# UNIVERSITÉ LILLE 1

Enseignants: **P. DÈBES, M. EMSALEM, Y. HANTOUT**
Filière: **Maîtrise de mathématiques**
Matière: **Algèbre**
Année universitaire: **2002/2003**
Devoir $n^o 1$: à rendre le

---

**1. Groupes opérant sur un ensemble.**

Soient $G$ un groupe et $E$ un ensemble. On appelle *action de $G$ sur $E$* la donnée d'un homomorphisme de groupes

$$\begin{cases} G \to S(E) \\ g \to g. \end{cases}$$

de $G$ dans le groupe des permutations de $E$. On dit que $G$ opère sur $E$. Etant donnée une action de $G$ sur $E$, on note, pour tout $x \in E$, $O_x$ l'ensemble des éléments $g.x$ où $g$ décrit $G$ et $\Gamma_x$ l'ensemble des éléments $g \in G$ tels que $g.x = x$. $O_x$ et $\Gamma_x$ sont appelés respectivement l'*orbite* et le *fixateur* de $x$ sous l'action de $G$.

(a) Montrer que si $G$ est fini, on a $|O_x| \times |\Gamma_x| = |G|$ pour tout $x \in E$.

(b) Vérifier que la relation sur $E$ définie par $x \equiv y$ si $\exists g \in G | y = g.x$ est une relation d'équivalence sur $E$. En déduire la "formule des classes": si $G$ et $E$ sont finis, on a

$$|E| = \sum_x \frac{|G|}{|\Gamma_x|}$$

où $x$ parcourt un ensemble de représentants des classes d'équivalence de $\equiv$.

**2. $p$-groupes.**

Soit $G$ un $p$-groupe, i.e., un groupe fini d'ordre $|G| = p^r$ ($p$ premier).

(a) Montrer que si $G$ opère sur un ensemble $E$ de cardinal $|E| = q$ où $p \wedge q = 1$, alors il existe $x \in E$ tel que $g.x = x$ pour tout $g \in G$.

(b) On note $Z(G)$ le centre de $G$, i.e., l'ensemble des éléments $g \in G$ qui commutent à tous les autres. Montrer que $Z(G)$ est un sous-groupe non trivial de $G$. (Indic: faire opérer $G$ sur lui même par conjugaison, i.e., $g.x = gxg^{-1}$).

(c) En utilisant (b), montrer qu'un groupe d'ordre $p^2$ est abélien. (Indic: raisonner par l'absurde et commencer par montrer que si $\alpha \notin Z(G)$, alors les ensembles $Z(G), \alpha Z(G), \ldots, \alpha^{p-1} Z(G)$ constituent une partition de $G$).

**3. Polynômes cyclotomiques.**

Pour tout entier $n \geq 1$, on note $\mu_n$ le sous-groupe de $\mathbb{C}$ des racines $n$-ièmes de 1 et $g_n$ l'ensemble des générateurs de $\mu_n$ (les éléments de $g_n$ sont aussi appelés les racines primitives $n$-ièmes de 1). Le $n$-ième polynôme cyclotomique $\Phi_n$ est alors défini par

$$\Phi_n(X) = \prod_{\zeta \in g_n} (X - \zeta)$$

(a) Montrer que pour tout $n \geq 1$, on a $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

(b) Montrer que, pour tout $n \geq 1$, on a
(i) $\Phi_n(X) \in \mathbb{Z}[X]$
(ii) Si $d|n$, alors $X^d - 1$ divise $X^n - 1$ dans $\mathbb{Z}[X]$
(iii) Si $d|n$ et $d \neq n$, alors $\Phi_n(X)$ divise $\frac{X^n-1}{X^d-1}$ dans $\mathbb{Z}[X]$

(c) Montrer que pour tout $n > 1$, on a $|\Phi_n(x)| > x - 1$ pour tout nombre réel $x \geq 2$.

**4. Théorème de Wedderburn.**

Soit $K$ un corps fini. Le but de cette partie est de montrer que le groupe multiplicatif $(K^\times, \times)$ est commutatif. Pour tout $a \in K$, on note $C_a$ le commutant de $a$, i.e., l'ensemble des éléments $x \in K$ tels que $xy = yx$ et $C$ l'ensemble des éléments $x \in K$ qui commutent à tous les éléments de $K$.

(a) On note $q = |C|$. Montrer qu'on a alors $|K| = q^n$ et $|C_a| = q^{d_a}$ avec $n, d_a \in \mathbb{N}$.

(b) En utilisant la partie 1., montrer qu'on a une égalité de la forme

$$q^n - 1 = q - 1 + \sum_d \frac{q^n - 1}{q^d - 1}$$

où $d$ décrit un ensemble de diviseurs de $n$ distincts de $n$. (Indic: faire opérer $K^\times$ sur lui même par conjugaison comme dans la partie 2).

(c) Conclure grâce à la partie 3. que $n = 1$, i.e., que $(K^\times, \times)$ est commutatif.

# UNIVERSITÉ LILLE 1

Enseignants: **P. DÈBES, M. EMSALEM, Y. HANTOUT**
Filière: **Maîtrise de mathématiques**
Matière: **Algèbre**
Année universitaire: **2002/2003**
Devoir $n^o 2$: à rendre le

---

**1. Second théorème de Sylow.**

Soit $G$ un groupe fini de cardinal $n = p^t m$ où $p$ est un nombre premier ne divisant pas $m$. On note $\mathcal{E}$ l'ensemble des $p$-sous-groupes de Sylow de $G$. On admettra le premier théorème de Sylow, démontré en cours, c'est-à-dire, que $\mathcal{E} \neq \emptyset$.

(a) Montrer que la conjugaison par les éléments de $G$ induit une action de $G$ sur $\mathcal{E}$.

On fixe $S \in \mathcal{E}$ et on désigne par $\Omega$ l'orbite de $S$ sous l'action de $G$ par conjugaison sur $\mathcal{E}$.

(b) Montrer que $\mathrm{card}(\Omega)$ divise l'indice $[G : S]$.

Soit $H$ un $p$-sous-groupe de $G$.

(c) Montrer qu'il existe $S' \in \Omega$ tel que $H \subset \mathrm{Norm}_G(S')$. (Indication: faire opérer $H$ par conjugaison sur $\Omega$ et appliquer la formule des classes).

(d) Montrer que si comme ci-dessus, $S'$ est un $p$-sous-groupe de Sylow normalisant $H$, alors $H/(H \cap S')$ est un sous-groupe de $\mathrm{Norm}_G(S')/S'$.

(e) En raisonnant sur les cardinaux, en déduire que $H \subset S'$.

(f) Etablir les conclusions du second théorème de Sylow:

- tout $p$-sous groupe $H$ d'un groupe $G$ est contenu dans un $p$-sous-groupe de Sylow,

- les $p$-sous-groupes de Sylow d'un groupe $G$ sont conjugués dans $G$. (Indication: appliquer ce qui précède au cas où $H$ est lui-même un $p$-sous-groupe de Sylow).

- le nombre de $p$-sous-groupes de Sylow divise $m$. (Indication: utiliser (b) dans le cas où $H$ est un $p$-sous-groupe de Sylow).

- le nombre de $p$-sous-groupes de Sylow est congru à 1 modulo $p$. (Indication: appliquer ce qui précède au cas où $H = S$ et appliquer la formule des classes).

# UNIVERSITÉ LILLE 1

Enseignants: **P. DÈBES, M. EMSALEM, Y. HANTOUT**
Filière: **Maîtrise de mathématiques**
Matière: **Algèbre**
Année universitaire: **2002/2003**
Date: **jeudi 28 novembre 2002 à 14h00**
Durée de l'épreuve: **4 heures**

---

**Ni calculatrices ni documents.**

**Le barème est donné à titre indicatif.**

**Chacune des trois parties devra être rédigée sur une copie différente.**

---

## PARTIE I

**Question de cours [2 pts]:** Donner la définition de "groupe résoluble". Montrer que si $H$ est un sous-groupe distingué d'un groupe $G$ tel que $H$ et $G/H$ soient résolubles, alors $G$ est résoluble.

**Exercice 1 [4 pts]:** Soient $G$ un groupe fini et $H$ un 2-sous-groupe de Sylow de $G$, d'ordre $2^n$. On suppose que $H$ est cyclique et on note $h$ un générateur.

On note $\rho : G \to \mathrm{Per}(G)$ l'action de $G$ sur lui-même par translation à gauche (c'est-à-dire, $\rho(g)(x) = gx$ $(g, x \in G)$).

(a) Soit $\rho(h) = \gamma_1 \cdots \gamma_r$ la décomposition en cycles à supports disjoints de $\rho(h)$. Montrer que $\gamma_i$ est un cycle de longueur $2^n$ $(i = 1, \ldots, r)$ et que $r = |G|/2^n$.

Soit $\varepsilon : \mathrm{Per}(G) \to \{-1, 1\}$ le morphisme "signature" ($\mathrm{Per}(G)$ désigne le groupe des permutations de $G$). On note $G'$ le noyau de $\varepsilon \circ \rho$.

(b) Montrer que $G'$ est un sous-groupe distingué de $G$ et que $G/G' \simeq \{-1, 1\}$.

(c) Montrer que $H' = G' \cap H$ est un 2-sous-groupe de Sylow de $G'$, d'ordre $2^{n-1}$, et qu'il est cyclique engendré par $h^2$.

(d) En effectuant une récurrence sur $n$, montrer que $G$ est résoluble.
(Indication: Pour le cas $n = 0$, on pourra utiliser le théorème de Feit-Thompson d'après lequel tout groupe d'ordre impair est résoluble).

(e) En déduire qu'un groupe d'ordre $2m$ où $m$ est impair est résoluble.

**Exercice 2 [1 pts]:** Montrer que le groupe alterné $A_5$ n'a pas de sous-groupe d'ordre 15.

## PARTIE II

**Exercice 3 [3,5 pts]:** Tous les groupes sont supposés finis. On dit qu'un sous-groupe $A$ d'un groupe $G$ est presque distingué dans $G$ s'il existe un sous-groupe distingué $N$ de $G$ tel que $AN = G$ et $A \cap N$ soit distingué dans $G$

(a) Vérifier que si $A$ est distingué dans $G$ alors $A$ est presque distingué dans $G$.

On dit qu'un groupe $G$ a la propriété (P) si pour tous sous-groupes $A$, $B$ de $G$ tels que $A$ soit un sous-groupe propre maximal de $B$, alors $A$ est presque distingué dans $B$.

(b) Montrer les propriétés suivantes:

(i) Si $G$ possède la propriété (P), alors tout sous-groupe $H < G$ possède (P) aussi.

(ii) Si $G$ possède la propriété (P), alors tout quotient de $G$ possède (P) aussi.

(iii) Si $G$ est simple et possède (P), alors $G$ est cyclique d'ordre premier (ou trivial).

(c) Montrer, par récurrence sur $\mathrm{card}(G)$, que si un groupe $G$ possède la propriété (P), alors $G$ est résoluble.

**Exercice 4 [3,5 pts]:** (a) Montrer que tout groupe d'ordre 12 est résoluble.
(Indication: on montrera que le nombre de 3-sous-groupes de Sylow est 1 ou 4, et dans le second cas, que le 2-sous-groupe de Sylow est distingué dans $G$).

(b) Décrire à isomorphisme près tous les groupes d'ordre 12.

(c) Soient $p$ et $q$ deux nombres premiers. Montrer que tout groupe d'ordre $p^2q$ est résoluble.
(Indication: on distinguera les cas $p = q$, $p > q$ et $p < q$; dans tous les cas, on montrera que, ou le $p$-sous-groupe de Sylow, ou le $q$-sous-groupe de Sylow est distingué dans $G$).

## PARTIE III

**Exercice 5 [4 pts]:** Pour tout entier $n \geq 1$, on note $\mu_m$ le sous-groupe de $\mathbb{C}^\times$ des racines $m$-ièmes de 1 et $g_m$ l'ensemble des générateurs de $\mu_m$ (les éléments de $g_m$ sont aussi appelés les racines primitives $m$-ièmes de 1). Le $m$-ième polynôme cyclotomique $\Phi_m$ est alors défini par

$$\Phi_m(X) = \prod_{\zeta \in g_m} (X - \zeta)$$

On rappelle que pour tout $m \geq 1$, on a $X^m - 1 = \prod_{d|m} \Phi_d(X)$.

(a) Montrer que, pour tout $m \geq 1$, on a

(i) $\Phi_m(X) \in \mathbb{Z}[X]$

(ii) Si $d|m$ et $d \neq m$, alors $(X^d - 1)\Phi_m(X)$ divise $X^m - 1$ dans $\mathbb{Z}[X]$.

(iii) Pour tout $m > 1$, on a $|\Phi_m(x)| > x - 1$ pour tout nombre réel $x \geq 2$.

(b) Soient $n \in \mathbb{Z}$ un entier et $p$ un diviseur premier de $\Phi_m(n)$. On note $\bar{n}$ la classe de $n$ modulo $p$.

(i) Montrer que $\bar{n}^m = 1$ dans $\mathbb{Z}/p\mathbb{Z}$.

(ii) Montrer que si $p$ ne divise pas $m$, alors $\bar{n}$ est d'ordre $m$ dans le groupe $(\mathbb{Z}/p\mathbb{Z})^\times, \times)$.

(iii) En déduire que $p \mid m$ ou que $p \equiv 1 \ [\mathrm{mod}\ m]$.

(c) Montrer que pour tout entier $m > 1$, il existe un infinité de nombres premiers congrus à 1 modulo $m$.

**Exercice 6 [2 pts]:** Soit $G$ un groupe fini. On rappelle que l'exposant de $G$, noté $\exp(G)$, est le ppcm des ordres des éléments du groupe $G$.

(a) Montrer que, pour tout nombre premier $p$, on a $p \mid \exp(G)$ si et seulement si $p \mid \mathrm{card}(G)$.

(b) Montrer que $\exp(G) = \mathrm{card}(G)$ si et seulement si tous les sous-groupes de Sylow de $G$ sont cycliques.

# UNIVERSITÉ LILLE 1

Enseignants: **P. DÈBES, M. EMSALEM, Y. HANTOUT**
Filière: **Maîtrise de mathématiques**
Matière: **Algèbre**
Année universitaire: **2002/2003**
Date: **lundi 27 janvier 2003 à 14h00**
Durée de l'épreuve: **4 heures**

---

**Ni calculatrices ni documents.**

**Le barème est donné à titre indicatif.**

**Chacune des trois parties devra être rédigée sur une copie différente.**

---

## PARTIE I

**Exercice 1 [8 pts]:** Soit $\alpha \in \mathbb{C}$ une racine du polynôme

$$P(X) = X^3 + X^2 - 2X - 1$$

On pose $K = \mathbb{Q}(\alpha)$.

(a) Quel est le degré de $K$ sur $\mathbb{Q}$?

(b) Vérifier que $\alpha^2 - 2$ est également racine de $P(X)$ et en déduire que l'extension $K/\mathbb{Q}$ est ienne de groupe de Galois cyclique.

(c) Montrer que $P(X)$ a 3 racines réelles dont une seule est positive.

On note $\sigma$ un générateur de $\mathrm{Gal}(K/\mathbb{Q})$ et on pose $\alpha_1 = \alpha$, $\alpha_2 = \sigma(\alpha_1)$, $\alpha_3 = \sigma(\alpha_2)$.
On note aussi $\theta_i$ un nombre complexe tel que $\theta_i^2 = \alpha_i$ $(i = 1, 2, 3)$ et on pose

$$L = \mathbb{Q}(\theta_1) \text{ et } M = \mathbb{Q}(\theta_1, \theta_2, \theta_3)$$

(d) Montrer qu'aucun des nombres complexes $\theta_1, \theta_2, \theta_3$ n'est dans $K$. En déduire $[L : \mathbb{Q}]$.

(e) Déterminer les conjugués de $\theta_1$ sur $\mathbb{Q}$ et en déduire que $M$ est la clôture galoisienne de $L$ sur $\mathbb{Q}$.

(f) En remarquant que $\alpha_1\alpha_2\alpha_3 = 1$, montrer que $M = \mathbb{Q}(\theta_1, \theta_2)$.

(g) Montrer que $\alpha_2/\alpha_1$ n'est pas un carré dans $K$. (Indication: on pourra raisonner par l'absurde, montrer qu'alors $\alpha_3/\alpha_2$ serait aussi un carré dans $K$ et utiliser (c)).

(h) Montrer que $\theta_2 \notin L$. (Indication: on pourra montrer que si $\theta_2 \in L$, alors $\theta_2/\theta_1 \in K$).

(i) En déduire $[M : \mathbb{Q}]$.

(j) Déterminer la structure du groupe de Galois $\mathrm{Gal}(M/K)$ et les corps intermédiaires entre $K$ et $M$.

(k) Déterminer les corps $F$ intermédiaires entre $\mathbb{Q}$ et $M$ tels que $[F : \mathbb{Q}] = 3$.

## PARTIE II

**Question de cours 1 [3 pts]:** Enoncer le théorème de structure des modules de type fini sur un anneau principal.

Application: déterminer tous les groupes abéliens finis de cardinal 392.

**Exercice 2 [3 pts]:** Soient $A$ un anneau intègre et $a \in A$ un élément non nul de $A$. On note $S$ la partie multiplicative $S = \{1, a, a^2, \ldots, a^n, \ldots\}$. Montrer que l'anneau de fractions $S^{-1}A$ est isomorphe à l'anneau quotient $A[X]/(aX - 1)$.

## PARTIE III

**Question de cours [3 pts]:** Enoncer le lemme d'Artin sur l'extension $L/L^G$ (où $G \subset \mathrm{Aut}(L)$) et le démontrer dans la situation simplifiée où le corps $L$ est de caractéristique 0 et l'extension $L/L^G$ est supposée de degré fini.

**Exercice 3 [3 pts]:** Soient $a > 0$ et $n > 0$ deux entiers avec $a$ non divisible par un carré. Le polynôme $X^n - a$ est alors irréductible dans $\mathbb{Q}[X]$ (par exemple d'après le critère d'Eisenstein). Soient $K/\mathbb{Q}$ une extension de degré fini $d$ et $\alpha \in \mathbb{C}$ une racine de $X^n - a$.

(a) Montrer que les conditions suivantes sont équivalentes:

(i) $X^n - a$ est irréductible dans $K[X]$

(ii) $[K(\alpha) : K] = [\mathbb{Q}(\alpha) : \mathbb{Q}]$

(iii) $[K(\alpha) : \mathbb{Q}(\alpha)] = [K : \mathbb{Q}]$

(b) Montrer que si $n$ et $d$ sont premiers entre eux, $X^n - a$ est irréductible dans $K[X]$.

(c) Montrer que $X^n - a$ est irréductible dans $\mathbb{Q}(i)[X]$.

# UNIVERSITÉ LILLE 1

Enseignants: **P. DÈBES, M. EMSALEM, Y. HANTOUT**
Filière: **Maîtrise de mathématiques**
Matière: **Algèbre**
Année universitaire: **2002/2003**
Date: **septembre 2003**
Durée de l'épreuve: **4 heures**

---

**Ni calculatrices ni documents.**
**Le barème est donné à titre indicatif.**

---

**Question de cours [2 pts]:** Soit $G$ un groupe fini agissant sur un ensemble fini $S$. Pour tout $s \in S$, on note $\mathcal{O}_s$ l'orbite de $s$ sous $G$ et $\Gamma_s$ le sous-groupe de $G$ des éléments $g \in G$ tels que $g \cdot s = s$. Montrer qu'on a

$$\mathrm{card}(\mathcal{O}_s) = \frac{\mathrm{card}(G)}{\mathrm{card}(\Gamma_s)}$$

**Exercice d'application [2 pts]:** Montrer que si un groupe fini $G$ agit transitivement sur un ensemble $S$, alors il existe un élément $g \in G$ tel que $g \cdot s \neq s$ pour tout $s \in S$. (Indication: on pourra montrer que si la conclusion n'était pas vraie, on aurait $G = \bigcup_{s \in S} \Gamma_s$ et utiliser un argument de dénombrement).

**Exercice 1 [7 pts]:** Soit $\alpha = \sqrt{1+\sqrt{5}}$ la racine réelle positive du polynôme

$$P(X) = X^4 - 2X^2 - 4$$

On pose $K = \mathbb{Q}(\alpha)$. On note aussi $\beta = \sqrt{1-\sqrt{5}}$ la racine carrée complexe de $1-\sqrt{5}$ de partie imaginaire positive.

(a) Montrer que $P(X)$ est irréductible sur $\mathbb{Q}$ et en déduire le degré de $K$ sur $\mathbb{Q}$.

(b) Montrer que la clôture galoisienne du corps $K$ est le corps $\widehat{K} = \mathbb{Q}(i, \alpha)$.

(c) Montrer que le groupe de Galois $G$ de l'extension $\widehat{K}/\mathbb{Q}$ contient un élément $\sigma$ tel que $\sigma(\alpha) = \beta$ et $\sigma(i) = -i$, et un élément $\tau$ tel que $\tau(\alpha) = \alpha$ et $\tau(i) = -i$. Montrer que $\sigma$ est d'ordre 4 et $\tau$ d'ordre 2.

(d) Montrer que $G$ est le groupe diédral d'ordre 8, c'est-à-dire, qu'il est engendré par un élément $\sigma$ d'ordre 4 et un élément $\tau$ d'ordre 2 tels que $\tau\sigma\tau^{-1} = \sigma^{-1}$.

(e) Déterminer la liste des sous-groupes de $G$; on montrera en particulier qu'il existe un sous-groupe isomorphe à $\mathbb{Z}/4\mathbb{Z}$ et deux sous-groupes isomorphes à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(f) En déduire la liste des extensions intermédiaires entre $\mathbb{Q}$ et $\widehat{K}$. (Indication: on pourra montrer que $\mathbb{Q}(i, \alpha+\beta)/\mathbb{Q}$ et $\mathbb{Q}(i, \alpha-\beta)/\mathbb{Q}$ sont deux des extensions intermédiaires de degré 4 (sans chercher à calculer $\alpha+\beta$ et $\alpha-\beta$)).

**Exercice 2 [2 pts]:** Montrer que le polynôme $P(X,Y) = Y^2 - X^2(X+1)$ est irréductible dans $\mathbb{C}[X,Y]$. Même question pour le polynôme $F(X,Y,Z) = Y^n - X^n(X+Z)$ dans $\mathbb{C}[X,Y,Z]$, où $n \geq 1$ est un entier.

**Exercice 3 [7 pts]:** Soit $G$ un groupe fini.

(a) Soient $d$ et $r$ deux entiers $\geq 1$. Soit $H$ le sous-groupe de $G$ engendré par tous les éléments de $G$ s'écrivant comme produit de $r$ éléments de $G$ d'ordre $d$. Montrer que $H$ est un sous-groupe distingué de $G$.

(b) On suppose ici que $G$ est un groupe simple non abélien.

(i) Montrer que $G$ possède au moins un élément d'ordre 2 (Indication: on pourra utiliser le théorème de Feit-Thompson).

(ii) Montrer que $G$ est engendré par ses éléments d'ordre 2.

(iii) Montrer que $G$ est engendré par l'ensemble de tous les produits $\alpha\beta$ de deux éléments $\alpha$ et $\beta$ d'ordre 2.

Soit $p$ un nombre premier.

(c) Montrer que tout $p$-groupe $P$ non trivial a un quotient isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
(Indication: on pourra raisonner par récurrence).

(d) Montrer que si $H_{p'}$ est le sous-groupe de $G$ engendré par ses éléments d'ordre premier à $p$, alors $H_{p'}$ est distingué et $G/H_{p'}$ est un $p$-groupe.

(e) Montrer que si $G$ n'est pas engendré par ses éléments d'ordre premier à $p$, alors il a un quotient isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

(f) Montrer la réciproque de la question (e): si $G$ a un quotient isomorphe à $\mathbb{Z}/p\mathbb{Z}$, alors $G$ n'est pas engendré par ses éléments d'ordre premier à $p$. (Un groupe $G$ ne satisfaisant pas ces propriétés équivalentes est dit *$p$-parfait*).

# UNIVERSITÉ LILLE 1

Enseignants: **N. BORNE, P. DÈBES, M. EMSALEM**
Filière: **Maîtrise de mathématiques**
Matière: **Algèbre**
Année universitaire: **2003/2004**
Date: **mardi 25 novembre 2003 à 14h00**
Durée de l'épreuve: **4 heures**

---

**Ni calculatrices ni documents.**

**Le barème est donné à titre indicatif.**

**Chacune des trois parties devra être rédigée sur une copie différente.**

---

## PARTIE I

**Question de cours [2 pts]**: Soient $G$ un groupe fini et $p$ un nombre premier tels que $p^n$ divise $|G|$ (pour un entier $n \geq 0$). Montrer qu'il existe une suite de sous-groupes $\{1\} = G_o \subset G_1 \subset \cdots \subset G_n$ telle que $|G_i| = p^i$ et $G_i$ est distingué dans $G_n$, $i = 0, 1, \ldots, n$.

**Exercice 1 [3,5 pts]:** Soient $G$ un groupe fini et $H$ un sous-groupe de $G$. On note $U$ l'ensemble réunion des sous-groupes $gHg^{-1}$ conjugués de $H$ par les éléments de $G$.

(a) Montrer que si $\{g_1, \ldots, g_n\}$ est un système de représentants des classes à gauche de $G$ modulo $H$, alors, $U \setminus \{1\} = \bigcup_{i=1}^{n} \left(g_i H g_i^{-1} \setminus \{1\}\right)$.

(b) En déduire que $\text{card}(U) \leq |G| - [G : H] + 1$

(c) *Application 1.* Soit $S$ un sous-ensemble de $G$ contenant au moins un élément dans chaque classe de conjugaison de $G$. Montrer que $S$ engendre $G$. (Indication: appliquer ce qui précède au sous-groupe $H = < S >$).

(d) *Application 2.* Soit $G$ un sous-groupe transitif de $S_n$ avec $n > 1$. Montrer que pour tout $i = 1, \ldots, n$, le fixateur $G(i)$ est un sous-groupe conjugué de $H = G(1)$. En utilisant (b), montrer que $G$ contient une permutation sans aucun point fixe.

**Exercice 2 [1 pt]:** Montrer qu'un groupe fini est un $p$-groupe si et seulement si tous ses éléments sont d'ordre une puissance de $p$.

## PARTIE II

**Exercice 3 [2 pts]:** (a) Soient $\mathcal{G}$ un groupe et $\mathcal{H}$ un sous-groupe inclus dans le centre $Z(\mathcal{G})$. On suppose que $\mathcal{G}/\mathcal{H}$ est monogène (c'est-à-dire, engendré par un élément). Montrer que $\mathcal{G}$ est abélien.

Soient $G$ un groupe et $(C_i(G))_{i \geq 0}$ sa suite centrale descendante. On suppose que $G/C_1(G)$ est monogène.

(b) Montrer qu'on a $C_1(G) = C_2(G)$. (Indication: on pourra, pour une des deux inclusions, appliquer le (a) au groupe $\mathcal{G} = G/C_2(G)$ ).

(c) En déduire que si $G$ est nilpotent, alors $G$ est monogène.

**Exercice 4 [3,5 pts]:** (a) Soit $H$ un groupe d'ordre 48 possédant trois 2-Sylows. En utilisant l'action $\rho : H \to S_3$ de $H$ par conjugaison sur l'ensemble des trois 2-Sylows, montrer qu'il existe un sous-groupe distingué d'ordre 8.

(b) Montrer que tout groupe d'ordre 624 est résoluble.

**Exercice 5 [1 pt]:** Les permutations ci-dessous sont-elles conjuguées dans $S_7$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 2 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix} \quad ?$$

## PARTIE III

**Exercice 6 [3,5 pts]:** Soit $G$ un groupe d'ordre 30.

(a) Montrer qu'il existe un unique 3-Sylow ou qu'il existe un unique 5-Sylow dans $G$.

(b) Montrer que $G$ possède un sous-groupe distingué d'ordre 15.

(c) Montrer qu'il existe un unique 3-Sylow et qu'il existe un unique 5-Sylow dans $G$.

(d) Tout groupe d'ordre 30 est-il nilpotent?

**Exercice 7 [1,5 pts]:** On considère le groupe des quaternions $\mathbf{H}_8$, composé des 8 éléments $\pm 1, \pm i, \pm j, \pm k$ vérifiant $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$ et $ki = -ik = j$.

(a) Déterminer tous les sous-groupes de $\mathbf{H}_8$.

(b) Un groupe dont tous les sous-groupes sont distingués est-il nécessairement abélien?

**Exercice 8 [2 pts]:** Quel est le nombre des classes d'isomorphisme de groupes abéliens d'ordre 400. Donner la liste de ceux de ces groupes qui sont d'exposant 20.

# UNIVERSITÉ LILLE 1

Enseignants: **N. BORNE, P. DÈBES, M. EMSALEM**
Filière: **Maîtrise de mathématiques**
Matière: **Algèbre**
Année universitaire: **2003/2004**
Date: **mardi 27 janvier 2004 à 14h00**
Durée de l'épreuve: **4 heures**

---

**Ni calculatrices ni documents.**

**Le barème est donné à titre indicatif.**

**Chacune des trois parties devra être rédigée sur une copie différente.**

---

## PARTIE I

**Exercice 1 [7,5 pts]:** On note $\sqrt[3]{10}$ la racine réelle du polynôme $X^3-10$ et $K$ le corps $\mathbb{Q}(\sqrt{3}, \sqrt[3]{10})$.

(a) Montrer que $\sqrt{3} \notin \mathbb{Q}(\sqrt[3]{10})$ et en déduire le degré de $K$ sur $\mathbb{Q}$. L'extension $K/\mathbb{Q}$ est-elle galoisienne?

(b) Montrer que $\mathbb{Q}(\sqrt{3})$ et $\mathbb{Q}(\sqrt[3]{10})$ sont les seuls sous-corps non triviaux de $K$.
(Indication: Pour les sous-corps de degré 3 sur $\mathbb{Q}$, on pourra montrer que si $E$ en est un, différent de $\mathbb{Q}(\sqrt[3]{10})$, alors $X^3-10$ est irréductible sur $E$).

(c) Montrer que tout élément $\alpha \in K$ s'écrit de façon unique sous la forme $\alpha = P(\sqrt[3]{10}, \sqrt{3})$ où $P(X,Y) = a_o + a_1X + a_2X^2 + a_3Y + a_4XY + a_5X^2Y$ est un polynôme à coefficients dans $\mathbb{Q}$.

(d) En utilisant (b), montrer qu'on a $\mathbb{Q}(\alpha) \neq K$ si et seulement si les quatre nombres $a_4$, $a_5$, $a_1a_3$ et $a_2a_3$ sont nuls.

(e) Soient $j = \exp(2i\pi/3)$ et $L = K(j)$. Montrer que l'extension $L/\mathbb{Q}$ est galoisienne de degré 12. On note $G$ son groupe de Galois.

(f) Montrer qu'il existe deux éléments $\sigma, \tau \in G$ vérifiant:

$$\begin{cases} \sigma(\sqrt[3]{10}) = j\sqrt[3]{10} \\ \sigma(\sqrt{3}) = \sqrt{3} \\ \sigma(j) = j \end{cases} \qquad \begin{cases} \tau(\sqrt[3]{10}) = \sqrt[3]{10} \\ \tau(\sqrt{3}) = -\sqrt{3} \\ \tau(j) = j \end{cases}$$

(g) Montrer que l'extension $L/\mathbb{Q}(j)$ est galoisienne de groupe de Galois isomorphe à $\mathbb{Z}/6\mathbb{Z}$.

(h) On note $c$ la restriction à $L$ de la conjugaison complexe. Calculer les automorphismes $c\,\sigma\,c$ et $c\,\tau\,c$ et en déduire que $G$ est isomorphe au groupe diédral $D_{12}$ d'ordre 12.

(i) Déterminer les sous-corps de $L$ de degré 3 et 4 sur $\mathbb{Q}$ (qui correspondent respectivement aux 2-Sylows et aux 3-Sylows). Donner le nombre des autres sous-corps, en précisant leur degré.

# PARTIE II

**Question de cours 1 [2,5 pts]:** Enoncer et démontrer le théorème de l'élément primitif dans le cas d'un corps de base infini.

**Exercice 2 [4 pts]:** Soit $n \geq 2$ un entier et $E/F$ une extension galoisienne de groupe de Galois $S_n$. On note $\Gamma(1)$ le sous-groupe de $S_n$ constitué des permutations qui fixent 1 et $C$ le sous-groupe de $S_n$ engendré par le $n$-cycle $(1\ 2\ \ldots\ n)$. On pose $E_1 = E^{\Gamma(1)}$ et $L = E^C$.

(a) Déterminer les degrés $[E_1 : F]$ et $[L : F]$ et les corps $E_1 \cap L$ et $E_1 L$.

(b) Montrer que si $M$ est un corps tel que $E_1 \subset M \subset E$ et $M/F$ est une extension galoisienne, alors $M = E$.

On suppose désormais que $n = p$ est un nombre premier.

(c) Calculer le nombre de corps $M$ intermédaires entre $F$ et $E$ tels que $[M : F] = (p-1)!$ Les extensions $M/F$ correspondantes sont-elles galoisiennes? sont-elles conjuguées?

(d) Montrer que si $M$ est un corps tel que $F \subset M \subset E_1$, alors $M = F$ ou $M = E_1$.

# PARTIE III

**Exercice 3 [2 pts]:** Soit $\alpha \in \mathbb{C}$ une racine du polynôme $P(X) = X^3 + 2X + 2$. L'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est-elle galoisienne? Déterminer le groupe de Galois de $P(X)$.

**Exercice 4 [4 pts]:** On fixe un nombre premier $p \neq 2$. Pour tout $a \in \mathbb{N}$, on note $\sqrt[p]{a}$ l'unique racine $p$-ième réelle de $a$. On pose $\zeta = \exp(2i\pi/p)$ et $k = \mathbb{Q}(\zeta)$.

(a) Montrer que si $\alpha, \beta \in \mathbb{C}$ sont deux racines distinctes du polynôme $X^p - p$, alors on a $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$.

(b) Montrer que l'extension $k(\sqrt[p]{p})/k$ est galoisienne de groupe isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

(c) Montrer que pour tout $a \in \mathbb{Z}$, on a $\sqrt[p]{a} \in k(\sqrt[p]{p})$ si et seulement si il existe $d \in \mathbb{Z}$ tel que $a/p^d$ est une puissance $p$-ième dans $k$. (Indication: pour la partie directe, on pourra montrer que si $\sqrt[p]{a} \in k(\sqrt[p]{p})$, alors il existe $d \in \mathbb{Z}$ tel que $\sqrt[p]{a}/(\sqrt[p]{p})^d \in k$).

