Correction de la fiche de révisions

Groupes

Exercice 17 (Ordre d'un élément)**.**

(1) Soient G, H deux groupes et $f \in \mathrm{Hom}(G, H)$. Soit $x \in G$. Comparer l'ordre de x et de $f(x)$.

Soit n l'ordre de x. Alors $(f(x))^n = f(x^n) = f(e) = e$. $\boxed{\text{Donc l'ordre de } f(x) \text{ divise } n}$.

(2) Soient $x, g \in G$. Comparer l'ordre de x et de gxg^{-1}.

Soit n l'ordre de x. Alors $(gxg^{-1})^n = gx^ng^{-1} = geg^{-1} = e$.
Donc l'ordre de gxg^{-1} divise n. Réciproquement, on voit que $g^{-1}(gxg^{-1})g = x$ donc le même raisonnement nous permet de dire que l'ordre de x divise l'ordre de gxg^{-1}. $\boxed{\text{Les deux ordres sont donc égaux.}}$

(3) Soient $a, b \in G$. Comparer l'ordre de ab et de ba.

Soit n l'ordre de ab. Alors $(ba)^{n+1} = b(ab)^na = bea = ba$. Donc $ba = (ba)(ba)^n$, c'est à dire que $(ba)^n = e$. Donc l'ordre de ba divise l'ordre de ab. Par symétrie du problème en a et b, on en déduit que $\boxed{\text{les deux ordres sont égaux.}}$

Exercice 19 (Pas de sous-groupe)**.**
Soit G un groupe non trivial n'ayant pas de sous-groupe non-trivial.

(1) Montrer que G est monogène.

Soit $x \neq e$. Alors le sous-groupe $\langle x \rangle$ engendré par x n'est pas réduit à $\{e\}$. Donc $\langle x \rangle = G$. C'est à dire que $\boxed{G \text{ est monogène}}$.

(2) Montrer que G est fini.

Soit x un générateur de G. il suffit de montrer que x est d'ordre fini pour savoir que G est fini. On considère le sous-groupe $H = \langle x^2 \rangle$ engendré par x^2. Si $H = \{e\}$ alors $x^2 = e$ donc x est d'ordre 2. Sinon $H = G$ et donc il existe $k \in \mathbb{N}$ tel que $(x^2)^k = x$. C'est à dire $x^{2k-1} = e$ donc $\boxed{x \text{ est d'ordre fini}}$.

(3) Montrer que $|G|$ est un nombre premier.

Si $|G| = pq$ avec p, q des entiers plus grand que 2. Et soit x un générateur de G. Alors x^p est d'ordre q donc le sous-groupe engendré par x^p n'est pas trivial. Contradiction. $\boxed{\text{Donc } |G| \text{ est premier.}}$

Exercice 21 (Groupes de cardinal premier)**.**
Soit p un nombre premier et G un groupe de cardinal p.

(1) Montrer que G est cyclique.

Soit $x \neq e$. L'ordre de x divise $|G| = p$. Donc l'ordre de x est p. Donc $G = \langle x \rangle$, c'est à dire que $\boxed{G \text{ est cyclique}}$.

(2) En déduire que tous les groupes de cardinal p sont isomorphes.

Soit G un groupe d'ordre p et g un générateur de G. Soit l'application $f : \mathbb{Z}/p\mathbb{Z} \to G$ définie par $f(k) = g^k$. Cette application est bien définie et est un isomorphisme. En conclusion tout groupe d'ordre p premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Exercice 2 (Examen 2013)**.**

Soit G un groupe fini d'ordre n. Soit p le plus petit nombre premier qui divise n et soit H un sous-groupe d'ordre $q = \dfrac{n}{p}$.

On note $G/H = \{aH \mid a \in G\}$ l'ensemble des classes à gauche modulo H.

(1) Montrer que G/H est de cardinal p.

D'aprés le théorème de Lagrange, $|G| = |H| \times \text{Card}(G/H)$. Donc $\text{Card}(G/H) = \frac{|G|}{|H|} = \frac{n}{n/p} = p$

Le groupe H agit sur l'ensemble G/H par multiplication à gauche, c'est à dire pour tout $h \in H$ et toute classe $xH \in G/H$ on a :

$$h \cdot (xH) = (hx)H$$

(2) Montrer que le cardinal d'une orbite est soit égal à 1 soit supérieur ou égal à p.

