CORRIGÉ DE L'EXAMEN DU 6 JUIN 2008

Problème 1. — Soient H un groupe fini et G un groupe cyclique ; suivant la convention adoptée dans le cours, les groupes cycliques sont finis. Désignons par n l'ordre du groupe G et par m l'ordre du groupe H.

(i) Supposons qu'il existe un homomorphisme de groupes surjectif $\varphi : \mathrm{G} \to \mathrm{H}$. Désignons par g un générateur de G. Tout élément y de H s'écrit sous la forme $y = \varphi(x)$ avec $x \in \mathrm{G}$, donc sous la forme

$$y = \varphi(g^k) = \varphi(g)^k$$

pour un entier naturel k convenable. Ceci montre que le groupe fini H est cyclique et engendré par $\varphi(g)$.

L'ordre du groupe cyclique H est l'ordre du générateur $\varphi(g)$. On a donc

$$\{k \in \mathbb{Z} \mid \varphi(g)^k = e_{\mathrm{H}}\} = m\mathbb{Z}$$

et, puisque $\varphi(g)^n = \varphi(g^n) = \varphi(e_{\mathrm{G}}) = e_{\mathrm{H}}$, nous en concluons que m divise n.

(ii) Supposons réciroquement que le groupe H soit cyclique et que son ordre divise l'ordre du groupe G. Désignons par g un générateur de G et par h un générateur de H. L'application

$$\mathbb{Z} \to \mathrm{G}, \quad k \mapsto g^k$$

est un homomorphisme de groupes surjectif de noyau $n\mathbb{Z}$, donc induit un isomorphisme de groupes $\varphi_{\mathrm{G}} : \mathbb{Z}/n\mathbb{Z} \to \mathrm{G}$ par application du théorème de Noether. De même, l'application $\mathbb{Z} \to \mathrm{H}, \quad k \mapsto h^k$ induit un isomorphisme de groupes $\varphi_{\mathrm{H}} : \mathbb{Z}/m\mathbb{Z} \to \mathrm{H}$.

Comme m divise n, $n\mathbb{Z} \subset m\mathbb{Z}$ et il découle de nouveau du théorème de Noether que la projection canonique $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \quad k \mapsto k \pmod m$ induit un homomorphisme de groupes surjectif $p : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

Il reste finalement à poser $\varphi = \varphi_{\mathrm{H}} \circ p \circ \varphi_{\mathrm{G}}^{-1}$ pour obtenir un homomorphisme surjectif du groupe G dans le groupe H.

Remarque : l'homomorphisme $\varphi : \mathrm{G} \to \mathrm{H}$ que l'on vient de définir envoie un élément x de G*, écrit sous la forme $x = g^k$ avec $k \in \mathbb{Z}$, sur l'élément $\varphi(x) = h^k$ de* H*. Si l'on veut utiliser ceci comme définition de φ, il faut vérifier que $\varphi(x)$ ne dépend pas du choix de l'entier k tel que $x = g^k$ et que l'application obtenue est un homomorphisme de groupes.*

Problème 2. — On rappelle que les diviseurs de zéro dans un anneau A sont tous les éléments a de A pour lesquels qu'il existe $b \in \mathrm{A} - \{0\}$ tel que $a.b = 0$.

1. Un élément (a,b) de $\mathbb{Z} \times \mathbb{Z}$ est un diviseur de zéro si et seulement s'il existe $(c,d) \in \mathbb{Z} \times \mathbb{Z} - \{(0,0)\}$ tel que $(a,b).(c,d) = (ab,cd) = (0,0)$, c'est-à-dire tel que $ac = bd = 0$.

Comme c ou d doit être non nul, une condition nécessaire est $a = 0$ ou $b = 0$ car l'anneau $\mathbb{Z}$ est intègre.

