Examen du 15 janvier 2010

Seules les notes de cours et de TD sont autorisées. Il est interdit de communiquer par un quelconque moyen. Les exercices sont indépendants.

Exercice 1 – Classification des groupes d'ordre 18. Soit G un groupe d'ordre 18.

a) Soit H un groupe **abélien** dont tous les éléments (sauf l'élément neutre) sont d'ordre p (où p est un nombre premier). Montrer que la loi externe

$$\cdot : \begin{cases} \mathbb{F}_p \times H \longrightarrow H \\ (\overline{n}, x) \longmapsto nx = \underbrace{x + \cdots + x}_{n \text{ termes}} \end{cases}$$

est bien définie et munit H d'une structure de $\mathbb{F}_p$-espace vectoriel ($\overline{n}$ désigne la classe de $n \in \mathbb{Z}$ modulo p).

b) Montrer qu'il existe deux classes d'isomorphisme de groupes d'ordre 9.

c) Déterminer $\mathrm{Aut}(\mathbb{Z}/9\mathbb{Z})$ et en particulier les éléments d'ordre 2 de ce groupe.

d) Montrer que $\mathrm{Aut}((\mathbb{Z}/3\mathbb{Z})^2) = \mathrm{GL}_2(\mathbb{F}_3)$ (on pourra montrer que tout automorphisme de $(\mathbb{Z}/3\mathbb{Z})^2$ est en fait $\mathbb{F}_3$-linéaire). En déduire les classes de conjugaison d'éléments d'ordre 2 de ce groupe.

e) Déterminer le nombre de 3-Sylow de G.

f) En déduire que G est extension de $\mathbb{Z}/2\mathbb{Z}$ par l'un de ses 3-Sylow.

g) Combien existe-t-il de classes d'isomorphisme de groupes d'ordre 18 ?

Exercice 2 – Élément premier. On considère l'anneau des entiers de Gauss :

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C}, \qquad a, b \in \mathbb{Z}\}$$

a) Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.

b) Décrire un isomorphisme entre $\mathbb{Z}[i]$ et $\mathbb{Z}[X]/\langle X^2 + 1\rangle$.

c) Soit $n \in \mathbb{Z}$. On suppose que n est un élément premier de $\mathbb{Z}[i]$. Montrer que n est un élément premier dans $\mathbb{Z}$.

d) Soit $p \in \mathbb{Z}$ un nombre premier. Montrer que p est premier dans $\mathbb{Z}[i]$, si et seulement si, l'anneau $\mathbb{F}_p[X]/\langle X^2 + 1\rangle$ est intègre.

e) Montrer que $\mathbb{F}_p[X]/\langle X^2 + 1\rangle$ est intègre, si et seulement si, $X^2 + 1$ est irréductible sur $\mathbb{F}_p$, si et seulement si, -1 n'est pas un carré modulo p, si et seulement si, $p = 3\,[4]$.

f) Factoriser $4 + 2i$ en irréductible dans $\mathbb{Z}[i]$ (on pourra penser à utiliser l'application N : $a + bi \in \mathbb{Z}[i] \to a^2 + b^2 \in \mathbb{N}$).

Définition – G-ensemble. Soit G un groupe et X un ensemble sur lequel G agit. On dit que X est alors un *G-ensemble*.

Si X et Y sont deux G-ensembles, un *morphisme de G-ensembles* (ou *G-morphisme*) de X dans Y est une application $f : X \to Y$ telle que pour tout $g \in G$ et $x \in X$, on ait $f(gx) = gf(x)$.

On dit que deux G-ensembles X et Y sont isomorphes, s'il existe $f : X \to Y$ et $f' : Y \to X$ deux G-morphismes vérifiant $ff' = \mathrm{id}_Y$ et $f'f = \mathrm{id}_X$. Un tel f est appelé un isomorphisme de G-ensembles.

On note $[X]$ la classe d'isomorphisme du G-ensemble X.

Un G-ensemble X est dit *transitif* si l'action de G sur X est transitive.

Exercice 3 – Anneau de Burnside. Soit G un groupe **fini**. On note $S(G)$ l'ensemble des classes d'isomorphisme de G-ensembles **finis**.