Le cardinal d'une orbite divise $|H|$. Or $|H|$ divise n. Donc le cardinal d'une orbite est un diviseur de n. Soit le cardinal est 1, soit le cardinal est plus grand que le plus petit diviseur non-trivial de n. D'après l'énoncé, le plus petit diviseur non trivial de n est p.

(3) Mettre en évidence une orbite de cardinal 1.

Soit eH la classe de l'élément neutre dans G/H. Alors pour tout $h \in H$ on a $h \cdot (eH) = hH = H = eH$. Donc l'orbite de eH est réduite à $\{eH\}$. Cette orbite est de cardinal 1

(4) Montrer que toutes les orbites sont de cardinal 1 en utilisant la formule des classes

D'après la formule des classes $p\text{Card}(G/H) = \sum_{x \in G/H} |\mathcal{O}_x|$. Et d'après la question 2, on a $|\mathcal{O}_x| = 1$ ou $|\mathcal{O}_x| \geq p$. On n'a donc que deux possibilités : Soit il y a p orbites de cardinal 1, soit il y a 1 orbite de cardinal p.
Comme il y a au moins une orbite de cardinal 1 on en déduit que toutes les orbites sont de cardinal 1.

(5) En déduire que pour tout $x \in G$ et $h \in H$, on a $hx \in xH$.

Soit $x \in G$ et $h \in H$. On sait que $(hx)H = h \cdot (xH)$. Or l'orbite de xH est réduite à un seul élément donc $h \cdot (xH) = xH$. On en déduit que $(hx)H = xH$ ce qui est équivalent à dire que $hx \in xH$.

(6) Conclure que H est un sous-groupe normal (ou distingué) de G.

Soit $x \in G$ et $h \in H$. Alors $x^{-1}hx \in x^{-1}(xH) = H$. Donc H est distingué.

Anneaux

Exercice 3 (Examen 2013, Entiers d'Eisenstein)**.**

Soit $\omega = e^{\frac{2i\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. On considère l'ensemble $A = \{a + b\omega \mid a, b \in \mathbb{Z}\}$.
Pour tout $x = a + b\omega \in A$, on définit $N(x) = a^2 + b^2 - ab$

(1) Montrer que A est un sous-anneau de $\mathbb{C}$.

- $(A, +)$ est un sous-groupe. En effet $0 = 0 + 0\omega$. D'autre part, pour tout $x = a + b\omega$ et $x' = a' + b'\omega$ dans A, on a $x - x' = (a - a') + (b - b')\omega$ est dans A.
- Soit $x = a + b\omega$ et $x' = a' + b'\omega$ dans A.
  Alors $xx' = (a+b\omega)(a'+b'\omega) = aa' + (ab' + ba')\omega + bb'\omega^2$. Or $\omega^2 = -\omega - 1$ (Cela vient du fait que $\omega^3 = 1$).
  Donc $xx' = (aa' - bb') + (ab' + ba' - bb')\omega$ est bien un élément de A.

(2) Montrer que pour tout $x \in A$, on a $N(x) = |x|^2$ (où $|x|$ désigne le module du nombre complexe x).

$|x|^2 = \left|a + \frac{b}{2} + i\sqrt{3}\frac{b}{2}\right|^2 = \left(a - \frac{b}{2}\right)^2 + 3\left(\frac{b}{2}\right)^2 = a^2 + b^2 - ab = N(x)$.

(3) Montrer que x est inversible dans A si et seulement si $N(x) = 1$.

Si $N(x) = 1$. On sait que dans $\mathbb{C}$ l'inverse de x est donné par $\frac{1}{x} = \frac{\overline{x}}{x\overline{x}} = \frac{\overline{x}}{|x|^2} = \overline{x}$. Et d'autre part $\overline{x} = a + b\overline{\omega} = (a - b) - b\omega$ est bien dans A. Donc $\frac{1}{x} \in A$ ce qui veut dire que x est inversible dans A.
Réciproquement, si x est inversible dans A, alors il existe $y \in A$ tel que $xy = 1$. Donc $N(xy) = |xy|^2 = |x|^2|y|^2 = N(x)N(y) = 1$. Or $N(x)$ et $N(y)$ sont des entiers positifs donc $N(x) = 1$.

(4) Déterminer tous les éléments inversibles de A.

