (non-nul) commutatif unitaire qui n'est pas un corps.
On note $U(A)$ le groupe multiplicatif des éléments inversibles dans A, et I l'ensemble des éléments de A qui ne sont pas inversibles dans A.

a) Montrer que $I \neq \{0\}$ et $I \neq A$.

b) Montrer que les trois conditions suivantes sont équivalentes:

(i) I est stable par addition ; (ii) I est un idéal de A ; (iii) A possède un unique idéal maximal.

On dit que l'anneau A est local s'il satisfait l'une de ces conditions équivalentes.

c) Montrer que, si A est local, alors tout élément $x \in A$ vérifie $x \in U(A)$ ou $1 - x \in U(A)$.

d) On suppose que A est local ; déterminer les éléments $x \in A$ qui vérifient $x^2 = x$.

2) On prend dans cette question $A = \mathbb{Z}/p^s\mathbb{Z}$, où p est un nombre premier et s un entier ≥ 2 fixé.

a) Donner une condition nécessaire et suffisante sur $n \in \mathbb{Z}$ pour que $\overline{n}$ soit inversible dans A.

b) En déduire que A est un anneau local.

3) On fixe un nombre premier p. On considère dans $\mathbb{Q}$ le sous-ensemble:

$$A = \{\ \frac{a}{b}\ ;\ a \in \mathbb{Z},\ b \in \mathbb{Z},\ b \not\equiv 0 \text{ modulo } p\ \}.$$

a) Montrer que A est un sous-anneau unitaire de $\mathbb{Q}$ contenant $\mathbb{Z}$.

b) Montrer que, si B est un sous-anneau de $\mathbb{Q}$ contenant A et distinct de A, alors $B = \mathbb{Q}$.

c) Montrer que, pour tout idéal non-nul I de A, il existe un unique entier naturel n tel que $I = p^n A$; [*indication:* on remarquera que, si $\frac{a}{b} \in I$ avec p ne divisant pas a, alors $\frac{b}{a} \in A$].

d) En déduire que l'anneau A est principal, et expliciter tous ses idéaux en précisant les relations d'inclusion entre eux.

e) En déduire les idéaux premiers de A, les idéaux maximaux de A, et que A est un anneau local.

f) Montrer que, pour tout $s \in \mathbb{N}^*$, l'anneau quotient A/p^sA est isomorphe à l'anneau $\mathbb{Z}/p^s\mathbb{Z}$.
[*Indication:* considèrer $h : \mathbb{Z} \to A/p^sA$ la restriction au sous-anneau $\mathbb{Z}$ de A de la surjection canonique $A \to A/p^sA$, vérifier que h est surjective et déterminer son noyau].

En déduire que l'anneau A/p^sA est local.

4) On considère le corps $K = \mathbb{R}(X)$ des fractions rationnelles en une indéterminée X à coefficients réels. On rappelle que K est le corps de fractions de l'anneau de polynômes $\mathbb{R}[X]$ et donc que tout élément de K s'écrit comme un quotient $F = \frac{P}{Q}$ de deux polynômes P et Q de $\mathbb{R}[X]$, $Q \neq 0$.

On fixe un réel a quelconque et on considère le sous-ensemble A de K formé des fractions rationnelles qui peuvent s'écrire $\frac{P}{Q}$ avec P et Q dans $\mathbb{R}[X]$ vérifiant $Q(a) \neq 0$.

a) Montrer que A est un sous-anneau unitaire de K contenant $\mathbb{R}[X]$.

b) Donnner une condition nécessaire et suffisante pour qu'un élément F soit inversible dans A.

c) En déduire que A est un anneau local.