# UNIVERSITÉ LILLE 1

Enseignants: **N. BORNE, P. DÈBES, M. EMSALEM**
Filière: **Maîtrise de mathématiques**
Matière: **Algèbre**
Année universitaire: **2003/2004**
Date: **septembre 2004**
Durée de l'épreuve: **4 heures**

---

**Ni calculatrices ni documents.**
**Le barème est donné à titre indicatif.**

---

**Exercice 1 [2 pts]:** Montrer que tout groupe d'ordre 99 est abélien.

**Exercice 2 [6,5 pts]:** On note $K$ le corps de décomposition sur $\mathbb{Q}$ du polynôme $P(X) = X^4 - 2X^2 - 4$.

(a) Résoudre l'équation $P(x) = 0$ dans $\mathbb{C}$ et montrer que le polynôme $P(X)$ est irréductible sur $\mathbb{Q}$.

(b) Montrer que $K = \mathbb{Q}(\sqrt{1+\sqrt{5}}, \sqrt{1-\sqrt{5}})$ et que $K/\mathbb{Q}$ est une extension galoisienne de degré 8. (Pour la suite, on pourra effectuer le produit $(1+\sqrt{5})(1-\sqrt{5})$ et en déduire que $i \in K$).

(c) Montrer qu'il existe $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ tel que $\begin{cases} \sigma(\sqrt{1+\sqrt{5}}) = \sqrt{1-\sqrt{5}} \\ \sigma(\sqrt{1-\sqrt{5}}) = -\sqrt{1+\sqrt{5}} \end{cases}$

(d) Montrer que $\mathrm{Gal}(K/\mathbb{Q})$ est isomorphe au groupe diédral $D_8$ d'ordre 8.
(Indication: vérifier que $\sigma$ est d'ordre 4 et que $c\sigma c = \sigma^{-1}$, où $c$ désigne la restriction à $K$ de la conjugaison complexe).

(e) Donner la liste des sous-groupes de $D_8$ et la liste correspondante des corps intermédiaires entre $\mathbb{Q}$ et $K$.

**Exercice 3 [4,5 pts]:** Etant donné un groupe fini, on appelle sous-groupe de Frattini de $G$ l'intersection des sous-groupes maximaux de $G$, distincts de $G$; on le note $\Phi(G)$.

(a) Montrer que $\Phi(G)$ est un sous-groupe caractéristique de $G$ et qu'il a la propriété suivante: si $H$ est un sous-groupe de $G$ tel que $H\Phi(G) = G$, alors $H = G$.

(b) Déterminer $\Phi(G)$
- pour $G = \mathbb{Z}/p^n\mathbb{Z}$ pour $p$ premier et $n > 0$ entier,
- pour $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, pour $p$ et $q$ premiers distincts,
- pour $G = \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, pour $p$ et $q$ premiers distincts.

(c) Montrer que si $P$ est un $p$-Sylow de $\Phi(G)$, alors pour tout $g \in G$, il existe $a \in \Phi(G)$ tel que $gPg^{-1} = aPa^{-1}$.

(d) Déduire de (c) et (a) que $G = \mathrm{Nor}_G(P)$, puis que $\Phi(G)$ est nilpotent.

**Exercice 4 [2 pts]**: Montrer qu'il n'existe pas de groupe simple d'ordre 72.
(Indication: On pourra raisonner sur les 3-Sylows du groupe).

**Exercice 5 [5 pts]:** (a) Montrer que si $p$ et $q$ sont deux nombres premiers distincts, alors l'extension $\mathbb{Q}(\sqrt{p}, \sqrt{q})/\mathbb{Q}$ est de degré 4.

(b) Soient $m \geq 1$ un entier et $p_1, \ldots, p_m$ $m$ nombres premiers distincts. Montrer que l'extension $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m})/\mathbb{Q}$ est galoisienne. On note $G_m$ son groupe de Galois.

(c) Montrer que pour $i = 1, \ldots, m$, il existe $\sigma_i \in G_m$ tel que $\sigma_i(\sqrt{p_i}) = -\sqrt{p_i}$ et $\sigma_i(\sqrt{p_j}) = \sqrt{p_j}$ pour $j \neq i$ et que $\sigma_1, \ldots, \sigma_m$ engendrent $G_m$.
(Indication: raisonner par récurrence sur $m$; pour montrer que $\sqrt{p_m} \notin \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{m-1}})$, on pourra supposer le contraire et construire un élément de la forme

$$\frac{\sqrt{p_m}}{\sqrt{p_1}^{e_1} \cdots \sqrt{p_{m-1}}^{e_{m-1}}}$$

avec $e_1, \ldots, e_{m-1}$ égaux à 0 ou 1, qui soit dans $\mathbb{Q}$).

(d) En déduire que $G_m$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^m$.

# UNIVERSITÉ LILLE 1

Enseignants: **P. DÈBES, Y. HANTOUT, D. MARKOUCHEVITCH**
Filière: **Master 1**
Matière: **Algèbre approfondie**
Année universitaire: **2004/2005**
Date: **mercredi 17 novembre à 16h00**
Durée de l'épreuve: **2 heures**

---

**Ni calculatrices ni documents.**
**Le barème est donné à titre indicatif.**
**Chacune des trois parties devra être rédigée sur une copie différente.**

---

## PARTIE I

**Question de cours [3,5 pts]:** Soit $G$ un groupe fini d'ordre $mp^n$ où $p$ est un nombre premier, $m$ et $n$ des entiers $\geq 1$ tels que $p$ ne divise pas $m$. Montrer que $G$ possède au moins un sous-groupe d'ordre $p^n$.

**Exercice 1 [2,5 pts]**: Montrer que si $G$ est un groupe simple d'ordre divisible par un nombre premier $p$, alors $G$ est engendré par ses éléments d'ordre $p$.

## PARTIE II

**Exercice 2 [4,5 pts]**: (a) Soit $G$ le groupe symétrique $S_4$. Montrer que pour tout diviseur $d$ de l'ordre de $G$, il existe un sous-groupe $H$ de $G$ d'ordre $d$.

(b) Montrer que la propriété ci-dessus est fausse pour $G$ égal au groupe alterné $A_4$.

**Exercice 3 [2,5 pts]**: Montrer que les sous-groupes simples de $S_n$ ($n \geq 2$) sont soit contenus dans $A_n$ soit d'ordre 2.

## PARTIE III

**Exercice 4 [3,5 pts]**: On considère le groupe $H_8$ composé des 8 éléments $\pm 1, \pm I, \pm J, \pm K$ où

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \ , \ I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \ , \ J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \ K = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

(avec $i \in \mathbb{C}$ tel que $i^2 = -1$)

et dont la table de multiplication est déterminée par les relations $I^2 = J^2 = K^2 = -1$, $IJ = -JI = K$, $JK = -KJ = I$ et $KI = -IK = J$.

(a) Déterminer le centre $Z(H_8)$ du groupe $H_8$ et montrer que tous les éléments de $H_8 \setminus Z(H_8)$ sont d'ordre 4.

(b) Montrer que tous les sous-groupes de $H_8$ sont distingués.

(c) Montrer que $H_8$ n'est isomorphe à aucun produit semi-direct de deux groupes non triviaux.

**Exercice 5 [3,5 pts]**: Montrer qu'il n'existe pas de groupe simple d'ordre 750.

# UNIVERSITÉ LILLE 1

Enseignants: **P. DÈBES, Y. HANTOUT, D. MARKOUCHEVITCH**
Filière: **Master 1**
Matière: **Algèbre approfondie**
Année universitaire: **2004/2005**
Date: **mardi 18 janvier 2005 de 8h à 11h**
Lieu: **bâtiment P1, amphi Joliot**

---

**Ni calculatrices ni documents.**

**Le barème est donné à titre indicatif.**

**Chacune des trois parties devra être rédigée sur une copie différente.**

---

## PARTIE I

**Question de cours [4 pts]**: Montrer que dans un groupe fini nilpotent $G$, aucun sous-groupe propre $H$ ne peut être égal à son normalisateur $\mathrm{Nor}_G(H)$ et en déduire que tous les sous-groupes de Sylow sont distingués dans $G$.

## PARTIE II

**Exercice 1 [9 pts]**: (a) Montrer que tout groupe d'ordre 245 est abélien.

(b) Montrer que tout groupe d'ordre $5 \cdot 7^2 \cdot 11^n$ avec $n \geq 0$ est résoluble.

(c) Déterminer tous les groupes abéliens d'ordre $5 \cdot 7^2 \cdot 11$.

(d) Montrer que tout groupe $G$ non abélien d'ordre $5 \cdot 7^2 \cdot 11$ est non nilpotent.

(e) Dans le cas où $G$ est non abélien d'ordre $5 \cdot 7^2 \cdot 11$, déterminer sa suite centrale descendante. (Indication: on pourra commencer par établir que le groupe dérivé $D(G)$ est égal au 11-Sylow de $G$).

## PARTIE III

**Exercice 2 [5 pts]**: Soit $G$ le sous-groupe du groupe symétrique $S_5$ engendré par le 3-cycle (1 2 3) et les transpositions (4 5) et (1 2). Le groupe $G$ est-il abélien? résoluble? nilpotent?

**Exercice 3 [2 pts]**: Les groupes

$$\mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/168\mathbb{Z}$$

sont-ils isomorphes? On déterminera leurs facteurs invariants.

# UNIVERSITÉ LILLE 1

Enseignants: **P. DÈBES, Y. HANTOUT, D. MARKOUCHEVITCH**
Filière: **Master 1 - Semestre 1**
Matière: **Algèbre approfondie**
Année universitaire: **2004/2005 - 2ème session**
Durée de l'épreuve: **3 heures**

---

**Ni calculatrices ni documents ni téléphone portable.**
**Le barème est donné à titre indicatif.**

---

**Question de cours [3,5 pts]**: donner la définition de la série centrale descendante $(C_i(G))_{i\geq 0}$ et de la série centrale ascendante $(Z_i(G))_{i\geq 0}$ d'un groupe $G$ et montrer que pour tout entier $n \geq 0$, on a $Z_n(G) = G$ si et seulement $C_n(G) = \{1\}$.

**Exercice 1 [5 pts]:** (a) Donner l'ensemble $\mathcal{D}$ des ordres possibles des éléments du groupe alterné $A_5$ et pour chaque $d \in \mathcal{D}$, indiquer le nombre d'éléments de $A_5$ d'ordre $d$.

(b) Montrer que, pour $d = 2$ et $d = 3$, les éléments d'ordre $d$ sont conjugués, et que les sous-groupes d'ordre 5 sont conjugués.

(c) Déduire une preuve de la simplicité de $A_5$.
(Indication: pour $H \neq \{1\}$ sous-groupe distingué de $A_5$, raisonner sur les éléments d'ordre 2, 3 et 5 contenus dans $H$).

**Exercice 2 [6 pts]**:
(a) Montrer que tout groupe d'ordre 50 soit est abélien soit est produit semi-direct d'un sous-groupe d'ordre 25 et d'un groupe d'ordre 2 non distingué.

(b) Montrer que tout groupe d'ordre $50 \cdot 11^n$ avec $n \geq 0$ est résoluble.

(c) Déterminer tous les groupes abéliens d'ordre $50 \cdot 11^2$.

(d) Montrer que tout groupe $G$ d'ordre $50 \cdot 11^2$ non abélien est non nilpotent.

**Exercice 3 [5,5 pts]:** Soient $G$ un groupe et $G \times^s \mathrm{Aut}(G)$ le produit semi-direct de $G$ par son groupe d'automorphismes Aut(G). Pour tout $g \in G$, on note $c_g \in \mathrm{Aut}(G)$ l'automorphisme de conjugaison par $g$, c'est-à-dire, $c_g(h) = ghg^{-1}$ $(h \in G)$.
(a) Montrer que l'application $\Phi : G \times^s \mathrm{Aut}(G) \to \mathrm{Per}(G)$ définie par

$$\text{pour tout } (g,\chi) \in G \times^s \mathrm{Aut}(G), \quad \Phi(g,\chi)(h) = g\,\chi(h) \qquad (\text{pour tout } h \in G)$$

définit une action de $G \times^s \mathrm{Aut}(G)$ sur $G$ et montrer que cette action est fidèle.

(b) Montrer que l'application $i : G \to G \times^s \mathrm{Aut}(G)$ définie par $i(g) = (g, 1)$ (pour $g \in G$) est un monomorphisme de groupes et que $\Phi \circ i$ est l'action par translation à gauche de $G$ sur lui-même.

(c) On pose $G_\gamma = \Phi \circ i(G)$. Montrer que si $\sigma \in \mathrm{Per}(G)$ normalise $G_\gamma$ et vérifie $\sigma(1) = 1$ alors $\sigma \in \Phi(\mathrm{Aut}(G))$.

(d) Montrer que le normalisateur dans $\mathrm{Per}(G)$ du groupe $G_\gamma$ est égal à $\Phi(G \times^s \mathrm{Aut}(G))$.

# UNIVERSITÉ LILLE 1

Enseignants: **P. DÈBES, D. MARKOUCHEVITCH, J.-F. ROBINET**
Filière: **Master 1 - Semestre 1**
Matière: **Algèbre approfondie**
Année universitaire: **2005/2006**
Épreuve: **Partiel**
Date: **mercredi 16 novembre 2005 de 10h à 12h**
Lieu: **bâtiment A4**
Durée de l'épreuve: **2 heures**

---

**Ni calculatrices ni documents ni téléphone portable.**

**Le barème est donné à titre indicatif.**

**Chacune des deux parties devra être rédigée sur une copie différente.**

---

## PARTIE I

**Question de cours [3 pts]** : Montrer qu'une suite normale d'un groupe $G$ est maximale si et seulement si ses facteurs sont des groupes simples.

**Exercice 1 [7 pts] :** (a) Montrer que la réunion de 3 sous-groupes distincts d'ordre 9 d'un groupe $G$ possède au moins 19 éléments.

On se donne un groupe fini $G$ d'ordre 306.

(b) Montrer que $G$ possède ou bien un 17-sous groupe de Sylow distingué ou bien un 3-sous groupe de Sylow distingué.

(c) Montrer que le groupe $G$ est de longueur 4 et préciser l'ensemble des facteurs d'une suite de composition.

## PARTIE II

**Exercice 2 [10 pts] :** Pour $n \geq 2$ et $0 < k < n$, on note $I = \{1, \ldots, k\}$, $J = \{k+1, \ldots, n\}$ et $\mathcal{G}_I$ le sous-groupe de $S_n$ des permutations de $\{1, \ldots, n\}$ qui laissent stable $I$.

(a) Montrer que $\mathcal{G}_I$ est isomorphe au produit direct $S_k \times S_{n-k}$ des groupes symétriques $S_k$ et $S_{n-k}$.

(b) On suppose $k < n/2$. Montrer que $\mathcal{G}_I$ est un sous-groupe propre maximal de $S_n$.
(Indication: on pourra montrer que pour tout $\sigma \in S_n \setminus \mathcal{G}_I$, il existe $j_1, j_2 \in J$ tels que $\sigma(j_1) = i \in I$ et $\sigma(j_2) = j \in J$, puis montrer que $\mathcal{G}_I$ contient toutes les transpositions.)

(c) Montrer que si $1 < k < n/2$, l'action naturelle de $S_n$ sur les parties de $\{1, \ldots, n\}$ à $k$ éléments est primitive mais pas 2-transitive.

(d) On prend ici $n = 4$. Montrer que le sous-groupe $H \subset S_n$ engendré par $\alpha = (1\,2)$ et $\omega = (1\,3\,2\,4)$ est isomorphe au groupe diédral d'ordre 8 et que, pour $I = \{1, 2\}$, le sous-groupe $\mathcal{G}_I \subset S_4$ n'est pas maximal.

# UNIVERSITÉ LILLE 1

Enseignants: **P. DÈBES, D. MARKOUCHEVITCH, J.-F. ROBINET**
Filière: **Master 1 - Semestre 1**
Matière: **Algèbre approfondie**
Date: **mercredi 16 novembre 2005 de 10h à 12h**
Épreuve: **Partiel**

---

## CORRIGÉ

---

**Exercice 1 :** (a) *Montrer que la réunion de* 3 *sous-groupes distincts d'ordre* 9 *d'un groupe* $G$ *possède au moins* 19 *éléments.*

**Correction**: Soient $H_1$, $H_2$, $H_3$ trois sous-groupes distincts d'ordre 9 d'un groupe $G$. L'intersection $H_1 \cap H_2$ est un sous-groupe propre de $H_1$ et est donc d'ordre $\leq 3$. On a donc $\mathrm{card}(H_1 \cup H_2) = \mathrm{card}(H_1) + \mathrm{card}(H_2) - \mathrm{card}(H_1 \cap H_2) \geq 9 + 9 - 3 = 15$.

On écrit ensuite $\mathrm{card}(H_1 \cup H_2 \cup H_3) = \mathrm{card}(H_1 \cup H_2) + \mathrm{card}(H_3) - \mathrm{card}((H_1 \cup H_2) \cap H_3)$. Comme $(H_1 \cup H_2) \cap H_3 = (H_1 \cap H_3) \cup (H_2 \cap H_3)$ et que l'intersection $(H_1 \cap H_3) \cap (H_2 \cap H_3) = H_1 \cap H_2 \cap H_3$ a au moins un élément (l'élément neutre 1), on obtient que $\mathrm{card}((H_1 \cup H_2) \cap H_3) = \mathrm{card}(H_1 \cap H_3) + \mathrm{card}(H_2 \cap H_3) - \mathrm{card}(H_1 \cap H_2 \cap H_3) \leq 3 + 3 - 1 = 5$, ce qui donne finalement $\mathrm{card}(H_1 \cup H_2 \cup H_3) \geq 15 + 9 - 5 = 19$.

*On se donne un groupe fini* $G$ *d'ordre* 306.

(b) *Montrer que* $G$ *possède ou bien un* 17*-sous groupe de Sylow distingué ou bien un* 3*-sous groupe de Sylow distingué.*

**Correction**: Le nombre de 17-Sylow d'un groupe d'ordre $306 = 2.3^2.17$ est $\equiv 1$ [mod 17] et divise 18; c'est donc 1 ou 18. De même le nombre de 3-Sylow est $\equiv 1$ [mod 3] et divise 34; c'est donc 1 ou 34. Supposons que ces deux nombres ne soient égaux à 1 ni l'un ni l'autre. Les 17-Sylow étant d'intersections deux à deux réduites à $\{1\}$, leur réunion privée de 1 est de cardinal $18(17-1)$. De plus cette réunion ne coupe aucun 3-Sylow (car 17 et 3 sont premiers entre eux), et donc ne coupe pas non plus leur réunion, qui d'après la question (a), est de cardinal $\geq 19$. L'inégalité $18(17-1) + 19 > 18.17 = |G|$ fournit une contradiction. Il existe donc ou bien un unique 17-Sylow ou bien un unique 3-Sylow. Cet unique Sylow est automatiquement distingué.

(c) *Montrer que le groupe* $G$ *est de longueur* 4 *et préciser l'ensemble des facteurs d'une suite de composition.*

**Correction**: On distingue deux cas.

1er cas: il existe un unique 17-Sylow, qu'on note $S_{17}$. On a alors $\ell(G) = \ell(S_{17}) + \ell(G/S_{17})$ où $\ell(H)$ désigne la longueur d'un groupe $H$.

Le groupe $S_{17}$ est cyclique d'ordre 17 et donc de longueur 1 avec $\mathbb{Z}/17\mathbb{Z}$ comme unique facteur.

Le groupe $G/S_{17}$ est d'ordre 18. Le nombre de ses 3-Sylow est $\equiv 1$ [mod 3] et divise 2. Donc c'est 1: il y a un unique 3-Sylow distingué, $\overline{S}_3$, d'ordre 9. Comme $9 = 3^2$, $\overline{S}_3$ est abélien, de longueur 2 avec $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ comme facteurs. Le quotient de $G/S_{17}$ par son 3-Sylow $\overline{S}_3$ est d'ordre 2 donc cyclique, de longueur 1, isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

Finalement, $\ell(G) = 1 + 2 + 1 = 4$ et ses facteurs sont: $\mathbb{Z}/17\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$.

2ème cas: il existe un unique 3-Sylow, qu'on note $S_3$. On a alors $\ell(G) = \ell(S_3) + \ell(G/S_3)$.

Le groupe $S_3$, d'ordre $9 = 3^2$, est abélien, de longueur 2 avec $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ comme facteurs.

Le groupe $G/S_3$ est d'ordre $34 = 2.17$. Il est donc isomorphe au produit semi-direct de son unique 17-Sylow, d'ordre 17, par un 2-Sylow, d'ordre 2. En particulier $G/S_3$ est de longueur $1+1$ est ses facteurs sont $\mathbb{Z}/17\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$.

Finalement, $\ell(G) = 2+2 = 4$ et ses facteurs sont: $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/17\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$.

**Exercice 2 :** *Pour $n \geq 2$ et $0 < k < n$, on note $I = \{1, \ldots, k\}$, $J = \{k+1, \ldots, n\}$ et $\mathcal{G}_I$ le sous-groupe de $S_n$ des permutations de $\{1, \ldots, n\}$ qui laissent stable $I$.*

(a) *Montrer que $\mathcal{G}_I$ est isomorphe au produit direct $S_k \times S_{n-k}$ des groupes symétriques $S_k$ et $S_{n-k}$.*

**Correction**: Pour tout $\sigma \in \mathcal{G}_I$ c'est-à-dire $\sigma(I) \subset I$, on a en fait $\sigma(I) = I$ (car $\sigma$ injective) et $\sigma(J) = J$. Ainsi la correspondance $\phi : \mathcal{G}_I \to \mathrm{Per}(I) \times \mathrm{Per}(J)$ qui associe à toute permutation $\sigma \in \mathcal{G}_I$ le couple $(\sigma|_I, \sigma|_J)$ de ses restrictions à $I$ et à $J$ est bien définie. Comme $I \cap J = \emptyset$, les éléments de $\mathrm{Per}(I) \subset S_n$ commutent à ceux de $\mathrm{Per}(J) \subset S_n$. On en déduit que $\phi$ est un homomorphisme. De $I \cup J = \{1, \ldots, n\}$ découle que $\phi$ est injective. Enfin $\phi$ est surjective: pour tout $(\omega, \omega') \in \mathrm{Per}(I) \times \mathrm{Per}(J)$, la permutation $\sigma = \omega\omega' = \omega'\omega$ vérifie $\phi(\sigma) = (\omega, \omega')$. Ainsi le groupe $\mathcal{G}_I$ est isomorphe à $\mathrm{Per}(I) \times \mathrm{Per}(J)$, lequel est isomorphe à $S_k \times S_{n-k}$ (puisque $\mathrm{card}(I) = k$ et $\mathrm{card}(J) = n-k$).

(b) *On suppose $k < n/2$. Montrer que $\mathcal{G}_I$ est un sous-groupe propre maximal de $S_n$.*

**Correction**: Soit $\sigma \in S_n \setminus \mathcal{G}_I$. On a $\sigma(J) \not\subset J$ (sinon $\sigma(J) = J$ et $\sigma(I) = I$). Il existe donc $j_1 \in J$ tels que $\sigma(j_1) = i \notin J$, c'est-à-dire $\sigma(j_1) = i \in I$. D'autre part, comme $\mathrm{card}(\sigma(J)) = \mathrm{card}(J) = n-k > k = \mathrm{card}(I)$ et que $\sigma$ est injective, on a $\sigma(J) \not\subset I$. Donc il existe $j_2 \in J$ tels que $\sigma(j_2) = j \notin I$, c'est-à-dire $\sigma(j_2) = j \in J$.

Soit $H$ un sous-groupe de $S_n$ contenant strictement $\mathcal{G}_I$. En particulier, $H$ contient toutes les transpositions $(u\ v)$ avec $u, v \in I$ et toutes celles avec $u, v \in J$. De plus il existe une permutation $\sigma \in H \setminus \mathcal{G}_I$ à laquelle on peut appliquer ce qui précède. Soient $j_1, j_2 \in J$, $i \in I$ et $j \in J$ comme ci-dessus. Comme $\sigma$ et $(j_1\ j_2)$ sont dans $H$, on a aussi $\sigma(j_1\ j_2)\sigma^{-1} = (i\ j) \in H$. Soient maintenant $u \in I$ et $v \in J$ quelconques. Définissons $\tau_u$ comme la permutation $(i\ u)$ si $u \neq i$ et l'identité si $u = i$ et $\tau_v$ comme $(j\ v)$ si $v \neq j$ et l'identité si $v = j$. On a $\tau_u, \tau_v \in H$ et donc aussi $(\tau_u\tau_v)(i\ j)(\tau_u\tau_v)^{-1} = (u\ v) \in H$. Finalement $H$ contient toutes les transpositions; c'est donc $S_n$. Le groupe $H$ est maximal.

(c) *Montrer que si $1 < k < n/2$, l'action naturelle de $S_n$ sur les parties de $\{1, \ldots, n\}$ à $k$ éléments est primitive mais pas 2-transitive.*

**Correction**: Le groupe $\mathcal{G}_I$ est le fixateur de $I$ dans l'action de $S_n$ sur les parties de $\{1, \ldots, n\}$ à $k$ éléments. On sait que la maximalité de ce groupe correspond à la primitivité de l'action.

Par contre, l'action n'est pas 2-transitive puisque deux parties à $k$ éléments disjointes (il en existe puisque $k < n/2$) ne peuvent être transformées *via* un élement de $S_n$ en deux parties distinctes non disjointes.

(d) *On prend ici $n = 4$. Montrer que le sous-groupe $H \subset S_n$ engendré par $\alpha = (1\,2)$ et $\omega = (1\,3\,2\,4)$ est isomorphe au groupe diédral d'ordre 8 et que, pour $I = \{1, 2\}$, le sous-groupe $\mathcal{G}_I \subset S_4$ n'est pas maximal.*

**Correction**: On a $\alpha\omega\alpha^{-1} = (2\ 3\ 1\ 4) = \omega^{-1}$. Cette condition, jointe à $\omega^4 = 1 = \alpha^2$ est une présentation du groupe diédral d'ordre 8.

On remarque ensuite que, pour $I = \{1, 2\}$, on a $\mathcal{G}_I \subset H$. En effet, d'après la question (a), $\mathcal{G}_I \simeq S_2 \times S_2$ est engendré par $\alpha = (1\ 2)$ et $\beta = (3\ 4)$. Or $\alpha$ et $\beta = \omega\alpha\omega^{-1}$ sont dans $H = <\alpha, \omega>$. De plus $H$ étant d'ordre 8 est différent de $\mathcal{G}_I$ qui est d'ordre 4 et de $S_4$ qui est d'ordre 24. Dans ce cas le groupe $\mathcal{G}_I$ n'est donc pas maximal.

# UNIVERSITÉ LILLE 1

Enseignants: **P. DÈBES, D. MARKOUCHEVITCH, J.-F. ROBINET**
Filière: **Master 1 - Semestre 1**
Matière: **Algèbre approfondie**
Année universitaire: **2005/2006**
Épreuve: **Examen - 1ère session - janvier**
Date: **mercredi 11 janvier 2006 de 14h à 17h**
Lieu: **Bâtiment A4**
Durée de l'épreuve: **3 heures**

---

**Ni calculatrices ni documents ni téléphone portable.**
**Le barème est donné à titre indicatif.**
**Chacune des deux parties devra être rédigée sur une copie différente.**

---

## PARTIE I

**Exercice 1 [9,5 pts]:** (a) Montrer que les groupes d'ordre $35^2$ sont abéliens.
(Indication: on montrera d'abord qu'ils sont nilpotents).

(b) Déterminer tous les groupes abéliens d'ordre $35^2$ (à isomorphisme près).

Soit $G$ un groupe d'ordre $2 \cdot 35^2$.

(c) Montrer que $G$ possède un unique 5-sous-groupe de Sylow $\mathcal{S}_5$.

Soit $\mathcal{S}_7$ un 7-sous-groupe de Sylow de $G$.

(d) Montrer que le sous-groupe de $G$ engendré par $\mathcal{S}_5$ et $\mathcal{S}_7$ est égal à $\mathcal{S}_5\mathcal{S}_7$ et qu'il est distingué dans $G$.

(e) Montrer que $\mathcal{S}_7$ est un sous-groupe caractéristique de $\mathcal{S}_5\mathcal{S}_7$.

(f) Déduire de "$\mathcal{S}_7$ caractéristique dans $\mathcal{S}_5\mathcal{S}_7$" et "$\mathcal{S}_5\mathcal{S}_7$ distingué dans $G$" que $\mathcal{S}_7$ est distingué dans $G$.

(g) Montrer que $G$ est résoluble. Déterminer sa longueur et l'ensemble de ses facteurs.

(h) Montrer que $G$ est nilpotent si et seulement s'il possède un unique 2-sous-groupe de Sylow et que dans ce cas il est abélien; indiquer alors toutes les possibilités pour $G$ (à isomorphisme près). Donner un exemple où $G$ n'est pas nilpotent.

## PARTIE II

**Question de cours [3 pts]**: Soit $G$ un groupe abélien fini d'ordre $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, où $p_1, \ldots, p_r$ sont des nombres premiers distincts et $\alpha_1, \ldots, \alpha_r$ des entiers $\geq 1$. Pour $i = 1, \ldots, r$, on note $T_i$ le noyau de l'homomorphisme $m_i : G \to G$ défini par $m_i(x) = p_i^{\alpha_i} x$ ($x \in G$). Montrer que $G$ est isomorphe au produit direct $T_1 \times \cdots \times T_r$ et que $T_1, \ldots, T_r$ sont les sous-groupes de Sylow de $G$.

.../...

**Exercice 2 [7,5 pts] :** Soit $G$ un $p$-groupe fini, d'ordre $p^r$ avec $p$ premier et $r \geq 1$.

(a) Montrer qu'un sous-groupe propre (c'est-à-dire différent de $G$) est maximal si et seulement s'il est d'ordre $p^{r-1}$. (Pour la partie directe, on invoquera un théorème du cours).

(b) Montrer que si $\rho : G \to S_n$ est une action primitive, alors $n = p$ et $|G/\ker(\rho)| = p$.

(c) Déterminer toutes les actions $\rho : G \to S_n$ primitives et fidèles.

(d) Montrer que si $M$ est un sous-groupe propre maximal de $G$, alors $M$ est distingué dans $G$ et $G/M \simeq \mathbb{Z}/p\mathbb{Z}$.
(Indication: on pourra montrer en utilisant (b) que $M$ est égal au noyau de l'action de $G$ par translation à gauche sur les classes à gauche de $G$ modulo $M$).

(e) Déduire de (d) que tout sous-groupe propre maximal $M$ de $G$ contient le groupe dérivé $D(G)$ de $G$ et que $M/D(G)$ est un sous-groupe propre maximal de $G/D(G)$.

(f) Montrer qu'il existe une correspondance bijective entre l'ensemble des sous-groupes propres maximaux de $G$ et l'ensemble des sous-groupes propres maximaux de $G/D(G)$.

# UNIVERSITÉ LILLE 1

Enseignants: **P. DÈBES, D. MARKOUCHEVITCH, J.-F. ROBINET**
Filière: **Master 1 - Semestre 1**
Matière: **Algèbre approfondie**
Année universitaire: **2005/2006**
Épreuve: **examen - 2ème session - février**
Date: **Février 2006**
Durée de l'épreuve: **3 heures**

---

**Ni calculatrices ni documents ni téléphone portable.**
**Le barème est donné à titre indicatif.**

---

**Question de cours [3,5 pts]**: Montrer que dans un groupe fini nilpotent $G$, aucun sous-groupe propre $H$ ne peut être égal à son normalisateur $\mathrm{Nor}_G(H)$ et en déduire que tous les sous-groupes de Sylow sont distingués dans $G$.

**Exercice 1 [5,5 pts] :** Soient $G \subset S_n$ un sous-groupe transitif de $S_n$; on note $\rho : G \hookrightarrow S_n$ l'inclusion canonique. Pour $i = 1, \dots, n$, soit $G(i)$ le fixateur de $i$.

(a) Montrer que les sous-groupes $G(1), \dots G(n)$ sont des sous-groupes conjugués de $G$ (c'est-à-dire, pour $i, j \in \{1, \dots, n\}$, il existe $\gamma \in G$ tel que $G(j) = \gamma G(i)\gamma^{-1}$).

On suppose $G$ abélien.

(b) Montrer que $n = |G|$ et que pour tout $i \in \{1, \dots, n\}$ il existe un unique élément $g_i \in G$ tel que $\rho(g_i)(1) = i$.

(c) Montrer que si $\mathcal{G} : \{1, \dots, n\} \to G$ est la bijection définie par $\mathcal{G}(i) = g_i$ $(i = 1, \dots, n)$, alors on a $\mathcal{G} \circ \rho(g)(i) = gg_i$ pour tout $i = 1, \dots, n$ et en déduire que $\rho$ est équivalente à l'action par translation sur les éléments de $G$.

**Exercice 2 [4,5 pts] :** Dans le groupe symétrique $S_9$ on considère les permutations

$$\begin{cases} \omega_1 = (1\,2\,3) \\ \omega_2 = (4\,5\,6) \\ \omega_3 = (7\,8\,9) \\ \tau = (1\,4\,7)(2\,5\,8)(3\,6\,9) \end{cases}$$

(a) Montrer que $\omega_1, \omega_2, \omega_3$ engendrent un groupe $\Omega$ isomorphe à $(\mathbb{Z}/3\mathbb{Z})^3$.

(b) Montrer que le sous-groupe $G \subset S_9$ engendré par $\omega_1, \omega_2, \omega_3$ et $\tau$ est isomorphe au produit semi-direct de $(\mathbb{Z}/3\mathbb{Z})^3$ par $\mathbb{Z}/3\mathbb{Z}$ et qu'il agit transitivement sur $\{1, \dots, 9\}$.

**Exercice 3 [6,5 pts] :** (a) Montrer que tout groupe $K$ d'ordre <u>divisant</u> $2.3^m$ $(m \geq 0)$ est résoluble.

(b) Montrer que tout groupe $H$ d'ordre <u>divisant</u> $2.3^2.7$ est résoluble.

Soit $G$ un groupe d'ordre $2.3^m.7$ $(m \geq 0)$.

(c) Montrer que si le nombre $n$ de 3-sous-groupes de Sylow de $G$ est $> 1$, alors l'action $\rho : G \to S_n$ par conjugaison sur les 3-sous-groupes de Sylow a pour groupe image $\rho(G)$ un sous-groupe de $S_n$ d'ordre divisible par 7 et divisant $2.3^2.7$.

(d) Montrer que $G$ est résoluble.

# UNIVERSITÉ LILLE 1

Enseignants: **G. BHOWMIK, P. DÈBES, J.-F. ROBINET**
Filière: **Master 1 - Semestre 1**
Matière: **Algèbre approfondie**
Année universitaire: **2006/2007**
Épreuve: **Partiel**
Date: **mercredi 22 novembre 2006 de 10h à 12h**
Lieu: **Bâtiment A5**
Durée de l'épreuve: **2 heures**

---

**Ni calculatrices ni documents ni téléphone portable.**
**Le barème est donné à titre indicatif.**
**Chacune des deux parties devra être rédigée sur une copie différente.**

---

## PARTIE I

**Questions de cours [3,5 pts]** : (a) Donner la définition d'action primitive et d'action imprimitive d'un groupe $G$ sur un ensemble fini $X$.

