Corrigé

Examen blanc

Groupes anneaux et corps

LPEM

Définition

Soit A un anneau unitaire. Un élément $e \in A$ est dit idempotent si $e^2 = e$.

Exercice 1 Soit p un nombre premier et G un groupe d'ordre p.

1. L'ordre de a est un diviseur de p, donc $o(a) = 1$ ou $o(a) = p$, comme $a \neq e$, il vient alors que $o(a) = p$. Le sous groupe engendré par a est de cardinal p, donc égale à G. Le groupe G est cyclique donc commutatif.
2. Considérons l'application $f : \mathbb{Z} \to G$ définie par $f(n) = a^n$. Clairement f est un morphisme de groupes. Puisque G est engendré par a, le morphisme f est surjectif. Pour tout $n \in \mathbb{N}$, on a $f(np) = a^{np} = e$, donc $p\mathbb{Z} \subseteq \ker f$. Soit $n \in \ker f$, donc $a^n = e$, en effectuant la division euclidienne de a par p, il existe $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = qp + r$ et $0 \leq r < p$. On a alors $a^n = a^{pq} a^r = a^r$, donc $a^r = e$. D'où $r = 0$ car $0 \leq r < p$ et a est un élément d'ordre p. Par suite $n = pq \in p\mathbb{Z}$. On en déduit alors que $\ker f = p\mathbb{Z}$. Le théorème d'isomorphisme conduit à l'isomorphisme voulu.

Exercice 2 Soit G un groupe d'ordre 15.

1. 3 est un diviseur premier de 15, par le théorème de Cauchy, G admet un élément a d'ordre 3, en particulier $a^3 = e$ et $a^2 \neq e$.
   N.B : Notons que les conditions $a^3 = e$ et $a^2 \neq e$, signifie que a est un élément d'ordre 3. En effet $a^3 = e$, signifie que l'ordre de a divise 3, donc a est d'ordre 1 ou 3, et l'ordre de a ne peut être égale à 1 car $a^2 \neq e$, donc a est d'ordre 3.
2. De même 5 est un diviseur premier de G, d'après le théorème de Cauchy, G admet un élément d'ordre 5, en particulier $a^5 = e$ et $a^4 \neq e$.
   N.B : Notons que les conditions $b^5 = e$ et $b^4 \neq e$, signifie que b est un élément d'ordre 5.
3. Soit $x \in \langle a \rangle \cap \langle b \rangle$. Il existe $0 \leq i \leq 2$ tel que $x = a^i$ et il existe $0 \leq j \leq 4$ tel que $x = b^j$. On a donc $x = x^6 x^{-5} = a^{i6} a^{-5j} = (a^3)^{2i} (b^5)^{-j} = e$.
4. On suppose dans cette question que $ab = ba$.
   4.1 L'ordre de ab est un diviseur de 15, donc égale à 1, 3, 5 ou 15.
   L'ordre de ab est différent de 1. En effet, si $ab = e$, alors $a = b^{-1}$ ce qui impossible car a est d'ordre 3 et b^{-1} est d'ordre 5.
   L'ordre de ab ne peut être égale à 3, car si $(ab)^3 = e$, alors dans ce cas $a^3 b^3 = e$ c'est-à-dire $b^3 = e$ ce qui n'est pas le cas.
   L'ordre de ab ne peut être égale à 5, car si $(ab)^5 = e$, alors $a^5 = e$ et donc $a^2 = e$, ce qui n'est pas le cas.
   Finalement ab est un élément d'ordre 15.

4.2 ab est un élément d'ordre 15 dans G et G est un groupe d'ordre 15, donc $G = \langle ab \rangle$. On considérons le morphisme de groupe $f : \mathbb{Z} \to G$ définie par $f(n) = (ab)^n$. Ce morphisme (surjectif et e noyau $\ker f = 15\mathbb{Z}$) induit un isomorphisme $\mathbb{Z}/15\mathbb{Z} \to G$.

Exercice 3 Soit A un anneau unitaire, tel que pour tout $x \in A$, $x^2 = x$.

1. Soit $x, y \in A$. On a $2x = 4x - 2x = 4x^2 - 2x = (2x)^2 - 2x = 2x - 2x = 0$, en d'autres termes, pour tout $x \in A$, $x = -x$. D'une part $(x+y)^2 = x+y$ et d'autre part $(x+y)^2 = x^2+xy+yx+y^2 = x+xy+yx+y$, donc $x + y = x + xy + yx + y = x + y$, on en déduit alors que $xy + yx = 0$, donc $xy = -yx = yx$. Donc l'anneau A est commutatif.
2. Soit $f : \mathbb{Z} \to A$ l'application définie par $f(n) = n1_A$. L'application f est un morphisme d'anneaux. Pour tout $n \in \mathbb{N}$, on a $f(2n) = 2n1_A = 0$, donc $2\mathbb{Z} \subseteq \ker f$. Si $n = 2r + 1$ est impair alors $f(n) = 2r1_1 + 1_A = 1_A \neq 0$. Ainsi le noyau de f est formé par les nombres pair c'est-à-dire $\ker f = 2\mathbb{Z}$. Soit $x \in A$, comme $x^2 = x$ c'est-à-dire $x(x - 1_A) = 0$ et A intègre alors $x = 0 = f(0)$ ou $x = 1_A = f(1)$, par suite f est surjectif. On en déduit, par le théorème d'isomorphisme, que A est isomorphisme à $\mathbb{Z}/2\mathbb{Z}$.
3. Soit P un idéal premier de A. L'anneau A/P et intègre et pour tout $\overline{x} \in A/P$, $\overline{x}^2 = \overline{x^2} = \overline{x}$, d'après le résultat de la question précédente, A/P est un corps (isomorphisme à $\mathbb{Z}/2\mathbb{Z}$), donc P est un idéal maximal.