Cette condition est suffisante car, pour tous $a, b \in \mathbb{Z}$, $(a,0)$ et $(0,b)$ sont des diviseurs de zéro dans $\mathbb{Z} \times \mathbb{Z}$ en vertu des identités

$$(a,0).(0,1) = (0,b).(1,0) = (0,0).$$

Nous avons ainsi démontré que les diviseurs de zéro dans l'anneau $\mathbb{Z} \times \mathbb{Z}$ sont les éléments (a,b) tels que $a = 0$ ou $b = 0$.

2. Soit A l'anneau des fonctions réelles sur $[0,1]$, l'addition et la multiplication étant définies de la manière usuelle. Une fonction réelle f sur $[0,1]$ est un diviseur de zéro dans A si et seulement s'il existe une fonction réelle non identiquement nulle g sur $[0,1]$ telle que $f.g = 0$, c'est-à-dire telle que $f(x)g(x) = 0$ pour tout $x \in [0,1]$.

- Si une fonction réelle f sur $[0,1]$ est un diviseur de zéro dans A, $f.g = 0$ avec g une fonction réelle non identiquement nulle sur $[0,1]$. Il existe alors un point x_0 de $[0,1]$ tel que $g(x_0) \neq 0$, ce qui implique $f(x_0) = 0$ puisque l'anneau $\mathbb{R}$ est intègre.
- Réciproquement, si une fonction réelle f sur $[0,1]$ s'annule en au moins un point x_0 de $[0,1]$, c'est un diviseur de zéro dans A : il suffit en effet de considérer la fonction réelle g sur $[0,1]$ définie par $g(x) = 0$ si $x \neq x_0$ et $g(x_0) = 1$; cette fonction n'est pas identitquement nulle et on a $f(x)g(x) = 0$ pour tout $x \in [0,1]$, donc $f.g = 0$.

Finalement, nous venons de prouver que les diviseurs de zéro dans l'anneau des fonctions réelles sur $[0,1]$ sont les fonctions s'annulant en au moins un point.

Remarque : les fonctions réelles sur $[0,1]$ *ne s'annulant nulle part sont exactement les éléments inversibles de l'anneau* A. *On a ainsi pour toute fonction réelle* f *sur* $[0,1]$ *l'alternative suivante : soit* f *est inversible dans* A, *soit* f *est un diviseur de zéro dans* A.

Problème 3. — 1. C'est une question de cours. Ayant rappelé que le contenu $c(\mathrm{P})$ d'un polynôme $\mathrm{P} \in \mathbb{Z}[x]$ est le pgcd de ses coefficients, les éléments irréductibles de l'anneau $\mathbb{Z}[x]$ sont

– les éléments irréductibles de $\mathbb{Z}$, c'est-à-dire les nombres premiers et leurs opposés ;
– les polynômes $\mathrm{P} \in \mathbb{Z}[x]$ irréductibles dans $\mathbb{Q}[x]$ et de contenu $c(\mathrm{P})$ égal à 1.

2. On rappelle que l'ensemble $\mathbb{Z}[x]^\times$ des éléments inversibles de l'anneau $\mathbb{Z}[x]$ est égal à $\{-1,1\}$.

L'idéal de $\mathbb{Z}[x]$ engendré par 2 et x n'est pas principal. Démonstration par l'absurde : supposons qu'il existe un polynôme $f \in \mathbb{Z}[x]$ engendrant l'idéal $(2,x)$; on a alors $2 = fg$ et $x = fh$ avec $g,h \in \mathbb{Z}[x]$. Comme 2 et x sont des éléments irréductibles de $\mathbb{Z}[x]$, la première condition implique $f \in \mathbb{Z}[x]^\times$ ou $f \in 2\mathbb{Z}[x]^\times$, donc $f = \pm 1$ ou $f = \pm 2$; la seconde condition implique $f \in \mathbb{Z}[x]^\times$ ou $f \in x\mathbb{Z}[x]^\times$, donc $f = \pm 1$ ou $f = \pm x$. On obtient ainsi $f = \pm 1$. La contradiction vient du fait que f doit également appartenir à l'idéal $(2,x)$: s'il existait des polynômes $a,b \in \mathbb{Z}[x]$ tels que $\pm 1 = 2a + xb$, on obtiendrait $\pm 1 = 2a(0)$ en faisant $x = 0$ et, comme $a(0) \in \mathbb{Z}$, ceci est absurde.