(b) Montrer que si $H$ est un sous-groupe d'un groupe fini $G$, alors l'action de $G$ sur lui-même par translation à gauche permute les classes à gauche de $G$ modulo $H$.

(c) Montrer que l'action d'un groupe fini $G$ sur lui-même par translation à gauche est primitive si et seulement si l'ordre de $G$ est premier.

**Exercice 1 [5 pts] :** Montrer que si $p$ est un nombre premier fixé, il n'existe, à isomorphisme près, qu'un nombre fini de groupes simples d'ordre $(p+1)p^n$ $(n \in \mathbb{N})$.
(Indication: on pourra commencer par déterminer le nombre de $p$-Sylows d'un tel groupe puis faire agir le groupe par conjugaison sur l'ensemble de ces $p$-Sylows).

## PARTIE II

**Exercice 2 [11,5 pts] :** (a) Montrer que les éléments d'ordre 3 du groupe alterné $A_6$ se répartissent en deux classes de conjugaison de 40 éléments chacune.

(b) En déduire que pour tout $\alpha \in A_6$ d'ordre 3, le sous-groupe $\mathrm{Cen}_{A_6}(\alpha)$ des éléments de $A_6$ commutant à $\alpha$ est d'ordre 9.

(c) Montrer que tout 3-sous-groupe de Sylow $S$ de $A_6$ est isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et que pour tout $\alpha \in S \setminus \{1\}$, on a $S = \mathrm{Cen}_{A_6}(\alpha)$. En déduire que les 3-sous-groupes de Sylow sont d'intersection deux à deux réduite à $\{1\}$.

(d) Montrer que pour toute partition $\mathcal{P}$ de $\{1, \ldots, 6\}$ en deux sous-ensembles $\{a, b, c\}$ et $\{d, e, f\}$, le sous-groupe $\mathcal{S}_\mathcal{P}$ engendré par les 3-cycles $\sigma = (a\,b\,c)$ et $\tau = (d\,e\,f)$ est un 3-sous-groupe de Sylow de $A_6$. Montrer que quand $\mathcal{P}$ décrit toutes les partitions comme ci-dessus, on obtient 10 sous-groupes $\mathcal{S}_\mathcal{P}$.

(e) Déterminer le nombre de 3-sous-groupes de Sylow de $A_6$ et en déduire que tout 3-sous-groupe de Sylow de $A_6$ est de la forme $\mathcal{S}_\mathcal{P}$.

# UNIVERSITÉ LILLE 1

## CORRIGÉ DU PARTIEL (M1-S1-2006/2007-Algèbre approfondie)

**Questions de cours [3,5 pts]** : (a) *Donner la définition d'action primitive et d'action imprimitive d'un groupe $G$ sur un ensemble fini $X$.*

**Correction**: Une action transitive $\rho : G \to \mathrm{Per}(X)$ d'un groupe $G$ sur un ensemble $X$ est dite *imprimitive* s'il existe une partition $X = \bigsqcup_{i\in I} X_i$ de $X$ non triviale (c'est-à-dire $1 < \mathrm{card}(X_i) < \mathrm{card}(X), i \in I$) qui soit stable par l'action $\rho$ (c'est-à-dire, $\rho(g)\left(\{X_i \mid i \in I\}\right) = \{X_i \mid i \in I\}$ pour tout $g \in G$). Une action transitive est dite *primitive* si l'opposé est vrai.

(b) *Montrer que si $H$ est un sous-groupe d'un groupe fini $G$, alors l'action de $G$ sur lui-même par translation à gauche permute les classes à gauche de $G$ modulo $H$.*

**Correction**: Notons $G/.H$ l'ensemble des classes à gauche de $G$ modulo $H$. Pour tous $g, x \in G$ et $h \in H$, la classe $(gxh)H$ ne dépend pas de $h \in H$. L'action de $G$ par translation à gauche sur lui-même induit donc une application $\gamma_g : xH \to gxH$ de $G/.H$ dans lui-même, qui est bijective: sa réciproque est $\gamma_{g^{-1}}$.

(c) *Montrer que l'action d'un groupe fini $G$ sur lui-même par translation à gauche est primitive si et seulement si l'ordre de $G$ est premier.*

**Correction**: L'action d'un groupe $G$ sur lui-même par translation à gauche est transitive. D'après le (a) et le (b), si elle est primitive, le cardinal des classes à gauche de $G$ modulo tout sous-groupe $H$, c'est-à-dire $|G|/|H|$, vaut 1 ou $|G|$, c'est-à-dire, $G$ n'a d'autre sous-groupe que $H = \{1\}$ et $H = G$. Cela n'est possible que si $G$ est cyclique (engendré par tout élément $\neq 1$), et de plus son ordre doit être premier. Inversement, les parties $X_i$ $(i \in I)$ d'une partition $\bigsqcup_{i\in I} X_i$ de $G$ stable par l'action de $G$ étant nécessairement de même cardinal, une telle partition est automatiquement triviale si $|G|$ est premier.

**Exercice 1 [5 pts] :** *Montrer que si $p$ est un nombre premier fixé, il n'existe, à isomorphisme près, qu'un nombre fini de groupes simples d'ordre $(p+1)p^n$ $(n \in \mathbb{N})$.*

**Correction**: Soit $G$ un groupe simple d'ordre $(p+1)p^n$. Le nombre de $p$-Sylows est congru à 1 modulo $p$ et divise $p+1$; c'est donc 1 ou $p+1$. Mais comme $G$ est simple ce ne peut être 1 car alors l'unique $p$-Sylow serait un sous-groupe distingué non trivial; c'est donc $p+1$. La conjugaison sur les $p$-Sylow induit un morphisme $G \to S_{p+1}$ qui est forcément injectif: en effet le noyau, sous-groupe distingué de $G$ et qui ne peut être tout $G$ car l'action étant transitive n'est pas triviale, est forcément le groupe $\{1\}$. On obtient que $(p+1)p^n$ divise l'ordre $(p+1)!$ du groupe $S_{p+1}$, ce qui n'est possible que pour $n = 1$. Il n'y a qu'un nombre fini de groupes correspondants.

**Exercice 2 [11,5 pts] :** (a) *Montrer que les éléments d'ordre 3 du groupe alterné $A_6$ se répartissent en deux classes de conjugaison de 40 éléments chacune.*

**Correction**: Les éléments d'ordre 3 de $A_6$ sont les 3-cycles et les produits de 2 3-cycles à supports disjoints.

On sait d'après le cours que l'ensemble $\mathbf{3}^1$ des 3-cycles est une classe de conjugaison de $S_6$. Si $\sigma, \sigma' \in \mathbf{3}^1$, il existe $\omega \in S_6$ tel que $\sigma' = \omega\sigma\omega^{-1}$. Si $\omega \in A_6$, alors $\sigma$ et $\sigma'$ sont conjugués dans $A_6$. Si $\omega \notin A_6$, alors, pour $\omega' = \omega\,(a\,b)$ avec $a, b$ distincts hors du support de $\sigma$, on a $\sigma' = \omega'\sigma(\omega')^{-1}$ et $\omega' \in A_6$. L'ensemble $\mathbf{3}^1$ est donc une classe de conjugaison de $A_6$. Elle possède $\binom{6}{3} \times 2 = 40$ éléments.

De même l'ensemble $\mathbf{3}^2$ des produits de 2 3-cycles à supports disjoints est une classe de conjugaison de $S_6$. Si $\sigma = (a\,b\,c)(d\,e\,f)$ et $\sigma' = (a'\,b'\,c')(d'\,e'\,f')$ sont dans $\mathbf{3}^2$, il existe $\omega \in S_6$ tel que $\sigma' = \omega\sigma\omega^{-1}$. Si $\omega \in A_6$, alors $\sigma$ et $\sigma'$ sont conjugués dans $A_6$. Si $\omega \notin A_6$, alors, pour $\omega' = (a'\,d')(b'\,e')(c'\,f')\,\omega$, on a $\sigma' = \omega'\sigma(\omega')^{-1}$ et $\omega' \in A_6$. L'ensemble $\mathbf{3}^2$ est donc une classe de conjugaison de $A_6$. Elle possède $\binom{5}{2} \times 2 \times 2 = 40$ éléments.

(b) *En déduire que pour tout $\alpha \in A_6$ d'ordre 3, le sous-groupe $\mathrm{Cen}_{A_6}(\alpha)$ des éléments de $A_6$ commutant à $\alpha$ est d'ordre 9.*

**Correction**: Si $\mathrm{Cl}(\alpha)$ est la classe de conjugaison de $\alpha$ dans $A_6$, on a $\mathrm{card}(\mathrm{Cl}(\alpha)) = |A_6|/|\mathrm{Cen}_{A_6}(\alpha)|$, d'où, d'après (a), $|\mathrm{Cen}_{A_6}(\alpha)| = |A_6|/40 = 9$.

(c) *Montrer que tout 3-sous-groupe de Sylow $S$ de $A_6$ est isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et que pour tout $\alpha \in S \setminus \{1\}$, on a $S = \mathrm{Cen}_{A_6}(\alpha)$. En déduire que les 3-sous-groupes de Sylow sont d'intersection deux à deux réduite à $\{1\}$.*

**Correction**: Le groupe $A_6$ étant d'ordre $360 = 2^3.3^2.5$, les 3-Sylow sont des sous-groupes d'ordre $3^2$; ils sont nécessairement abéliens. Comme $A_6$ n'a pas d'éléments d'ordre 9, il n'y a dans chaque 3-Sylow $S$ que des éléments d'ordre $\leq 3$. L'un des deux arguments suivants permet de conclure:

argument 1: d'après le théorème de classification des groupes abéliens de type fini, les groupes abéliens d'ordre $3^2$ sont, à isomorphisme près, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/9\mathbb{Z}$. La seconde possibilité a été exclue.

argument 2: soient $\sigma, \tau \in S \setminus \{1\}$ tels que $\tau$ n'est pas dans le groupe engendré par $\sigma$, c'est-à-dire, $\tau \neq 1, \sigma, \sigma^2$. La correspondance $(n, m) \in \mathbb{Z}^2 \to \sigma^n\tau^m$ induit une application $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \to S$ bien définie (car $\sigma$ et $\tau$ d'ordre 3); c'est de plus un morphisme (car $\sigma$ et $\tau$ commutent), injectif (car les groupes engendrés par $\sigma$ et $\tau$ ont une intersection réduite à $\{1\}$) et donc bijectif (puisque $|S| = 9 = |\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}|$.

Fixons un 3-Sylow $S$ et $\alpha \in S \setminus \{1\}$. Comme $S$ est abélien, on a $S \supset \mathrm{Cen}_{A_6}(\alpha)$. Mais d'après ce qui précède, ces deux groupes dont de même ordre: 9; ils sont donc égaux.

Si $S'$ est un 3-Sylow distinct de $S$, alors $S \cap S' = \{1\}$ car sinon, pour $\alpha \in S \cap S' \setminus \{1\}$, on a $S = \mathrm{Cen}_{A_6}(\alpha) = S'$.

(d) *Montrer que pour toute partition $\mathcal{P}$ de $\{1, \ldots, 6\}$ en deux sous-ensembles $\{a, b, c\}$ et $\{d, e, f\}$, le sous-groupe $\mathcal{S}_\mathcal{P}$ engendré par les 3-cycles $\sigma = (a\,b\,c)$ et $\tau = (d\,e\,f)$ est un 3-sous-groupe de Sylow de $A_6$. Montrer que quand $\mathcal{P}$ décrit toutes les partitions comme ci-dessus, on obtient 10 sous-groupes $\mathcal{S}_\mathcal{P}$.*

**Correction**: On montre comme dans l'argument 2 ci-dessus que la correspondance $(n, m) \in \mathbb{Z}^2 \to \sigma^n\tau^m$ induit un isomorphisme $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \to \mathcal{S}_\mathcal{P}$ (comme ci-dessus, les éléments $\sigma$ et $\tau$ de cette question sont d'ordre 3, commutent et engendrent des groupes d'intersection $\{1\}$; la surjectivité provient ici de la définition de $\mathcal{S}_\mathcal{P}$). Le groupe $\mathcal{S}_\mathcal{P}$ est donc d'ordre 9 et donc un 3-Sylow de $A_6$.

Le nombre de partitions possibles $\mathcal{P}$ est $\binom{5}{2} = 10$. Si $\mathcal{P} = \{\{a, b, c\}, \{d, e, f\}\}$ et $\mathcal{P}' = \{\{a', b', c'\}, \{d', e', f'\}\}$ sont deux partitions distinctes, alors $\{a, b, c\}$ est distinct de $\{a', b', c'\}$ et de $\{d', e', f'\}$. Il en résulte que $(a\,b\,c)\,(a'\,b'\,c') \neq (a'\,b'\,c')(a\,b\,c)$ et donc que $(a'\,b'\,c') \notin \mathrm{Cen}_{A_6}((a\,b\,c)) = \mathcal{S}_\mathcal{P}$. D'où $\mathcal{S}_\mathcal{P} \neq \mathcal{S}_{\mathcal{P}'}$. Il y a donc 10 groupes distincts $\mathcal{S}_\mathcal{P}$.

(e) *Déterminer le nombre de 3-sous-groupes de Sylow de $A_6$ et en déduire que tout 3-sous-groupe de Sylow de $A_6$ est de la forme $\mathcal{S}_\mathcal{P}$.*

**Correction**: Tout 3-Sylow de $A_6$ contient 8 éléments d'ordre 3. Comme les 3-Sylow sont d'intersection deux à deux réduite à $\{1\}$ et qu'il y a au total 80 éléments d'ordre 3, il y a exactement 10 3-Sylow; ce sont les 10 groupes $\mathcal{S}_\mathcal{P}$.

# UNIVERSITÉ LILLE 1

Enseignants: **G. BHOWMIK, P. DÈBES, J.-F. ROBINET**
Filière: **Master 1 - Semestre 1**
Matière: **Algèbre approfondie**
Année universitaire: **2006/2007**
Épreuve: **Examen - 1ère session - janvier**
Date: **le 11 janvier 2007 à 8h**
Lieu: **C1 Kuhlmann**
Durée de l'épreuve: **3 heures**

---

**Ni calculatrices ni documents ni téléphone portable.**

**Le barème est donné à titre indicatif.**

**Chacune des deux parties devra être rédigée sur une copie différente.**

---

## PARTIE I

**Question de cours [3 pts]:** Donner la définition de "groupe résoluble". Montrer que si $H$ est un sous-groupe distingué d'un groupe $G$ tel que $H$ et $G/H$ soient résolubles, alors $G$ est résoluble.

**Exercice 1 [3 pts]:** Soit $p$ un nombre premier. Déterminer les $p$-sous-groupes de Sylow du groupe symétrique $S_p$ et établir que $(p-1)!+1$ est congru à 1 modulo $p$.

**Exercice 2 [4,5 pts]:** (a) Soient $\mathcal{G}$ un groupe et $\mathcal{H}$ un sous-groupe inclus dans le centre $Z(\mathcal{G})$. On suppose que $\mathcal{G}/\mathcal{H}$ est monogène (c'est-à-dire, engendré par un élément). Montrer que $\mathcal{G}$ est abélien.

Soient $G$ un groupe et $(C_i(G))_{i\geq 0}$ sa suite centrale descendante. On suppose que $G/C_1(G)$ est monogène.

(b) Montrer qu'on a $C_1(G) = C_2(G)$. (Indication: on pourra, pour une des deux inclusions, appliquer le (a) au groupe $\mathcal{G} = G/C_2(G)$ ).

(c) En déduire que si $G$ est nilpotent, alors $C_1(G) = \{1\}$ et $G$ est monogène.

## PARTIE II

**Exercice 3 [3 pts]:** Montrer que les assertions suivantes sont équivalentes:

(i) Tout groupe fini d'ordre impair est résoluble.

(ii) Tout groupe fini simple non abélien est d'ordre pair.

**Exercice 4 [6,5 pts] :** (a) Soit $p \geq 5$ un nombre premier. Montrer qu'un groupe $G$ d'ordre $4p$ est isomorphe au produit semi-direct $\mathbb{Z}/p\mathbb{Z} \rtimes S$ de $\mathbb{Z}/p\mathbb{Z}$ et d'un groupe $S$ d'ordre 4.

.../...

**Exercice 4** (suite)

Soit $\mathcal{G}$ un groupe fini d'ordre 380.

(b) Montrer que $\mathcal{G}$ possède un 19-sous groupe de Sylow distingué ou un 5-sous groupe de Sylow distingué.

(c) Déterminer la longueur du groupe $\mathcal{G}$ et préciser l'ensemble des facteurs d'une suite de composition. Le groupe $\mathcal{G}$ est-il résoluble?

(d) Quelles sont les possibilités pour le groupe $\mathcal{G}$ si on le suppose abélien?

# UNIVERSITÉ LILLE 1

Enseignants: **G. BHOWMIK, P. DÈBES, J.-F. ROBINET**
Filière: **Master 1 - Semestre 1**
Matière: **Algèbre approfondie**
Année universitaire: **2006/2007**
Épreuve: **Examen - 2ème session**
Date: **jeudi 8 mars à 8h**
Lieu: **Bâtiment SN1 Amphi Gosselet**
Durée de l'épreuve: **3 heures**

---

**Ni calculatrices ni documents ni téléphone portable.**
**Le barème est donné à titre indicatif.**

---

**Question de cours [3 pts]**: Donner la définition de la longueur d'un groupe. En utilisant des résultats du cours, montrer que la longueur d'un groupe d'ordre $p^n$ avec $p$ premier et $n \geq 1$ est $n$. (On énoncera de façon précise les résultats du cours invoqués).

**Exercice 1 [2,5 pts]**: Les groupes

$$\mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/168\mathbb{Z}$$

sont-ils isomorphes? On déterminera leurs facteurs invariants.

**Exercice 2 [4,5 pts]:** (a) Soit $H$ un groupe d'ordre 48 possédant trois 2-sous-groupes de Sylow. Montrer que le noyau de l'action $\rho : H \to S_3$ de $H$ par conjugaison sur l'ensemble de ses 2-sous-groupes de Sylow est un sous-groupe distingué d'ordre 8.
(Indication: on pourra étudier l'ordre du groupe image $\rho(H)$ et chercher à éliminer les cas où celui-ci vaudrait 1, 2 ou 3).

(b) Montrer que tout groupe d'ordre 624 est résoluble.
(Indication: on pourra commencer par étudier les 13-sous-groupes de Sylow).

**Exercice 3 [4 pts]**: Soit $G$ le sous-groupe du groupe symétrique $S_5$ engendré par le 3-cycle (1 2 3) et les transpositions (4 5) et (1 2).

(a) Montrer que le groupe $G$ est isomorphe au produit direct $S_3 \times \mathbb{Z}/2\mathbb{Z}$.

(b) Le groupe $G$ est-il abélien? nilpotent? résoluble?

.../...

**Exercice 4 [6 pts]**: Soit $n \geq 1$ un entier. On note $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ le groupe des automorphismes du groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe multiplicatif des éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

(a) Montrer que l'application $\Phi : \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z}$ qui, à $\chi \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ associe $\chi(1) \in \mathbb{Z}/n\mathbb{Z}$ induit un isomorphisme de groupes $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})^\times$.

(b) Soient $a \geq 1$ un entier et $\rho : \mathbb{Z}/a\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ une action de $\mathbb{Z}/a\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$. Montrer qu'il existe $u \in \mathbb{Z}/n\mathbb{Z}$ tel que

$$\begin{cases} u^a = 1 \\ \rho(h)(m) = u^h m \quad (m \in \mathbb{Z}/n\mathbb{Z}, h \in \mathbb{Z}/a\mathbb{Z}) \end{cases}$$

(c) Déterminer à isomorphisme près tous les sous-groupes d'ordre 52 possédant un élément d'ordre 4.
(Indication: on pourra commencer par montrer qu'un tel groupe possède un sous-groupe distingué d'ordre 13).

# UNIVERSITÉ LILLE 1

Enseignants: **N. BORNE, P. DÈBES, G. TUYNMAN**
Filière: **Licence - Semestre 5**
Matière: **M 308**
Année universitaire: **2008/2009**
Épreuve: **Partiel**
Date: **vendredi 14 novembre à 10h30**
Lieu: **Bâtiment A5**
Durée de l'épreuve: **2 heures**

---

**Ni calculatrices ni documents ni téléphone portable.**
**Une grande importance sera accordée à la rédaction.**
**Le barème est donné à titre indicatif.**

---

**Question de cours [3,5 pts]**: Donner les définitions d'action imprimitive, d'action primitive, d'action 2-transitive et montrer que si une action est 2-transitive, alors elle est primitive.

**Exercice 1 [3,5 pts]:** Les permutations suivantes sont-elles conjuguées dans le groupe symétrique $S_7$?

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 2 & 7 & 6 & 1 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 5 & 6 & 7 & 4 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 6 & 7 & 4 & 3 & 1 \end{pmatrix}$$

Pour celles qui le sont, écrire une relation de conjugaison $\sigma_j = \omega\, \sigma_i\, \omega^{-1}$. Ces permutations sont-elles conjuguées par un élément du groupe alterné $A_7$?

**Exercice 2 [3,5 pts]**: On note 1, $I$, $J$, $K$ les matrices $2 \times 2$ à coefficients complexes

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \; I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \; J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \; K = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

(avec $i \in \mathbb{C}$ tel que $i^2 = -1$)

et on considère le groupe $H_8$ composé des 8 éléments $\pm 1, \pm I, \pm J, \pm K$ et dont la table de multiplication est déterminée par les relations $I^2 = J^2 = K^2 = -1$, $IJ = -JI = K$, $JK = -KJ = I$ et $KI = -IK = J$.

(a) Déterminer le centre $Z(H_8)$ du groupe $H_8$ et montrer que tous les éléments de $H_8 \setminus Z(H_8)$ sont d'ordre 4.

(b) Montrer que tous les sous-groupes de $H_8$ sont distingués.

**T.S.V.P.**

**Exercice 3 [6 pts]**: (a) Montrer que dans un groupe fini $G$, si $H$ et $K$ sont deux sous-groupes distincts d'ordre égaux à un nombre premier $p$, alors $H \cap K = \{1\}$.

(b) Montrer qu'un groupe abélien $G$ d'ordre 55 est nécessairement cyclique.
(Indication: on pourra commencer par montrer que le groupe possède un élément d'ordre 5 et un élément d'ordre 11).

(c) Montrer que le groupe symétrique $S_{11}$ n'a pas de sous-groupe abélien d'ordre 55.

(d) On note $H \subset S_{11}$ le sous-groupe engendré par le 11-cycle $\alpha = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11)$ et $K \subset S_{11}$ le sous-groupe engendré par $\beta = (2\ 5\ 6\ 10\ 4)\ (3\ 9\ 11\ 8\ 7)$. Vérifier que $\beta\alpha\beta^{-1} = \alpha^4$ et en déduire que $H$ est distingué dans le groupe $\langle \alpha, \beta \rangle$ et que l'ensemble $HK$ est un sous-groupe de $S_{11}$, d'ordre 55.

**Exercice 4 [3,5 pts]**: (a) Montrer qu'un sous-groupe $G$ de $S_n$ tel que $G \cap A_n = \{1\}$ est nécessairement abélien. (Indication: pour tout $g \in S_n$, on a $g^2 \in A_n$).

(b) Montrer que les sous-groupes simples de $S_n$ sont soit contenus dans $A_n$ soit d'ordre 2.

# UNIVERSITÉ LILLE 1

Enseignants: **N. BORNE, P. DÈBES, G. TUYNMAN**
Filière: **Licence - Semestre 5**
Matière: **M 308**
Année universitaire: **2008/2009**
Épreuve: **Partiel**
Date: **vendredi 14 novembre de 10h30 à 12h30**

---

## CORRIGÉ

---

**Question de cours [3,5 pts]**: *Donner les définitions d'action imprimitive, d'action primitive, d'action 2-transitive et montrer que si une action est 2-transitive, alors elle est primitive.*

**Correction**: Soit $\rho : G \to \mathrm{Per}(X)$ une action d'un groupe $G$ sur un ensemble $X$.

Cette action est dite imprimitive si elle est transitive et satisfait la condition:

(*) Il existe une partition de $X$ en sous-ensembles $X_i$ $(i \in I)$ non triviale [c'est-à-dire: $\mathrm{card}(I) \geq 2$ et $\mathrm{card}(X_i) \geq 2$ $(i \in I)$] qui soit invariante par l'action [c'est-à-dire: $\rho(g)(\{X_i \,|\, i \in I\}) = \{X_i \,|\, i \in I\}$ pour tout $g \in G$].

L'action est dite primitive si elle est transitive et ne satisfait pas la condition (*).

Elle est dite 2-transitive si pour tous couples $(a,b),(a',b') \in X^2$ avec $a \neq b$ et $a' \neq b'$, il existe $g \in G$ tel que $\rho(g)(a) = a'$ et $\rho(g)(b) = b'$.

Supposons que l'action $\rho$ soit 2-transitive. En particulier elle est transitive. Fixons $i \in I$, $a$, $b$ distincts dans $X_i$, $a' \in X_i$ et $b' \notin X_i$. Alors il existe $g \in G$ tel que $\rho(g)(a) = a'$ et $\rho(g)(b) = b'$. Cela ne peut avoir lieu sous la condition (*).

**Exercice 1 [3,5 pts]:** *Les permutations suivantes sont-elles conjuguées dans le groupe symétrique $S_7$?*

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 2 & 7 & 6 & 1 \end{pmatrix} \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 5 & 6 & 7 & 4 \end{pmatrix} \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 6 & 7 & 4 & 3 & 1 \end{pmatrix}$$

*Pour celles qui le sont, écrire une relation de conjugaison $\sigma_j = \omega\, \sigma_i\, \omega^{-1}$. Ces permutations sont-elles conjuguées par un élément du groupe alterné $A_7$?*

**Correction**: On décompose $\sigma_1$, $\sigma_2$ et $\sigma_3$ en produit de cycles à supports disjoints:

$$\sigma_1 = (1\ 3\ 5\ 7)\ (2\ 4)\ ,\ \sigma_2 = (4\ 5\ 6\ 7)\ (1\ 3)\ ,\ \sigma_3 = (1\ 2\ 5\ 4\ 7)\ (3\ 6)$$

La forme de ces décompositions indique que $\sigma_1$ et $\sigma_2$ sont conjuguées dans $S_7$, mais ne sont pas conjuguées à $\sigma_3$. Plus précisément, on peut écrire: $\sigma_2 = \omega\sigma_1\omega^{-1}$ où $\omega$ vérifie: $(\omega(1)\ \omega(3)\ \omega(5)\ \omega(7))\ (\omega(2)\ \omega(4)) = (4\ 5\ 6\ 7)\ (1\ 3)$. La permutation $\omega = (1\ 4\ 3\ 5\ 6\ 2)$ convient mais aussi $\omega = (1\ 4)\ (2\ 3\ 5\ 6)$. La seconde est dans $A_7$; $\sigma_1$ et $\sigma_2$, qui sont dans $A_7$, sont également conjugués dans $A_7$.

**Exercice 2 [3,5 pts]**: *On note 1, $I$, $J$, $K$ les matrices $2 \times 2$ à coefficients complexes*

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\ ,\ I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}\ ,\ J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\ K = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

*(avec $i \in \mathbb{C}$ tel que $i^2 = -1$)*

*et on considère le groupe $H_8$ composé des 8 éléments $\pm 1, \pm I, \pm J, \pm K$ et dont la table de multiplication est déterminée par les relations $I^2 = J^2 = K^2 = -1$, $IJ = -JI = K$, $JK = -KJ = I$ et $KI = -IK = J$.*

(a) *Déterminer le centre $Z(H_8)$ du groupe $H_8$ et montrer que tous les éléments de $H_8 \setminus Z(H_8)$ sont d'ordre* 4.

**Correction**: Les éléments 1 et $-1$ sont dans le centre et $\pm I, \pm J, \pm K$ n'y sont pas. D'où $Z(H_8) = \{1, -1\}$. Les formules $I^2 = J^2 = K^2 = -1 \neq 1$ et $(-1)^2 = 1$ montrent que $\pm I, \pm J, \pm K$ sont d'ordre 4.

(b) *Montrer que tous les sous-groupes de $H_8$ sont distingués.*

**Correction**: Les sous-groupes triviaux $\{1\}$ et $H_8$ sont distingués. Les autres sous-groupes sont soit d'ordre 4, auquel cas ils sont distingués car d'indice 2, soit d'ordre 2, auquel cas ils sont engendrés par un élément d'ordre 2, qui ne peut être que $-1$ et alors le sous-groupe engendré est le centre $Z(H_8)$ qui est distingué.

**Exercice 3 [6 pts]**: (a) *Montrer que dans un groupe fini $G$, si $H$ et $K$ sont deux sous-groupes distincts d'ordre égaux à un nombre premier $p$, alors $H \cap K = \{1\}$.*

**Correction**: L'ordre de $H \cap K$ divisant $p = |H|$, on a ou bien $|H \cap K| = 1$ et alors $H \cap K = \{1\}$, ou bien $|H \cap K| = p$ et alors $H \cap K = H$. Dans ce second cas, $H \subset K$, ce qui entraîne $H = K$ et contredit l'hypothèse.

(b) Montrer qu'un groupe abélien $G$ d'ordre 55 est nécessairement cyclique. (Indication: commencer par montrer que le groupe possède un élément d'ordre 5 et un d'ordre 11).

**Correction**: Supposons $G$ non cyclique. Les éléments de $G$ différents de 1 sont d'ordre 5 ou 11. S'ils étaient tous d'ordre 5, les sous-groupes qu'ils engendrent, auxquels on retire 1, formeraient une partition de $G \setminus \{1\}$ (d'après (a)). Cela n'est pas possible car $55 - 1 = 54$ n'est pas divisible par $5 - 1 = 4$. Il existe donc un élément $a$ d'ordre 11. De même, comme 54 n'est pas divisible par $11 - 1 = 10$, il existe un élément $b$ d'ordre 5. Mais le groupe étant abélien, l'élément $ab$ est d'ordre $\text{ppcm}(5, 11) = 55$, ce qui contredit l'hypothèse "$G$ non cyclique". Le groupe $G$ est donc cyclique.
**N.B.**: pour montrer l'existence d'un élément d'ordre 5 et celle d'un élément d'ordre 11, on peut aussi invoquer le théorème de Cauchy.

(c) *Montrer que le groupe symétrique $S_{11}$ n'a pas de sous-groupe abélien d'ordre* 55.

**Correction**: D'après (b), si $S_{11}$ a un sous-groupe abélien d'ordre 55, celui-ci est cyclique. Il existe un élément $\omega \in S_{11}$ d'ordre 55. Sa décomposition en cycles à support disjoints doit comprendre un 11-cycle et un 5-cycle, ce qui n'est pas possible, puisque $11 + 5 > 11$.

(d) *On note $H \subset S_{11}$ le sous-groupe engendré par le* 11*-cycle $\alpha = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11)$ et $K \subset S_{11}$ le sous-groupe engendré par $\beta = (2\ 5\ 6\ 10\ 4)\ (3\ 9\ 11\ 8\ 7)$. Vérifier que $\beta\alpha\beta^{-1} = \alpha^4$ et en déduire que $H$ est distingué dans le groupe $\langle \alpha, \beta \rangle$ et que l'ensemble $HK$ est un sous-groupe de $S_{11}$, d'ordre* 55.

**Correction**: La formule est immédiate. On en déduit que $H$ est distingué dans le groupe $\langle \alpha, \beta \rangle$. On sait alors que l'ensemble $HK$ est un groupe et que $HK/H \simeq K/H \cap K$. Comme $H \cap K = \{1\}$ (car $|H \cap K|$ divise 5 et 1), on obtient $|HK| = |H||K| = 55$.

**Exercice 4 [3,5 pts]**: (a) *Montrer qu'un sous-groupe $G$ de $S_n$ tel que $G \cap A_n = \{1\}$ est nécessairement abélien. (Indication: pour tout $g \in S_n$, on a $g^2 \in A_n$).*

**Correction**: Comme $A_n$ est distingué dans $S_n$ et d'indice 2, on $g^2 \in A_n$ pour tout $g \in S_n$. Pour tout $g \in G$, on a donc $g^2 \in G \cap A_n$ et donc $g^2 = 1$ d'après l'hypothèse. On sait que cela entraîne que $G$ est abélien.

(b) *Montrer que les sous-groupes simples de $S_n$ sont soit contenus dans $A_n$ soit d'ordre* 2.

**Correction**: Soit $G$ un sous-groupe simple de $S_n$. Le groupe $G \cap A_n$ est distingué dans $G$. On a donc $G \cap A_n = \{1\}$ ou $G \cap A_n = G$. Dans le premier cas, $G$ est abélien d'après (a), et comme il est simple, il est forcément cyclique d'ordre $p$, et donc contenu dans $A_n$ sauf si $p = 2$. Dans le second cas, $G \cap A_n = G$ donne aussi $G \subset A_n$.

# UNIVERSITÉ LILLE 1

Enseignants: **N. BORNE, P. DÈBES, G. TUYNMAN**
Filière: **Licence - Semestre 5**
Matière: **M 308**
Année universitaire: **2008/2009**
Épreuve: **Examen - 1ère session**
Date: **jeudi 8 janvier à 8h**
Lieu: **Bâtiment SN1 Amphi Malaquin**
Durée de l'épreuve: **3 heures**

---

**CHAQUE PARTIE SERA RÉDIGÉE SUR UNE COPIE DIFFÉRENTE**

---

**Ni calculatrices ni documents ni téléphone portable.**
**Une grande importance sera accordée à la rédaction.**
**Le barème est donné à titre indicatif.**

---

## PARTIE I

**Question de cours [3 pts]**: Soit $G$ un groupe fini d'ordre $p^n$, où $p$ est un nombre premier et $n \geq 0$ un entier. Montrer qu'il existe une suite de sous-groupes

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

telle que $|G_i| = p^i$ et $G_i$ est distingué dans $G$, $i = 0, 1, \ldots, n$. (On pourra utiliser sans le démontrer que le centre d'un $p$-groupe non trivial possède un élément d'ordre $p$).

En déduire que si $n \geq 1$, le groupe $G$ a un quotient isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

**Exercice 1 [5 pts]:** Soient $G$ un groupe fini, $p$ un nombre premier et $H \subset G$ le sous-groupe engendré par les éléments d'ordre premier à $p$.

(a) Montrer que $H$ est un sous-groupe distingué. (Indication: commencer par montrer que pour tous $h, g \in G$, les éléments $h$ et $ghg^{-1}$ ont le même ordre).