PROBLÈME

Soit A un anneaux commutatif unitaire.

Première partie : Éléments idempotents

Soient A_1, A_2 deux anneaux commutatifs unitaires non réduits à un seul élément.

1. Soit e est un élément idempotent de A, alors $(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e$, ainsi $1 - e$ est un élément idempotent.
2. Si A est intègre et e un élément idempotent de A, alors $e(1-e) = e - e^2 = 0$, donc $e = 0$ ou $e = 1$.
3. On a $(1,0)^2 = (1^2, 0^2) = (1,0)$, donc $(1,0)$ est un élément idempotent de $A_1 \times A_2$.
4. Soit $f : A_1 \times A_2 \to A$ un isomorphisme et $a = f(1,0)$. On a $a^2 = f((1,0)^2) = f(1,0) = a$, donc a est un élément idempotent de A. Puisque $(1,0) \neq (1,1)$ et f injectif, alors $1 = f(1,1) \neq f(1,0) = a$. De même $(1,0) \neq (0,0)$ et f injectif, donc $0 = f(0,0) \neq f(1,0) = a$.

Deuxième partie : Théorème chinois

Soient I et J deux idéaux de A tels que $I + J = A$. Soit $\varphi : A \to (A/I) \times (A/J)$ l'application définie par $\varphi(x) = (\overline{x}, \overline{x})$.

5. Immédiate.
6. On a $1 \in A = I + J$, donc il existe $(i_0, j_0) \in I \times J$ tel que $1 = i_0 + j_0$.
7. Soit x, y deux éléments de A. On pose $a = xj_0 + yi_0$.
   - 7.1 On a $a - x = xj_0 + yi_0 - x = x(j_0 - 1) + yi_0 = -xi_0 + yi_0 \in I$, de même $a - y = xj_0 + yi_0 - y = xj_0 + y(i_0 - 1) = xj_0 - yj_0 \in J$.
   - 7.2 On a $\varphi(a) = (\overline{a}, \overline{a}) = (\overline{x} + \overline{a - x}, \overline{y} + \overline{a - y}) = (\overline{x}, \overline{y})$. Donc φ est surjectif.

$\boxed{8.}$ En appliquant le théorème d'isomorphisme, il suffit alors de montrer que $\ker\varphi = I \cap J$. En effet si $x \in I \cap J$, alors $\varphi(x) = (\overline{x}, \overline{x}) = 0$, donc $I \cap J \subseteq \ker\varphi$. Réciproquement, si $x \in \ker\varphi$,alors $\varphi(x) = (\overline{x}, \overline{x}) = 0$, par suite $x \in I$ et $x \in J$, d'où $x \in I \cap J$. Il vient alors que $\ker\varphi = I \cap J$.

Troisième partie :
Idempotent et produit

On suppose que A admet un élément idempotent e différent de 0 et de 1. Notons I (respectivement J) l'idéal de A engendré par e (respectivement par $1-e$).

$\boxed{9.}$ On a $1 = e + (1-e) \in I + J$, donc $I + J = A$.

$\boxed{10.}$ Soit $x \in I \cap J$, il existe $a \in A$ tel que $x = ae$ et il existe $b \in A$ tel que $x = b(1-e)$. On a $xe = b(1-e)e = b(e-e^2) = 0$ et $x(1-e) = ae(1-e) = a(e-e^2) = 0$, donc $x = (1-e+e)x = (1-e)x+ex = 0$.

$\boxed{11.}$ On a $I + J = A$ et $I \cap J = \{0\}$, d'après le résultat de partie précédente, $A = A/(I \cap J)$ est isomorphe à $(A/I) \times (A/J)$. Il reste à montrer que les deux anneaux A/I et A/J ne sont pas réduits à un seul élément. Si $\overline{0} = \overline{1}$ dans A/I, alors $1 = \alpha e$ où $\alpha \in A$, puis $1 - e = \alpha e(1-e) = 0$, ce qui conduit à $1 = e$ (mais $e \neq 1$). De même si $\overline{1} = \overline{0}$ dans A/J, alors $1 = \beta(1-e)$ où $\beta \in A$, puis $e = \beta(1-e)e = 0$ (mais $e \neq 0$).