3. Écrivons la racine α sous la forme $\alpha = \frac{a}{b}$ avec $a,b \in \mathbb{Z}$, $b \neq 0$ et $\mathrm{pgcd}(a,b) = 1$. On a par hyothèse

$$0 = f(\alpha) = \frac{a^n + a_1 b a^{n-1} + \ldots + a_{n-1} b^{n-1} a + a_n b^n}{b^n}$$

en réduisant au même dénominateur b^n, donc

$$-a^n = b a_1 a^{n-1} + \ldots + a_{n-1} b^{n-1} a + a_n b^n.$$

Comme b divise le membre de droite, $b | a^n$ et donc $b = \pm 1$ puisque a et b sont premiers entre eux ; on obtient ainsi $\alpha = \pm a \in \mathbb{Z}$.

4. (a) Oui, appliquer le critère d'Eisenstein avec le nombre premier 3.
(b) Non, on vérifie que 2 est une racine de h et que $h = (x-2)(x^2 - 9x + 20)$.

5. (a) L'application $j : \mathbb{Q}[x,y] \to \mathbb{Q},\ f \mapsto f(0,0)$ est un homomorphisme d'anneau surjectif et de noyau I. Il en découle que j induit un isomorphisme entre l'anneau quotient $\mathbb{Q}[x,y]/\mathrm{I}$ et l'anneau $\mathbb{Q}$. Comme $\mathbb{Q}$ est un corps, il en est de même de l'anneau $\mathbb{Q}[x,y]/\mathrm{I}$ et I est donc un idéal maximal de $\mathbb{Q}[x,y]$.

(b) L'idéal I est égal à (x,y) et n'est pas principal.
L'inclusion $(x,y) \subset \mathrm{I}$ est évidente ; pour obtenir l'inclusion réciproque, il suffit d'obsercer que tout polynôme $f \in \mathbb{Q}[x,y]$ s'écrit sous la forme $f = f(0,0) + xg + yh$ avec $g,h \in \mathbb{Q}[x,y]$.
La démonstration du fait que l'idéal (x,y) n'est pas principal est analogue à celle de la question 2 en utilisant le fait que x et y sont des éléments irréductibles de $\mathbb{Q}[x,y]$ ainsi que l'identité $\mathbb{Q}[x,y]^\times = \mathbb{Q}^\times$.

(c) Tout anneau euclidien est principal ; comme l'idéal (x,y) n'est pas principal, l'anneau $\mathbb{Q}[x,y]$ n'est pas principal et donc, *a fortiori*, n'est pas euclidien.
Si A est un anneau factoriel, l'anneau $\mathrm{A}[x]$ est factoriel (théorème de Gauss). Comme l'anneau $\mathbb{Q}[x]$ est factoriel car euclidien, l'anneau $\mathbb{Q}[x,y] = (\mathbb{Q}[x])[y]$ est factoriel.

Problème 4. — 1. On a $a = (1,2,3,4)(5,6,7,8)$ et $b = (1,5,3,7)(2,6,4,8)$. En particulier, $a^4 = b^4 = 1$.

2. On a

$$ab = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 7 & 8 & 5 & 4 & 1 & 2 & 3 \end{pmatrix} = (1,6)(2,7)(3,8)(4,5),$$

$$a^2 = (1,2,3,4)^2(5,6,7,8)^2 = (1,3)(2,4)(5,7)(6,8) \quad \text{et} \quad b^2 = (1,3)(5,7)(2,4)(6,8).$$

Observons que l'on a $a^2 = b^2$ et $(ab)^2 = 1$.