(b) Montrer que si $g \in G$ est d'ordre $p^u m$ avec $p$ ne divisant pas $m$ et si $\overline{g}$ désigne la classe de $g$ dans $G/H$, alors $\overline{g}^{(p^u)} = \overline{1}$. (Indication: commencer par donner l'ordre de $g^{(p^u)}$ dans $G$).

(c) Déduire de (b) que $G/H$ est un $p$-groupe.

(d) Montrer que si $G$ n'est pas engendré par ses éléments d'ordre premier à $p$, il a un quotient isomorphe à $\mathbb{Z}/p\mathbb{Z}$. (Indication: appliquer la question de cours au groupe $G/H$).

**T.S.V.P.**

# PARTIE II

**Exercice 2 [6 pts]**: (a) Déterminer, à isomorphisme près, tous les groupes abéliens d'ordre 882.

(b) Les groupes $\mathbb{Z}/63\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/147\mathbb{Z}$ sont-ils isomorphes?

Soit $G$ un groupe d'ordre 882 non abélien.

(c) Montrer que $G$ n'est pas nilpotent. (Indication: on rappelle que tout groupe d'ordre $p^2$ avec $p$ premier est abélien).

(d) Montrer que $G$ a un unique sous-groupe distingué $H$ d'ordre 49.

(e) Montrer que le groupe quotient $G/H$ est isomorphe au produit semi-direct d'un groupe d'ordre 9 et d'un groupe d'ordre 2.

**Exercice 3 [6 pts] :** On note $I = \{1, 2, 3\}$, $J = \{4, 5, 6, 7\}$ et $\mathcal{G}_I$ le sous-groupe de $S_7$ des permutations de $\{1, \ldots, 7\}$ qui laissent globalement invariant l'ensemble $I$.

(a) Pour $\sigma \in S_7$, on note respectivement $\sigma_I$ et $\sigma_J$ les restrictions de $\sigma$ à $I$ et à $J$. Montrer que la correspondance $\sigma \to (\sigma_I, \sigma_J)$ détermine un isomorphisme entre le groupe $\mathcal{G}_I$ et le groupe produit $\mathrm{Per}(I) \times \mathrm{Per}(J)$ (où $\mathrm{Per}(I)$ et $\mathrm{Per}(J)$ désignent les groupes de permutations des ensembles $I$ et $J$ respectivement). En déduire l'ordre du groupe $\mathcal{G}_I$.

Soit $\sigma \in S_7$ n'appartenant pas au sous-groupe $\mathcal{G}_I$.

(b) Montrer qu'on a $\sigma(J) \not\subset J$ et $\sigma(J) \not\subset I$.

(c) En déduire qu'il existe $j_1, j_2 \in J$ tels que $\sigma(j_1) = i_0 \in I$ et $\sigma(j_2) = j_0 \in J$.

(d) Pour $i \in I$ et $j \in J$ quelconques, calculer le produit dans $S_7$

$$[(i_0\ i)\ (j_0\ j)\ \sigma]\ (j_1\ j_2)\ [(i_0\ i)\ (j_0\ j)\ \sigma]^{-1}$$

(où on convient que $(i_0\ i)$ (resp. $(j_0\ j)$) vaut Id si $i_0 = i$ (resp. $j_0 = j$)).

(e) Montrer que le groupe $\langle \mathcal{G}_I, \sigma \rangle$ engendré par $\mathcal{G}_I$ et $\sigma$ contient toutes les transpositions de $S_7$. Que peut-on en déduire?

(f) On considère l'action $\rho$ de $S_7$ sur les parties de $\{1, \ldots, 7\}$ à 3 éléments définie par:

$$\rho(\sigma)(\{a, b, c\}) = \{\sigma(a), \sigma(b), \sigma(c)\} \quad (\sigma \in S_7 \text{ et } a, b, c \text{ distincts dans } \{1, \ldots, 7\}).$$

Montrer que cette action est primitive.

# UNIVERSITÉ LILLE 1

Enseignants: **N. BORNE, P. DÈBES, G. TUYNMAN**
Filière: **Licence - Semestre 5**
Matière: **M 308**
Année universitaire: **2008/2009**
Épreuve: **Examen - 1ère session**
Date: **jeudi 8 janvier de 8h à 11h**

---

## CORRIGÉ

---

**Question de cours [3 pts]**: *Soit $G$ un groupe fini d'ordre $p^n$, où $p$ est un nombre premier et $n \geq 0$ un entier. Montrer qu'il existe une suite de sous-groupes*

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

*telle que $|G_i| = p^i$ et $G_i$ est distingué dans $G$, $i = 0, 1, \ldots, n$. (On pourra utiliser sans le démontrer que le centre d'un $p$-groupe non trivial possède un élément d'ordre $p$).*

*En déduire que si $n \geq 1$, le groupe $G$ a un quotient isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

**Correction**: On raisonne par récurrence sur $n$. L'énoncé est évident pour $n = 0$. Supposons $n > 0$. On fixe un élément $x \in Z(G)$ d'ordre $p$. Le sous-groupe $\langle x \rangle$ est distingué et le quotient $G/\langle x \rangle$ est d'ordre $p^{n-1}$. D'après l'hypothèse de récurrence, il existe une suite de sous-groupes $\{1\} = \mathcal{G}_0 \subset \cdots \subset \mathcal{G}_{n-1} = G/\langle x \rangle$ telle que $|\mathcal{G}_i| = p^i$ et $\mathcal{G}_i$ est distingué dans $G/\langle x \rangle$, $i = 0, 1, \ldots, n-1$. Pour $s : G \to G/\langle x \rangle$ la surjection canonique, on pose $G_i = s^{-1}(\mathcal{G}_{i-1})$, $i = 1, \ldots, n$ et $G_0 = \{1\}$. On vérifie que la suite $(G_i)_{0 \leq i \leq n}$ répond à la question; par exemple, $|G_i| = p^i$ résulte de $G_i/\langle x \rangle = \mathcal{G}_{i-1}$.

Le groupe quotient $G/G_{n-1}$ est d'ordre $p$, donc est cyclique, isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

**Exercice 1 [5 pts]:** *Soient $G$ un groupe fini, $p$ un nombre premier et $H \subset G$ le sous-groupe engendré par les éléments d'ordre premier à $p$.*

(a) *Montrer que $H$ est un sous-groupe distingué. (Indication: commencer par montrer que pour tous $h, g \in G$, les éléments $h$ et $ghg^{-1}$ ont le même ordre).*

**Correction**: Si $h \in G$ est d'ordre premier à $p$, alors, pour tout $g \in G$, il en est de même de $ghg^{-1}$, puisque celui-ci est de même ordre que $h$ (en effet le groupe $\langle h \rangle$ et le groupe conjugué $g \langle h \rangle g^{-1} = \langle ghg^{-1} \rangle$ sont de même ordre). Le groupe $gHg^{-1}$ qui est engendré par les $ghg^{-1}$ avec $h \in G$ d'ordre premier à $p$ est donc contenu dans $H$, pour tout $g \in G$.

(b) *Montrer que si $g \in G$ est d'ordre $p^u m$ avec $p$ ne divisant pas $m$ et si $\overline{g}$ désigne la classe de $g$ dans $G/H$, alors $\overline{g}^{(p^u)} = \overline{1}$. (Indication: commencer par donner l'ordre de $g^{(p^u)}$ dans $G$).*

**Correction**: si $g \in G$ est d'ordre $p^u m$, alors $g^{(p^u)}$ est d'ordre $m$ et donc appartient à $H$. D'où $\overline{g^{(p^u)}} = \overline{g}^{(p^u)} = \overline{1}$.

(c) *Déduire de (b) que $G/H$ est un $p$-groupe.*

**Correction**: d'après le (b), tout élément $\overline{g}$ du groupe $G/H$ est d'ordre une puissance de $p$. Il en résulte classiquement que $G/H$ est d'ordre une puissance de $p$: en effet, sinon $G/H$ serait d'ordre divisible par un premier $q \neq p$ et d'après le théorème de Cauchy (ou le théorème de Sylow) aurait un élément d'ordre $q$.

(d) *Montrer que si $G$ n'est pas engendré par ses éléments d'ordre premier à $p$, il a un quotient isomorphe à $\mathbb{Z}/p\mathbb{Z}$. (Indication: appliquer la question de cours au groupe $G/H$).*

**Correction**: si $G$ n'est pas engendré par ses éléments d'ordre premier à $p$, alors $H$ est strictement inclus dans $G$ et le quotient $G/H$ est un $p$-groupe non trivial. D'après la question de cours, il possède un quotient isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Mais ce quotient de $G/H$ est aussi un quotient de $G$. En effet, si on l'écrit $(G/H)/(K/H)$ avec $K$ sous-groupe distingué de $G$ contenant $H$, alors, d'après les théorèmes d'isomorphisme, il est isomorphe à $G/K$.

**Complément:** *la réciproque de la question (d) est vraie: si $G$ a un quotient isomorphe à $\mathbb{Z}/p\mathbb{Z}$, alors $G$ n'est pas engendré par ses éléments d'ordre premier à $p$. (Indication: montrer que s'il existe un épimorphisme $s : G \to \mathbb{Z}/p\mathbb{Z}$, alors $H \subset \ker(s)$).*

**Preuve**: supposons que $G$ ait un quotient $G/K$ isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Soit $s : G \to \mathbb{Z}/p\mathbb{Z}$ l'épimorphisme obtenu en composant la surjection canonique $G \to G/K$ et l'isomorphisme $G/K \to \mathbb{Z}/p\mathbb{Z}$. Si $h \in H$ est d'ordre $d$ premier à $p$, alors $s(h)$ est d'ordre divisant à la fois $d$ (car $s(h)^d = s(h^d) = 1$) et $p$ (car $s(h) \in \mathbb{Z}/p\mathbb{Z}$), et donc $s(h) = 1$. Cela prouve que $H \subset \ker(s)$. Or, $s$ étant surjectif, $G/\ker(s)$ est non-trivial, c'est-à-dire, $\ker(s) \neq G$. D'où $H \neq G$ ce qui signifie que $G$ n'est pas engendré par ses éléments d'ordre premier à $p$.

**Exercice 2 [6 pts]**: (a) *Déterminer, à isomorphisme près, tous les groupes abéliens d'ordre* 882.

**Correction**: On a $882 = 2.3^2.7^2$. Le 2-Sylow est d'ordre 2, l'unique possibilité est $\mathbb{Z}/2\mathbb{Z}$. Le 3-Sylow est d'ordre $3^2$, il y a 2 possibilités: $\mathbb{Z}/9\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Le 7-Sylow est d'ordre $7^2$, il y a 2 possibilités: $\mathbb{Z}/49\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$. Un groupe abélien d'ordre 882 est produit direct de ses $p$-Sylows. Il y a donc exactement 4 possibilités, qu'on peut écrire comme suit en utilisant le lemme chinois: $\mathbb{Z}/882\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/126\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/294\mathbb{Z}$, $\mathbb{Z}/21\mathbb{Z} \times \mathbb{Z}/42\mathbb{Z}$.

(b) *Les groupes $\mathbb{Z}/63\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/147\mathbb{Z}$ sont-ils isomorphes?*

**Correction**: par le lemme chinois, on a

$$\mathbb{Z}/63\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z})$$

et

$$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/147\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/49\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/49\mathbb{Z})$$

Les 3-Sylows n'étant pas isomorphes, les deux groupes ne sont pas isomorphes.

*Soit $G$ un groupe d'ordre* 882 *non abélien.*

(c) *Montrer que $G$ n'est pas nilpotent. (Indication: on rappelle que tout groupe d'ordre $p^2$ avec $p$ premier est abélien).*

**Correction**: Si $G$ était nilpotent, il serait produit direct de ses $p$-Sylows, lesquels sont nécessairement abéliens: en effet, le 2-Sylow est d'ordre 2 donc cyclique et le 3-Sylow et le 7-Sylow sont d'ordre $3^2$ et $7^2$, et donc abéliens d'après le rappel. Le groupe $G$, produit direct de groupes abéliens, serait alors lui-même abélien.

(d) *Montrer que $G$ a un unique sous-groupe distingué $H$ d'ordre* 49.

**Correction**: Un sous-groupe d'ordre 49 est un 7-Sylow. D'après les théorèmes de Sylow, le nombre de 7-Sylows est congru à 1 modulo 7 et divise 18; il vaut donc 1. Il existe un unique 7-Sylow, qui est distingué.

(e) *Montrer que le groupe quotient $G/H$ est isomorphe au produit semi-direct d'un groupe d'ordre* 9 *et d'un groupe d'ordre* 2.

**Correction**: Le groupe $G/H$ est d'ordre $18 = 2.3^2$. Le nombre de 3-Sylows d'un tel groupe est congru à 1 modulo 3 et divise 2; il vaut donc 1. Soit $U$ l'unique 3-Sylow de $G/H$, qui est distingué, et fixons un 2-Sylow, $V$, qui est d'ordre 2. Le sous-groupe $U$ étant distingué, l'ensemble $UV$ est un sous-groupe de $G$. De plus, comme $U \cap V = \{1\}$ (puisque d'ordre divisant 9 et 2), on a $UV/V \simeq U$. Le groupe $UV$ est donc d'ordre $|UV| = |U|\,|V| = 18$, ce qui donne $UV = G/H$. On a ainsi une suite exacte $1 \to U \to G \to G/U \to 1$. Cette suite est scindée: l'isomorphisme $UV/U \to V$ en est en effet une section. On peut ainsi conclure que $G$ est isomorphe au produit semi-direct de $U$ (d'ordre 9) par $V$ (d'ordre 2).

**Exercice 3 [6 pts] :** *On note $I = \{1, 2, 3\}$, $J = \{4, 5, 6, 7\}$ et $\mathcal{G}_I$ le sous-groupe de $S_7$ des permutations de $\{1, \ldots, 7\}$ qui laissent globalement invariant l'ensemble $I$.*

(a) *Pour $\sigma \in S_7$, on note respectivement $\sigma_I$ et $\sigma_J$ les restrictions de $\sigma$ à $I$ et à $J$. Montrer que la correspondance $\sigma \to (\sigma_I, \sigma_J)$ détermine un isomorphisme entre le groupe $\mathcal{G}_I$ et le groupe produit* $\mathrm{Per}(I) \times \mathrm{Per}(J)$ *(où* $\mathrm{Per}(I)$ *et* $\mathrm{Per}(J)$ *désignent les groupes de permutations des ensembles $I$ et $J$ respectivement). En déduire l'ordre du groupe $\mathcal{G}_I$.*

**Correction**: Si $\sigma \in \mathcal{G}_I$, la restriction $\sigma_I$ est une application injective de $I$ dans $I$ et donc une bijection $\sigma_I \in \mathrm{Per}(I)$. De plus $\sigma$ laisse également globalement invariant $J$ (c'est le complémentaire de $I$), et donc $\sigma_J \in \mathrm{Per}(J)$. La correspondance $\sigma \to (\sigma_I, \sigma_J)$ définit ainsi une application $\mathcal{G}_I \to \mathrm{Per}(I) \times \mathrm{Per}(J)$. Cette application est un morphisme de groupes (la restriction d'une composée est la composée des restrictions). Elle est injective: si $\sigma_I$ et $\sigma_J$ sont l'identité sur $I$ et $J$ respectivement, alors $\sigma$ est l'identité sur $\{1, \ldots, 7\}$ car $I \cup J = \{1, \ldots, 7\}$. Enfin elle est surjective: comme $I \cap J = \emptyset$, la donnée de $\alpha \in \mathrm{Per}(I)$ et $\beta \in \mathrm{Per}(J)$ permet de définir une bijection $\sigma \in S_7$, qui, laissant $I$ invariant par construction, est dans $\mathcal{G}_I$.

L'isomorphisme $\mathcal{G}_I \simeq \mathrm{Per}(I) \times \mathrm{Per}(J)$, combiné à $\mathrm{Per}(I) \simeq S_3$ et $\mathrm{Per}(J) \simeq S_4$, donnent $|\mathcal{G}_I| = |\mathrm{Per}(I)|\,|\mathrm{Per}(J)| = |S_3|\,|S_4| = 3!\,4! = 144$.

*Soit $\sigma \in S_7$ n'appartenant pas au sous-groupe $\mathcal{G}_I$.*

(b) *Montrer qu'on a $\sigma(J) \not\subset J$ et $\sigma(J) \not\subset I$.*

**Correction**: Si $\sigma(J) \subset J$ alors $\sigma(I) \subset I$ ce qui contredit l'hypothèse $\sigma \notin \mathcal{G}_I$, d'où la première inclusion. La seconde résulte de $\mathrm{card}(J) > \mathrm{card}(I)$ et de l'injectivité de $\sigma$.

(c) *En déduire qu'il existe $j_1, j_2 \in J$ tels que $\sigma(j_1) = i_0 \in I$ et $\sigma(j_2) = j_0 \in J$.*

**Correction**: Comme $\sigma(J) \not\subset J$, il existe $j_1 \in J$ tel que $\sigma(j_1) \notin J$, mais alors $\sigma(j_1) \in I$. De même, de $\sigma(J) \not\subset I$, on déduit qu'il existe $j_2 \in J$ tel que $\sigma(j_2) \notin I$ et donc $\sigma(j_2) \in J$.

(d) *Pour $i \in I$ et $j \in J$ quelconques, calculer le produit dans $S_7$*

$$[(i_0\ i)\ (j_0\ j)\ \sigma]\ (j_1\ j_2)\ [(i_0\ i)\ (j_0\ j)\ \sigma]^{-1}$$

*(où on convient que $(i_0\ i)$ (resp. $(j_0\ j)$) vaut* Id *si $i_0 = i$ (resp. $j_0 = j$)).*

**Correction**: Le produit à calculer est la transposition qui échange les deux éléments image de $j_1$ et $j_2$ par la permutation $(i_0\ i)\ (j_0\ j)\ \sigma$: ces deux éléments sont $i$ et $j$. Le résultat du calcul est la transposition $(i\ j)$.

(e) *Montrer que le groupe $\langle \mathcal{G}_I, \sigma \rangle$ engendré par $\mathcal{G}_I$ et $\sigma$ contient toutes les transpositions de $S_7$. Que peut-on en déduire?*

**Correction**: D'après la question (a), le groupe $\mathcal{G}_I$ contient toutes les transpositions de deux éléments dans $I$ et toutes les transpositions de deux éléments dans $J$. En particulier, il contient les transpositions $(i_0\ i)$ et $(j_0\ j)$ de la question précédente. La formule qui a

été obtenue montre alors que la transposition $(i\ j)$ est dans le groupe $\langle \mathcal{G}_I, \sigma \rangle$. Finalement, on obtient que toutes les transpositions de $S_7$ sont dans le groupe $\langle \mathcal{G}_I, \sigma \rangle$. Ce groupe est donc $S_7$ tout entier.

(f) *On considère l'action $\rho$ de $S_7$ sur les parties de $\{1, \ldots, 7\}$ à 3 éléments définie par:*

$$\rho(\sigma)(\{a, b, c\}) = \{\sigma(a), \sigma(b), \sigma(c)\} \qquad (\sigma \in S_7 \text{ et } a, b, c \text{ distincts dans } \{1, \ldots, 7\}).$$

*Montrer que cette action est primitive.*

**Correction**: La transitivité de l'action est facile. (On peut la voir comme résultant de la question (a): en effet, le cardinal de l'orbite de $I = \{1, 2, 3\}$ est $|S_7|/|\mathcal{G}_I| = 7!/(3!\,4!)$, soit le nombre de parties de 3 éléments distincts dans un ensemble à 7 éléments; il y a donc une seule orbite).

On utilise ensuite le critère de primitivité: il s'agit de voir que $\mathcal{G}_I$ est un sous-groupe propre maximal. Cela résulte de ce qui précède: si $\sigma \notin \mathcal{G}_I$, alors le groupe $\langle \mathcal{G}_I, \sigma \rangle$ est $S_7$.

# UNIVERSITÉ LILLE 1

Enseignants: **N. BORNE, P. DÈBES, G. TUYNMAN**
Filière: **Licence - Semestre 5**
Matière: **M 308**
Année universitaire: **2008/2009**
Épreuve: **Examen - 2ème session**
Date: **septembre 2009**
Durée de l'épreuve: **3 heures**

---

**CHAQUE PARTIE SERA RÉDIGÉE SUR UNE COPIE DIFFÉRENTE**

---

**Ni calculatrices ni documents ni téléphone portable.**
**Une grande importance sera accordée à la rédaction.**
**Le barème est donné à titre indicatif.**

---

## PARTIE I

**Question de cours [2 pts]:** Soit $G$ un groupe fini agissant sur un ensemble fini $S$. Pour tout $s \in S$, on note $\mathcal{O}_s$ l'orbite de $s$ sous $G$ et $\Gamma_s$ le sous-groupe de $G$ des éléments $g \in G$ tels que $g \cdot s = s$. Montrer qu'on a

$$\mathrm{card}(\mathcal{O}_s) = \frac{\mathrm{card}(G)}{\mathrm{card}(\Gamma_s)}$$

**Exercice 1 [3 pts]:** Soit $G$ un groupe fini agissant transitivement sur un ensemble $S$.

(a) Déterminer le cardinal de chaque groupe $\Gamma_s$ pour $s \in S$.

(b) Montrer que le cardinal de l'ensemble $\bigcup_{s \in S} \Gamma_s$ est $\leq |G| - |S| + 1$.

(c) Montrer que si $\mathrm{card}(S) \geq 2$, il existe $g \in G$ tel que $g \cdot s \neq s$ pour tout $s \in S$.
(Indication: commencer par montrer que si ce n'était pas vrai, on aurait $G \subset \bigcup_{s \in S} \Gamma_s$).

**Exercice 2 [3,5 pts]**: Soit $G$ un groupe d'ordre 72 qu'on suppose simple.

(a) Montrer que le nombre de 3-sous-groupes de Sylow de $G$ est 4.

(b) On numérote les 3-Sylows de $G$ de 1 à 4. Montrer que l'action de $G$ par conjugaison sur ces 4 sous-groupes détermine un morphisme injectif $G \to S_4$.

(c) En déduire qu'il n'existe pas de groupe simple d'ordre 72. (Indication: considérer les ordres de $G$ et de $S_4$ dans la question (b)).

**T.S.V.P.**

# PARTIE II

**Exercice 3 [7,5 pts]**: Soit $G$ un groupe d'ordre 490.

(a) Montrer que $G$ a un sous-groupe distingué d'ordre 245. (Indication: montrer que si $\mathcal{S}_5$ est un 5-Sylow et $\mathcal{S}_7$ un 7-Sylow, alors l'ensemble $\mathcal{S}_5\mathcal{S}_7$ constitué des produits $xy$ où $x \in \mathcal{S}_5$ et $y \in \mathcal{S}_7$ répond à la question).

(b) Montrer que $G$ a un unique sous-groupe $H$ d'ordre 245.

(c) Montrer que le groupe $G$ est isomorphe au produit semi-direct du sous-groupe $H$ et d'un groupe d'ordre 2.

(d) Montrer que $H$ est abélien. (Indication: montrer que tout groupe d'ordre 245 est abélien).

(e) Donner toutes les possibilités pour $H$ à isomorphisme près.

(f) Donner 5 exemples de groupes d'ordre 490 non-isomorphes deux à deux.

**Exercice 4 [4 pts] :** Dans le groupe symétrique $S_9$ on considère les permutations

$$\begin{cases} \omega_1 = (1\,2\,3) \\ \omega_2 = (4\,5\,6) \\ \omega_3 = (7\,8\,9) \\ \tau = (1\,4\,7)(2\,5\,8)(3\,6\,9) \end{cases}$$

(a) Montrer que le sous-groupe $G \subset S_9$ engendré par $\omega_1, \omega_2, \omega_3$ et $\tau$ agit transitivement sur $\{1, \ldots, 9\}$.

(b) Montrer que $\omega_1, \omega_2, \omega_3$ engendrent un sous-groupe $\Omega \subset G$ isomorphe à $(\mathbb{Z}/3\mathbb{Z})^3$. (Indication: construire explicitement un monomorphisme $\Phi : (\mathbb{Z}/3\mathbb{Z})^3 \to G$ d'image $\Omega$).

(c) Montrer que le sous-groupe $G$ est isomorphe à un produit semi-direct de $(\mathbb{Z}/3\mathbb{Z})^3$ par $\mathbb{Z}/3\mathbb{Z}$. (Indication: commencer par calculer $\tau\omega_i\tau^{-1}$ pour $i = 1, 2, 3$).

# UNIVERSITÉ LILLE 1

Enseignants: **N. BORNE, P. DÈBES, G. TUYNMAN**
Filière: **Licence - Semestre 5**
Matière: **M 308**
Année universitaire: **2009/2010**
Épreuve: **Devoir no 1**

---

**à rendre en TD le jeudi 26 ou le vendredi 27 octobre 2009**

---

**Exercice 1**: On considère le groupe $H_8$ composé des 8 éléments $\pm 1, \pm I, \pm J, \pm K$ où

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \ , \ I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \ , \ J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \ K = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

(avec $i \in \mathbb{C}$ tel que $i^2 = -1$)

et dont la table de multiplication est déterminée par les relations $I^2 = J^2 = K^2 = -1$, $IJ = -JI = K$, $JK = -KJ = I$ et $KI = -IK = J$.

(a) Déterminer le centre $Z(H_8)$ du groupe $H_8$ et montrer que tous les éléments de $H_8 \setminus Z(H_8)$ sont d'ordre 4.

(b) Montrer que tous les sous-groupes de $H_8$ sont distingués.

(c) Un groupe dont tous les sous-groupes sont distingués est-il nécessairement abélien?

**Exercice 2**: (a) Soient $d$ et $r$ deux entiers $\geq 1$. Soient $G$ un groupe et $H$ le sous-groupe engendré par tous les éléments de $G$ s'écrivant comme produit de $r$ éléments de $G$ d'ordre $d$. Montrer que $H$ est un sous-groupe distingué de $G$.

(b) Montrer que si $G$ est un groupe simple possédant un élément d'ordre un entier $d \geq 0$, alors $G$ est engendré par ses éléments d'ordre $d$.

**Exercice 3**: (a) Montrer qu'un sous-groupe $G$ de $S_n$ tel que $G \cap A_n = \{1\}$ est nécessairement abélien. (Indication: utiliser, après l'avoir montré, que pour tout $g \in S_n$, on a $g^2 \in A_n$).

(b) Montrer que les sous-groupes simples de $S_n$ sont soit contenus dans $A_n$ soit d'ordre 2.

**Exercice 4:** Soient $G$ un groupe fini et $H$ un sous-groupe de $G$. On note $U$ l'ensemble réunion des sous-groupes $gHg^{-1}$ conjugués de $H$ par les éléments de $G$.

(a) Montrer que si $\{g_1, \ldots, g_n\}$ est un système de représentants des classes à gauche de $G$ modulo $H$, alors, $U \setminus \{1\} = \bigcup_{i=1}^{n} \left(g_i H g_i^{-1} \setminus \{1\}\right)$.

(b) En déduire que $\text{card}(U) \leq |G| - [G : H] + 1$

(c) *Application.* Soit $S$ un sous-ensemble de $G$ contenant au moins un élément dans chaque classe de conjugaison de $G$. Montrer que $S$ engendre $G$. (Indication: appliquer ce qui précède au sous-groupe $H = < S >$).

**T.S.V.P.**

**Exercice 5:** Etant donné un groupe fini, on appelle sous-groupe de Frattini de $G$ l'intersection des sous-groupes maximaux parmi les sous-groupes distincts de $G$. On le note $\Phi(G)$.

(a) Montrer que $\Phi(G)$ est un sous-groupe caractéristique de $G$ et qu'il a la propriété suivante: si $H$ est un sous-groupe de $G$ tel que $H\Phi(G) = G$, alors $H = G$.

(b) Déterminer $\Phi(G)$

- pour $G = \mathbb{Z}/p^n\mathbb{Z}$ pour $p$ premier et $n > 0$ entier,
- pour $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, pour $p$ et $q$ premiers distincts,
- pour $G = \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, pour $p$ et $q$ premiers distincts.

(On justifiera ses réponses).

# UNIVERSITÉ LILLE 1

Enseignants: **N. BORNE, P. DÈBES, G. TUYNMAN**
Filière: **Licence - Semestre 5**
Matière: **M 308**
Année universitaire: **2009/2010**
Épreuve: **Examen - 1ère session**
Date: **mercredi 6 janvier à 14h**
Lieu: **SN1 Maige**
Durée de l'épreuve: **3 heures**

---

**CHAQUE PARTIE SERA RÉDIGÉE SUR UNE COPIE DIFFÉRENTE**

---

**Ni calculatrices ni documents ni téléphone portable.**
**Une grande importance sera accordée à la rédaction.**
**Le barème est donné à titre indicatif.**

---

## PARTIE I

**Exercice 1 [2,5 pts] :** (a) Donner l'énoncé, hypothèses comprises, du théorème d'isomorphisme relatif au quotient $HK/H$, pour $H$, $K$ deux sous-groupes d'un groupe $G$.

(b) Montrer que si un sous-groupe $G$ du groupe symétrique $S_n$ contient une permutation de signature $-1$ alors $G$ a un sous-groupe d'indice 2.

**Exercice 2 [6,5 pts] :** (a) Montrer que tout groupe $H$ d'ordre 35 est cyclique.

Soit $G$ un groupe d'ordre 105.

(b) Que donne le théorème de Sylow sur le nombre de $p$-sous groupes de Sylow de $G$?

(c) Montrer que $G$ a un unique 5-sous-groupe de Sylow ou un unique 7-sous-groupe de Sylow. (Indication: raisonner par l'absurde).

(d) Montrer que $G$ a un sous-groupe cyclique $H$ d'ordre 35.

(e) Après avoir rappelé la définition de groupe fini nilpotent, montrer que si $G$ est nilpotent, alors $G$ est cyclique.

**Exercice 3 [3 pts] :** Soit $G$ un groupe d'ordre $p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ où $p_1, \ldots, p_n$ sont $n$ nombres premiers tels que $p_1 < \ldots < p_n$ et $\alpha_i > 0$, $i = 1, \ldots, n$. Soit $N$ un sous-groupe distingué de $G$ d'ordre $p_1$.

(a) Montrer que si $N \cap Z(G) \neq \{1\}$ alors $N \subset Z(G)$.

(b) Ecrire la formule des classes pour l'action de $G$ sur $N$ par conjugaison. En déduire que cette action n'a aucune orbite de cardinal $> 1$.

(c) Montrer que $N \subset Z(G)$.

**T.S.V.P.**

# PARTIE II

**Exercice 4 [3 pts] :** (a) Déterminer tous les groupes abéliens d'ordre 360 à isomorphisme près.

(b) Les groupes $\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$ et $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ sont-ils isomorphes?

**Exercice 5 [5 pts]:** Soient $G$ un groupe et $H \subset G$ un sous-groupe. On note $G/\cdot H$ l'ensemble des classes à gauche $xH$ de $G$ modulo $H$ ($x \in G$) et $\gamma : G \to \mathrm{Per}(G/H)$ l'action de $G$ sur $G/\cdot H$ par multiplication à gauche, laquelle est définie par $\gamma(g)(xH) = gxH$, pour tous $g, x \in G$.

(a) Montrer que $\ker(\gamma)$ est l'intersection de tous les sous-groupes $xHx^{-1}$ (conjugués de $H$ par $x$) où $x$ décrit $G$.

**Application**: Soit $G$ un groupe d'ordre 150.

(b) On suppose dans cette question que $G$ a moins deux 5-sous-groupes de Sylow. On note $H$ l'un d'entre eux et $\gamma : G \to \mathrm{Per}(G/\cdot H)$ l'action associée considérée ci-dessus. Montrer que

(i) $G$ a exactement six 5-sous-groupes de Sylow.

(ii) $|\ker(\gamma)|$ divise 25.

(iii) $|\ker(\gamma)| \neq 25$.

(iv) $|\ker(\gamma)| \neq 1$.

(c) Montrer que $G$ a un sous-groupe distingué d'ordre 25 ou a un sous-groupe distingué d'ordre 5.

# UNIVERSITÉ LILLE 1

Enseignants: **N. BORNE, P. DÈBES, G. TUYNMAN**
Filière: **Licence - Semestre 5**
Matière: **M 308**
Année universitaire: **2009/2010**
Épreuve: **Examen - 1ère session**
Date: **mercredi 6 janvier à 14h**
Durée de l'épreuve: **3 heures**

---

# CORRIGÉ

---

## PARTIE I

**Exercice 1:** (a) *Donner l'énoncé, hypothèses comprises, du théorème d'isomorphisme relatif au quotient $HK/H$.*

**Correction**: Si $H$ et $K$ sont deux sous-groupes d'un groupe $G$ et que $H$ est distingué dans $G$, alors l'ensemble $HK = \{hk | h \in H, k \in K\}$ est un groupe, égal au groupe engendré par $H \cup K$. De plus, $H$ est distingué dans $HK$, $H \cap K$ est distingué dans $K$ et les deux groupes quotient $HK/H$ et $K/(H \cap K)$ sont isomorphes.

(b) *Montrer que si un sous-groupe $G$ du groupe symétrique $S_n$ contient une permutation de signature $-1$ alors $G$ a un sous-groupe d'indice 2.*

**Correction**: Le groupe alterné $A_n$ est distingué dans $S_n$. D'après la question précédente, les deux groupes quotient $GA_n/A_n$ et $G/(G \cap A_n)$ sont isomorphes. Par hypothèse, $G$ n'est pas contenu dans $A_n$ et donc $GA_n \neq A_n$. Comme $[S_n : GA_n] \leq [S_n : A_n] = 2$, on a $GA_n = S_n$. D'où $[G : (G \cap A_n)] = [S_n : A_n] = 2$. Le groupe $G \cap A_n$ répond à la question.

**Exercice 2:** (a) *Montrer que tout groupe $H$ d'ordre 35 est cyclique.*

**Correction**: D'après le théorème de Cauchy (ou le théorème de Sylow), $G$ a un élément $a$ d'ordre 5 et un élément $b$ d'ordre 7. Le nombre de 5-Sylows est $\equiv 1$ [mod 5] et divise 7; c'est donc 1. De même le nombre de 7-Sylows est $\equiv 1$ [mod 7] et divise 5; c'est donc 1. Le groupe $\mathcal{S}_5 = \langle a \rangle$ (resp. $\mathcal{S}_7 = \langle b \rangle$) est donc l'unique 5-Sylow (resp. l'unique 7-Sylow) de $G$ et il est distingué. On déduit que $a(ba^{-1}b^{-1}) = (aba^{-1})b^{-1} \in \mathcal{S}_5 \cap \mathcal{S}_7$ et donc que $aba^{-1}b^{-1} = 1$ puisque $\mathcal{S}_5 \cap \mathcal{S}_7 = \{1\}$, l'ordre $|\mathcal{S}_5 \cap \mathcal{S}_7|$ devant diviser 5 et 7. Ainsi $a$ et $b$ commutent et $ab$ est d'ordre $5 \cdot 7 = 35$; le groupe $H$ est cyclique, engendré par $ab$.