Université Blaise Pascal,
UFR Sciences et Technologies
Département de Mathématiques et Informatique

lundi 20 juin 2011

LICENCE DE MATHÉMATIQUES, TROISIÈME ANNÉE
U.E. Algèbre et Géométrie

Durée: trois heures. *L'usage du polycopié du cours est autorisé, à l'exclusion de tout autre document ; l'usage des calculatrices, ordinateurs et téléphones portables est interdit durant l'épreuve.*

Le sujet est composé de trois exercices indépendants (deux exercices brefs d'applications du cours, et un troisième constituant un petit problème). La rigueur des raisonnements, la clarté des justifications et la qualité de la rédaction sont des éléments importants dans l'appréciation de la copie.

EXERCICE I.

On considère dans le groupe symétrique S_{16} l'élément

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 10 & 7 & 11 & 4 & 8 & 15 & 3 & 12 & 13 & 9 & 16 & 5 & 1 & 14 & 6 & 2 \end{pmatrix}.$$

Donner le support, les orbites, la décomposition en cycles disjoints, l'ordre et la signature de σ. Cette permutation appartient-elle au groupe alterné A_{16}?

EXERCICE II.

Pour tout couple $(a, b) \in \mathbb{R}^* \times \mathbb{R}$, on considère l'application $f_{a,b} : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = ax + b$ pour tout $x \in \mathbb{R}$.

1) On note $G = \{f_{a,b}\,;\, a \in \mathbb{R}^*,\ b \in \mathbb{R}\}$ l'ensemble de toutes les applications de cette forme.

- **a)** Montrer que tout élément de G est une bijection de $\mathbb{R}$ sur $\mathbb{R}$.
- **b)** Montrer que G est un groupe non abélien [on pourra montrer que G est un sous-groupe du groupe $S_{\mathbb{R}}$ de toutes les bijections de $\mathbb{R}$ sur $\mathbb{R}$].

2) On considère dans G les deux sous-ensembles:

$$T = \{f_{1,b}\,;\, b \in \mathbb{R}\} \qquad \text{et} \qquad K = \{f_{a,0}\,;\, a \in \mathbb{R}^*\}.$$

- **a)** Montrer que T est un sous-groupe de G isomorphe au groupe additif $\mathbb{R}$, et que K est un sous-groupe de G isomorphe au groupe multiplicatif $\mathbb{R}^*$.
- **b)** Montrer que T est normal dans G et que $G/T \simeq \mathbb{R}^*$; [on pourra construire un morphisme de groupes $G \to \mathbb{R}^*$ surjectif de noyau T].
- **c)** Montrer que G est le produit semi-direct de T par K.

.../...

Exercice III.

On appelle nombre décimal tout nombre rationnel x qui peut s'écrire sous la forme $x = \frac{a}{10^n}$ avec $a \in \mathbb{Z}$ et $n \in \mathbb{N}$. L'ensemble des nombres décimaux est noté $\mathbb{D}$.

1) Montrer que : $\mathbb{Z} \subset \mathbb{D} \subset \mathbb{Q}$; vérifier que ces inclusions sont strictes en donnant un exemple d'un décimal qui n'est pas entier, et d'un rationnel qui n'est pas décimal.

2) Montrer que $\mathbb{D}$ est un sous-anneau unitaire intègre de $\mathbb{Q}$. Est-ce un sous-corps ?

3) Montrer que tout nombre décimal non-nul x admet une écriture unique de la forme $x = \frac{a}{2^n 5^m}$ avec $m, n, a \in \mathbb{Z}$ et a non divisible par 2 ni par 5.

4) On note $U(\mathbb{D})$ le groupe multiplicatif formé des éléments de $\mathbb{D}$ qui sont inversibles dans $\mathbb{D}$.

- **a)** Montrer que $0{,}25 \in U(\mathbb{D})$ mais que $0{,}24 \notin U(\mathbb{D})$.
- **b)** Montrer qu'un nombre décimal appartient à $U(\mathbb{D})$ si et seulement s'il est de la forme $\varepsilon 2^n 5^m$ avec $m, n \in \mathbb{Z}$ et $\varepsilon = \pm 1$.
- **c)** En notant C le sous-groupe $\{1, -1\}$ de $U(\mathbb{D})$, montrer que le groupe quotient $U(\mathbb{D})/C$ est isomorphe au groupe additif $\mathbb{Z}^2$; [*indication:* on pourra utiliser la question précédente pour construire un morphisme de groupes surjectif $U(\mathbb{D}) \to \mathbb{Z}^2$ de noyau C].