On résout l'équation $a^2 + b^2 - ab = 1$ dans $\mathbb{Z}$. Pour un b fixé, cette équation en a possède une solution réelle si et seulement si le discriminant $\Delta = b^2 - 4(b^2 - 1) = 4 - 3b^2$ est positif. On voit donc que nécessairement $|b| \leq 1$. Par symétrie, on en déduit aussi que $|a| \leq 1$. Il y a donc 9 possibilités à tester. On trouve 6 solutions en (a, b) qui sont $\{(1, 0); (1, 1); (0, 1); (-1, 0); (-1, -1); (0, -1)\}$. En conclusion :

$$A^\times = \{1;\ (1 + \omega);\ \omega;\ -1;\ (-1 - \omega);\ -\omega\}$$

(5) Montrer que pour tout $z \in \mathbb{C}$, il existe $q \in A$ tel que $|z - q| < 1$.

On peut donner un argument géométrique en disant que les points de A sont les points d'une grille formée par des triangles équilatéraux de coté 1. Un point dans un tel triangle est à distance strictement inférieure à 1 de l'un des sommets.
Pour le montrer "à la main", c'est un peu plus pénible : Soit $z = x + iy \in \mathbb{C}$. On pose c l'entier le plus proche de x et d l'entier le plus proche de $\frac{1}{\sqrt{3}}y$. On pose $q = c + i\sqrt{3}d$.(C'est bien un élément de A car $i\sqrt{3} \in A$) On vérifie alors que

$$|z - q|^2 = |(x - c) + i(y - d\sqrt{3})|^2 = (x - c)^2 + (y - d\sqrt{3})^2 \leq \frac{1}{4} + 3\frac{1}{4} \leq 1$$

Si l'inégalité est stricte, on a trouvé le q qui convient.
Si il y a égalité alors $|x - c| = \frac{1}{2}$ et $|y - d\sqrt{3}| = \frac{\sqrt{3}}{2}$. Donc dans ce cas particulier y est un élément de A et il suffit de prendre $q = y$.

(6) En déduire que pour tout $x, y \in A, y \neq 0$, il existe $q, r \in A$ tels que $x = qy + r$ et $N(r) < N(y)$.

On a $\frac{x}{y} \in C$ donc il existe q tel que $|\frac{x}{y} - q| < 1$ On pose alors $r = x - qy$ et on vérifie que:

$$N(r) = |r|^2 = |x - qy|^2 = |y|^2 \left| \frac{x}{y} - q \right| < N(y)$$

(7) En déduire que A est principal.

Soit I un idéal non trivial de A. Soit y un élément non nul de I de norme minimale (un tel élément existe car l'ensemble des normes est un ensemble non vide de $\mathbb{N}^*$.) Alors soit x un autre élément de I. Il existe $q, r \in A$ tels que $x = qy + r$ avec $N(r) < N(y)$. Or $r = x - qy$ est aussi un élément de I. Donc par minimalité de $N(y)$ on en déduit que $N(r) = 0$ donc $r = 0$ donc $x = qy$ donc $x \in \langle y \rangle$. On en déduit que $I = \langle y \rangle$ est principal.
En conclusion tout idéal de A est principal, donc $\boxed{A \text{ est principal}}$

Exercice 4 (radical)**.** Soit I un idéal d'un anneau A commutatif. on appelle *radical* de I l'ensemble

$$\mathbf{rad}(I) = \{x \in A | \exists n \in \mathbb{N}, x^n \in I\}$$

(1) Montrer que $\mathbf{rad}(I)$ est un idéal de A.

On montre d'abord que $\mathbf{rad}(I)$ est un sous-groupe :

- $0 \in I$ car I est un idéal. Alors, comme $0^1 = 0$ on en déduit que $0 \in \mathbf{rad}(I)$.
- Soit $x, y \in \mathbf{rad}(I)$. Soit $n, m \in \mathbb{N}$ tels que x^n et y^m sont dans I. Alors comme A est commutatif :

$$(x - y)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} (-1)^i y^i x^{m+n-i}$$

Si $i \geq m$ alors $y^i \in I$. Sinon $x^{m+n-i} \in I$. Donc dans chaque terme de la somme un des termes est dans I, et I est un idéal. Donc $(x - y)^{m+n} \in I$. On en déduit que $(x - y) \in \mathbf{rad}(I)$.

Soit $x, y \in \mathbf{rad}(I)$ et $n \in N$ tel que $x^n \in I$. Alors $(xy)^n = x^n y^n \in I$. Donc $xy \in \mathbf{rad}(I)$.
En conclusion $\mathbf{rad}(I)$ est un idéal de A.
(Rq : Il est nécessaire de supposer la commutativité de A, sinon le résultat est faux)

(2) En déduire que l'ensemble des nilpotents d'un anneau est un idéal.