*Soit $G$ un groupe d'ordre 105.*

(b) *Que donne le théorème de Sylow sur le nombre de $p$-sous groupes de Sylow de $G$?*

**Correction**: On a $105 = 3.5.7$. Le nombre de 3-Sylows est $\equiv 1$ [mod 3] et divise 35; c'est donc 1 ou 7. Le nombre de 5-Sylows est $\equiv 1$ [mod 5] et divise 21; c'est donc 1 ou 21. Le nombre de 7-Sylows est $\equiv 1$ [mod 7] et divise 15; c'est donc 1 ou 15.

(c) *Montrer que $G$ a un unique 5-sous-groupe de Sylow <u>ou</u> un unique 7-sous-groupe de Sylow. (<u>Indication</u>: raisonner par l'absurde).*

**Correction**: Si la conclusion voulue n'était pas vraie, $G$ aurait 21 5-sous-groupes de Sylow et 15 7-sous-groupes de Sylow. Ces groupes sont d'intersection deux à deux réduite à $\{1\}$: pour un 5-Sylow et un 7-Sylow, cela découle du fait que l'ordre de l'intersection divise 5 et 7; pour deux 5-Sylows ou pour deux 7-Sylows, cela provient du fait que ces sous-groupes de Sylow sont d'ordre premier et donc que l'intersection est forcément $\{1\}$

s'ils sont distincts. On déduit alors que le groupe $G$ aurait au moins $(21 \cdot 4) + (15 \cdot 6) + 1$ éléments, ce qui est absurde.

(d) *Montrer que $G$ a un sous-groupe cyclique $H$ d'ordre 35.*

**Correction**: D'après la question précédente, pour $p = 5$ ou $p = 7$, il existe un unique $p$-Sylow, qui est alors distingué. Notons le $\sigma_p$ et notons $\sigma_q$ un $q$-Sylow pour l'autre premier $q \in \{5, 7\}$. D'après la question (a) de l'exercice 1, l'ensemble $\sigma_p\sigma_q$ est un groupe et son ordre vaut $|\sigma_p| \cdot |\sigma_q|/|\sigma_q \cap \sigma_q| = 5 \cdot 7/1$. Le groupe $H = \sigma_p\sigma_q$ est un sous-groupe de $G$ d'ordre 35. D'après le (a), il est cyclique.

(e) *Après avoir rappelé la définition de groupe fini nilpotent, montrer que si $G$ est nilpotent, alors $G$ est cyclique.*

**Correction**: Un groupe fini est dit nilpotent s'il est isomorphe au produit direct de $p$-sous-groupes de Sylow. Supposons le groupe $G$ nilpotent. Ses $p$-Sylows étant cycliques (puisque d'ordre premier), $G$ est alors isomorphe au produit direct $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$, lequel, d'après le lemme chinois, est isomorphe à $\mathbb{Z}/105\mathbb{Z}$: $G$ est cyclique d'ordre 105.

**Exercice 3:** Soit $G$ un groupe d'ordre $p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ où $p_1, \ldots, p_n$ sont $n$ nombres premiers tels que $p_1 < \ldots < p_n$ et $\alpha_i > 0$, $i = 1, \ldots, n$. Soit $N$ un sous-groupe distingué de $G$ d'ordre $p_1$.

(a) *Montrer que si $N \cap Z(G) \neq \{1\}$ alors $N \subset Z(G)$.*

**Correction**: $N \cap Z(G)$ est un sous-groupe de $N$, lequel est d'ordre $p_1$. Comme $p_1$ est premier, $|N \cap Z(G)|$ vaut 1 ou $p_1$. Si $N \cap Z(G) \neq \{1\}$, alors $|N \cap Z(G)| = p_1$, c'est-à-dire $N \cap Z(G) = N$ et donc $N \subset Z(G)$;

(b) *Ecrire la formule des classes pour l'action de $G$ sur $N$ par conjugaison. En déduire que cette action n'a aucune orbite de cardinal $> 1$.*

**Correction**: L'ensemble $N^G$ des points fixes de l'action est l'ensemble des éléments $x \in N$ tels que $gxg^{-1} = x$ pour tout $g \in G$. D'où $N^G = N \cap Z(G)$. La formule des classes est que $\mathrm{card}(N)$ est égal à la somme de $\mathrm{card}(N^G)$ et des cardinaux des orbites de l'action de cardinal $> 1$. On sait aussi que ces orbites sont de cardinal divisant $|G|$; elles sont donc de cardinal $\geq p_1$. Comme $\mathrm{card}(N) = p_1$ et que $\mathrm{card}(N^G) = |N \cap Z(G)| \geq 1$, une telle orbite ne peut pas exister.

(c) *Montrer que $N \subset Z(G)$.*

**Correction**: La formule des classes s'écrit donc $p_1 = |N \cap Z(G)|$. D'après la question (a), $N \subset Z(G)$.

## PARTIE II

**Exercice 4:** (a) *Déterminer tous les groupes abéliens d'ordre 360 à isomorphisme près.*

**Correction**: D'après le théorème de structure des groupes abéliens finis, les groupes abéliens d'ordre 360 sont, à isomorphisme près, tous les groupes de la forme $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$ où $r \geq 1$ et $d_1, \ldots, d_r$ sont des entiers tels que (*) $1 < d_1 \mid d_2 \mid \ldots \mid d_r$ et (**) $d_1 \cdots d_r = 1$. On a $360 = 2^3.3^2.5$. Pour $i = 1, \ldots, r$ et $p$ premier, notons $n_{i,p}$ l'exposant de $p$ dans la décomposition en facteurs premiers de $d_i$. Les seuls premiers $p$ pour lesquels $d_i \neq 1$ sont 2, 3 et 5. Les deux conditions (*) et (**) se traduisent de la façon suivante:
(*) $1 \leq n_{1,p} \leq \ldots \leq n_{r,p}$, pour $p = 2, 3, 5$,
(**) $\sum_{i=1}^r n_{i,2} = 3$, $\sum_{i=1}^r n_{i,3} = 2$ et $\sum_{i=1}^r n_{i,5} = 1$

On déduit que $1 \leq r \leq 3$ et que les possibilités pour les $n_{i,p}$ sont
- pour $p = 2$: $(3), (1,2), (1,1,1)$
- pour $p = 3$: $(2), (1,1)$
- pour $p = 5$: $(1)$

ce qui, *via* le lemme chinois, fournit les groupes suivants:
$\mathbb{Z}/360\mathbb{Z}$ , $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z}$ , $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$ ,
$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}$ , $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}$ , $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ .

(b) *Les groupes* $\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$ *et* $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ *sont-ils isomorphes?*

**Correction**: Le lemme chinois fournit les isomorphismes:
$\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z}$
$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}$.
Comme les groupes de la liste (a) sont non isomorphes, on peut conclure que les groupes proposés ne sont pas isomorphes.

**Exercice 5:** Soient $G$ un groupe et $H \subset G$ un sous-groupe. On note $G/\cdot H$ l'ensemble des classes à gauche $xH$ de $G$ modulo $H$ ($x \in G$) et $\gamma : G \to \mathrm{Per}(G/\cdot H)$ l'action de $G$ sur $G/\cdot H$ par multiplication à gauche par $g$, laquelle est définie par $\gamma(g)(xH) = gxH$, pour tous $g, x \in G$.

(a) *Montrer que* $\ker(\gamma)$ *est l'intersection de tous les sous-groupes* $xHx^{-1}$ *(conjugués de* $H$ *par* $x$*) où* $x$ *décrit* $G$*.*

**Correction**: Un élément $g \in G$ est dans le noyau $\ker(\gamma)$ si et seulement si pour tout $x \in G$, on $\gamma(g)(xH) = xH$, c'est-à-dire $gxH = xH$, soit $x^{-1}gx \in H$ ou encore $g \in xHx^{-1}$. Cela fournit la réponse souhaitée.

**Application**: Soit $G$ un groupe d'ordre 150.

(b) *On suppose dans cette question que* $G$ *a moins* <u>deux</u> 5*-sous-groupes de Sylow. On note* $H$ *l'un d'entre eux et* $\gamma : G \to \mathrm{Per}(G/\cdot H)$ *l'action associée considérée ci-dessus. Montrer que*

(i) $G$ *a exactement* <u>six</u> 5*-sous-groupes de Sylow.*

(ii) $|\ker(\gamma)|$ *divise* 25*.*

(iii) $|\ker(\gamma)| \neq 25$*.*

(iv) $|\ker(\gamma)| \neq 1$*.*

**Correction**: On a $150 = 2.3.5^2$. D'après le théorème de Sylow, le nombre $n_5$ de 5-Sylow est $\equiv 1$ [mod 5] et divise 6; c'est donc 1 ou 6. Puisqu'on suppose qu'il y en a au moins 2, il y en a 6, d'où (i). D'après la question (a), $\ker(\gamma) \subset H$ et donc $|\ker(\gamma)|$ divise $|H| = 25$, d'où (ii). Les conjugués $xHx^{-1}$ de $H$ sont exactement les 5-sous-groupes de Sylow de $G$. Comme il sont au moins deux, leur intersection est strictement contenue dans $H$, ce qui donne $|\ker(\gamma)| \neq 25$, soit (iii). Enfin si $|\ker(\gamma)| = 1$, alors $\gamma$ est injective et $G$ est isomorphe à un sous-groupe de $\mathrm{Per}(G/\cdot H)$, lequel est isomorphe à $S_6$. Cela n'est pas possible car $150 = |G|$ ne divise pas $6! = |S_6|$, d'où (iv).

(c) *Montrer que* $G$ *a un sous-groupe distingué d'ordre* 25 <u>*ou*</u> *a un sous-groupe distingué d'ordre* 5*.*

**Correction**: Si $G$ possède un unique 5-Sylow, alors celui-ci est un sous-groupe distingué de $G$ d'ordre 25. Sinon, on est sous l'hypothèse de la question (b) de laquelle on peut conclure que $\ker(\gamma)$ est un sous-groupe de $G$ d'ordre 5, et il est distingué;

# UNIVERSITÉ LILLE 1

Enseignants: **N. BORNE, P. DÈBES, G. TUYNMAN**
Filière: **Licence - Semestre 5**
Matière: **M 308**
Année universitaire: **2009/2010**
Épreuve: **Examen - 2ème session**
Date: **mardi 23 février à 14h**
Lieu: **SN1 Gosselet**
Durée de l'épreuve: **3 heures**

---

**CHAQUE PARTIE SERA RÉDIGÉE SUR UNE COPIE DIFFÉRENTE**

**Ni calculatrices ni documents ni téléphone portable.**
**Une grande importance sera accordée à la rédaction.**
**Le barème est donné à titre indicatif.**

---

## PARTIE I

**Exercice 1 [2 pts] :** Montrer qu'un groupe d'ordre 2010 n'est pas simple.

**Exercice 2 [5 pts] :** (a) Donner la liste $\mathcal{L}_2$ des éléments d'ordre 2 du groupe alterné $A_4$ et la liste $\mathcal{L}_3$ des éléments d'ordre 3.

(b) Vérifier que $V = \mathcal{L}_2 \cup \{1\}$ est un sous-groupe de $A_4$.

(c) Montrer que $A_4$ n'a pas de sous-groupe d'ordre 6.

(d) Montrer que pour tout diviseur $d$ de $|A_4|$ différent de 6, il existe un sous-groupe de $A_4$ d'ordre $d$.

**Exercice 3 [4,5 pts] :** Soit $G$ un groupe d'ordre $p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ où $p_1, \ldots, p_n$ sont $n$ nombres premiers tels que $p_1 < \ldots < p_n$ et $\alpha_i > 0$, $i = 1, \ldots, n$. Soit $U$ un sous-groupe de $G$ d'indice $p_1$. Le but de l'exercice est de montrer que $U$ est distingué dans $G$.

(a) Montrer que le pgcd de $p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ et de $p_1!$ est $p_1$. (Rappel: $p_1! = p_1 \cdot (p_1 - 1) \cdots 2 \cdot 1$).

On note $G/\cdot U$ l'ensemble des classes à gauche $xU$ de $G$ modulo $U$ (pour $x \in G$) et $\gamma : G \to \mathrm{Per}(G/\cdot U)$ l'action de $G$ sur $G/\cdot U$ par multiplication à gauche par $g$, laquelle est définie par $\gamma(g)(xU) = gxU$, pour tous $g, x \in G$.

(b) Montrer que le groupe quotient $G/\ker(\gamma)$ est isomorphe à un sous-groupe du groupe symétrique $S_{p_1}$.

(c) Montrer que $|G/\ker(\gamma)| = p_1$. (Indication: utiliser la question (a)).

(d) Montrer que $\ker(\gamma) = U$ et conclure. (Indication: vérifier une inclusion et conclure à l'égalité par un argument sur les ordres des groupes).

**T.S.V.P.**

# PARTIE II

**Exercice 4 [4,5 pts] :** Soit $G$ un $p$-groupe non trivial, c'est-à-dire d'ordre $p^r$ avec $r > 0$.

(a) Montrer en utilisant un théorème du cours sur les $p$-groupes que tout sous-groupe $U \subset G$ maximal parmi les sous-groupes distincts de $G$ est d'ordre $p^{r-1}$. En déduire que $U$ est distingué dans $G$ (Indication: pour la seconde partie, utiliser l'exercice 3).

(b) Rappeler la définition de l'action de $G$ par conjugaison sur lui-même, écrire la formule des classes pour cette action et en déduire que le centre $Z(G)$ est non trivial.

(c) Montrer qu'un groupe $G$ d'ordre $p^2$ est abélien (Indication: commencer par montrer que $G/Z(G)$ est cyclique et que si $\gamma$ est un élément de $G$ dont la classe modulo $Z(G)$ engendre $G/Z(G)$, alors tout élément $g \in G$ s'écrit $g = \gamma^n z$ avec $n \in \mathbb{Z}$ et $z \in Z(G)$).

**Exercice 5 [4 pts] :** Soit $G$ un groupe nilpotent d'ordre 450.

(a) Rappeler la définition de groupe fini nilpotent.

(b) Montrer que $G$ est nécessairement abélien. (Indication: utiliser la question (a) ci-dessus et la question (c) de l'exercice précédent).

(c) Déterminer tous les groupes abéliens d'ordre 450 à isomorphisme près.

(b) Les groupes $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/75\mathbb{Z}$ et $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/45\mathbb{Z}$ sont-ils isomorphes?

# UNIVERSITÉ LILLE 1

Enseignants: **A. BROUSTET, P. DÈBES, M. HUTTNER**
Filière: **Licence - Semestre 5**
Matière: **M 51**
Année universitaire: **2010/2011**
Épreuve: **DS**
Date: **vendredi 22 octobre de 8h à 11h**
Lieu: **Bâtiment A5**
Durée de l'épreuve: **3 heures**

---

**CHAQUE PARTIE SERA RÉDIGÉE SUR UNE COPIE DIFFÉRENTE**

---

**Ni calculatrice ni documents ni téléphone portable.**
**Une grande importance sera accordée à la rédaction.**
**Le barème est donné à titre indicatif.**

---

## PARTIE I

**Question de cours [3,5 pts]:** Soit $\rho : G \to \mathrm{Per}(E)$ une action d'un groupe fini $G$ sur un ensemble fini $E$.

(a) Rappeler les définitions de l'orbite $\mathcal{O}(x)$ et du fixateur $G(x)$ pour l'action $\rho$ d'un élément $x \in E$.

(b) Montrer que pour tout $x \in E$, on a $\mathrm{card}(\mathcal{O}(x)) = \dfrac{|G|}{|G(x)|}$.

**Exercice 2 [3,5 pts]:** Les permutations suivantes sont-elles conjuguées dans le groupe symétrique $S_7$ ? (On justifiera sa réponse).

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 2 & 7 & 6 & 1 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 5 & 6 & 7 & 4 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 6 & 7 & 4 & 3 & 1 \end{pmatrix}$$

Pour celles qui le sont, écrire une relation de conjugaison $\sigma_j = \omega\, \sigma_i\, \omega^{-1}$. Ces permutations sont-elles conjuguées par un élément du groupe alterné $A_7$ ?

**Exercice 3 [4 pts]**: (a) Montrer que dans un groupe fini $G$, si $H$ et $K$ sont deux sous-groupes distincts d'ordre égaux à un nombre premier $p$, alors $H \cap K = \{1\}$.

(b) Montrer qu'un groupe abélien $G$ d'ordre 35 est nécessairement cyclique.
(Indication: commencer par montrer en raisonnant par l'absurde que le groupe $G$ possède un élément d'ordre 5, puis qu'il possède un élément d'ordre 7).

(c) Montrer que le groupe symétrique $S_{11}$ n'a pas de sous-groupe abélien d'ordre 35.

**T.S.V.P.**

# PARTIE II

**Exercice 4 [4,5 pts]**: (a) Soit $G$ un groupe. Pour $d \geq 1$, soit $H_d$ le sous-groupe de $G$ engendré par tous les éléments de $G$ d'ordre $d$. Montrer que $H_d$ est un sous-groupe distingué de $G$. (Indication: commencer par montrer que pour tous $h, g \in G$, les éléments $h$ et $ghg^{-1}$ ont le même ordre).

(b) Montrer que si $G$ est un groupe fini d'ordre pair, alors $G$ possède au moins un élément d'ordre 2. (Indication: penser à grouper chaque élément de $G$ avec son inverse).

(c) Montrer que si $G$ est un groupe simple d'ordre pair, alors il est engendré par ses éléments d'ordre 2.

**Exercice 5 [4,5 pts]** Dans le groupe symétrique $S_9$ on considère les permutations

$$\begin{cases} \omega_1 = (1\,2\,3) \\ \omega_2 = (4\,5\,6) \\ \omega_3 = (7\,8\,9) \\ \tau = (1\,4\,7)(2\,5\,8)(3\,6\,9) \end{cases}$$

On note $\Omega$ le sous-groupe de $S_9$ engendré par $\omega_1, \omega_2, \omega_3$ et $G$ le sous-groupe de $S_9$ engendré par $\omega_1, \omega_2, \omega_3$ et $\tau$.

(a) Montrer que $G$ agit transitivement sur $\{1, \ldots, 9\}$.

(b) Montrer que l'application $(n_1, n_2, n_3) \in \mathbb{Z}^3 \to \omega_1^{n_1}\omega_2^{n_2}\omega_3^{n_3} \in S_9$ permet de définir une application $\Phi : (\mathbb{Z}/3\mathbb{Z})^3 \to \Omega$ et que cette application est un isomorphisme.

(c) Montrer que $G$ est isomorphe à un produit semi-direct de $(\mathbb{Z}/3\mathbb{Z})^3$ par $\mathbb{Z}/3\mathbb{Z}$.
(Indication: commencer par calculer $\tau\omega_i\tau^{-1}$ pour $i = 1, 2, 3$).

# UNIVERSITÉ LILLE 1

Enseignants: **A. BROUSTET, P. DÈBES, M. HUTTNER**
Filière: **Licence - Semestre 5**
Matière: **M 51**
Année universitaire: **2010/2011**
Épreuve: **DS**
Date: **vendredi 22 octobre de 8h à 11h**

---

## CORRIGÉ

---

**Question de cours [3,5 pts]**: *Soit $\rho : G \to \mathrm{Per}(E)$ une action d'un groupe fini $G$ sur un ensemble fini $E$.*

(a) *Rappeler les définitions de l'orbite $\mathcal{O}(x)$ et du fixateur $G(x)$ pour l'action $\rho$ d'un élément $x \in E$.*

**Correction**: L'orbite $\mathcal{O}(x)$ est le sous-ensemble de $E$ de tous les éléments $\rho(g)(x)$ quand $g$ décrit $G$. Le fixateur $G(x)$ est le sous-groupe de $G$ de tous les éléments $g$ tels que $\rho(g)(x) = x$.

(b) *Montrer que pour tout $x \in E$, on a* $\mathrm{card}(\mathcal{O}(x)) = \dfrac{|G|}{|G(x)|}$.

**Correction**: Pour $g_1, g_2 \in G$, on a $\rho(g_1)(x) = \rho(g_2)(x)$ si et seulement si $g_1^{-1} g_2 \in G(x)$. Cette équivalence montre que l'application $G/\cdot G(x) \to \mathcal{O}(x)$ qui à $gG(x)$ associe $\rho(g)(x)$ est bien définie et qu'elle est injective. Elle est d'autre part surjective par définition de $\mathcal{O}(x)$. Elle est donc bijective. La formule demandée correspond à l'égalité des cardinaux des ensembles de départ et d'arrivée.

**Exercice 2 [3,5 pts]:** *Les permutations suivantes sont-elles conjuguées dans le groupe symétrique $S_7$ ?*

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 2 & 7 & 6 & 1 \end{pmatrix} \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 5 & 6 & 7 & 4 \end{pmatrix} \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 6 & 7 & 4 & 3 & 1 \end{pmatrix}$$

*Pour celles qui le sont, écrire une relation de conjugaison $\sigma_j = \omega\, \sigma_i\, \omega^{-1}$. Ces permutations sont-elles conjuguées par un élément du groupe alterné $A_7$ ?*

**Correction**: On décompose $\sigma_1$, $\sigma_2$ et $\sigma_3$ en produit de cycles à supports disjoints:

$$\sigma_1 = (1\ 3\ 5\ 7)\ (2\ 4)\ ,\ \sigma_2 = (4\ 5\ 6\ 7)\ (1\ 3)\ ,\ \sigma_3 = (1\ 2\ 5\ 4\ 7)\ (3\ 6)$$

Les permutations $\sigma_1$ et $\sigma_2$ sont de même type: $1^1.2^1.4^1$ et sont donc conjuguées dans $S_7$, mais elle ne sont pas conjuguées à $\sigma_3$ qui de type $2^1.5^1$. Plus précisément, on peut écrire: $\sigma_2 = \omega\sigma_1\omega^{-1}$ où $\omega$ vérifie: $(\omega(1)\ \omega(3)\ \omega(5)\ \omega(7))\ (\omega(2)\ \omega(4)) = (4\ 5\ 6\ 7)\ (1\ 3)$. La permutation $\omega = (1\ 4\ 3\ 5\ 6\ 2)$ convient mais aussi $\omega = (1\ 4)\ (2\ 3\ 5\ 6)$. La seconde est dans $A_7$; $\sigma_1$ et $\sigma_2$, qui sont dans $A_7$, sont également conjugués dans $A_7$.

**Exercice 3 [4 pts]**: (a) *Montrer que dans un groupe fini $G$, si $H$ et $K$ sont deux sous-groupes distincts d'ordre égaux à un nombre premier $p$, alors $H \cap K = \{1\}$.*

**Correction**: L'ordre de $H \cap K$ divisant $p = |H|$, on a ou bien $|H \cap K| = 1$ et alors $H \cap K = \{1\}$, ou bien $|H \cap K| = p$ et alors $H \cap K = H$. Dans ce second cas, $H \subset K$, ce qui entraîne $H = K$ et contredit l'hypothèse.

(b) *Montrer qu'un groupe abélien $G$ d'ordre 35 est nécessairement cyclique. (Indication: commencer par montrer en raisonnant par l'absurde que le groupe $G$ possède un élément d'ordre 5, puis qu'il possède un élément d'ordre 7).*

**Correction**: Supposons $G$ non cyclique. Les éléments de $G$ différents de 1 sont d'ordre 5 ou 7. S'ils étaient tous d'ordre 7, les sous-groupes qu'ils engendrent, auxquels on retire 1, formeraient une partition de $G \setminus \{1\}$ (d'après (a)). Cela n'est pas possible car $35-1=34$ n'est pas divisible par $7-1=6$. Il existe donc un élément $a$ d'ordre 5. De même, comme 34 n'est pas divisible par $5-1=4$, il existe un élément $b$ d'ordre 7. Mais le groupe étant abélien, l'élément $ab$ est d'ordre $\text{ppcm}(5,7)=35$, ce qui contredit l'hypothèse "$G$ non cyclique". Le groupe $G$ est donc cyclique.
**N.B.**: pour montrer l'existence d'un élément d'ordre 5 et celle d'un élément d'ordre 7, on peut aussi invoquer le théorème de Cauchy.

(c) *Montrer que le groupe symétrique $S_{11}$ n'a pas de sous-groupe abélien d'ordre 35.*

**Correction**: D'après (b), si $S_{11}$ a un sous-groupe abélien d'ordre 35, celui-ci est cyclique: il existe un élément $\omega \in S_{11}$ d'ordre 35. Sa décomposition en cycles à support disjoints doit comprendre un 7-cycle et un 5-cycle, ce qui n'est pas possible, puisque $7+5>11$.

**Exercice 4 [4,5 pts]**: (a) *Soit $G$ un groupe. Pour $d \geq 1$, soit $H_d$ le sous-groupe de $G$ engendré par tous les éléments de $G$ d'ordre $d$. Montrer que $H_d$ est un sous-groupe distingué de $G$. (Indication: commencer par montrer que pour tous $h, g \in G$, les éléments $h$ et $ghg^{-1}$ ont le même ordre).*

**Correction**: Si $h \in G$ est d'ordre $d$, alors, pour tout $g \in G$, il en est de même de $ghg^{-1}$, puisque celui-ci est de même ordre que $h$ (en effet le groupe $\langle h \rangle$ et le groupe conjugué $g \langle h \rangle g^{-1} = \langle g\,h\,g^{-1} \rangle$ sont de même ordre). Le groupe $gH_dg^{-1}$ qui est engendré par les $ghg^{-1}$ avec $h \in G$ d'ordre $d$ est donc contenu dans $H_d$, pour tout $g \in G$.

(b) *Montrer que si $G$ est un groupe fini d'ordre pair, alors $G$ possède au moins un élément d'ordre 2. (Indication: penser à grouper chaque élément de $G$ avec son inverse).*

**Correction**: L'ensemble $G$ est égal à $\bigcup_{x \in G} \{x, x^{-1}\}$. Les ensembles $\{x, x^{-1}\}$ ont 2 éléments sauf si $x = x^{-1}$, c'est-à-dire si $x^2 = 1$. Si $G$ ne possédait pas d'élément d'ordre 2, alors $x^2 = 1$ aurait pour seule solution $x = 1$ et l'ensemble $\bigcup_{x \in G} \{x, x^{-1}\}$ serait de cardinal impair, ce qui contredit l'hypothèse.

(c) *Montrer que si $G$ est un groupe simple d'ordre pair, alors il est engendré par ses éléments d'ordre 2.*

**Correction**: D'après le (a), le sous-groupe $H_2 \subset G$ est distingué et d'après le (b), $H_2 \neq \{1\}$. Comme $G$ est simple, on déduit $H_2 = G$.

**Exercice 5 [4,5 pts]** *Dans le groupe symétrique $S_9$ on considère les permutations*

$$\begin{cases} \omega_1 = (1\,2\,3) \\ \omega_2 = (4\,5\,6) \\ \omega_3 = (7\,8\,9) \\ \tau = (1\,4\,7)(2\,5\,8)(3\,6\,9) \end{cases}$$

*On note $\Omega$ le sous-groupe de $S_9$ engendré par $\omega_1, \omega_2, \omega_3$ et $G$ le sous-groupe de $S_9$ engendré par $\omega_1, \omega_2, \omega_3$ et $\tau$.*

*(a) Montrer que $G$ agit transitivement sur $\{1, \ldots, 9\}$.*

**Correction**: La décomposition de $\omega_1$ indique que l'orbite de 1 contient $\{1, 2, 3\}$. Elle contient donc aussi les orbites de 1, de 2 et de 3, lesquelles, au vu de la décomposition de $\tau$, recouvrent l'ensemble $\{1, \ldots, 9\}$.

(b) *Montrer que l'application* $(n_1, n_2, n_3) \in \mathbb{Z}^3 \to \omega_1^{n_1}\omega_2^{n_2}\omega_3^{n_3} \in S_9$ *permet de définir une application* $\Phi : (\mathbb{Z}/3\mathbb{Z})^3 \to \Omega$ *et que cette application est un isomorphisme.*

**Correction**: $\omega_1, \omega_2, \omega_3$ sont d'ordre 3 dans $S_9$. L'expression $\omega_1^{n_1}\omega_2^{n_2}\omega_3^{n_3}$ ne dépend donc que des classes modulo 3 de $n_1, n_2, n_3$, et définit bien une application $\Phi : (\mathbb{Z}/3\mathbb{Z})^3 \to \Omega$. On vérifie facilement que cette application est un morphisme; il faut juste noter que $\omega_1, \omega_2, \omega_3$ commutent deux à deux. Par définition de $\Omega$, $\Phi$ est surjective. Enfin on a $\omega_1^{n_1}\omega_2^{n_2}\omega_3^{n_3} = 1$ si et seulement si $\omega_1^{n_1} = \omega_2^{n_2} = \omega_3^{n_3} = 1$ si et seulement si $n_1, n_2, n_3$ sont des multiples de 3. Cela prouve l'injectivité de $\Phi$.

(c) *Montrer que* $G$ *est isomorphe à un produit semi-direct de* $(\mathbb{Z}/3\mathbb{Z})^3$ *par* $\mathbb{Z}/3\mathbb{Z}$. *(Indication: commencer par calculer* $\tau\omega_i\tau^{-1}$ *pour* $i = 1, 2, 3$*).*

**Correction**: On calcule facilement $\tau\omega_1\tau^{-1} = \omega_2$, $\tau\omega_2\tau^{-1} = \omega_3$ et $\tau\omega_3\tau^{-1} = \omega_1$. Ces formules montrent, d'une part que $\Omega$ est distingué dans $G$ et donc $\Omega \cdot \langle\tau\rangle = G$, et d'autre part que $\tau \notin \Omega$ (puisque $\Omega$ est abélien) et donc $\Omega \cap \langle\tau\rangle = \{1\}$ (puisque $\tau$ est d'ordre 3 (premier)). Les théorèmes d'isomorphisme fournissent alors un isomorphisme $G/\Omega \to \langle\tau\rangle$ qui est une section de la suite exacte

$$1 \to \Omega \to G \to G/\Omega \to 1$$

On conclut que le groupe $G$ est isomorphe à un produit semi-direct de $\Omega$ par $G/\Omega$, lequel est isomorphe à un produit semi-direct de $(\mathbb{Z}/3\mathbb{Z})^3$ par $\mathbb{Z}/3\mathbb{Z}$.

# UNIVERSITÉ LILLE 1

Enseignants: **A. BROUSTET, P. DÈBES, M. HUTTNER**
Filière: **Licence - Semestre 5**
Matière: **M 51**
Année universitaire: **2010/2011**
Épreuve: **Devoir Surveillé 2**
Date: **lundi 13 décembre à 14h**
Lieu: **Bâtiment M1 Amphi Archimède**

---

**ÉTUDIANTS REPASSANT M301: PARTIE II SEULE EN 2 HEURES**

**ÉTUDIANTS REPASSANT M308: PARTIE I SEULE EN 2 HEURES**

**AUTRES ÉTUDIANTS: PARTIES I ET II EN 3 HEURES 30 MINUTES**

**PARTIES I ET II SUR DEUX COPIES DIFFÉRENTES**

**Ni calculatrice ni documents ni téléphone portable.**
**Une grande importance sera accordée à la rédaction.**
**Le barème, donné à titre indicatif sur 10 pour chaque partie,**
**sera adapté aux différentes durées de composition.**

---

## PARTIE I

**Exercice 1 [5,5 pts]**: Soit $G$ un groupe d'ordre 42.

(a) Montrer que si $\mathcal{S}_3$ et $\mathcal{S}_7$ désignent respectivement un 3-sous-groupe de Sylow et un 7-sous-groupe de Sylow de $G$, alors l'ensemble $H = \mathcal{S}_3 \cdot \mathcal{S}_7$ est un sous-groupe distingué d'ordre 21 de $G$.

(b) Montrer que $H$ est isomorphe à un produit semi-direct de $\mathbb{Z}/7\mathbb{Z}$ par $\mathbb{Z}/3\mathbb{Z}$. Préciser quelles sont les actions possibles de $\mathbb{Z}/3\mathbb{Z}$ sur $\mathbb{Z}/7\mathbb{Z}$.

(c) Montrer que $H$ est l'unique sous-groupe d'ordre 21 de $G$ et que $G$ est isomorphe à un produit semi-direct de $H$ par $\mathbb{Z}/2\mathbb{Z}$. (Indication: pour l'unicité de $H$, on pourra commencer par montrer que pour tout $x \in G$, $x^2 \in H$).

(d) Montrer que si $G$ est abélien, il est cyclique.

**Exercice 2 [4,5 pts]**:
(a) (*Question de cours*). Soit $n \geq 2$ un entier. On note $\mathcal{G}(\mathbb{Z}/n\mathbb{Z})$ l'ensemble des générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe multiplicatif des éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$. Montrer que

$$\mathcal{G}(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^\times = \{m + n\mathbb{Z} \mid (m, n) = 1\}$$

(où $(m, n)$ désigne le pgcd de $m$ et $n$).

**T.S.V.P.**

(b) Montrer que le groupe $((\mathbb{Z}/49\mathbb{Z})^\times, \times)$ est isomorphe au groupe $(\mathbb{Z}/42\mathbb{Z}, +)$. (Indication: on pourra combiner la question (a) ci-dessus avec la question (d) de l'exercice 1).

(c) Vérifier que $2^{10} \equiv -5$ [mod 49] et en déduire que la classe de 2 modulo 49 est d'ordre 21 dans $(\mathbb{Z}/49\mathbb{Z})^\times$ et que la classe de $-2$ est un générateur de $(\mathbb{Z}/49\mathbb{Z})^\times$.

(d) Combien de générateurs le groupe $((\mathbb{Z}/49\mathbb{Z})^\times, \times)$ possède-t-il? Les décrire.

# PARTIE II

**Exercice 3 [1,5 pts]** (*Question de cours*): Donner les définitions d'anneau principal et d'anneau euclidien et démontrer que tout anneau euclidien est principal.

**Exercice 4 [8,5pts]**: Soient $p \geq 2$ un nombre premier.

(a) Montrer que $F(Y) = \dfrac{(Y+1)^p - 1}{Y}$ est un polynôme en $Y$ à coefficients dans $\mathbb{Z}$.

(b) Montrer que $F(Y)$ est irréductible dans $\mathbb{Q}[Y]$. (Indication: on pourra appliquer le critère d'Eisenstein).

On considère le polynôme $\Phi(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$.

(c) Montrer que $F(X-1) = \Phi(X)$ et en déduire que $\Phi(X)$ est irréductible dans $\mathbb{Q}[X]$.

(d) On note $\mathbb{Q}[e^{2i\pi/p}]$ l'image du morphisme d'évaluation $E : \mathbb{Q}[X] \to \mathbb{C}$ qui envoie $X$ sur $e^{2i\pi/p}$. Montrer que $\mathbb{Q}[e^{2i\pi/p}]$ est le plus petit sous-anneau de $\mathbb{C}$ contenant le corps $\mathbb{Q}$ et le nombre $e^{2i\pi/p}$.