5) Soit I un idéal non-nul de $\mathbb{D}$.

- **a)** Montrer que I contient nécessairement des entiers strictement positifs. On note k le plus petit élément de $I \cap \mathbb{N}^*$; vérifier que k n'est divisible ni par 2 ni par 5, et que $k\mathbb{D} \subset I$.
- **b)** Justifier que tout élément x de I est de la forme $\frac{qk+r}{10^n}$ avec $q \in \mathbb{Z}$, $n, r \in \mathbb{N}$ et $0 \leq r < k$; vérifier que l'on a nécessairement $r = 0$.
- **c)** Conclure que $I = k\mathbb{D}$.
- **d)** Quelle propriété de l'anneau $\mathbb{D}$ vient-on d'établir ?

6) Soit δ l'application $\mathbb{D}^* \to \mathbb{N}$ qui, à tout nombre décimal non-nul x écrit sous la forme canonique $x = \frac{a}{2^n 5^m}$ avec $m, n, a \in \mathbb{Z}$ et a non divisible par 2 ni par 5 (voir question 3), associe $\delta(x) = |a|$. Montrer que l'anneau $\mathbb{D}$ est euclidien de stathme δ.

7) Soit p un nombre premier distinct de 2 et de 5.

- **a)** Justifier que, dans $\mathbb{Z}/p\mathbb{Z}$, l'élément $\overline{10}$ est inversible. Pour tout nombre décimal $x = \frac{a}{10^n}$ avec $a \in \mathbb{Z}$ et $n \in \mathbb{N}$, on pose $f(x) = \overline{a}.(\overline{10})^{-n}$ dans $\mathbb{Z}/p\mathbb{Z}$. Montrer que l'application $f : \mathbb{D} \to \mathbb{Z}/p\mathbb{Z}$ est bien définie.
- **b)** Montrer que f est un morphisme d'anneaux unitaires, surjectif, et déterminer son noyau.
- **c)** Conclure que les anneaux $\mathbb{D}/p\mathbb{D}$ et $\mathbb{Z}/p\mathbb{Z}$ sont isomorphes.
- **d)** Quelle propriété peut-on en déduire pour l'anneau $\mathbb{D}/p\mathbb{D}$? Quelle propriété peut-on en déduire pour l'idéal $p\mathbb{D}$ de $\mathbb{D}$?

8) On se place dans l'anneau de polynômes $\mathbb{Z}[X]$. On note $J = (1 - 10X)\mathbb{Z}[X]$ l'idéal principal engendré par le polynôme $1 - 10X$. On considère le morphisme de substitution $f : \mathbb{Z}[X] \to \mathbb{Q}$ défini par $f(X) = \frac{1}{10}$; en d'autres termes, l'image par f d'un polynôme quelconque $P(X) = \sum_{i=1}^{n} c_i X^i$ à coefficients entiers est le nombre rationnel $f(P) = \sum_{i=1}^{n} \frac{c_i}{10^i}$.

- **a)** Montrer que $\operatorname{Im} f = \mathbb{D}$, puis que $\operatorname{Ker} f = J$.
- **b)** En déduire que $\mathbb{D}$ est isomorphe à $\mathbb{Z}[X]/J$.
- **c)** Conclure que J est premier mais non maximal dans $\mathbb{Z}[X]$. Que peut-on en déduire pour l'anneau $\mathbb{Z}[X]$?