3. L'application $\varphi : \langle a \rangle \times \langle b \rangle \to \mathrm{S}_8,\ (s,t) \mapsto st$ est un homomorphisme de groupes si et seulement si, pour tous entiers naturels n, n', m, m',

$$\varphi((a^n, b^m).(a^{n'}, b^{m'})) = \varphi(a^n, b^m)\varphi(a^{n'}, b^{m'}),$$

c'est-à-dire

$$a^{n+n'}b^{m+m'} = a^n b^m a^{n'} b^{m'}.$$

On voit donc que φ est un homomorphisme de groupes si et seulement si a et b commutent.

Tel est effectivement le cas : en effet, vu les identités $b^4 = 1$, $a^2 = b^2$ et $(ab)^2 = 1$ établies précédemment, on obtient

$$aabb = a^2b^2 = b^4 = 1 \quad \text{et} \quad abab = 1,$$

donc

$$ab = a^{-1}b^{-1} = ba.$$

Nous avons ainsi prouvé que l'application φ est un homomorphisme de groupes. Son image est le sous-groupe de S_8 engendré par a et b, c'est-à-dire H.

4. Le noyau de φ est composé des couples (a^n, b^m) tels que $a^n b^m = 1$. Comme les permutations a et b sont d'ordre 4, il suffit de considérer m et n dans $\{0,1,2,3\}$.

On connaît déjà l'identité $a^2b^2 = 1$ (question 2) ; si $m \geq 2$ et $n \geq 2$, alors $a^n b^m = a^{n-2}b^{m-2}$ et il suffit donc de trouver tous les couples (a^n, b^m) tels que $a^n b^m = 1$ avec $n, m \in \{0,1,2,3\}$ et $n \leq 1$ ou $m \leq 1$.

Le cas des couples (n,m) avec $1 \leq n \leq 3$ et $m \in \{0,1\}$ se traite facilement :
– aucun des éléments a, a^2, a^3 n'est égal à 1 puisque a est d'ordre 4 ;
– par ailleurs, $ab \neq 1$ (question 2) et $a \neq b$, donc $a^3 b \neq a^4 = 1$;
– enfin, $a^2 \neq b$ puisque a^2 est d'ordre 2 tandis que b est d'ordre 4, donc $a^2 b \neq a^4 = 1$.

Par un raisonnement analogue, on vérifie qu'aucun des éléments $a^n b^m$ avec $n \in \{0,1\}$ et $1 \leq m \leq 3$ n'est égal à 1.

Finalement, pour tous $n, m \in \{0,1,2,3\}$ avec $n \leq 1$ ou $m \leq 1$,

$$a^n b^m = 1 \Longleftrightarrow n = m = 0$$

et donc

$$\mathrm{Ker}(\varphi) = \{(1,1), (a^2, b^2)\}.$$

5. L'homomorphisme φ induit un isomorphisme entre le groupe quotient $\langle a \rangle \times \langle b \rangle / \mathrm{Ker}(\varphi)$ et H. On a donc

$$|\mathrm{H}| = \frac{|\langle a \rangle \times \langle b \rangle|}{|\mathrm{Ker}(\varphi)|} = \frac{|\langle a \rangle| \times |\langle b \rangle|}{|\mathrm{Ker}(\varphi)|} = \frac{16}{2} = 8.$$

Remarque : on peut répondre plus rapidement aux questions 4 et 5 : $|\mathrm{H}|$ *divise* $|\langle a \rangle \times \langle b \rangle| = 16$*, donc* $|\mathrm{H}| \in \{1,2,4,8,16\}$ *; comme* H *contient le sous-groupe cyclique* $\langle a \rangle$ *d'ordre* 4, $|\mathrm{H}| \geq 4$ *; ayant vérifié que l'élément* b *de* H *n'appartient pas au sous-groupe* $\langle a \rangle$*, on obtient ensuite* $|\mathrm{H}| > 4$*, donc* $|\mathrm{H}| = 8$ *ou* $|\mathrm{H}| = 16$ *; finalement, comme* $a^2b^2 = 1$*, l'homomorphisme* φ *n'est pas injectif, donc* $|\mathrm{H}| < 16$*. Nous obtenons ainsi* $|\mathrm{H}| = 8$ *et* $|\mathrm{Ker}(\varphi)| = \frac{16}{|\mathrm{H}|} = 2$*, d'où* $\mathrm{Ker}(\varphi) = \{(1,1), (a^2, b^2)\}$.