(e) Montrer que $\ker(E)$ est l'idéal de $\mathbb{Q}[X]$ engendré par $\Phi(X)$ et en déduire que $\mathbb{Q}[e^{2i\pi/p}]$ est un sous-corps de $\mathbb{C}$.

(f) Montrer que $(X-1)$ divise $X^p - 1$ et que $(X-1)^2$ ne divise pas $X^p - 1$ dans $\mathbb{Q}[X]$.

(g) Montrer que $Y^p + X^p - 1$ est un polynôme irréductible dans $\mathbb{Q}[X, Y]$.

(h) Montrer que l'anneau quotient $\mathbb{Q}[X,Y]/\langle Y^p + X^p - 1\rangle$ de $\mathbb{Q}[X,Y]$ par l'idéal engendré par $Y^p + X^p - 1$ est intègre mais que la classe de $X$ modulo $\langle Y^p + X^p - 1\rangle$ n'est pas inversible dans cet anneau.

# UNIVERSITÉ LILLE 1

Enseignants: **A. BROUSTET, P. DÈBES, M. HUTTNER**
Filière: **Licence - Semestre 5**
Matière: **M 51**
Année universitaire: **2010/2011**
Épreuve: **Devoir Surveillé 2**
Date: **lundi 13 décembre à 14h**
Durée de l'épreuve: **3h30**

---

**CORRIGÉ**

---

## PARTIE I

**Exercice 1 [5,5 pts]**: *Soit $G$ un groupe d'ordre 42.*

(a) *Montrer que si $\mathcal{S}_3$ et $\mathcal{S}_7$ désignent respectivement un 3-sous-groupe de Sylow et un 7-sous-groupe de Sylow de $G$, alors l'ensemble $H = \mathcal{S}_3 \cdot \mathcal{S}_7$ est un sous-groupe distingué d'ordre 21 de $G$.*

**Correction**: Le nombre de 7-sous-groupes de Sylow de $G$ est congru à 1 modulo 7 et divise 6; il vaut donc 1. Le groupe $\mathcal{S}_7$ est donc l'unique 7-Sylow et il est nécessairement distingué dans $G$. Il en résulte que l'ensemble $H = \mathcal{S}_3 \cdot \mathcal{S}_7$ est un sous-groupe de $G$. De plus, $\mathcal{S}_3 \cap \mathcal{S}_7 = \{1\}$ (puisque d'ordre divisant 7 et 3). Le théorème d'isomorphisme "$NM/N \simeq M/N\cap M$" donne ici que $H/\mathcal{S}_7 \simeq \mathcal{S}_3$ et que $H$ est d'ordre $|H| = |\mathcal{S}_3|\,|\mathcal{S}_7| = 21$. Le sous-groupe $H$ étant d'indice 2 dans $G$ est distingué.

(b) *Montrer que $H$ est isomorphe à un produit semi-direct de $\mathbb{Z}/7\mathbb{Z}$ par $\mathbb{Z}/3\mathbb{Z}$. Préciser quelles sont les actions possibles de $\mathbb{Z}/3\mathbb{Z}$ sur $\mathbb{Z}/7\mathbb{Z}$.*

**Correction**: On sait aussi que de $\mathcal{S}_3 \cap \mathcal{S}_7 = \{1\}$ résulte que la suite exacte $1 \to \mathcal{S}_7 \to H \to H/\mathcal{S}_7 \to 1$ est scindée. De façon équivalente, $H$ est isomorphe à un produit semi-direct de $\mathcal{S}_7 \simeq \mathbb{Z}/7\mathbb{Z}$ par $H/\mathcal{S}_7 \simeq \mathbb{Z}/3\mathbb{Z}$.

Le groupe $\mathbb{Z}/3\mathbb{Z}$ étant cyclique, une action $\rho : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$ est déterminée par $\rho(\bar{1})$, l'image du générateur $\bar{1} \in \mathbb{Z}/3\mathbb{Z}$ (classe de 1 modulo 3). De plus, $\rho(\bar{1})$ peut être tout élément d'ordre divisant 3 dans $\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$. On sait que $\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) \simeq (\mathbb{Z}/7\mathbb{Z})^\times \simeq \mathbb{Z}/6\mathbb{Z}$. Il existe 3 valeurs possibles pour $\rho(\bar{1})$ qui correspondent aux 3 éléments $\bar{0}$, $\bar{2}$, $\bar{4}$ d'ordres respectifs 0, 3 et 3 dans $\mathbb{Z}/6\mathbb{Z}$. Les automorphismes correspondants $\mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$ sont les applications $x \to x$, $x \to 2x$ et $x \to 4x$; 1, 3 et 4 correspondent aux puissances d'exposants 0, 2, 4 (modulo 6) du générateur $\bar{3}$ de $((\mathbb{Z}/7\mathbb{Z})^\times, \times)$.

(c) *Montrer que $H$ est l'unique sous-groupe d'ordre 21 de $G$ et que $G$ est isomorphe à un produit semi-direct de $H$ par $\mathbb{Z}/2\mathbb{Z}$.*

**Correction**: Le groupe $H$ est d'indice 2 dans $G$, il est donc distingué. Soit $H'$ un sous-groupe d'ordre 21 de $G$. Pour tout $x \in H'$, on a d'une part $x^{21} = 1$, et d'autre part $x^2 \in H$ (puisque $(xH)^2 = x^2H = H$ dans $G/H$). On en déduit que $x = x^{21}(x^2)^{-10} \in H$. D'où $H' \subset H$ et finalement $H' = H$ puisque $H$ et $H'$ ont même cardinal.

Soit $\mathcal{S}_2$ un 2-Sylow de $G$. Comme $H$ est distingué dans $G$ et que $H \cap \mathcal{S}_2 = \{1\}$ (puisque d'ordre divisant 21 et 2), en raisonnant comme dans les questions (a) et (b), on obtient que $G$ est isomorphe à un produit semi-direct de $H$ par $\mathcal{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$.

(d) *Montrer que si $G$ est abélien, il est cyclique.*

**Correction**: D'après les questions précédentes, $G$ est isomorphe à un produit semi-direct de $H$ par $\mathbb{Z}/2\mathbb{Z}$, et $H$ est isomorphe à un produit semi-direct de $\mathbb{Z}/7\mathbb{Z}$ par $\mathbb{Z}/3\mathbb{Z}$. Si $G$ est abélien, $H$ l'est aussi et les deux actions associées à ces produits semi-directs sont triviales. Ce qui donne $H \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/21\mathbb{Z}$ et $G \simeq \mathbb{Z}/21\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/42\mathbb{Z}$ (les seconds isomorphismes résultant du lemme chinois).

On peut aussi dire que si $G$ est abélien, il est isomorphe au produit direct de ses sous-groupes de Sylow (autrement dit $G$ est nilpotent), c'est-à-dire, de ses trois sous-groupes isomorphes à $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$. Le lemme chinois permet ici aussi de conclure que $G \simeq \mathbb{Z}/42\mathbb{Z}$.

**Exercice 2 [4,5 pts]**:

(a) (Question de cours). *Soit $n \geq 2$ un entier. On note $\mathcal{G}(\mathbb{Z}/n\mathbb{Z})$ l'ensemble des générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe multiplicatif des éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$. Montrer que*

$$\mathcal{G}(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^\times = \{m + n\mathbb{Z} \mid (m, n) = 1\}$$

*(où $(m, n)$ désigne le pgcd de $m$ et $n$).*

**Correction**: Un élément $m + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement s'il existe une classe $u + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ telle que $(m + n\mathbb{Z})(u + n\mathbb{Z}) = 1 + n\mathbb{Z}$, c'est-à-dire si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $um + vn = 1$. Un élément $m + n\mathbb{Z}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si la classe $1 + n\mathbb{Z}$ est dans le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par $m + n\mathbb{Z}$, c'est-à-dire si et seulement s'il existe $u \in \mathbb{Z}$ tel que $1 + n\mathbb{Z} = u\,(m + n\mathbb{Z})$ soit si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $um + vn = 1$. Dans les deux cas, la condition trouvée est une identité de Bezout qui exprime que $(m, n) = 1$.

(b) *Montrer que le groupe $((\mathbb{Z}/49\mathbb{Z})^\times, \times)$ est isomorphe au groupe $(\mathbb{Z}/42\mathbb{Z}, +)$. (Indication: on pourra combiner la question (a) ci-dessus avec la question (d) de l'exercice 1).*

**Correction**: D'après la question (a), le groupe $(\mathbb{Z}/49\mathbb{Z})^\times$ est l'ensemble des classes modulo 49 des entiers compris entre 1 et 49 qui sont premiers à 49; les entiers à exclure sont les $49/7 = 7$ multiples de 7 entre 1 et 49. Le groupe $(\mathbb{Z}/49\mathbb{Z})^\times$ est donc d'ordre 42. Comme il est abélien, d'après la question (d) de l'exercice 1, $(\mathbb{Z}/49\mathbb{Z})^\times \simeq \mathbb{Z}/42\mathbb{Z}$.

(c) *Vérifier que $2^{10} \equiv -5$ [mod 49] et en déduire que la classe de 2 modulo 49 est d'ordre 21 dans $(\mathbb{Z}/49\mathbb{Z})^\times$ et que la classe de $-2$ est un générateur de $(\mathbb{Z}/49\mathbb{Z})^\times$.*

**Correction**: On a $2^{10} = 1024 = 49 \times 21 - 5$ ce qui donne $2^{10} \equiv -5$ [mod 49]. On en déduit que $2^{21} \equiv (-5)^2 \cdot 2 \equiv 1$ [mod 49]. Comme $2^1$, $2^3$ et $2^7$ ne sont pas congrus à 1 modulo 49, on obtient que 2 est d'ordre 21 modulo 49. Comme $-1$ est d'ordre 2 et que 2 est premier à 21 (l'ordre de 2), on obtient que $-2 = (-1) \cdot 2$ est d'ordre 42 modulo 49.

(d) *Combien de générateurs le groupe $((\mathbb{Z}/49\mathbb{Z})^\times, \times)$ possède-t-il? Les décrire.*

**Correction**: Le groupe $((\mathbb{Z}/49\mathbb{Z})^\times, \times)$ est isomorphe au groupe $(\mathbb{Z}/42\mathbb{Z}, +)$. D'après la question (a), ces groupes possèdent 12 générateurs (nombre d'entiers entre 1 et 42 premiers à 42). Vus dans $(\mathbb{Z}/49\mathbb{Z})^\times$, ce sont les éléments $(-\bar{2})^m$ où $m$ décrit l'ensemble des nombres premiers à 42 (et où $\bar{2}$ est la classe de 2 modulo 49).

# PARTIE II

**Exercice 3 [1,5 pts]** (*Question de cours*): *Donner les définitions d'anneau principal et d'anneau euclidien et démontrer que tout anneau euclidien est principal.*

**Correction**: Un anneau intègre $A$ est dit principal si tout idéal peut être engendré par un élément. Il est dit euclidien s'il existe une application $\phi : A \setminus \{0\} \to \mathbb{N}$ ayant la propriété suivante: pour tout $a, b \in A$ avec $b \neq 0$, il existe $q, r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $\phi(r) < \phi(b)$.

Supposons que $A$ soit euclidien. Soit $I$ un idéal de $A$. Si $I = \{0\}$ alors $I$ est engendré par 0. Supposons désormais $I \neq \{0\}$. Considérons l'ensemble $F$ des élément $\phi(x) \in \mathbb{N}$ où $x$ décrit $I \setminus \{0\}$. Comme $F \subset \mathbb{N}$ et $F \neq \emptyset$, $F$ a un plus petit élément, de la forme $\phi(b)$ avec $b \in I$. Montrons que $b$ engendre $I$. Soit $a \in I$. Par l'hypothèse, on peut écrire $a = bq + r$ avec $q, r \in A$ et ($r = 0$ ou $\phi(r) < \phi(b)$). Mais comme $r = a - bq \in I$, la condition $\phi(r) < \phi(b)$ contredirait la minimalité de $\phi(b)$. On a donc $r = 0$, $a = bq$, et $I$ est inclus dans l'idéal engendré par $b$, et lui est en fait égal puisque $b \in I$.

**Exercice 4 [8,5 pts]**: *Soient $p \geq 2$ un nombre premier.*

(a) *Montrer que $F(Y) = \dfrac{(Y+1)^p - 1}{Y}$ est un polynôme en $Y$ à coefficients dans $\mathbb{Z}$.*

**Correction**: La formule du binôme de Newton donne

$$F(Y) = \frac{(\sum_{k=0}^{p} \binom{p}{k} Y^k) - 1}{Y} = \sum_{k=1}^{p} \binom{p}{k} Y^{k-1}$$

Les coefficients de $F$, les coefficients binomiaux $\binom{p}{1}, \ldots, \binom{p}{p}$, sont des entiers.

(b) *Montrer que $F(Y)$ est irréductible dans $\mathbb{Q}[Y]$. (Indication: on pourra appliquer le critère d'Eisenstein).*

**Correction**: On sait que $p$ divise tous les coefficients binomiaux $\binom{p}{k}$, $k = 1, \ldots, p-1$. Il divise donc tous les coefficients de $F$ sauf le coefficients dominant qui vaut 1, et $p^2$ ne divise pas le coefficient constant $\binom{p}{1}$ qui vaut $p$. D'après le critère d'Eisenstein, le polynôme $F(Y)$ est irréductible dans $\mathbb{Q}[Y]$.

*On considère le polynôme $\Phi(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$.*

(c) *Montrer que $F(X-1) = \Phi(X)$ et en déduire que $\Phi(X)$ est irréductible dans $\mathbb{Q}[X]$.*

**Correction**: On a $F(X-1) = \dfrac{X^p - 1}{X - 1} = \sum_{k=0}^{p-1} X^k = \Phi(X)$.

Supposons que l'on ait $\Phi(X) = Q(X)\,R(X)$ avec $Q, R \in \mathbb{Q}[X]$. Cela entraîne que $\Phi(X+1) = Q(X+1)\,R(X+1)$ c'est-à-dire $F(X) = Q(X+1)\,R(X+1)$. Comme $F$ est irréductible, on déduit que $\deg(Q(X+1)) = 0$ ou bien $\deg(R(X+1)) = 0$ ce qui équivaut à $\deg(Q(X)) = 0$ ou bien $\deg(R(X)) = 0$ puisque $\deg(Q(X+1)) = \deg(Q(X))$ et $\deg(R(X+1)) = \deg(R(X))$. Cela montre que $\Phi(X)$ est irréductible dans $\mathbb{Q}[X]$.

(d) *On note $\mathbb{Q}[e^{2i\pi/p}]$ l'image du morphisme d'évaluation $E : \mathbb{Q}[X] \to \mathbb{C}$ qui envoie $X$ sur $e^{2i\pi/p}$. Montrer que $\mathbb{Q}[e^{2i\pi/p}]$ est le plus petit sous-anneau de $\mathbb{C}$ contenant le corps $\mathbb{Q}$ et le nombre $e^{2i\pi/p}$.*

**Correction**: L'ensemble $\mathbb{Q}[e^{2i\pi/p}] = E(\mathbb{Q}[X])$ est un anneau car image d'un anneau par un morphisme, et il contient $e^{2i\pi/p} = E(X)$ et $\mathbb{Q}$. Par ailleurs, si $A \subset \mathbb{C}$ est un anneau

contenant $e^{2i\pi/p}$ et $\mathbb{Q}$, alors $A$ est stable par somme et produit et contient donc tous les éléments de la forme $P(e^{2i\pi/p})$ avec $P \in \mathbb{Q}[X]$; c'est-à-dire $A \supset \mathbb{Q}[e^{2i\pi/p}]$.

(e) *Montrer que* $\ker(E)$ *est l'idéal de* $\mathbb{Q}[X]$ *engendré par* $\Phi(X)$ *et en déduire que* $\mathbb{Q}[e^{2i\pi/p}]$ *est un sous-corps de* $\mathbb{C}$.

**Correction**: On a $\Phi(e^{2i\pi/p}) = ((e^{2i\pi/p})^p - 1)/(e^{2i\pi/p} - 1) = 0$ et donc $\Phi(X) \in \ker(E)$. Il en résulte que $\ker(E)$ contient l'idéal $\langle \Phi(X) \rangle$ de $\mathbb{Q}[X]$ engendré par $\Phi(X)$. Mais comme l'anneau $\mathbb{Q}[X]$ est principal et que $\Phi(X)$ est irréductible, l'idéal $\langle \Phi(X) \rangle$ est maximal. L'inclusion $\langle \Phi(X) \rangle \subset \ker(E)$ associée au fait que l'idéal $\ker(E)$ est propre (1 n'y appartient pas) entraîne donc que $\langle \Phi(X) \rangle = \ker(E)$. En conséquence, le noyau $\ker(E)$ est un idéal maximal de $\mathbb{Q}[X]$, l'anneau quotient $\mathbb{Q}[X]/\ker(E)$ est un corps, et comme $\mathbb{Q}[X]/\ker(E) \simeq E(\mathbb{Q}[X])$, l'anneau $E(\mathbb{Q}[X]) = \mathbb{Q}[e^{2i\pi/p}]$ est aussi un corps.

(f) *Montrer que* $(X-1)$ *divise* $X^p - 1$ *et que* $(X-1)^2$ *ne divise pas* $X^p - 1$ *dans* $\mathbb{Q}[X]$.

**Correction**: Le polynôme $X - 1$ divise le polynôme $X^p - 1$ car ce dernier s'annule en $X = 1$. Si $(X-1)^2$ divisait $X^p - 1$, le nombre 1 serait une racine d'ordre au moins 2 de $X^p - 1$, et 1 serait racine de $(X^p - 1)' = pX^{p-1}$, ce qui n'est pas le cas: $p \cdot 1^{p-1} = p \neq 0$.

(g) *Montrer que* $Y^p + X^p - 1$ *est un polynôme irréductible dans* $\mathbb{Q}[X, Y]$.

**Correction**: Le polynôme $X - 1$ divise tous les coefficients, dans $\mathbb{Q}[X]$, du polynôme $Y^p + X^p - 1 \in \mathbb{Q}[X][Y]$ sauf le coefficient dominant, qui vaut 1, et d'après ce qui précède, $(X-1)^2$ ne divise pas son coefficient constant. D'après le critère d'Eisenstein, le polynôme $Y^p + X^p - 1$ est irréductible dans $\mathbb{Q}[X, Y]$.

(h) *Montrer que l'anneau quotient* $\mathbb{Q}[X, Y]/\langle Y^p + X^p - 1 \rangle$ *de* $\mathbb{Q}[X, Y]$ *par l'idéal engendré par* $Y^p + X^p - 1$ *est intègre mais que la classe de* $X$ *modulo* $\langle Y^p + X^p - 1 \rangle$ *n'est pas inversible dans cet anneau.*

**Correction**: De l'irréductibilité de $Y^p + X^p - 1$ dans l'anneau factoriel $\mathbb{Q}[X, Y]$ résulte que l'idéal $\langle Y^p + X^p - 1 \rangle$ est premier, c'est-à-dire que l'anneau quotient $\mathbb{Q}[X, Y]/\langle Y^p + X^p - 1 \rangle$ est intègre.

Supposons la classe de $X$ modulo $\langle Y^p + X^p - 1 \rangle$ inversible dans $\mathbb{Q}[X, Y]/\langle Y^p + X^p - 1 \rangle$. Il existe alors $U(X, Y), V(X, Y) \in \mathbb{Q}[X, Y]$ tels que $X\,U(X, Y) + V(X, Y)\,(Y^p + X^p - 1) = 1$. En substituant 0 à $X$ et 1 à $Y$, on obtient $0 = 1$, la contradiction voulue.

# UNIVERSITÉ LILLE 1

Enseignants: **A. BROUSTET, P. DÈBES, M. HUTTNER**
Filière: **Licence - Semestre 5**
Matière: **M 51**
Année universitaire: **2010/2011**
Épreuve: **Session de rattrapage**
Date: **mercredi 19 janvier à 8h**
Lieu: **Bâtiment A5**

---

**ÉTUDIANTS REPASSANT M301: PARTIE II SEULE EN 2 HEURES**

**ÉTUDIANTS REPASSANT M308: PARTIE I SEULE EN 2 HEURES**

**AUTRES ÉTUDIANTS: PARTIES I ET II EN 3 HEURES 30 MINUTES**

**PARTIES I ET II SUR DEUX COPIES DIFFÉRENTES**

**Ni calculatrice ni documents ni téléphone portable.**
**Une grande importance sera accordée à la rédaction.**
**Le barème, donné à titre indicatif sur 10 pour chaque partie,**
**sera adapté aux différentes durées de composition.**

---

## PARTIE I

**Exercice 1 [5 pts]**: Soit $G$ un groupe d'ordre 225.

(a) Quel est l'ordre des 3-sous-groupes de Sylow et celui des 5-sous-groupes de Sylow? Expliquer pourquoi ces sous-groupes sont abéliens et les déterminer à isomorphisme près.

(b) Montrer que si $\mathcal{S}_3$ et $\mathcal{S}_5$ désignent respectivement un 3-sous-groupe de Sylow et un 5-sous-groupe de Sylow de $G$, alors $G$ est isomorphe au produit semi-direct de $\mathcal{S}_5$ par $\mathcal{S}_3$.

(c) On suppose dans cette question que $\mathcal{S}_5$ est cyclique. Montrer qu'alors l'action de $\mathcal{S}_3$ sur $\mathcal{S}_5$ est triviale et que $G$ est abélien. (Indication: on pourra commencer par montrer que le groupe $\mathrm{Aut}(\mathcal{S}_5)$ des automorphismes de $\mathcal{S}_5$ est d'ordre 20).

(d) On suppose dans cette question que $G$ est abélien. Déterminer toutes les possibilités pour $G$ à isomorphisme près et indiquer celles pour lesquelles $\mathcal{S}_5$ est cyclique.

**Exercice 2 [5 pts]**: (a) Vérifier que la matrice $A = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$ est d'ordre 3 dans le groupe $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$ des matrices à coefficients dans $\mathbb{Z}/5\mathbb{Z}$ de déterminant non nul.

**T.S.V.P.**

Dans la suite, on identifie $A$ à l'automorphisme $\mathcal{A} \in \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$ défini par

$$\mathcal{A}(x, y) = (-y, x - y) \qquad (x, y) \in \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

(b) Soit $\rho : \mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$ l'homomorphisme défini par $\rho(n) = \mathcal{A}^n$ $(n \in \mathbb{N})$. Montrer que $\rho$ se factorise par $\mathbb{Z}/3\mathbb{Z}$, c'est-à-dire, s'écrit $\rho = \bar{\rho} \circ s$ avec $s = \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ la surjection canonique et $\bar{\rho} : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$ un homomorphisme.

(c) Expliquer comment définir grâce au morphisme $\bar{\rho}$ un produit semi-direct du groupe $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ par le groupe $\mathbb{Z}/3\mathbb{Z}$. Expliciter la loi de groupe et montrer qu'elle n'est pas commutative. Quel est l'ordre de ce produit semi-direct?

(d) Donner un exemple de groupe d'ordre 225 qui ne soit pas abélien.

## PARTIE II

**Exercice 3 [5 pts]**: Soit $P \in \mathbb{Z}[X]$ le polynôme défini par $P(X) = X^3 + X + 5$.

(a) Montrer que $P$ n'a pas de racine $a/b \in \mathbb{Q}$.

(b) Montrer que $P$ est irréductible dans $\mathbb{Q}[X]$ et dans $\mathbb{Z}[X]$.

(c) Montrer que l'anneau quotient $\mathbb{Q}[X]/P\,\mathbb{Q}[X]$ de $\mathbb{Q}[X]$ par l'idéal engendré par $P$ dans $\mathbb{Q}[X]$ est un corps.

(d) Montrer que l'anneau quotient $\mathbb{Z}[X]/P\,\mathbb{Z}[X]$ de $\mathbb{Z}[X]$ par l'idéal engendré par $P$ dans $\mathbb{Z}[X]$ est intègre mais n'est pas un corps. (Indication: pour la seconde partie, on pourra montrer que la classe de 5 modulo $P$ n'est pas inversible dans $\mathbb{Z}[X]/P\,\mathbb{Z}[X]$).

(e) Montrer que pour tout entier $n \geq 1$, le polynôme $Y^n - (X^3 + X + 5)$ est irréductible dans $\mathbb{Q}[X, Y]$ et dans $\mathbb{Z}[X, Y]$. (Indication: on pourra appliquer le critère d'Eisenstein).

**Exercice 4 [5 pts]**: Soit $p$ un nombre premier et $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$. On note

$$r : \mathbb{Z}[X] \to \mathbb{F}_p[X]$$

le morphisme qui à $F = \sum_{i=0}^{n} f_i X^i \in \mathbb{Z}[X]$ associe le polynôme $r(F) = \sum_{i=0}^{n} \overline{f_i} X^i \in \mathbb{F}_p[X]$ dont les coefficients sont les classes $\overline{f_i}$ modulo $p$ des coefficients $f_i$ de $F$ et

$$s : \mathbb{F}_p[X] \to \mathbb{F}_p[X]/\langle X^3 + X + \overline{5} \rangle$$

la surjection canonique associée au quotient de $\mathbb{F}_p[X]$ par l'idéal $\langle X^3 + X + \overline{5} \rangle$ engendré par $r(P) = X^3 + X + \overline{5}$ dans $\mathbb{F}_p[X]$.

(a) Montrer que $r$, $s$ et $s \circ r$ sont surjectives.

(b) Montrer que le noyau $\ker(s \circ r)$ est l'idéal $\langle p, X^3 + X + 5 \rangle$ engendré par $p$ et $X^3 + X + 5$ dans $\mathbb{Z}[X]$.

(c) En déduire que les anneaux $\mathbb{F}_p[X]/\langle X^3 + X + \overline{5} \rangle$ et $\mathbb{Z}[X]/\langle p, X^3 + X + 5 \rangle$ sont isomorphes.

(d) On prend ici $p = 2$. Montrer que $\langle 2, X^3 + X + 5 \rangle$ est un idéal maximal de $\mathbb{Z}[X]$. (Indication: on pourra montrer d'abord que $X^3 + X + \overline{5}$ est irréductible dans $\mathbb{F}_2[X]$).

(e) On prend ici $p = 5$. Montrer que $\langle 5, X^3 + X + 5 \rangle$ n'est pas un idéal premier de l'anneau $\mathbb{Z}[X]$.

# UNIVERSITÉ LILLE 1

Enseignants: **A. BROUSTET, P. DÈBES, S. DELAUNAY**
Filière: **Licence - Semestre 5**
Matière: **M 51**
Année universitaire: **2011/2012**
Épreuve: **Devoir surveillé**
Date: **vendredi 4 novembre à 14h**
Lieu: **P1 Fresnel**
Durée de l'épreuve: **2 heures**

---

**Ni calculatrices ni documents ni téléphone portable.**
**Une grande importance sera accordée à la rédaction.**

---

*(On pourra utiliser sans les redémontrer des résultats vus en TD à condition d'en rappeler précisément les énoncés).*

Dans le groupe symétrique $S_6$ on considère les permutations

$$\begin{cases} \omega_1 = (1\,2\,3) \\ \omega_2 = (4\,5\,6) \\ \tau = (1\,4)(2\,5)(3\,6) \end{cases}$$

et on note $G$ le sous-groupe engendré par $\omega_1$, $\omega_2$ et $\tau$.

(a) /1 Donner l'ordre et la signature de chacun des éléments $\omega_1$, $\omega_2$, $\tau$ du groupe $S_6$.

(b) /1,5 Calculer les éléments $\tau\omega_1\tau^{-1}$, $\tau\omega_2\tau^{-1}$, $\tau\omega_1$.

(c) /0,5 Le groupe $G$ est-il abélien?

(d) /1,75 Donner la définition de l'énoncé: "l'action de $G$ sur l'ensemble $\{1,\ldots,6\}$ est transitive" (question de cours). Préciser ensuite si cet énoncé est vrai en justifiant la réponse.

On note $H$ le sous-groupe de $G$ engendré par $\omega_1, \omega_2$ et $K$ le sous-groupe engendré par $\tau$.

(e) /2,5 Montrer que l'application $(n_1, n_2) \in \mathbb{Z}^2 \to \omega_1^{n_1}\omega_2^{n_2} \in S_6$ permet de définir une application $\Phi : (\mathbb{Z}/3\mathbb{Z})^2 \to H$ et que cette application est un isomorphisme de groupes.

(f) /1,5 Montrer que $H$ est un sous-groupe distingué de $G$.

(g) /1 Montrer que $H \cap K = \{1\}$.

(h) /1,25 (question de cours) Que permettent de déduire les questions (f) et (g) sur la structure du groupe engendré par $H$ et $K$ (c'est-à-dire du groupe $G$)?

**T.S.V.P.**

(i) /1 Montrer que $G$ est isomorphe à un produit semi-direct de $(\mathbb{Z}/3\mathbb{Z})^2$ par $\mathbb{Z}/2\mathbb{Z}$.

(j) /1,25 Montrer que l'ordre de $G$ divise l'ordre du groupe alterné $A_6$ mais que $G$ n'est pas inclus dans $A_6$.

(k) /1,25 (question de cours) Quelles sont les classes de conjugaison dans $S_6$ de $\omega_1$, de $\omega_2$ et de $\omega_1\omega_2$?

(l) /2 Montrer qu'un sous-groupe distingué de $S_6$ qui contient $H$ contient nécessairement $A_6$ et que le seul sous-groupe distingué de $S_6$ qui contient $G$ est $S_6$.

(m) /1 Montrer que la classe de conjugaison, notée $\mathcal{O}(\omega_1\omega_2)$, de l'élément $\omega_1\omega_2$ dans $S_6$ possède 40 éléments.

On note $\mathrm{Cen}_{S_6}(\omega_1\omega_2) = \{g \in S_6 \mid g(\omega_1\omega_2) = (\omega_1\omega_2)g\}$ le centralisateur de $\omega_1\omega_2$ dans le groupe $S_6$.

(n) /1,5 Montrer que $\mathrm{Cen}_{S_6}(\omega_1\omega_2)$ est le fixateur de $\omega_1\omega_2$ dans l'action de $S_6$ par conjugaison sur lui-même. Quel est le lien entre $|\mathrm{Cen}_{S_6}(\omega_1\omega_2)|$, $|S_6|$ et $\mathrm{card}(\mathcal{O}(\omega_1\omega_2))$?

(o) /1,5 Montrer que $\mathrm{Cen}_{S_6}(\omega_1\omega_2)$ contient le groupe $G$.

(p) /1 Calculer les indices $[S_6 : G]$, $[S_6 : \mathrm{Cen}_{S_6}(\omega_1\omega_2)]$ et montrer que $\mathrm{Cen}_{S_6}(\omega_1\omega_2) = G$.

# UNIVERSITÉ LILLE 1

Enseignants: **A. BROUSTET, P. DÈBES, S. DELAUNAY**
Filière: **Licence - Semestre 5**
Matière: **M 51**
Année universitaire: **2011/2012**
Épreuve: **Devoir Surveillé**
Date: **vendredi 4 novembre 2011 de 14h à 16h**

---

## CORRIGÉ

---

*Dans le groupe symétrique $S_6$ on considère les permutations*

$$\begin{cases} \omega_1 = (1\,2\,3) \\ \omega_2 = (4\,5\,6) \\ \tau = (1\,4)(2\,5)(3\,6) \end{cases}$$

*et on note $G$ le sous-groupe engendré par $\omega_1$, $\omega_2$ et $\tau$.*

(a) *Donner l'ordre et la signature de chacun des éléments $\omega_1$, $\omega_2$, $\tau$ du groupe $S_6$.*

**Correction**: $\omega_1$, $\omega_2$, $\tau$ sont respectivement d'ordre 3, 3, 2, et de signature 1, 1, $-1$.

(b) *Calculer les éléments $\tau\omega_1\tau^{-1}$, $\tau\omega_2\tau^{-1}$, $\tau\omega_1$.*

**Correction**: On a $\tau\omega_1\tau^{-1} = (\tau(1)\,\tau(2)\,\tau(3)) = (4\,5\,6) = \omega_2$. De la même façon, on trouve $\tau\omega_2\tau^{-1} = \omega_1$. Enfin $\tau\omega_1 = (1\,5\,2\,6\,3\,4)$.

(c) *Le groupe $G$ est-il abélien?*

**Correction**: Comme $\tau\omega_1\tau^{-1} = \omega_2 \neq \omega_1$, le groupe $G$ n'est pas abélien.

(d) *Donner la définition de l'énoncé: "l'action de $G$ sur l'ensemble $\{1,\dots,6\}$ est transitive" (question de cours). Préciser ensuite si cet énoncé est vrai en justifiant la réponse.*

**Correction**: L'action de $G$ sur l'ensemble $\{1,\dots,6\}$ est transitive si pour tous $i,j \in \{1,\dots,6\}$, il existe $g \in G$ tel que $g(i) = j$, ou de façon équivalente, si l'action n'a qu'une seule orbite: $\{1,\dots,6\}$. Cette énoncé est vrai: $G$ contient le 6-cycle $\tau\omega_1$ dont la seule orbite est $\{1,\dots,6\}$.

*On note $H$ le sous-groupe de $G$ engendré par $\omega_1, \omega_2$ et $K$ le sous-groupe engendré par $\tau$.*

(e) *Montrer que l'application $(n_1, n_2) \in \mathbb{Z}^2 \to \omega_1^{n_1}\omega_2^{n_2} \in S_6$ permet de définir une application $\Phi : (\mathbb{Z}/3\mathbb{Z})^2 \to H$ et que cette application est un isomorphisme de groupes.*

**Correction**: Comme $\omega_1, \omega_2$ sont d'ordre 3, l'expression $\omega_1^{n_1}\omega_2^{n_2}$ ne dépend que des classes modulo 3 de $n_1, n_2 \in \mathbb{Z}$, et définit bien une application $\Phi : (\mathbb{Z}/3\mathbb{Z})^2 \to H$. On vérifie facilement que cette application est un morphisme; juste noter que $\omega_1, \omega_2$ commutent. Par définition de $H$, $\Phi$ est surjective. Enfin on a $\omega_1^{n_1}\omega_2^{n_2} = 1$ si et seulement si $\omega_1^{n_1} = \omega_2^{n_2} = 1$ si et seulement si $n_1, n_2$ sont des multiples de 3. Cela prouve l'injectivité de $\Phi$.

(f) *Montrer que $H$ est un sous-groupe distingué de $G$.*

**Correction**: Il suffit de vérifier que $ghg^{-1} \in H$ pour $h \in \{\omega_1, \omega_2\}$ et $g \in \{\omega_1, \omega_2, \tau\}$. Pour $g \in \{\omega_1, \omega_2\}$, c'est clair puisque $H$ est abélien. Pour $g = \tau$, cela résulte des formules $\tau\omega_1\tau^{-1} = \omega_2$ et $\tau\omega_2\tau^{-1} = \omega_1$ vues en (b).