Université Blaise Pascal,
UFR Sciences et Technologies
Département de Mathématiques et Informatique

mardi 10 janvier 2012

LICENCE DE MATHÉMATIQUES, TROISIÈME ANNÉE
U.E. Algèbre et Géométrie

Durée: trois heures. *L'usage du polycopié du cours est autorisé, à l'exclusion de tout autre document ; l'usage des calculatrices, ordinateurs et téléphones portables est interdit durant l'épreuve.*

EXERCICES D'APPLICATION DU COURS.

Ex 1. Soit $\mathbb{U}$ le groupe multiplicatif des nombres complexes de module égal à 1. Montrer que l'application $f : \mathbb{R} \to \mathbb{C}^*$ définie par $f(t) = \exp(2i\pi t)$ pour tout $t \in \mathbb{R}$ est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{C}^*, \times)$ et que $\mathbb{R}/\mathbb{Z}$ est isomorphe à $\mathbb{U}$. Montrer de même, en introduisant un morphisme de groupes bien choisi que $\mathbb{C}^*/\mathbb{U}$ est isomorphe au groupe multiplicatif $\mathbb{R}_+^*$.

Ex 2. Quelles sont les valeurs possibles de $1 \leq a, b \leq 12$ pour que $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 6 & 5 & a & 4 & 11 & 10 & b & 9 & 7 & 12 & 2 \end{smallmatrix}\right)$ soit une permutation dans S_{12} ? Pour quelles valeurs de a et b la permutation σ est-elle d'ordre 20 dans S_{12} ; [*indication:* on pourra utiliser la décomposition de σ en produit de cycles disjoints].

Ex 3. On considère le nombre complexe $\omega = i\sqrt{3}$, l'anneau $A = \mathbb{Z}[\omega] = \{a + bi\sqrt{3}\,;\, a, b \in \mathbb{Z}\}$ et son corps de fractions $K = \mathbb{Q}[\omega] = \{x + yi\sqrt{3}\,;\, x, y \in \mathbb{Q}\}$. Montrer que le polynôme $P = X^2 - X + 1$ est irréductible dans $\mathbb{Z}[X]$, irréductible dans $A[X]$, mais non irréductible dans $K[X]$. Que peut-on en déduire pour l'anneau A ?

PROBLÈME.

Les cinq parties du problème sont largement indépendantes (sauf mention explicite) et le résultat d'une question non résolue peut être admis et utilisé pour traiter la suite.

Pour tout entier $n \geq 1$, on note G_n le groupe $U(\mathbb{Z}/n\mathbb{Z})$, c'est-à-dire le groupe multiplicatif formé des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. On rappelle qu'un élément $\overline{x}$ de $\mathbb{Z}/n\mathbb{Z}$ appartient à G_n si et seulement si les entiers x et n sont premiers entre eux.

Un entier naturel n est dit *primaire* lorsqu'il est une puissance non triviale d'un nombre premier, c'est-à-dire lorsqu'il existe un nombre premier p et un entier $\alpha \in \mathbb{N}^*$ tel que $n = p^\alpha$.

1) L'ensemble des éléments non-inversibles de $\mathbb{Z}/n\mathbb{Z}$. Pour tout entier $n \geq 1$, on note B_n le sous-ensemble de $\mathbb{Z}/n\mathbb{Z}$ formé des éléments non-inversibles dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.

a) Soit $n \geq 2$ un entier qui n'est pas primaire. Montrer qu'il s'écrit $n = ab$ avec $1 < a < n$ et $1 < b < n$ deux entiers premiers entre eux ; [*indication:* considérer la décomposition de n en produit de facteurs premiers]. Vérifier que $\overline{a} \in B_n$ et $\overline{b} \in B_n$. Montrer que $a + b$ est premier avec n.

b) Soit $n = p^\alpha$ un entier primaire, avec p premier et $\alpha \in \mathbb{N}^*$. Montrer que pour tout $x \in \mathbb{Z}$, on a: $\overline{x} \in B_n$ si et seulement si p divise x.

c) Soit $n \geq 2$ un entier. Déduire de a) et b) que B_n est un sous-groupe du groupe additif $\mathbb{Z}/n\mathbb{Z}$ si et seulement n est primaire.