Problème 5. — 1. Pour toute orbite O de G dans X, $|\mathrm{O}|$ divise $|\mathrm{G}|$ et donc, comme $|\mathrm{G}|$ est une puissance de p,

$$|\mathrm{O}| = 1 \quad \text{ou} \quad |\mathrm{O}| \equiv 0 \pmod{p}.$$

Si l'on désigne par $\mathscr{O}$ l'ensemble des orbites de G dans X, l'équation aux classes s'écrit sous la forme

$$|\mathrm{X}| = \sum_{\mathrm{O} \in \mathscr{O}} |\mathrm{O}|.$$

Par hypothèse, le membre de gauche $|\mathrm{X}|$ n'est pas divisible par p ; le membre de droite ne l'est donc pas non plus et il existe par conséquent au moins une orbite O telle que $|\mathrm{O}| = 1$. Cette orbite est réduite à un point x de X tel que $gx = x$ pour tout $g \in \mathrm{G}$, ce qui prouve l'existence d'un point fixe de G dans X.

2. (a) Le choix d'une base de V fournit un isomorphisme entre V et le $\mathbb{F}_p$-espace vectoriel standard $\mathbb{F}_p^n$, donc V est un ensemble fini de cardinal p^n.

Tout automorphisme $\mathbb{F}_p$-linéaire de V préserve l'origine de V et donc stabilise le sous-ensemble $\mathrm{V} - \{0\}$ de V. En particulier, l'action naturelle d'un sous-groupe G de $\mathrm{GL}(\mathrm{V})$ sur V induit une opération de G sur $\mathrm{V} - \{0\}$. Si $|\mathrm{G}|$ est une puissance de p, on peut alors appliquer la question précédente avec l'ensemble $\mathrm{X} = \mathrm{V} - \{0\}$ de cardinal $|\mathrm{V} - \{0\}| = p^n - 1$ premier à p. On en déduit ainsi l'existence d'un vecteur non nul $v \in \mathrm{V}$ tel que $gv = v$ pour tout $g \in \mathrm{G}$.

(b) Pour tout élément g de G, $gv_1 = v_1$ et donc sa matrice dans la base b est de la forme

$$\left(\begin{array}{c|ccc} 1 & * & \dots & * \\ \hline 0 & & & \\ \vdots & & \mathrm{M}'(g) & \\ 0 & & & \end{array}\right)$$

avec $\mathrm{M}'(g) \in \mathrm{M}_{n-1}(\mathbb{F}_p)$. Quels que soient les éléments $g, h \in \mathrm{G}$,

$$\mathrm{Mat}_b(gh) = \mathrm{Mat}_b(g)\mathrm{Mat}_b(h) = \left(\begin{array}{c|ccc} 1 & * & \dots & * \\ \hline 0 & & & \\ \vdots & & \mathrm{M}'(g) & \\ 0 & & & \end{array}\right)\left(\begin{array}{c|ccc} 1 & * & \dots & * \\ \hline 0 & & & \\ \vdots & & \mathrm{M}'(h) & \\ 0 & & & \end{array}\right)$$

$$= \left(\begin{array}{c|ccc} 1 & * & \dots & * \\ \hline 0 & & & \\ \vdots & & \mathrm{M}'(g)\mathrm{M}'(h) & \\ 0 & & & \end{array}\right)$$

donc $\mathrm{M}'(gh) = \mathrm{M}'(g)\mathrm{M}'(h)$. Comme $\mathrm{M}'(1) = \mathrm{I}_{n-1}$, on en déduit que toutes les matrices $\mathrm{M}'(g)$, $g \in \mathrm{G}$, sont inversibles.