Partie 1 G-ensemble transitif

a) Montrer que tout G-ensemble transitif est isomorphe à un G-ensemble de la forme G/H où H est un sous-groupe de G.

b) Soient H, H' deux sous-groupes de G. Donner une condition nécessaire et suffisante pour qu'il existe un morphisme (resp. un isomorphisme) de G-ensembles de G/H dans G/H' ?

c) En déduire que les classes d'isomorphisme de G-ensembles transitifs sont en bijection avec les classes de conjugaison de sous-groupes de G.

d) Montrer que tout G-ensemble fini est la réunion disjointe finie de G-ensembles transitifs.

e) Soit $f : X \to Y$ un G-morphisme où Y est un G-ensemble transitif et $X \neq \emptyset$. Montrer que f est surjectif.

f) Soit H un sous-groupe de G et X un G-ensemble. Décrire une bijection entre les G-orbites de $G/H \times X$ et les H-orbites de X (voir la question **b** de la partie 3 pour la construction de la structure de G-ensemble sur le produit $G/H \times X$). Soit $x \in X$. Quel est le stabilisateur de $(H, x) \in G/H \times X$?

Partie 2 Un critère d'isomorphie

Soit X et Y deux G-ensembles finis.

a) Montrer que si X et Y sont des G-ensembles isomorphes alors $|X^H| = |Y^H|$ pour tout H sous-groupe de G.

Dans le reste de cette partie, on suppose que $|X^H| = |Y^H|$ pour tout H sous-groupe de G. L'objectif est de montrer que X et Y sont G-isomorphes.

b) Montrer que si $X = \emptyset$ alors Y aussi.

c) Dans la suite, on suppose X et Y non vides. Montrer l'existence d'un sous-groupe H de G maximal pour la propriété $X^H \neq \emptyset$. Montrer que $Y^H \neq \emptyset$.

d) On considère $x \in X^H$ et $y \in Y^H$. Déterminer le stabilisateur de x et de y.

e) En déduire que l'orbite $\mathcal{O}(x)$ de x sous G et l'orbite $\mathcal{O}(y)$ de y sous G sont G-isomorphes.

f) Montrer que $X' = X \setminus \mathcal{O}(x)$ et $Y' = Y \setminus \mathcal{O}(y)$ sont des G-ensembles et vérifient $|X'^H| = |Y'^H|$ pour tout $H \leqslant G$.

g) Conclure.

Partie 3 Lois sur $S(G)$

a) Soient X et Y deux G-ensembles. Munir $X \sqcup Y$ d'une structure de G-ensemble. Montrer que la classe d'isomorphisme du G-ensemble $X \sqcup Y$ ne dépend que des classes d'isomorphisme de X et de Y.

b) Soient X et Y deux G-ensembles. Munir $X \times Y$ d'une structure de G-ensemble. Montrer que la classe d'isomorphisme du G-ensemble $X \times Y$ ne dépend que des classes d'isomorphisme de X et de Y.

c) En déduire que les deux lois internes suivantes sur $S(G)$ sont bien définies et munissent toutes les deux $S(G)$ d'une structure de monoïde commutatif (on explicitera en particulier les éléments neutres pour $+$ et $\times$)

$$+ : \begin{cases} S(G) \times S(G) \longrightarrow S(G) \\ ([X],[Y]) \longmapsto [X]+[Y] = [X \sqcup Y] \end{cases} \quad \text{et} \quad \cdot : \begin{cases} S(G) \times S(G) \longrightarrow S(G) \\ ([X],[Y]) \longmapsto [X][Y] = [X \times Y] \end{cases}$$

d) Montrer que $\cdot$ est distributive par rapport à $+$.

e) Montrer que $(S(G),+)$ est isomorphe à $\mathbb{N}^r$ où r est le nombre de classes de conjugaison de sous-groupes de G.

f) En déduire que tout élément de $S(G)$ est régulier pour $+$: pour tout $x \in S(G)$, si $x+y = x+z$ alors $y = z$.