2) Fonctions arithmétiques multiplicatives. On appelle fonction arithmétique multiplicative toute application non-nulle $f : \mathbb{N}^* \to \mathbb{Z}$ qui vérifie $f(ab) = f(a)f(b)$ pour tout couple (a, b) d'entiers naturels non-nuls premiers entre eux.

a) Montrer qu'une telle application vérifie $f(1) = 1$.

b) Montrer que, si f est une fonction arithmétique multiplicative, il suffit, pour connaître les valeurs $f(n)$ pour tout entier $n \geq 1$, de connaître $f(n)$ pour tout entier n primaire.

c) Soit $f : \mathbb{N}^* \to \mathbb{Z}$ une fonction arithmétique multiplicative. On définit $g : \mathbb{N}^* \to \mathbb{Z}$ par $g(n) = \sum_{d|n} f(d)$ pour tout $n \in \mathbb{N}^*$ (ce qui signifie que $g(n)$ est la somme des valeurs prises par f sur tous les diviseurs positifs de n). Montrer que g est une fonction arithmétique multiplicative ; [*indication:* vérifier d'abord que, si a et b sont premiers entre eux, tout diviseur de ab est produit d'un diviseur de a par un diviseur de b].

3) Le groupe G_n et la fonction indicatrice d'Euler. On rappelle que l'on appelle indicatrice d'Euler l'application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ définie par $\varphi(1) = 1$ et, pour tout entier $n \geq 2$, $\varphi(n)$ est le nombre d'entiers compris entre 1 et $n-1$ qui sont premiers avec n.

a) Rappeler (sans démonstration) quel lien existe entre l'entier $\varphi(n)$ et le groupe G_n.

b) Calculer $\varphi(n)$ pour $1 \leq n \leq 10$. Donner la valeur de $\varphi(p)$ pour tout nombre premier p.

c) Montrer que les groupes G_{10} et G_{12} sont de même ordre mais ne sont pas isomorphes.

d) Soit $n = p^\alpha$ un entier primaire, avec p premier et $\alpha \geq 1$. Montrer que les entiers compris entre 1 et $n-1$ qui ne sont pas premiers avec n sont ceux qui sont divisibles par p; [*indication:* on pourra utiliser 1.b)]. Combien y en a-t-il ? Conclure que $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

e) Soit a et b deux entiers naturels non-nuls. Montrer qu'un élément $(\widehat{x}, \widehat{y})$ est inversible dans l'anneau $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ si et seulement si $\widehat{x}$ est inversible dans $\mathbb{Z}/a\mathbb{Z}$ et $\widehat{y}$ est inversible dans $\mathbb{Z}/b\mathbb{Z}$.

f) En utilisant le théorème chinois, déduire des questions a) et e) que φ est une fonction arithmétique multiplicative.

g) Déduire de d) et f) une formule donnant explicitement $\varphi(n)$ pour tout entier $n \geq 2$ en fonction de la décomposition de n en produit de facteurs premiers.

4) Le groupe G_n et la fonction indicatrice d'Euler (suite). On établit dans cette question deux applications des questions précédentes.

a) Montrer que l'on a la formule (dite identité d'Euler): $\sum_{d|n} \varphi(d) = n$ pour tout $n \in \mathbb{N}^*$; [*indication:* établir la formule pour n primaire, puis utiliser 3.f), 2.c) et 2.b)].

b) Soit $n \geq 2$ un entier. Montrer que, pour tout entier $a \geq 1$ premier avec n, on a la propriété (dite d'Euler) suivante : $a^{\varphi(n)} \equiv 1 \mod n$; [*indication:* considérer $\overline{a}$ dans G_n].