(g) *Montrer que $H \cap K = \{1\}$.*

**Correction**: $H \cap K$ est un groupe d'ordre divisant $|H| = 9$ et $|K| = 2$. D'où $|H \cap K| = 1$ et $H \cap K = \{1\}$.

(h) *(question de cours) Que permettent de déduire les questions (f) et (g) sur la structure du groupe engendré par $H$ et $K$ (c'est-à-dire du groupe $G$)?*

**Correction**: Les questions (f) et (g) permettent de déduire que $\langle H \cup K \rangle = HK = G$, que $G/H \simeq K/(H \cap K) \simeq K$ et que la suite exacte $1 \to H \to G \to G/H \to 1$ est scindée; de façon équivalente, $G$ est isomorphe à un produit semi-direct de $H$ par $K$.

(i) *Montrer que $G$ est isomorphe à un produit semi-direct de $(\mathbb{Z}/3\mathbb{Z})^2$ par $\mathbb{Z}/2\mathbb{Z}$.*

**Correction**: Comme $H \simeq (\mathbb{Z}/3\mathbb{Z})^2$ et $K \simeq \mathbb{Z}/2\mathbb{Z}$, le groupe $G$ est isomorphe à un produit semi-direct de $(\mathbb{Z}/3\mathbb{Z})^2$ par $\mathbb{Z}/2\mathbb{Z}$.

(j) *Montrer que l'ordre de $G$ divise l'ordre du groupe alterné $A_6$ mais que $G$ n'est pas inclus dans $A_6$.*

**Correction**: De (i), on déduit que $|G| = 18$. Comme $|A_6| = 6!/2 = 360 = 20 \times 18$, l'ordre de $G$ divise celui de $A_6$ mais $G \not\subset A_6$ puisque $\tau \in G$ et $\tau \notin A_6$.

(k) *(question de cours) Quelles sont les classes de conjugaison dans $S_6$ de $\omega_1$, de $\omega_2$ et de $\omega_1\omega_2$?*

**Correction**: La classe de conjugaison de $\omega_1$ dans $S_6$ est l'ensemble $3^1$ de tous les 3-cycles. *Idem* pour $\omega_2$. La classe de conjugaison de $\omega_1\omega_2$ est l'ensemble $3^2$ de tous les produits de deux 3-cycles à supports disjoints.

(l) *Montrer qu'un sous-groupe distingué de $S_6$ qui contient $H$ contient nécessairement $A_6$ et que le seul sous-groupe distingué de $S_6$ qui contient $G$ est $S_6$.*

**Correction**: Soit $N$ un sous-groupe distingué de $S_6$. Si $N \supset H$, il contient tous les 3-cycles et donc $A_6$ puisque $A_6$ est engendré par les 3-cycles. Si $N \supset G$, il contient $A_6$ d'après ce qui précède. Donc $N$ est égal soit à $A_6$ soit à $S_6$. Mais $N$ ne peut être égal à $A_6$ car alors on aurait $G \subset A_6$. D'où $N = S_6$.

(m) *Montrer que la classe de conjugaison, notée $\mathcal{O}(\omega_1\omega_2)$, de l'élément $\omega_1\omega_2$ dans $S_6$ possède 40 éléments.*

**Correction**: D'après (k), il faut compter le nombre de produits de deux 3-cycles à supports disjoints. Il y a $5 \times 4 = 20$ possibilités pour le 3-cycle contenant l'élément 1 dans son support. Un tel 3-cycle étant donné, il y a 2 possibilités pour le second 3-cycle. La classe $\mathcal{O}(\omega_1\omega_2)$ comporte donc 40 éléments.

*On note $\mathrm{Cen}_{S_6}(\omega_1\omega_2) = \{g \in S_6 \mid g(\omega_1\omega_2) = (\omega_1\omega_2)g\}$ le centralisateur de $\omega_1\omega_2$ dans le groupe $S_6$.*

(n) *Montrer que $\mathrm{Cen}_{S_6}(\omega_1\omega_2)$ est le fixateur de $\omega_1\omega_2$ dans l'action de $S_6$ par conjugaison sur lui-même. Quel est le lien entre $|\mathrm{Cen}_{S_6}(\omega_1\omega_2)|$, $|S_6|$ et $\mathrm{card}(\mathcal{O}(\omega_1\omega_2))$?*

**Correction**: Pour la première partie, il suffit de récrire $g(\omega_1\omega_2) = (\omega_1\omega_2)g$ dans la définition de $\mathrm{Cen}_{S_6}(\omega_1\omega_2)$ sous la forme équivalente $g(\omega_1\omega_2)g^{-1} = \omega_1\omega_2$. On sait ensuite que $\mathrm{card}(\mathcal{O}(\omega_1\omega_2)) = |S_6|/|\mathrm{Cen}_{S_6}(\omega_1\omega_2)|$.

(o) *Montrer que $\mathrm{Cen}_{S_6}(\omega_1\omega_2)$ contient le groupe $G$.*

**Correction**: Comme $\mathrm{Cen}_{S_6}(\omega_1\omega_2)$ est un groupe, il suffit de vérifier que $\omega_1, \omega_2, \tau \in \mathrm{Cen}_{S_6}(\omega_1\omega_2)$. Comme $\omega_1$ et $\omega_2$ commutent, on a que $\omega_i(\omega_1\omega_2)\omega_i^{-1} = \omega_1\omega_2$, $i = 1, 2$. On a d'autre part $\tau(\omega_1\omega_2)\tau^{-1} = \tau\omega_1\tau^{-1}\tau\omega_2\tau^{-1} = \omega_2\omega_1 = \omega_1\omega_2$.

(p) *Calculer les indices $[S_6 : G]$, $[S_6 : \mathrm{Cen}_{S_6}(\omega_1\omega_2)]$ et montrer que $\mathrm{Cen}_{S_6}(\omega_1\omega_2) = G$.*

**Correction**: On a $[S_6 : G] = 6!/18 = 40$. D'après (m) et (n), on a $[S_6 : \mathrm{Cen}_{S_6}(\omega_1\omega_2)] = \mathrm{card}(\mathcal{O}(\omega_1\omega_2)) = 40$. On déduit que $|G| = |\mathrm{Cen}_{S_6}(\omega_1\omega_2)|$. Comme on sait déjà que $G \subset \mathrm{Cen}_{S_6}(\omega_1\omega_2)$, on a $G = \mathrm{Cen}_{S_6}(\omega_1\omega_2)$.

# UNIVERSITÉ LILLE 1

Enseignants: **A. BROUSTET, P. DÈBES, S. DELAUNAY**
Module: **Licence - Semestre 5 - M 51**
Année universitaire: **2011/2012**
Épreuve: **Devoir Surveillé 2**
Date: **mercredi 11 janvier de 8h à 12h**
Lieu: **Halles Grémeaux**

---

**CHAQUE PARTIE SERA RÉDIGÉE SUR UNE COPIE DIFFÉRENTE**
**UNE GRANDE IMPORTANCE SERA ACCORDÉE À LA RÉDACTION.**
**Ni calculatrices ni documents ni téléphone portable.**
**Le barème est donné à titre indicatif.**

---

## PARTIE I

**Exercice 1 [7,5 pts]**: (a) Montrer que si pour un nombre premier $p$, un groupe $G$ admet un unique $p$-Sylow $\mathcal{S}$, alors $\mathcal{S}$ est nécessairement distingué dans $G$.

(b) Soit $K$ un groupe d'ordre 15.

(b-1) Montrer qu'il existe un élément $\omega \in K$ qui engendre le groupe $K$.

(b-2) Montrer que si $\varphi : K \to A$ est un homomorphisme de groupes, alors $\varphi$ est déterminé par l'élément $\varphi(\omega) \in A$, et que $\varphi(\omega)$ est d'ordre 1, 3, 5 ou 15 dans le groupe $A$.

Soit $G$ un groupe d'ordre 345.

(c) Montrer que $G$ possède un 23-Sylow $H$ qui est distingué dans $G$.

(d) Montrer que

(d-1) $G$ possède un 5-Sylow qui est distingué dans $G$,

(d-2) $G$ possède un sous-groupe $K$ d'ordre 15.

(e) Montrer que $G$ est le produit semi-direct de $H$ par $K$, pour une action du sous-groupe $K$ sur le sous-groupe $H$.

(f) Déterminer les actions possibles de $K$ sur $H$ (Indication: on pourra utiliser la question (b) et le fait que le groupe des automorphismes du groupe $(\mathbb{Z}/23\mathbb{Z}, +)$ est d'ordre 22).

(g) Montrer que $G$ est cyclique.

**Exercice 2 [2,5 pts]**: (a) Vérifier que $Y^2 + XY + X^2 = (Y - jX)(Y - j^2X)$ dans $\mathbb{C}[X, Y]$ (où $j = e^{2i\pi/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$).

(b) Donner la définition d'"anneau factoriel".

(c) Les anneaux $\mathbb{C}[X, Y]$ et $\mathbb{R}[X, Y]$ sont-ils factoriels? Justifier la réponse.

(d) Ecrire la factorisation en irréductibles du polynôme $Y^2 + XY + X^2$ dans l'anneau $\mathbb{C}[X, Y]$, puis dans l'anneau $\mathbb{R}[X, Y]$. Justifier la réponse.

(e) Montrer que l'anneau $\mathbb{R}[X, Y]/\langle X^2 + XY + Y^2 \rangle$ est intègre.

**T.S.V.P.**

# PARTIE II

**Exercice 3 [2 pts]**: On note $A$ l'anneau intègre $\mathbb{R}[X,Y]/\langle X^2+XY+Y^2\rangle$ et $\overline{X}$ et $\overline{Y}$ les classes respectives de $X$ et de $Y$ modulo l'idéal $\langle X^2+XY+Y^2\rangle$.

(a) Montrer que $\overline{X} \neq \overline{0}$ dans $A$.

(b) Rappeler les définitions de "partie multiplicative $S$ de l'anneau $A$" et d'"anneau $S^{-1}A$ des fractions de $A$ à dénominateur dans $S$".

(c) Montrer que l'ensemble $S = \{\overline{X}^m \mid m \in \mathbb{N}\}$ est une partie multiplicative de $A$ et que les éléments $\overline{X}$ et $\overline{Y}$ sont inversibles dans $S^{-1}A$. (Indication: pour $\overline{Y}$, noter que $\overline{X}^2 + \overline{XY} + \overline{Y}^2 = 0$ dans $A$).

**Exercice 4 [8 pts]**: On note $\alpha = \sqrt[3]{2}$ l'unique racine cubique de 2 dans $\mathbb{R}$.

(a) Montrer que le polynôme $X^3-2$ est irréductible dans $\mathbb{Z}[X]$ et que $\alpha \notin \mathbb{Q}$.

On note $v_\alpha : \mathbb{Z}[X] \to \mathbb{R}$ le morphisme qui à tout polynôme $f \in \mathbb{Z}[X]$ associe l'élément $f(\alpha) \in \mathbb{R}$ et $\mathbb{Z}[\alpha]$ l'anneau image de $v_\alpha$, c'est-à-dire $\mathbb{Z}[\alpha] = \{f(\alpha) \mid f \in \mathbb{Z}[X]\}$.

(b) Montrer que

(b-1) $\mathbb{Z}[\alpha]$ est un sous-anneau de $\mathbb{R}$ qui contient $\mathbb{Z}$ et $\alpha$,

(b-2) $\mathbb{Z}[\alpha]$ est le plus petit sous-anneau de $\mathbb{R}$ qui contient $\mathbb{Z}$ et $\alpha$.

(c-1) Pour $f \in \mathbb{Z}[X]$, écrire avec précision la division euclidienne de $f$ par $X^3-2$, après en avoir justifié l'existence.

(c-2) Montrer que pour tout polynôme $R \in \mathbb{Q}[X]$ non nul de degré $\leq 2$, il existe deux polynômes $U, V \in \mathbb{Q}[X]$ tels que

$$U(X)R(X) + V(X)(X^3-2) = 1$$

(On ne cherchera pas à expliciter les polynômes $U$ et $V$).

(d) En utilisant la question (c), montrer, en détaillant bien les raisonnements, que

(d-1) $\mathbb{Z}[\alpha]$ est isomorphe à l'anneau $\mathbb{Z}[X]/\langle X^3-2\rangle$,

(d-2) $\mathbb{Z}[\alpha] = \{a + b\alpha + c\alpha^2 \mid a,b,c \in \mathbb{Z}\}$.

(e) Montrer que

(e-1) il n'existe pas de polynômes $A, B \in \mathbb{Z}[X]$ tels que $2A(X) + B(X)(X^3-2) = 1$. (Indication: chercher une contradiction en considérant une valeur spéciale de $X$ dans $\mathbb{Z}$).

(e-2) 2 n'est pas inversible dans l'anneau $\mathbb{Z}[\alpha]$.

(f) Montrer que pour tout nombre nombre premier $p \in \mathbb{N}$, on a

$$\mathbb{Z}[\alpha]/\langle p\rangle \simeq \mathbb{Z}[X]/\langle p, X^3-2\rangle \simeq (\mathbb{Z}/p\mathbb{Z})[X]/\langle X^3-\overline{2}\rangle$$

où on désigne par $\overline{2}$ la classe de 2 modulo $p$. (On justifiera soigneusement les différentes étapes du raisonnement en rappelant les résultats du cours utilisés).

(g) On prend ici $p = 11$. Montrer que

(g-1) $X^3-\overline{2}$ a une racine dans $\mathbb{Z}/11\mathbb{Z}$,

(g-2) L'idéal $\langle 11\rangle$ engendré par 11 dans $\mathbb{Z}[\alpha]$ n'est pas premier.

# UNIVERSITÉ LILLE 1

Enseignants: **A. BROUSTET, P. DÈBES, S. DELAUNAY**
Module: **Licence - Semestre 5 - M 51**
Année universitaire: **2011/2012**
Épreuve: **Devoir Surveillé 2**
Date: **mercredi 11 janvier de 8h à 12h**

---

**CORRIGÉ**

---

## PARTIE I

**Exercice 1 [7,5 pts]**: (a) *Montrer que si pour un nombre premier $p$, un groupe $G$ admet un unique $p$-Sylow $\mathcal{S}$, alors $\mathcal{S}$ est nécessairement distingué dans $G$.*

**Correction**: Pour tout $g \in G$, le groupe $g\mathcal{S}g^{-1}$, image de $G$ par l'automorphisme de conjugaison par $g$, est de même ordre que $\mathcal{S}$; c'est donc un $p$-Sylow de $G$. Par unicité de $\mathcal{S}$, on obtient $g\mathcal{S}g^{-1} = \mathcal{S}$. Comme $g \in G$ est arbitraire, $\mathcal{S}$ est distingué dans $G$.

(b) *Soit $K$ un groupe d'ordre* 15.

(b-1) *Montrer qu'il existe un élément $\omega \in K$ qui engendre le groupe $K$.*

**Correction**: D'après les théorèmes de Sylow, le nombre de 3-Sylows de $K$ est congru à 1 modulo 3 et divise 5 et le nombre de 5-Sylows de $K$ est congru à 1 modulo 5 et divise 3. Ces deux nombres valent donc 1, d'où il existe un unique 3-Sylow $\mathcal{S}_3$ et un unique 5-Sylow $\mathcal{S}_5$. D'après le (a), ces deux sous-groupes sont distingués. On en déduit que tout élément $a \in \mathcal{S}_3$ commute à tout élément $b \in \mathcal{S}_5$: en effet $aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) = (aba^{-1})b^{-1}$ appartient à $\mathcal{S}_3 \cap \mathcal{S}_5$ lequel est le groupe trivial puisque d'ordre divisant 3 et 5. Si $a$ et $b$ sont des générateurs respectifs de $\mathcal{S}_3$ et $\mathcal{S}_5$ (qui sont cycliques puisque 3 et 5 sont premiers), alors $\omega = ab$ est d'ordre $\text{ppcm}(3,5) = 15$; $\omega$ engendre $K$.

(b-2) *Montrer que si $\varphi : K \to A$ est un homomorphisme de groupes, alors $\varphi$ est déterminé par l'élément $\varphi(\omega) \in A$, et que $\varphi(\omega)$ est d'ordre* 1, 3, 5 *ou* 15 *dans le groupe $A$.*

**Correction**: Tout élément $x \in K$ s'écrit $x = \omega^n$ pour un $n \in \mathbb{Z}$. On a alors $\varphi(x) = \varphi(\omega^n) = \varphi(\omega)^n$. L'élément $\varphi(\omega)$ détermine donc $\varphi$. De $\omega^{15} = 1$, on déduit $\varphi(\omega)^{15} = 1$. L'élément $\varphi(\omega) \in A$ est donc d'ordre divisant 15, soit d'ordre 1, 3, 5 ou 15.

*Soit $G$ un groupe d'ordre* 345.

(c) *Montrer que $G$ possède un* 23*-Sylow $H$ qui est distingué dans $G$.*

**Correction**: On a $345 = 3.5.23$. Le nombre de 23-Sylows de $G$ est congru à 1 modulo 23 et divise 15; c'est donc 1. Il existe un unique 23-Sylow $H$ qui est distingué dans $G$ d'après le (a).

(d) *Montrer que*

(d-1) $G$ possède un 5-Sylow qui est distingué dans $G$,

**Correction**: Le nombre de 5-Sylows de $G$ est congru à 1 modulo 5 et divise 69; c'est donc 1. Il existe un unique 5-Sylow $\mathcal{S}_5$ qui est distingué dans $G$ d'après le (a).

(d-2) *$G$ possède un sous-groupe $K$ d'ordre* 15.

**Correction**: Soit $\mathcal{S}_3$ un 3-Sylow de $G$. Comme $\mathcal{S}_5$ est distingué dans $G$, l'ensemble $K = \mathcal{S}_3.\mathcal{S}_5$ est un sous-groupe de $G$ (le sous-groupe $\langle \mathcal{S}_3 \cup \mathcal{S}_5 \rangle$) et $K/\mathcal{S}_5 \simeq \mathcal{S}_3/(\mathcal{S}_3 \cap \mathcal{S}_5)$. Comme $\mathcal{S}_3 \cap \mathcal{S}_5 = \{1\}$, on obtient que $K$ est d'ordre $|\mathcal{S}_3|.|\mathcal{S}_5| = 3.5 = 15$.

(e) *Montrer que $G$ est le produit semi-direct de $H$ par $K$, pour une action du sous-groupe $K$ sur le sous-groupe $H$.*

**Correction**: Le sous-groupe $H$ est distingué dans $G$ et $H \cap K = \{1\}$ ($|H \cap K|$ divise 23 et 15). On sait alors que $H.K$ est un sous-groupe de $G$ (le sous-groupe $\langle H \cup K \rangle$) et qu'il est isomorphe au produit semi-direct de $H$ par $K$, pour une action $\varphi : K \to \mathrm{Aut}(H)$ de $K$ sur $H$. De plus on a alors $|H.K| = |H|.|K| = 23.15 = |G|$ et donc $H.K = G$.

(f) *Déterminer les actions possibles de $K$ sur $H$ (Indication: on pourra utiliser la question (b) et le fait que le groupe des automorphismes du groupe $(\mathbb{Z}/23\mathbb{Z}, +)$ est d'ordre 22).*

**Correction**: D'après la question (b-1), le groupe $K$ peut être engendré par un élément $\omega \in K$ et d'après la question (b-2), l'homomorphisme $\varphi : K \to \mathrm{Aut}(H)$ correspondant à l'action de $K$ sur $H$, est déterminé par l'élément $\varphi(\omega) \in \mathrm{Aut}(H)$ et cet élément est d'ordre 1, 3, 5 ou 15. Comme $H \simeq \mathbb{Z}/23\mathbb{Z}$, le groupe $\mathrm{Aut}(H)$, isomorphe à $\mathrm{Aut}(\mathbb{Z}/23\mathbb{Z})$, est d'ordre 22. On en déduit que l'elément $\varphi(\omega) \in \mathrm{Aut}(H)$ est d'ordre divisant 22. Comme 15 et 22 sont premiers entre eux, $\varphi(\omega)$ est d'ordre 1, c'est-à-dire $\varphi(\omega) = \mathrm{Id}_H$. Il n'y a qu'une action de $K$ sur $H$: l'action triviale.

(g) *Montrer que $G$ est cyclique.*

**Correction**: L'action de $K$ sur $H$ étant l'action triviale, $G$ est le produit direct de $H$ par $K$ et donc $G \simeq \mathbb{Z}/23\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/345\mathbb{Z}$ d'après le lemme chinois; le groupe $G$ est cyclique d'ordre 345.

**Exercice 2 [2,5 pts]**: (a) *Vérifier que $Y^2 + XY + X^2 = (Y - jX)(Y - j^2X)$ dans $\mathbb{C}[X, Y]$ (où $j = e^{2i\pi/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$).*

**Correction**: On a $(Y - jX)(Y - j^2X) = Y^2 - (j + j^2)XY + j^3X^2 = Y^2 + XY + X^2$ puisque $j^3 = 1$ et $1 + j + j^2 = 0$.

(b) *Donner la définition d'"anneau factoriel".*

**Correction**: Un anneau intègre $A$ est dit factoriel si tout élément non nul de $A$ s'écrit comme produit d'irréductibles de $A$ et, si les facteurs irréductibles sont considérés à un facteur inversible près (c'est-à-dire, modulo la relation d'association), si cette factorisation est unique à l'ordre près des facteurs.

(c) *Les anneaux $\mathbb{C}[X, Y]$ et $\mathbb{R}[X, Y]$ sont-ils factoriels? Justifier la réponse.*

**Correction**: $\mathbb{C}$ et $\mathbb{R}$ étant des corps, les anneaux $\mathbb{C}[X]$ et $\mathbb{R}[X]$ sont principaux, *a fortiori* factoriels. D'après le théorème de transfert de Gauss, les anneaux $\mathbb{C}[X][Y] \simeq \mathbb{C}[X, Y]$ et $\mathbb{R}[X][Y] \simeq \mathbb{R}[X, Y]$ sont factoriels.

(d) *Ecrire la factorisation en irréductibles du polynôme $Y^2 + XY + X^2$ dans l'anneau $\mathbb{C}[X, Y]$, puis dans l'anneau $\mathbb{R}[X, Y]$. Justifier la réponse.*

**Correction**: Les polynômes $Y - jX$ et $Y - j^2X$, étant de degré 1, sont irréductibles dans $\mathbb{C}[X, Y]$. L'égalité $Y^2 + XY + X^2 = (Y - jX)(Y - j^2X)$ est une factorisation, et donc la factorisation en irréductibles de $Y^2 + XY + X^2$ dans $\mathbb{C}[X, Y]$. Dans $\mathbb{R}[X, Y]$, le polynôme $Y^2+XY+X^2$ est irréductible. En effet, une factorisation non triviale serait un produit de deux polynômes de $\mathbb{R}[X, Y]$ de degré 1. Elle serait aussi une factorisation en irréductibles de $\mathbb{C}[X, Y]$. Par unicité de cette dernière, les deux facteurs seraient $Y - jX$ et $Y - j^2X$, à un inversible de $\mathbb{C}[X, Y]$ près, c'est-à-dire, à un élément de $\mathbb{C}^\times$ près, ce qui est absurde puisque $\alpha(Y - jX), \alpha(Y - j^2X) \notin \mathbb{R}[X, Y]$, pour tout $\alpha \in \mathbb{C}^\times$.

(e) *Montrer que l'anneau* $\mathbb{R}[X,Y]/\langle X^2+XY+Y^2\rangle$ *est intègre.*

**Correction**: L'anneau $\mathbb{R}[X,Y]$ étant factoriel, l'idéal $\langle X^2+XY+Y^2\rangle$ qui est engendré par un élément irréductible de $\mathbb{R}[X,Y]$ est premier. L'anneau quotient $\mathbb{R}[X,Y]/\langle X^2+XY+Y^2\rangle$ est donc intègre.

## PARTIE II

**Exercice 3 [2 pts]**: *On note* $A$ *l'anneau intègre* $\mathbb{R}[X,Y]/\langle X^2+XY+Y^2\rangle$ *et* $\overline{X}$ *et* $\overline{Y}$ *les classes respectives de* $X$ *et de* $Y$ *modulo l'idéal* $\langle X^2+XY+Y^2\rangle$.

(a) *Montrer que* $\overline{X}\neq\overline{0}$ *dans* $A$.

**Correction**: Supposons $\overline{X}=\overline{0}$. On aurait alors $X\in\langle X^2+XY+Y^2\rangle$ c'est-à-dire, $X^2+XY+Y^2$ diviserait $X$ dans $\mathbb{R}[X,Y]$, ce qui, pour des raisons de degré, est absurde.

(b) *Rappeler les définitions de "partie multiplicative* $S$ *de l'anneau* $A$*" et d'"anneau* $S^{-1}A$ *des fractions de* $A$ *à dénominateur dans* $S$*".*

**Correction**: Une partie $S$ d'un anneau $A$ est dite multiplicative si $0\notin S$, $1\in S$ et si pour tous $s,s'\in S$, on $ss'\in S$. Si $S\subset A$ est une partie multiplicative, l'anneau des fractions de $A$ à dénominateur dans $S$ est l'ensemble $S^{-1}A=\{\frac{a}{s}\mid a\in A, s\in S\}$ muni des deux lois $+$ et $\times$ définies par:

$$\frac{a}{s}+\frac{a'}{s'}=\frac{as'+a's}{ss'}\quad\text{et}\quad\frac{a}{s}\times\frac{a'}{s'}=\frac{aa'}{ss'}\quad(\frac{a}{s},\frac{a'}{s'}\in S^{-1}A)$$

(c) *Montrer que l'ensemble* $S=\{\overline{X}^m\mid m\in\mathbb{N}\}$ *est une partie multiplicative de* $A$ *et que les éléments* $\overline{X}$ *et* $\overline{Y}$ *sont inversibles dans* $S^{-1}A$*. (Indication: pour* $\overline{Y}$*, noter que* $\overline{X}^2+\overline{XY}+\overline{Y}^2=0$ *dans* $A$*).*

**Correction**: On a $0\notin S$, $1\in S$ ($1=\overline{X}^0$) et si $m,m'\in\mathbb{N}$, alors $\overline{X}^m\cdot\overline{X}^{m'}=\overline{X}^{m+m'}\in S$; la partie $S\subset A$ est bien multiplicative. L'élément $\overline{X}\in A$ est inversible d'inverse $1/\overline{X}$. De $\overline{X}^2+\overline{XY}+\overline{Y}^2=0$, on déduit que $-(\overline{X}+\overline{Y})\overline{Y}/\overline{X}^2=1$, d'où $\overline{Y}$ est inversible dans $A$ d'inverse $-(\overline{X}+\overline{Y})/\overline{X}^2$.

**Exercice 4 [8 pts]**: *On note* $\alpha=\sqrt[3]{2}$ *l'unique racine cubique de* $2$ *dans* $\mathbb{R}$.

(a) *Montrer que le polynôme* $X^3-2$ *est irréductible dans* $\mathbb{Z}[X]$ *et que* $\alpha\notin\mathbb{Q}$.

**Correction**: Le critère d'Eisenstein appliqué avec le nombre premier $p=2$ montre que le polynôme $X^3-2$ est irréductible dans $\mathbb{Q}[X]$. Il résulte de l'irréductibilité dans $\mathbb{Q}[X]$ qu'il n'a pas de racine dans $\mathbb{Q}$. Sa racine réelle $\alpha$ ne peut donc pas être dans $\mathbb{Q}$.

On peut aussi d'abord montrer que $X^3-2$ n'a pas de racine dans $\mathbb{Q}$: s'il en avait une, disons $a/b$ avec $a,b\in\mathbb{Z}$ premiers entre eux et $b>0$, on aurait $a^3=2b^3$ et donc $a|2$ et $b|1$; ainsi $a/b\in\{\pm1,\pm2\}$ ce qu'on vérifie être absurde. Comme $\deg(X^3-2)=3$, l'absence de racine dans $\mathbb{Q}$ garantit l'irréductibilité dans $\mathbb{Q}[X]$; elle redonne aussi que $\alpha\notin\mathbb{Q}$.

D'une façon ou de l'autre, on déduit ensuite l'irréductibilité dans $\mathbb{Z}[X]$ de l'irréductibilité dans $\mathbb{Q}[X]$ et du fait que $X^3-2$ est primitif dans $\mathbb{Z}[X]$.

On note $v_\alpha : \mathbb{Z}[X] \to \mathbb{R}$ le morphisme qui à tout polynôme $f \in \mathbb{Z}[X]$ associe l'élément $f(\alpha) \in \mathbb{R}$ et $\mathbb{Z}[\alpha]$ l'anneau image de $v_\alpha$, c'est-à-dire $\mathbb{Z}[\alpha] = \{f(\alpha) \mid f \in \mathbb{Z}[X]\}$.

(b) *Montrer que*

(b-1) $\mathbb{Z}[\alpha]$ *est un sous-anneau de* $\mathbb{R}$ *qui contient* $\mathbb{Z}$ *et* $\alpha$*,*

**Correction**: $\mathbb{Z}[\alpha]$ est l'anneau image du morphisme $v_\alpha : \mathbb{Z}[X] \to \mathbb{R}$; c'est un sous-anneau de $\mathbb{R}$ et il contient $\alpha = v_\alpha(X)$ et $m = v_\alpha(m)$ pour tout $m \in \mathbb{Z}$.

(b-2) $\mathbb{Z}[\alpha]$ *est le plus petit sous-anneau de* $\mathbb{R}$ *qui contient* $\mathbb{Z}$ *et* $\alpha$*.*

**Correction**: Si $C$ est un sous-anneau de $\mathbb{R}$ qui contient $\mathbb{Z}$ et $\alpha$, alors, étant stable par somme et produit, il contient tous les éléments de $\mathbb{R}$ de la forme $f(\alpha)$ où $f$ décrit $\mathbb{Z}[X]$. On a donc $C \supset \mathbb{Z}[\alpha]$.

(c-1) *Pour* $f \in \mathbb{Z}[X]$*, écrire avec précision la division euclidienne de* $f$ *par* $X^3 - 2$*, après en avoir justifié l'existence.*

**Correction**: Le coefficient dominant de $X^3 - 2$, à savoir 1, est inversible dans $\mathbb{Z}$. Cela garantit l'existence de la division euclidienne de tout polynôme $f \in \mathbb{Z}[X]$ par $X^3 - 2$: il existe $Q, R \in \mathbb{Z}[X]$ tels que $f = (X^3 - 2)Q + R$ avec $R = 0$ ou $\deg(R) < 3$.

(c-2) *Montrer que pour tout polynôme* $R \in \mathbb{Q}[X]$ *non nul de degré* $\leq 2$*, il existe deux polynômes* $U, V \in \mathbb{Q}[X]$ *tels que*

$$U(X)R(X) + V(X)(X^3 - 2) = 1$$

*(On ne cherchera pas à expliciter les polynômes* $U$ *et* $V$*).*

**Correction**: Le polynôme $X^3 - 2$, étant irréductible dans $\mathbb{Q}[X]$, est premier avec tout polynôme $R \in \mathbb{Q}[X]$ qu'il ne divise pas. Si $R \in \mathbb{Q}[X]$ est un polynôme non nul de degré $\leq 2$, il n'est pas divisible par $X^3-2$ (puisque celui-ci est de degré $> 2$). Ainsi $X^3-2$ et $R$ sont premiers dans $\mathbb{Q}[X]$. Comme l'anneau $\mathbb{Q}[X]$ est principal, on peut appliquer le théorème de Bezout: il existe deux polynômes $U, V \in \mathbb{Q}[X]$ tels que $U(X)R(X)+V(X)(X^3-2) = 1$.

(d) *En utilisant la question (c), montrer, en détaillant bien les raisonnements, que*

(d-1) $\mathbb{Z}[\alpha]$ *est isomorphe à l'anneau* $\mathbb{Z}[X]/\langle X^3 - 2\rangle$*,*

**Correction**: Pour $f \in \mathbb{Z}[X]$, notons comme en (c-1), $f = (X^3 - 2)Q + R$ avec $R = 0$ ou $\deg(R) < 3$ la division euclidienne de $f$ par $X^3 - 2$. Si $f \in \ker(v_\alpha)$, alors $f(\alpha) = R(\alpha) = 0$. Mais le (c-2) donne ensuite, en substituant $\alpha$ à $X$, que si $R \neq 0$ alors $1 = 0$, ce qui est absurde. D'où $R = 0$, c'est-à-dire, $X^3 - 2$ divise $f$ dans $\mathbb{Z}[X]$. Cela montre que $\ker(v_\alpha) \subset \langle X^3 - 2\rangle$. L'inclusion inverse étant évidente, on a $\ker(v_\alpha) = \langle X^3 - 2\rangle$. D'autre part, l'anneau $\mathbb{Z}[\alpha]$ est par définition l'image du morphisme $v_\alpha$. Les théorèmes d'isomorphisme classiques fournissent $\mathbb{Z}[X]/\langle X^3 - 2\rangle \simeq \mathbb{Z}[\alpha]$.

(d-2) $\mathbb{Z}[\alpha] = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Z}\}$.

**Correction**: L'inclusion "$\supset$" est triviale. Pour l'inclusion inverse, fixons $f \in \mathbb{Z}[X]$. Soit $f = (X^3-2)Q+R$ avec $R = 0$ ou $\deg(R) < 3$ sa division euclidienne par $X^3-2$. Notons $R = cX^2 + bX + a$ où $a, b, c \in \mathbb{Z}$. On a alors $f(\alpha) = R(\alpha) = a + b\alpha + c\alpha^2$, ce qui prouve l'inclusion voulue.

(e) *Montrer que*

(e-1) *il n'existe pas de polynômes* $A, B \in \mathbb{Z}[X]$ *tels que* $2A(X) + B(X)(X^3 - 2) = 1$*. (Indication: chercher une contradiction en considérant une valeur spéciale de* $X$ *dans* $\mathbb{Z}$*).*

**Correction**: Supposons le contraire. En faisant $X = 0$, on obtient $2A(0) - 2B(0) = 1$, ce qui est absurde puisque le terme de gauche est un entier pair.

(e-2) 2 *n'est pas inversible dans l'anneau* $\mathbb{Z}[\alpha]$.

**Correction**: Supposons que 2 soit inversible dans l'anneau $\mathbb{Z}[\alpha]$. Il l'est alors aussi dans l'anneau isomorphe $\mathbb{Z}[X]/\langle X^3-2\rangle$. Cela signifie qu'il existe $A \in \mathbb{Z}[X]$ tel que $2 \cdot A(X) = 1$ dans l'anneau quotient $\mathbb{Z}[X]/\langle X^3-2\rangle$, c'est-à-dire, il existe $A, B \in \mathbb{Z}[X]$ tel que $2A(X) - 1 = B(X)(X^3-2)$ dans $\mathbb{Z}[X]$. La question précédente indique que ce n'est pas possible; on a la contradiction cherchée.