Dans A, l'ensemble $\{0\}$ est un idéal. L'ensemble des nilpotents est exactement $\mathbf{rad}(\{0\})$

(3) Montrer que si J est un autre idéal $\mathbf{rad}(I \cap J) = \mathbf{rad}(I) \cap \mathbf{rad}(J)$

Soit $x \in \mathbf{rad}(I \cap J)$ et $n \in \mathbb{N}$ tel que $x^n \in I \cap J$. En particulier $x^n \in I$ et $x^n \in J$. Donc $x \in \mathbf{rad}(I)$ et $x \in \mathbf{rad}(J)$. Donc $\mathbf{rad}(I \cap J) \subset \mathbf{rad}(I) \cap \mathbf{rad}(J)$

Soit $x \in \mathbf{rad}(I) \cap \mathbf{rad}(J)$ et n, m tels que $x^n \in I$ et $x^m \in J$. Alors $x^{m+n} = x^m x^n$.
Comme I et J sont des idéaux on en déduit que $x^m x^n \in I$ et $x^m x^n \in J$. Donc $x^{m+n} \in I \cap J$.
Donc $x^{m+n} \in \mathbf{rad}(I \cap J)$.
Donc $\mathbf{rad}(I) \cap \mathbf{rad}(J) \subset \mathbf{rad}(I \cap J)$.

(4) Calculer $\mathbf{rad}(2\mathbb{Z})$, $\mathbf{rad}(4\mathbb{Z})$, $\mathbf{rad}(6\mathbb{Z})$ et $\mathbf{rad}(12\mathbb{Z})$

Soit $x \in Z$. Soit $n \in \mathbb{N}$ et p un nombre premier. D'après le lemme de Gauss :

$$x \in \mathbf{rad}(p\mathbb{Z}) \Leftrightarrow \exists n \in \mathbb{N}, x^n \in p\mathbb{Z} \Leftrightarrow \exists n \in \mathbb{N}, p \text{ divise } x^n \Leftrightarrow p \text{ divise } x \Leftrightarrow x \in p\mathbb{Z}$$

Donc il est clair que $\mathbf{rad}(p\mathbb{Z}) = p\mathbb{Z}$. Donc $\mathbf{rad}(2\mathbb{Z}) = 2\mathbb{Z}$.

Si $x \in \mathbf{rad}(4\mathbb{Z})$ alors il existe $n \in \mathbb{N}$ tel que 4 divise x^n. En particulier 2 divise n donc $x \in 2\mathbb{Z}$. Réciproquement si $x \in 2\mathbb{Z}$ alors $x^2 \in 4\mathbb{Z}$. Donc $\mathbf{rad}(4\mathbb{Z}) = 2\mathbb{Z}$.
De même on montre $\mathbf{rad}(6\mathbb{Z}) = 6\mathbb{Z}$ et $\mathbf{rad}(12\mathbb{Z}) = 6\mathbb{Z}$ en utilisant le fait que $6\mathbb{Z} = 2\mathbb{Z} \cap 3\mathbb{Z}$ et la question précédente.

(5) Plus généralement, montrer que si p est premier alors $\mathbf{rad}(p^n\mathbb{Z}) = p\mathbb{Z}$.

Si $x \in p\mathbb{Z}$ alors $x^n \in p^n\mathbb{Z}$. donc $p\mathbb{Z} \subset \mathbf{rad}(p^n\mathbb{Z})$.
D'autre part si il existe $m \in \mathbb{N}$ tel que p^n divise x^m alors p divise x^m. Donc p divise x (Lemme de Gauss) donc $x \in p\mathbb{Z}$. Donc $\mathbf{rad}(p^n\mathbb{Z}) \subset p\mathbb{Z}$.

(6) Pour n quelconque, déterminer $\mathbf{rad}(n\mathbb{Z})$ en fonction des facteurs premiers de n.