5) Le groupe G_n pour n premier. On fixe ici un nombre premier p et l'on étudie le groupe G_p.

a) Rappeler quel est l'ordre de G_p.

b) Pour tout diviseur d de $p-1$, on note E_d l'ensemble des éléments $\overline{x}$ de G_p qui vérifient $\overline{x}^d = \overline{1}$. Montrer que E_d est un sous-groupe de G_p. En considérant le polynôme $X^d - \overline{1}$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$, justifier que l'ordre de E_d est au plus d.

c) Pour tout diviseur d de $p-1$, on note Γ_d l'ensemble des éléments $\overline{x}$ de G_p qui sont d'ordre d dans G_p. Montrer que Γ_d est inclus dans E_d, et n'est pas un sous-groupe de G_p.

d) Soit d un diviseur de $p-1$ tel que $\Gamma_d \neq \emptyset$. Montrer que, pour tout $\overline{x} \in \Gamma_d$, le groupe E_d est égal au groupe cyclique engendré par $\overline{x}$. En déduire que le cardinal de Γ_d est $\varphi(d)$.

e) Montrer à l'aide du théorème de Lagrange que: $\sum_{d|p-1} \operatorname{Card} \Gamma_d = p-1$.

f) Déduire de d), e) et 4.a) que $\Gamma_d \neq \emptyset$ pour tout diviseur d de $p-1$.

g) En appliquant ce qui précède à $d = p-1$, conclure que G_p est cyclique.

Université Blaise Pascal,
UFR Sciences et Technologies
Département de Mathématiques et Informatique

lundi 25 juin 2012

Licence de Mathématiques, troisième année

U.E. Algèbre et Géométrie

Durée: trois heures. *L'usage du polycopié du cours est autorisé, à l'exclusion de tout autre document ; l'usage des calculatrices, ordinateurs et téléphones portables est interdit durant l'épreuve.*

Premier exercice.

Soit A un anneau commutatif intègre.

1) Montrer que, pour tout élément $a \neq 0$ de A, l'application $f_a : x \mapsto ax$ de A dans A est injective.

2) En déduire que, si A est fini, alors A est un corps.

3) En déduire que, dans un anneau fini, tout idéal premier est maximal.

Deuxième exercice.

On se place dans le groupe symétrique S_n, avec $n \geq 2$.

1) Montrer que, si $\tau = [i, j]$ est une transposition dans S_n, alors, pour toute permutation $\sigma \in S_n$, la conjuguée $\sigma\tau\sigma^{-1}$ est égale à la transposition $[\sigma(i), \sigma(j)]$.

2) En déduire que deux transpositions quelconques de S_n sont toujours conjuguées dans S_n.

3) Soit H un sous-groupe de S_n normal dans S_n tel que H contienne une transposition. Montrer que $H = S_n$.

Troisième exercice.

On considère le polynôme $F = X^3 - X + 2$ dans $\mathbb{Z}[X] \subset \mathbb{Q}[X]$, et $\overline{F}$ sa réduction modulo 3 dans $(\mathbb{Z}/3\mathbb{Z})[X]$.

1) Montrer que $\overline{F}$ est irréductible dans $(\mathbb{Z}/3\mathbb{Z})[X]$.

2) En déduire que F est irréductible dans $\mathbb{Z}[X]$, puis que F est irréductible dans $\mathbb{Q}[X]$ (on citera avec soin les théorèmes utilisés).

3) Soit $I = (F) = F\mathbb{Q}[X]$ l'idéal principal de $\mathbb{Q}[X]$ engendré par F. Montrer que $\mathbb{Q}[X]/I$ est un corps. Quel est l'inverse dans ce corps de la classe de X ?

Quatrième exercice.

On considère l'anneau $A = \mathbb{Z}[i] = \{a + bi\,;\, a, b \in \mathbb{Z}\}$ des entiers de Gauss. On rappelle qu'il est principal. On note $N : A \to \mathbb{N}$ l'application multiplicative définie par $N(z) = |z|^2 = a^2 + b^2$ pour tout $z = a + bi \in A$. On rappelle enfin que le groupe des éléments inversibles de A est: $U(A) = \{1, -1, i, -i\} = \{z \in A\,;\, N(z) = 1\}$. On considère dans A les trois idéaux:

$$I = (1 + i)A, \quad J = (3 + i)A, \quad K = (5 + i)A.$$

suite au verso...