Partie 4 L'anneau de Burnside $B(G)$

a) On considère sur l'ensemble $S(G) \times S(G)$ la relation $\mathcal{R}$ définie par

$$(x,y)\ \mathcal{R}\ (x',y') \quad \Longleftrightarrow \quad x+y' = x'+y\,.$$

Montrer que $\mathcal{R}$ est une relation d'équivalence sur $S(G) \times S(G)$. On note l'ensemble quotient $B(G) = (S(G) \times S(G))/\mathcal{R}$ et $\pi : S(G) \times S(G) \to B(G)$ la surjection canonique

b) Montrer que la loi $+$ sur $S(G) \times S(G)$ donnée par $(x,y)+(x',y') = (x+x', y+y')$ passe au quotient et munit $B(G)$ d'une structure de groupe abélien.

c) Montrer que la loi $\cdot$ sur $S(G) \times S(G)$ donnée par $(x,y)(x',y') = (xx'+yy', xy'+yx')$ passe au quotient et munit $B(G)$ d'une structure de monoïde abélien.

d) Montrer que $B(G)$ muni de ces deux lois (qu'on note encore $+$ et $\cdot$) est un anneau commutatif unitaire et que l'application

$$c : \begin{cases} S(G) \longrightarrow B(G) \\ x \longmapsto \pi(x,0) \end{cases}$$

est un morphisme injectif de monoïdes pour $+$ et aussi pour $\cdot$.

e) Montrer que $(B(G),+)$ est isomorphe à $\mathbb{Z}^r$ où r est le nombre de classes de conjugaison de sous-groupes de G : en notant $(G_i)_{1 \leqslant i \leqslant r}$ une famille de représentants des classes de conjugaison de sous-groupes de G, montrer que tout élément de $B(G)$ s'écrit de manière unique sous la forme

$$\sum_{i=1}^{r} a_i [G/G_i] \qquad \text{avec} \quad a_i \in \mathbb{Z}.$$

f) Soit A un anneau commutatif unitaire et $\varphi : S(G) \to A$ une application qui est à la fois un morphisme de monoïdes pour $+$ et pour $\cdot$. Montrer que φ se prolonge de manière unique en un morphisme d'anneaux de $B(G) \to A$: montrer qu'il existe un unique morphisme d'anneau $\widetilde{\varphi} : B(G) \to A$ vérifiant $\widetilde{\varphi} \circ c = \varphi$.

g) Soit $H \leqslant G$. Montrer qu'il existe un unique morphisme d'anneaux $\psi_H : B(G) \to \mathbb{Z}$ vérifiant

$$\psi_H([X]) = |X^H| = |\{x \in X, \quad \forall\, h \in H,\ hx = x\}|$$

pour tout $[X] \in S(G)$.

h) Soient H, K deux sous-groupes de G. Montrer que $\psi_H = \psi_K$ si et seulement si H et K sont conjugués.

i) Soit ψ un morphisme d'anneaux de $B(G)$ dans $\mathbb{Z}$. Montrer qu'il existe H un sous-groupe de G tel que $\psi = \psi_H$.

j) Déterminer
$$\bigcap_{H \leqslant G} \ker \psi_H\,.$$

k) On note $(G_i)_{1 \leqslant i \leqslant r}$ une famille de représentants des classes de conjugaison de sous-groupes de G. Montrer que l'application

$$\varphi\colon \begin{cases} B(G) \longrightarrow \mathbb{Z}^r \\ \quad x \quad \longmapsto (\psi_{G_1}(x), \ldots, \psi_{G_r}(x)) \end{cases}$$

est injective.

l) En déduire que $B(G)$ ne contient pas d'élément nilpotent non nul.

Partie 5 Exemples

Dans cette partie, p désigne un nombre premier.

a) Quel est l'anneau de Burnside de $G = \{1_G\}$?

Dans toute la suite, on suppose que $G = \mathbb{Z}/p\mathbb{Z}$.

b) En utilisant l'écriture de la question **e** de la partie 4, donner le produit de deux éléments de $B(G)$.

c) L'anneau $B(G)$ est-il intègre ? un corps ?

d) Déterminer les éléments inversibles de $B(G)$. Quelle est la structure du groupe $B(G)^\times$?

e) Déterminer les idéaux premiers et maximaux de $B(G)$? Quels sont les quotients correspondants ?

f) Déterminer l'image de φ (question **k** de la partie 4).