Soit $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ avec les p_i des nombres premiers distincts et $n_i \geq 1$. D'après les question précédentes :

$$\begin{aligned}
\mathbf{rad}(n\mathbb{Z}) &= \mathbf{rad}(p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}\mathbb{Z}) \\
&= \mathbf{rad}\left((p_1^{n_1}\mathbb{Z}) \cap (p_2^{n_2}\mathbb{Z}) \cap \cdots \cap (p_k^{n_k}\mathbb{Z})\right) \\
&= \mathbf{rad}(p_1^{n_1}\mathbb{Z}) \cap \mathbf{rad}(p_2^{n_2}\mathbb{Z}) \cap \cdots \cap \mathbf{rad}(p_k^{n_k}\mathbb{Z}) \\
&= (p_1\mathbb{Z}) \cap (p_2\mathbb{Z}) \cap \cdots \cap (p_k\mathbb{Z}) \\
&= (p_1 p_2 \cdots p_n)\mathbb{Z}
\end{aligned}$$

Exercice 5 (Examen 2013)**.**

On rappelle qu'un idéal P d'un anneau commutatif et unitaire A est dit *premier* si, pour tout couple d'éléments x, y de A on a la condition :

$$xy \in P \Leftrightarrow (x \in P) \text{ ou } (y \in P)$$

(1) Déterminer les idéaux premiers de l'anneau $\mathbb{Z}$ des entiers.

Soit $p \in \mathbb{Z}$ est un nombre premier et $x, y \in \mathbb{Z}$. Si $xy \in p\mathbb{Z}$ alors p divise xy et d'après le lemme de Gauss, p divise x ou y. Donc $x \in p\mathbb{Z}$ ou $y \in p\mathbb{Z}$. Donc les idéaux de la forme $p\mathbb{Z}$ avec p un nombre premier sont premiers.
Réciproquement, Si I est un idéal de $\mathbb{Z}$, alors $I = n\mathbb{Z}$ car $\mathbb{Z}$ est principal. Si n n'est pas premier, alors soit $n = 0$ soit $n = km$ avec $k, m \geq 1$. Alors dans ce dernier cas $k, m \notin n\mathbb{Z}$ et pourtant $km \in n\mathbb{Z}$ Donc l'idéal $n\mathbb{Z}$ n'est pas premier.
Par contre, l'anneau étant intègre, l'idéal $\{0\}$ est premier.
Les idéaux premiers de $\mathbb{Z}$ sont donc les idéaux de la forme $p\mathbb{Z}$ avec p premier ou $p = 0$.

(2) Montrer que $\mathbb{Z}[X]/(X+5)$ est isomorphe à $\mathbb{Z}$.

On définit l'application $\phi : \mathbb{Z}[X] \to \mathbb{Z}$ par $\phi(P) = P(-5)$. Cette application est bien un morphisme d'anneau (c'est le morphisme d'évaluation). ϕ est surjective car tout élément $n \in \mathbb{Z}$ peut s'écrire $\phi(\mathbf{n})$ avec $\mathbf{n}$ le polynôme constant égal à n. Et d'autre part Kerϕ est l'idéal engendré par $(X+5)$ en effet $P(-5) = 0$ si et seulement si P est un multiple de $X+5$.
D'après le théorème d'isomorphisme, on en déduit que $\mathbb{Z}[X]/(X+5)$ est isomorphe à $\mathbb{Z}$.

(3) En déduire que l'idéal $(X+5)$ est premier dans $\mathbb{Z}[X]$, mais n'est pas maximal.

$\mathbb{Z}[X]/(X+5)$ est intègre puisque $\mathbb{Z}$ l'est. Donc $(X+5)$ est premier.
Par contre $\mathbb{Z}[X]/(X+5)$ n'est pas un corps, donc $(X+5)$ n'est pas maximal.

(4) Soit $I = (5, X)$ l'idéal engendré par 5 et X. Montrer que $\mathbb{Z}[X]/I$ est isomorphe à $\mathbb{Z}/5\mathbb{Z}$, et en déduire que I est un idéal maximal.

On définit l'application $\psi : \mathbb{Z}[X] \to \mathbb{Z}/5\mathbb{Z}$ par $\psi(P) = P(0)\text{mod}(5)$.
Cette application est un morphisme d'anneaux. ψ est surjective (facile). Et si $P \in \text{Ker}\psi$ alors 5 divise $P(0)$ donc P peut s'écrire

$$P = 5k + XQ, \text{ avec } k \in \mathbb{Z}, Q \in \mathbb{Z}[X]$$

Donc $P \in (5, X)$. Réciproquement, tout élément de $(5, X)$ est dans le noyau. Donc $\text{Ker}\psi = I$.
D'après le théorème d'isomorphisme, $\mathbb{Z}[X]/I$ est isomorphe à $\mathbb{Z}/5\mathbb{Z}$.
Comme $\mathbb{Z}/5\mathbb{Z}$ est un corps, on en déduit que I est maximal.