1) Lesquels des trois éléments $1+i$, $3+i$, $5+i$ sont irréductibles dans A (justifier la réponse) ? Que peut-on en déduire pour les idéaux I, J, K ?

2) Montrer que $I = J + K$. Quels sont les pgcd de $3+i$ et $5+i$ dans A ?

3) Déterminer c, d dans $\mathbb{Z}$ tels que $J \cap K = (c+di)A$. Quelle interprétation peut-on donner de ce résultat pour les éléments $3+i$ et $5+i$?

4) On note $L = (3+2i)A$ et $h : \mathbb{Z} \to A/L$ l'application qui, à tout entier $n \in \mathbb{Z}$, associe sa classe $h(n) = \overline{n}$ dans le quotient A/L (ceci a un sens puisque $\mathbb{Z} \subset A$); il est clair que h est un morphisme d'anneaux unitaires de $\mathbb{Z}$ dans A/L (on ne demande pas de le démontrer).

- **a)** Montrer que, pour tous $a, b \in \mathbb{Z}$, il existe $n \in \mathbb{Z}$ tels que $(a+ib) - n \in L$. En déduire que h est surjective.
- **b)** Montrer que $\operatorname{Ker} h = 13\mathbb{Z}$.
- **c)** Que peut-on en déduire pour l'idéal L ?

Cinquième exercice.

Soit G un groupe fini non trivial; on note $|G| \geq 2$ son ordre.

1) Rappelons que le centre de G est l'ensemble $Z(G)$ formé des éléments de G qui commutent avec tous les éléments de G; rappelons aussi que $Z(G)$ est un sous-groupe normal de G.

- **a)** Vérifier que G est abélien si et seulement si $Z(G) = G$.
- **b)** Montrer que, si $G/Z(G)$ est cyclique, alors G est abélien.
- **c)** En déduire que, si G n'est pas abélien, alors $|Z(G)| \leq \frac{|G|}{4}$.

2) Pour tout $x \in G$, on note $C(x)$ l'ensemble des éléments de G qui commutent avec x.

- **a)** Montrer que $C(x)$ est un sous-groupe de G pour tout $x \in G$.
- **b)** Déterminer $C(x)$ lorsque $x \in Z(G)$?
- **c)** En déduire que $x \notin Z(G)$ si et seulement si $|C(x)| \leq \frac{|G|}{2}$

3) On note $t(G)$ le nombre de couples $(x, y) \in G \times G$ qui vérifient $xy = yx$, et on pose $d(G) = \frac{t(G)}{|G|^2}$.

- **a)** Calculer $d(G)$ lorsque G est abélien.
- **b)** Calculer $d(G)$ lorsque G est le groupe symétrique S_3.
- **c)** Calculer $d(G)$ lorsque G est le groupe diédral D_4.

4) On suppose dans cette question que G n'est pas abélien.

- **a)** Montrer que $t(G) = t_1 + t_2$ avec $t_1 = \sum_{x \in Z(G)} |C(x)|$ et $t_2 = \sum_{x \notin Z(G)} |C(x)|$.
- **b)** Calculer t_1 à l'aide de la question 2.b.
- **c)** En déduire à l'aide de la question 2.c que $t(G) \leq \frac{|G|}{2}(|G| + |Z(G)|)$.
- **d)** Conclure avec la question 1.c que $d(G) \leq \frac{5}{8}$.

5) Conclure que tout groupe G qui vérifie $d(G) > \frac{5}{8}$ est abélien, et que ce minorant est optimal au sens où il existe des groupes non abéliens pour lesquels $d(G) = \frac{5}{8}$.