Pour tout $g \in \mathrm{G}$, la matrice $\mathrm{M}'(g)$ définit un unique automorphisme $\rho(g)$ de $\mathrm{V}' = \mathrm{Vect}(v_2, \dots, v_n)$ tel que

$$\mathrm{Mat}_{b'}(\rho(g)) = \mathrm{M}'(g).$$

Quels que soient $g, h \in \mathrm{G}$,

$$\mathrm{Mat}_{b'}(\rho(gh)) = \mathrm{M}'(gh) = \mathrm{M}'(g)\mathrm{M}'(h) = \mathrm{Mat}_{b'}(\rho(g))\mathrm{Mat}_{b'}(\rho(h))$$

donc $\rho(gh) = \rho(g)\rho(h)$ et ainsi l'application $\rho : \mathrm{G} \to \mathrm{GL}(\mathrm{V}')$ que l'on a définie est un homomorphisme de groupes.

(c) Soit donc G un sous-groupe de $\mathrm{GL}(\mathrm{V})$ d'ordre p^r avec $r \geq 0$; en raisonnant par récurrence sur la dimension de V, nous allons démontrer qu'il existe une base b de V telle que, pour tout $g \in \mathrm{G}$, la matrice $\mathrm{Mat}_b(g)$ soit triangulaire supérieure avec tous ses coefficients diagonaux égaux à 1.

- Le résultat est acquis si $\dim(\mathrm{V}) = 1$. Il existe en effet un vecteur non nul v de V tel que $gv = v$ pour tout $g \in \mathrm{G}$ d'après la question 2 (a) ; $b = \{v\}$ est une base de V et $\mathrm{Mat}_b(g) = (1) = \mathrm{I}_1$ pour tout $g \in \mathrm{G}$.
- Soit $n \geq 2$ et supposons le résultat acquis pour un espace vectoriel de dimension $n-1$. D'après la question 2 (a), il existe une base $b = \{v_1, \dots, v_n\}$ de V telle que $gv_1 = v_1$ pour tout $g \in \mathrm{G}$. Posant $\mathrm{V}' = \mathrm{Vect}(v_2, \dots, v_n)$ et $b' = \{v_2, \dots, v_n\}$, il existe en vertu de la question précédente un homomorphisme de groupes $\rho : \mathrm{G} \to \mathrm{GL}(\mathrm{V}')$ tel que, pour tout $g \in \mathrm{G}$,

$$\mathrm{Mat}_b(g) = \left(\begin{array}{c|ccc} 1 & * & \dots & * \\ \hline 0 & & & \\ \vdots & & \mathrm{Mat}_{b'}(\rho(g)) & \\ 0 & & & \end{array}\right).$$

L'image $\mathrm{G}' = \rho(\mathrm{G})$ de ρ est un sous-groupe de $\mathrm{GL}(\mathrm{V}')$ isomorphe à $\mathrm{G}/\mathrm{Ker}(\rho)$; son ordre divise par conséquent celui de G et donc $|\mathrm{G}'|$ est une puissance de p. Comme $\dim(\mathrm{V}') = n-1$, nous pouvons appliquer l'hypothèse de récurrence : il existe une base β' de V′ telle que la matrice $\mathrm{Mat}_{\beta'}(\rho(g))$ soit triangulaire supérieure avec tous ses coefficients diagonaux égaux à 1.
Dans ces conditions, $\beta = \{v_1\} \cup \beta'$ est une base de V et, pour tout $g \in \mathrm{G}$, la matrice

$$\mathrm{Mat}_\beta(g) = \left(\begin{array}{c|ccc} 1 & * & \dots & * \\ \hline 0 & & & \\ \vdots & & \mathrm{Mat}_{\beta'}(\rho(g)) & \\ 0 & & & \end{array}\right) = \left(\begin{array}{c|ccc} 1 & * & \dots & * \\ \hline 0 & 1 & * & * \\ \vdots & 0 & \ddots & * \\ 0 & 0 & 0 & 1 \end{array}\right)$$

est triangulaire supérieure avec tous ses coefficients diagonaux égaux à 1.