(f) *Montrer que pour tout nombre nombre premier* $p \in \mathbb{N}$, *on a*

$$\mathbb{Z}[\alpha]/\langle p\rangle \simeq \mathbb{Z}[X]/\langle p, X^3-2\rangle \simeq (\mathbb{Z}/p\mathbb{Z})[X]/\langle X^3-\overline{2}\rangle$$

*où on désigne par* $\overline{2}$ *la classe de* 2 *modulo* $p$. *(On justifiera soigneusement les différentes étapes du raisonnement en rappelant les résultats du cours utilisés).*

**Correction**: *Via* l'isomorphisme $\mathbb{Z}[X]/\langle X^3-2\rangle \simeq \mathbb{Z}[\alpha]$ de la question (d-1), l'idéal $\langle p\rangle \subset \mathbb{Z}[\alpha]$ correspond à l'idéal engendré dans $\mathbb{Z}[X]/\langle X^3-2\rangle$ par la classe de $p \in \mathbb{Z}[X]$ modulo $\langle X^3-2\rangle$, c'est-à-dire l'idéal $\langle s(p)\rangle$ si $s : \mathbb{Z}[X] \to \mathbb{Z}[X]/\langle X^3-2\rangle$ désigne la surjection canonique. On obtient ainsi l'isomorphisme

$$\frac{\mathbb{Z}[X]}{\langle X^3-2\rangle}\Big/\langle s(p)\rangle \;\simeq\; \mathbb{Z}[\alpha]/\langle p\rangle$$

Les théorèmes d'isomorphisme du cours permettent ensuite d'écrire

$$\frac{\mathbb{Z}[X]}{\langle X^3-2\rangle}\Big/\langle s(p)\rangle \simeq \mathbb{Z}[X]/\langle p, X^3-2\rangle \simeq \frac{\mathbb{Z}[X]}{\langle p\rangle}\Big/\sigma(\langle X^3-2\rangle)$$

avec $\sigma : \mathbb{Z}[X] \to \mathbb{Z}[X]/\langle p\rangle$ la surjection canonique. On sait aussi que l'anneau du haut du dernier terme est isomorphe à $(\mathbb{Z}/p\mathbb{Z})[X]$. On en déduit que le dernier terme est isomorphe à $(\mathbb{Z}/p\mathbb{Z})[X]/\langle X^3-\overline{2}\rangle$. On a bien montré le résultat souhaité.

(g) *On prend ici* $p = 11$. *Montrer que*

(g-1) $X^3-\overline{2}$ *a une racine dans* $\mathbb{Z}/11\mathbb{Z}$,

**Correction**: On a $7^2 \equiv 5 \pmod{11}$ et $7^3 \equiv 2 \pmod{11}$. La classe de 7 modulo 11 est une racine dans $\mathbb{Z}/11\mathbb{Z}$ du polynôme $X^3-\overline{2}$.

(g-2) *L'idéal* $\langle 11\rangle$ *engendré par* 11 *dans* $\mathbb{Z}[\alpha]$ *n'est pas premier.*

**Correction**: Supposons que $\langle 11\rangle$ soit un idéal premier de $\mathbb{Z}[\alpha]$. L'anneau quotient $\mathbb{Z}[\alpha]/\langle 11\rangle$ est alors intègre. D'après la question (f), l'anneau $(\mathbb{Z}/11\mathbb{Z})[X]/\langle X^3-\overline{2}\rangle$ l'est également, ou, de façon équivalente, $\langle X^3-\overline{2}\rangle$ est un idéal premier de $(\mathbb{Z}/11\mathbb{Z})[X]$. Mais cela entraîne que le polynôme $X^3-\overline{2}$ est irréductible dans $(\mathbb{Z}/11\mathbb{Z})[X]$, ce qui est absurde puisque ce polynôme a une racine dans $\mathbb{Z}/11\mathbb{Z}$ et qu'il est de degré $> 1$.

# UNIVERSITÉ LILLE 1

Enseignants: **A. BROUSTET, P. DÈBES, S. DELAUNAY**
Filière: **Licence - Semestre 5**
Matière: **M 51**
Année universitaire: **2012/2013**
Épreuve: **Devoir surveillé**
Date: **vendredi 9 novembre à 16h30**
Lieu: **M1 Painlevé**
Durée de l'épreuve: **2 heures**

---

**CHAQUE PARTIE SERA RÉDIGÉE SUR UNE COPIE DIFFÉRENTE**

---

**Ni calculatrices ni documents ni téléphone portable.**
**Une grande importance sera accordée à la rédaction.**
**Le barème est donné à titre indicatif.**

---

*(On pourra utiliser sans les redémontrer des résultats vus en TD à condition d'en rappeler précisément les énoncés).*

## PARTIE I

**Exercice 1 [6 pts]**: On note $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe des éléments inversibles pour la multiplication dans $\mathbb{Z}/n\mathbb{Z}$.

(a) Quel est l'ordre de $(\mathbb{Z}/n\mathbb{Z})^\times$? (Justifier la réponse; question de cours).

(b) Vérifier que $2^9 \equiv -1$ [mod 27] et en déduire que la classe de 2 modulo 27 est un générateur de $(\mathbb{Z}/27\mathbb{Z})^\times$.

(c) Combien de générateurs le groupe $((\mathbb{Z}/27\mathbb{Z})^\times, \times)$ possède-t-il? Les décrire.

(d) Montrer que le groupe $((\mathbb{Z}/108\mathbb{Z})^\times, \times)$ n'est pas cyclique.

**Exercice 2 [3,5 pts]:** Soient $G$ un groupe et $G \times^s \mathrm{Aut}(G)$ le produit semi-direct de $G$ par son groupe d'automorphismes Aut(G) (l'action $\rho(\chi)$ d'un élément $\chi \in \mathrm{Aut}(G)$ sur $G$ est donnée par $\rho(\chi)(g) = \chi(g)$ pour tout $g \in G$).
Montrer que l'application $\Phi : G \times^s \mathrm{Aut}(G) \to \mathrm{Per}(G)$ définie par

$$\text{pour tout } (g,\chi) \in G \times^s \mathrm{Aut}(G), \quad \Phi(g,\chi)(h) = g\,\chi(h) \qquad (\text{pour tout } h \in G)$$

définit une action de $G \times^s \mathrm{Aut}(G)$ sur $G$ et montrer que cette action est fidèle.

**T.S.V.P.**

# PARTIE II

**Exercice 3 [4 pts]** Dans le groupe symétrique $S_5$ on considère les permutations

$$\begin{cases} \omega = (1\,2\,3\,4\,5) \\ \tau = (1\,3)(4\,5) \end{cases}$$

(a) Donner l'ordre et la signature de chacun des éléments $\omega$ et $\tau$.

(b) Montrer que le sous-groupe $H$ engendré par $\omega$ et $\tau$ est isomorphe au groupe diédral $D_{10}$ d'ordre 10.

**Exercice 4 [6,5 pts]** Soit $G$ un groupe fini et $H$ un sous-groupe de $G$.

(a) Donner la définition de l'action $\gamma_H$ du groupe $G$ par translation à gauche sur l'ensemble $G/\cdot H$ des classes à gauche de $G$ modulo $H$.

On note $\rho$ la restriction à $H$ de l'action $\gamma_H$.

(b) Quelle est l'orbite de la classe neutre $H \in G/\cdot H$ sous l'action $\rho$?

(c) Montrer que si $\mathcal{O}$ est une orbite de l'action $\rho$ qui n'est pas un singleton, alors

$$\begin{cases} \text{card}(\mathcal{O}) \text{ divise } |H| \\ 2 \leq \text{card}(\mathcal{O}) \leq \dfrac{|G|}{|H|} - 1 \end{cases}$$

On suppose que l'indice de $H$ dans $G$ (c'est-à-dire le nombre $|G|/|H|$) est égal au plus petit nombre premier divisant l'ordre de $G$.

(d) Montrer que toutes les orbites de $\rho$ sont des singletons.

(e) En déduire que le sous-groupe $H$ est distingué dans $G$.

# UNIVERSITÉ LILLE 1

Enseignants: **A. BROUSTET, P. DÈBES, S. DELAUNAY**
Filière: **Licence - Semestre 5**
Matière: **M 51**
Année universitaire: **2012/2013**
Épreuve: **Devoir surveillé no 2**
Date: **lundi 17 décembre à 8h**
Lieu: **Halle Grémeaux**
Durée de l'épreuve: **4 heures**

---

**CHAQUE PARTIE SERA RÉDIGÉE SUR UNE COPIE DIFFÉRENTE**

---

**UNE GRANDE IMPORTANCE SERA ACCORDÉE À LA RÉDACTION.**
**Ni calculatrices ni documents ni téléphone portable.**
**Le barème est donné à titre indicatif.**

---

*(On pourra utiliser sans les redémontrer des résultats vus en TD à condition d'en rappeler précisément les énoncés).*

## PARTIE I

**Exercice 1 [5 pts]:** Soient $G$ un groupe et $H \subset G$ un sous-groupe. On note $G/\cdot H$ l'ensemble des classes à gauche $xH$ de $G$ modulo $H$ ($x \in G$) et $\gamma : G \to \mathrm{Per}(G/\cdot H)$ l'action de $G$ sur $G/\cdot H$ par multiplication à gauche, laquelle est définie par $\gamma(g)(xH) = gxH$, pour tous $g, x \in G$.

(a) Montrer que $\ker(\gamma)$ est l'intersection de tous les sous-groupes $xHx^{-1}$ (conjugués de $H$ par $x$) où $x$ décrit $G$.

(b) En déduire que, si $H$ est un $p$-sous-groupe de Sylow de $G$ pour un nombre premier $p$ donné, alors $\ker(\gamma)$ est l'intersection de tous les $p$-sous-groupes de Sylow de $G$. (On rappellera précisément les résultats du cours utilisés).

**Application**: Soit $G$ un groupe d'ordre 392.

(c) On suppose dans cette question que $G$ a <u>au moins deux</u> 7-sous-groupes de Sylow. On note $H$ l'un d'entre eux et $\gamma : G \to \mathrm{Per}(G/\cdot H)$ l'action associée considérée ci-dessus. Montrer que

(i) $G$ a exactement <u>huit</u> 7-sous-groupes de Sylow.

(ii) $|\ker(\gamma)|$ divise 49.

(iii) $|\ker(\gamma)| \neq 49$.

(iv) $|\ker(\gamma)| \neq 1$. (<u>Indication:</u> On pourra supposer le contraire et raisonner sur les ordres des groupes).

(d) Montrer que $G$ a un sous-groupe distingué d'ordre 49 <u>ou</u> a un sous-groupe distingué d'ordre 7.

**T.S.V.P.**

**Exercice 2 [4 pts]**: (a) Montrer que le groupe $(\mathbb{Z}/59\mathbb{Z})^\times$ des inversibles de l'anneau $\mathbb{Z}/59\mathbb{Z}$ est cyclique.

(b) Vérifier que $2^6 \equiv 5$ [mod 59] et $5^5 \equiv -2$ [mod 59]. En déduire que $2^{29} \equiv -1$ [mod 59].

(c) Montrer que la classe de 2 modulo 59 est un générateur de $(\mathbb{Z}/59\mathbb{Z})^\times$.

(d) Combien de générateurs le groupe $((\mathbb{Z}/59\mathbb{Z})^\times, \times)$ possède-t-il? Les décrire.

## PARTIE II

**Exercice 3 [4,5 pts]**: (a) Etant donné un anneau $A$, donner les définitions d'"élément irréductible de $A$" et de "pgcd de deux éléments $a$ et $b$ de $A$".

On considère l'anneau $\mathbb{Z}[X, Y]$.

(b) Montrer que les éléments $X$ et $Y$ sont deux irréductibles de l'anneau $\mathbb{Z}[X, Y]$ et que leur pgcd vaut 1.

(c) Quelle est la forme générale des éléments des idéaux $\langle X\rangle$ et $\langle Y\rangle$ de $\mathbb{Z}[X, Y]$ engendrés respectivement par $X$ et $Y$? Quelle est la forme générale de ceux de l'idéal $\langle X\rangle + \langle Y\rangle$?

(d) Montrer que $\langle X\rangle + \langle Y\rangle \neq \langle\, 1\,\rangle$.

(e) Montrer que $\mathbb{Z}[X, Y]$ est un anneau factoriel non principal.

**Exercice 4 [6,5 pts]**: On note $\alpha = \sqrt{7}$ la racine carrée positive de 7 dans $\mathbb{R}$. On pourra utiliser sans le démontrer que $\alpha \notin \mathbb{Q}$.

(a) Montrer que le polynôme $X^2 - 7$ est irréductible dans $\mathbb{Q}[X]$ et dans $\mathbb{Z}[X]$.

On note $v_\alpha : \mathbb{Z}[X] \to \mathbb{R}$ le morphisme d'anneaux qui à tout polynôme $f \in \mathbb{Z}[X]$ associe l'élément $f(\alpha) \in \mathbb{R}$ et $\mathbb{Z}[\alpha]$ l'anneau image de $v_\alpha$, c'est-à-dire $\mathbb{Z}[\alpha] = \{f(\alpha) \mid f \in \mathbb{Z}[X]\}$.

(b) Montrer que

(b-1) $\mathbb{Z}[\alpha]$ est un sous-anneau de $\mathbb{R}$ qui contient $\mathbb{Z}$ et $\alpha$,

(b-2) $\mathbb{Z}[\alpha]$ est le plus petit sous-anneau de $\mathbb{R}$ qui contient $\mathbb{Z}$ et $\alpha$.

(c) Pour $f \in \mathbb{Z}[X]$, écrire la division euclidienne dans $\mathbb{Z}[X]$ de $f$ par $X^2 - 7$, après en avoir justifié l'existence.

(d) En déduire, en détaillant bien les raisonnements, que

(d-1) $\mathbb{Z}[\alpha]$ est isomorphe à l'anneau $\mathbb{Z}[X]/\langle X^2 - 7\rangle$,

(d-2) $\mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}\}$.

(e) Montrer que pour tout nombre nombre premier $p \in \mathbb{N}$, on a

$$\mathbb{Z}[\alpha]/\langle p\rangle \simeq \mathbb{Z}[X]/\langle p, X^2 - 7\rangle \simeq (\mathbb{Z}/p\mathbb{Z})[X]/\langle X^2 - \overline{7}\rangle$$

où on désigne par $\overline{7}$ la classe de 7 modulo $p$. (On justifiera soigneusement les différentes étapes du raisonnement en rappelant les résultats du cours utilisés).

(f) On prend ici $p = 19$. Montrer que

(f-1) $\overline{8}$ est une racine de $X^2 - \overline{7}$ dans $\mathbb{Z}/19\mathbb{Z}$,

(f-2) L'idéal $\langle 19\rangle$ engendré par 19 dans $\mathbb{Z}[\alpha]$ n'est pas premier.

# UNIVERSITÉ LILLE 1

Enseignants: **A. BROUSTET, P. DÈBES, S. DELAUNAY**
Filière: **Licence - Semestre 5**
Matière: **M 51**
Année universitaire: **2012/2013**
Épreuve: **Examen - 2ème session**
Date: **mercredi 12 juin**
Durée de l'épreuve: **4 heures**

---

**Ni calculatrices ni documents ni téléphone portable.**
**Une grande importance sera accordée à la rédaction.**
**Le barème est donné à titre indicatif.**

---

## PARTIE I (12 points)

On note $D_n$ le groupe diédral à $2n$ éléments. Pour un groupe $G$ et un nombre premier $p$, on note $n_p = n_p(G)$ le nombre de $p$-sous-groupes de Sylow de $G$ et $o(p)$ le nombre d'éléments d'ordre $p$ dans $G$.

1) Soip $p$ un nombre premier impair et $G$ un groupe d'ordre $2p$. Démontrer que $G$ s'écrit comme produit semi-direct de $\mathbb{Z}/2\mathbb{Z}$ et de $\mathbb{Z}/p\mathbb{Z}$. En étudiant les actions possibles en déduire que $G$ est isomorphe à $\mathbb{Z}/2p\mathbb{Z}$ ou à $D_p$.

2) Pour $G = D_p$, donner les valeurs de $n_2$ et de $n_p$.

3) Soit $G$ un groupe, $e$ son élément neutre, $S$ et $T$ deux sous-groupes de $G$ tels que $S \cap T = \{e\}$.

a) On suppose $S$ distingué dans $G$, démontrer qu'alors $ST = TS$ est un sous-groupe de $G$ de cardinal $|S|.|T|$.

b) On suppose $S$ et $T$ distingués dans $G$, démontrer que $ST$ est isomorphe au groupe produit $S \times T$. En déduire qu'un groupe de cardinal 35 est cyclique.

4) Soit $G$ un groupe de cardinal 70.

a) Donner les valeurs possibles de $n_2$, $n_5$ et $n_7$.

b) Exprimer $o(p)$ en fonction de $n_p$ et de $p$, pour $p \in \{2, 5, 7\}$.

c) Démontrer que $G$ possède un sous-groupe $K$ d'ordre 35 et que $K \triangleleft G$.

d) Calculer $n_2$ dans le cas des quatre groupes suivants : $\mathbb{Z}/70\mathbb{Z}, D_7 \times \mathbb{Z}/5\mathbb{Z}, D_5 \times \mathbb{Z}/7\mathbb{Z}$ et $D_{35}$ ; en déduire que ces groupes ne sont pas isomorphes.

e) Démontrer que $G$ est isomorphe à l'un des quatre groupes ci-dessus.

## PARTIE II (8 points)

Soit $p \geq 2$ un nombre premier. On note

$$F(Y) = \frac{(Y+1)^p - 1}{Y}$$

et

$$\Phi(X) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

On note également $\mathbb{Q}[e^{2i\pi/p}]$ l'image du morphisme d'évaluation :

$$\begin{aligned} \mathcal{E} : \mathbb{Q}[X] &\to \mathbb{C} \\ X &\mapsto e^{2i\pi/p} \end{aligned}$$

1) Démontrer que $F(Y)$ est un polynôme en $Y$ à coefficients dans $\mathbb{Z}$.

2) Démontrer que $F(Y)$ est irréductible dans $\mathbb{Q}[Y]$ (on pourra utiliser le critère d'Eisenstein).

3) Démontrer que $F(X-1) = \Phi(X)$ et en déduire que $\Phi(X)$ est irréductible dans $\mathbb{Q}[X]$.

4) Démontrer que $\mathbb{Q}[e^{2i\pi/p}]$ est le plus petit sous-anneau de $\mathbb{C}$ contenant le corps $\mathbb{Q}$ et le nombre $e^{2i\pi/p}$.

5) Démontrer que $\ker \mathcal{E}$ est l'idéal de $\mathbb{Q}[X]$ engendré par $\Phi(X)$ et en déduire que $\mathbb{Q}[e^{2i\pi/p}]$ est un sous-corps de $\mathbb{C}$.

6) Démontrer que $(X-1)$ divise $(X^p-1)$ et que $(X-1)^2$ ne divise pas $(X^p-1)$ dans $\mathbb{Q}[X]$.

7) Démontrer que $Y^p + X^p - 1$ est un polynôme irréductible dans $\mathbb{Q}[X,Y]$.

8) Démontrer que l'anneau quotient de $\mathbb{Q}[X,Y]$ par l'idéal engendré par le polynôme $Y^p + X^p - 1$,

$$\mathbb{Q}[X,Y]/\langle Y^p + X^p - 1 \rangle,$$

est intègre mais que la classe de $X$ n'est pas inversible dans cet anneau.

# UNIVERSITÉ LILLE 1

Enseignants: **A. BROUSTET, P. DÈBES, S. DELAUNAY, L. DENIS**
Module: **Licence - Semestre 5 - M 51**
Année universitaire: **2013/2014**
Épreuve: **Devoir Surveillé 2**
Date: **jeudi 9 janvier de 14h à 18h**
Lieu: **Halles Vallin**
Durée de l'épreuve: **4 heures**

---

**CHAQUE PARTIE SERA RÉDIGÉE SUR UNE COPIE DIFFÉRENTE**
**UNE GRANDE IMPORTANCE SERA ACCORDÉE À LA RÉDACTION**
**NI CALCULATRICES NI DOCUMENTS NI TÉLÉPHONE PORTABLE**
**LE BARÊME EST DONNÉ Á TITRE INDICATIF**

---

## PARTIE I

**Exercice 1 [5 pts]:** On suppose qu'il existe un groupe $G$, simple, d'ordre 1100.

(a) Déterminer le nombre de 11-Sylow de $G$ et en déduire le nombre d'éléments d'ordre 11 dans $G$.

(b) Déterminer le nombre de 5-Sylow de $G$. Démontrer que les 5-Sylow sont abéliens.

(c) Soient $S$ et $T$ deux 5-Sylow de $G$ distincts. On suppose qu'il existe un élément $h \neq 1$ dans $S \cap T$. On note $C(h) = \{g \in G | ghg^{-1} = h\}$ son centralisateur.
(c-1) Démontrer que $S$ et $T$ sont des sous-groupes de $C(h)$.
(c-2) Ecrire la liste des ordres possibles de $C(h)$ compte tenu de $S \subset C(h) \subset G$.
(c-3) Démontrer que $C(h) \neq G$ et que $C(h)$ n'est pas d'indice 2.
(c-4) Démontrer qu'un groupe d'ordre 25 ou 50 ou 100 possède un unique 5-Sylow.
(c-5) Démontrer que $G$ n'a pas de sous-groupe d'ordre 275. (Indication: on pourra compter le nombre d'éléments d'ordre 11 dans un tel sous-groupe).
(c-6) Démontrer que $S \cap T = \{1\}$.

(d) Démontrer qu'il n'existe pas de groupe simple d'ordre 1100.

**Questions de cours [2 pts]:**

(a) Soient $G$ un groupe et $H$ un sous-groupe distingué de $G$.
(a-1) Enoncer et démontrer le résultat donnant la forme des sous-groupes $\mathcal{U}$ du groupe quotient $G/H$.
(a-2) Soit $\mathcal{U}$ un sous-groupe distingué de $G/H$. Montrer que le quotient de $G/H$ par $\mathcal{U}$ est isomorphe à un groupe quotient de $G$ par un sous-groupe distingué $V$ de $G$.

(b) Soit $G$ un $p$-groupe, d'ordre $p^r$ avec $r \geq 1$. Montrer que
- $G$ admet un sous-groupe distingué $H$ d'ordre $p^{r-1}$, et
- $G/H$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
(On donnera une preuve ou on justifiera par des résultats du cours).

**T.S.V.P.**

**Exercice 2 [3 pts]:** Soient $G$ un groupe fini et $p$ un nombre premier. On note $H_p$ le sous-groupe de $G$ engendré par l'ensemble des éléments de $G$ d'ordre premier à $p$.

(a) Démontrer que $H_p$ est un sous-groupe distingué de $G$.

(b) Démontrer que pour tout $g \in G$, si $g$ est d'ordre $p^u m$ avec $u, m \in \mathbb{N}$ et $p$ ne divisant pas $m$, alors $g^{p^u} \in H_p$.

(c) En déduire que tous les éléments de $G/H_p$ sont d'ordre une puissance de $p$.

(d) En déduire que le groupe quotient $G/H_p$ est un $p$-groupe. (Indication: on pourra utiliser le théorème de Cauchy).

(e) Démontrer que si $G$ n'est pas engendré par ses éléments d'ordre premier à $p$, alors il existe un sous-groupe $V$ distingué dans $G$ tel que $G/V$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. (Indication: on pourra combiner la question (d), la question de cours (b) et la question de cours (a)).

# PARTIE II

**Exercice 3 [5 pts]**: On note $j$ le nombre complexe $j = e^{2i\pi/3}$ et $\mathbb{Z}[j]$ l'ensemble des nombres complexes de la forme $m + jn$ avec $m, n \in \mathbb{Z}$. On rappelle que $1 + j + j^2 = 0$.

(a) Montrer que $\mathbb{Z}[j]$ est le plus petit sous-anneau de $\mathbb{C}$ contenant $\mathbb{Z}$ et $j$.

(b) Montrer que
(b-1) pour tous $c, d \in \mathbb{R}$, $| c + jd |^2 = c^2 + d^2 - cd = (c - d)^2 + cd$,
(b-2) pour tous $\alpha, \beta \in \mathbb{R}$, il existe $m, n \in \mathbb{Z}$ tel que le nombre complexe $(\alpha - m) + j(\beta - n)$ soit de module $< 1$.

(c) Montrer qu'un élément $c + jd \in \mathbb{Z}[j]$ est inversible si et seulement si $| c + jd |^2 = 1$. Puis en déduire que $\mathbb{Z}[j]^\times = \{\pm 1, \pm j, \pm j^2\}$.

(d) Montrer que pour tout $a, b \in \mathbb{Z}[j]$ avec $b \neq 0$, il existe $q, r \in \mathbb{Z}[j]$ tels que $a = bq + r$ avec $|r| < |b|$.

(e) Montrer que l'anneau $\mathbb{Z}[j]$ est principal.

**Exercice 4 [5 pts]**: On considère l'anneau $\mathbb{Z}[j] = \{m + jn | m, n \in \mathbb{Z}\}$ de l'exercice précédent (mais ce nouvel exercice peut être traité de façon indépendante).

(a) Montrer que le polynôme $X^2 + X + 1$ est irréductible dans $\mathbb{Q}[X]$ et dans $\mathbb{Z}[X]$.

(b) Montrer que pour tout polynôme $f \in \mathbb{Z}[X]$, il existe un polynôme $Q \in \mathbb{Z}[X]$ et deux entiers $u, v \in \mathbb{Z}$ tels que $f(X) = (X^2 + X + 1)Q(X) + uX + v$.

(c) Montrer que $\mathbb{Z}[j]$ est isomorphe à l'anneau $\mathbb{Z}[X]/\langle X^2 + X + 1 \rangle$,

(d) Montrer que pour tout nombre premier $p \in \mathbb{N}$, on a

$$\mathbb{Z}[j]/\langle p \rangle \simeq \mathbb{Z}[X]/\langle p, X^2 + X + 1 \rangle \simeq (\mathbb{Z}/p\mathbb{Z})[X]/\langle X^2 + X + \overline{1} \rangle$$

où on désigne par $\overline{1}$ la classe de 1 modulo $p$. (On justifiera soigneusement les différentes étapes du raisonnement en rappelant les résultats du cours utilisés).

(e) On prend ici $p = 7$. Montrer que
(e-1) $X^2 + X + \overline{1}$ a une racine dans $\mathbb{Z}/7\mathbb{Z}$,
(e-2) L'idéal $\langle 7 \rangle$ engendré par 7 dans $\mathbb{Z}[j]$ n'est pas premier.

# UNIVERSITÉ LILLE 1

Enseignants: **A. BROUSTET, P. DÈBES, S. DELAUNAY, L. DENIS**
Module: **Licence - Semestre 5 - M 51**
Année universitaire: **2013/2014**
Épreuve: **Devoir Surveillé 2**
Date: **jeudi 9 janvier de 14h à 18h**
Lieu: **Halles Vallin**
Durée de l'épreuve: **4 heures**

---

**CORRIGÉ**

---

## PARTIE I

**Exercice 1 [5 pts]:** *On suppose qu'il existe un groupe $G$, simple, d'ordre* 1100*.*

(a) *Déterminer le nombre de* 11*-Sylow de $G$ et en déduire le nombre d'éléments d'ordre* 11 *dans $G$.*

**Correction**: D'après le théorème de Sylow, le nombre de 11-sous-groupes de Sylow de $G$ est congru à 1 modulo 11 et divise 100; il vaut donc 1 ou 100. Si c'était 1, l'unique 11-Sylow serait distingué dans $G$, ce qui contredirait l'hypothèse "$G$ simple". Il y a donc 100 11-Sylow dans $G$, et $100 \times 10 = 1000$ éléments d'ordre 10 puisque ces éléments sont inclus dans un 11-Sylow, que chaque 11-Sylow, d'ordre 11 (et donc cyclique d'ordre 11), en contient 10 et que deux 11-Sylow n'ont que l'élément neutre 1 de commun.

(b) *Déterminer le nombre de* 5*-Sylow de $G$. Démontrer que les* 5*-Sylow sont abéliens.*

**Correction**: Le nombre de 5-Sylow de $G$ est congru à 1 modulo 5 et divise 44. Comme d'autre part ce ne peut être 1 (puisque $G$ est simple), il vaut 11. Chaque 5-Sylow est d'ordre $5^2$ et est donc abélien (comme tout groupe d'ordre le carré d'un nombre premier).

(c) *Soient $S$ et $T$ deux* 5*-Sylow de $G$ distincts. On suppose qu'il existe un élément $h \neq 1_G$ dans $S \cap T$. On note $C(h) = \{g \in G | ghg^{-1} = h\}$ son centralisateur.*
(c-1) *Démontrer que $S$ et $T$ sont des sous-groupes de $C(h)$.*

**Correction**: Comme $S$ est abélien et que $h \in S$, on a $S \subset C(h)$. L'ensemble $C(h)$ est de plus un sous-groupe de $G$ puisque c'est le fixateur de $h$ pour l'action de $G$ par conjugaison sur lui-même. *Idem* pour $T$.
(c-2) *Ecrire la liste des ordres possibles de $C(h)$ compte tenu de $S \subset C(h) \subset G$.*

**Correction**: D'après le théorème de Lagrange, l'ordre $|C(h)|$ de $C(h)$ est un multiple de $|S| = 25$ et divise $|G| = 1100$. On a donc $|C(h)| \in \{25, 50, 100, 275, 550, 1100\}$.
(c-3) *Démontrer que $C(h) \neq G$ et que $C(h)$ n'est pas d'indice* 2*.*

**Correction**: On a $C(h) \neq G$ car sinon $h$ serait dans le centre $Z(G)$ de $G$, lequel serait alors non trivial. Comme $G$ est simple, on aurait $Z(G) = G$, ce qui est impossible puisque que les seuls groupes simples abéliens sont d'ordre premier. Par ailleurs $C(h)$ n'est pas d'indice 2 car ce serait sinon un sous-groupe distingué non trivial de $G$.
(c-4) *Démontrer qu'un groupe d'ordre* 25 *ou* 50 *ou* 100 *possède un unique* 5*-Sylow.*

**Correction**: Un groupe d'ordre $25 = 5^2$ est évidemment égal à son unique 5-Sylow. Dans un groupe d'ordre 50 (resp. d'ordre 100), le nombre de 5-Sylow est congru à 1 modulo 5 et divise 2 (resp. divise 4). Dans les deux cas, ce nombre vaut nécessairement 1; il y a donc un unique 5-Sylow, lequel est distingué.

(c-5) *Démontrer que $G$ n'a pas de sous-groupe d'ordre* 275.

**Correction**: Supposons que $G$ possède un sous-groupe $H$ d'ordre $275 = 5^2 \cdot 11$. Le nombre de 11-Sylow de $H$ est congru à 1 modulo 11 et divise 25. Ce nombre vaut nécessairement 1. L'unique 11-Sylow de $H$, qui est d'ordre 11, contiendrait tous les éléments d'ordre 11 dans $H$, qui seraient donc au nombre de 10. D'après (a), il devrait alors y avoir $1000 - 10 = 990$ éléments d'ordre 11 dans l'ensemble $G \setminus H$, lequel est d'ordre $1100 - 275 = 825$. On obtient la contradiction cherchée.

(c-6) *Démontrer que $S \cap T = \{1_G\}$.*

**Correction**: Ce qui précède montre que l'hypothèse que $S \cap T$ contienne un élément $h \neq 1_G$ conduit à une contradiction. En effet, l'ordre de $|C(h)|$, *a priori* dans la liste $\{25, 50, 100, 275, 550, 1100\}$ (c-2), ne peut être ni 1100 ni 550 (c-3). Il ne peut être non plus 25, 50 ou 100 car alors il ne pourrait pas contenir $S$ et $T$ qui en seraient deux 5-Sylow distincts (c-4), ce qui contredit (c-1). Enfin $|C(h)|$ ne peut être 275 (c-5).

(d) *Démontrer qu'il n'existe pas de groupe simple d'ordre* 1100.

**Correction**: S'il existait un groupe simple $G$ d'ordre 1100, d'après ce qui précède, il aurait 11 5-Sylow d'intersection deux à deux égale à $\{1_G\}$; leur réunion serait d'ordre $11 \times 24 + 1 = 265$. Et d'après (a), $G$ aurait 1000 éléments d'ordre 11, lesquels ne seraient évidemment aucun des éléments de la réunion précédente. Il y aurait donc au moins 1265 éléments dans $G$. Contradiction.

**Questions de cours [2 pts]:**

(a) *Soient $G$ un groupe et $H$ un sous-groupe distingué de $G$.*

(a-1) *Enoncer et démontrer le résultat donnant la forme des sous-groupes $\mathcal{U}$ du groupe quotient $G/H$.*

**Correction**: Les sous-groupes $\mathcal{U}$ du groupe quotient $G/H$ sont les groupes de la forme $V/H$, ou si on préfère $s(V)$ avec $s : G \to G/H$ la surjection canonique, avec $V$ un sous-groupe de $G$ contenant $H$. En effet si $V$ est un tel sous-groupe, $s(V)$ est un sous-groupe de $G/H$, et réciproquement, si $\mathcal{U}$ est un sous-groupe de $G/H$, alors la préimage $V = s^{-1}(\mathcal{U})$ est un sous-groupe de $G$ comme indiqué.

(a-2) *Soit $\mathcal{U}$ un sous-groupe distingué de $G/H$. Montrer que le quotient de $G/H$ par $\mathcal{U}$ est isomorphe à un groupe quotient de $G$ par un sous-groupe distingué $V$ de $G$.*

**Correction**: Soit $\mathcal{U} = V/H$ un sous-groupe de $G/H$, avec $V$ comme ci-dessus. On sait de plus que si $\mathcal{U}$ est distingué dans $G/H$, alors $V = s^{-1}(\mathcal{U})$ est distingué dans $G$, et que le quotient de $G/H$ par $\mathcal{U}$ est isomorphe au groupe quotient $G/V$.

(b) *Soit $G$ un $p$-groupe, d'ordre $p^r$ avec $r \geq 1$. Montrer que*
*- $G$ admet un sous-groupe distingué $H$ d'ordre $p^{r-1}$, et*
*- $G/H$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*
*(On donnera une preuve ou on justifiera par des résultats du cours).*

**Correction**: On sait que pour tout groupe d'ordre $p^r$ avec $r \geq 1$, il existe une chaine croissante de sous-groupes $G_i$, distingués dans $G$ et d'ordre $p^i$, $i = 0, \ldots, r$. Le sous-groupe $H = G_{r-1}$ répond à la première demande. Le groupe quotient $G/H$ est alors d'ordre $p^r/p^{r-1} = p$. Comme $p$ est premier, ce groupe est cyclique, et isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

**Exercice 2 [3 pts]:** *Soient $G$ un groupe fini et $p$ un nombre premier. On note $H_p$ le sous-groupe de $G$ engendré par l'ensemble des éléments de $G$ d'ordre premier à $p$.*

(a) *Démontrer que $H_p$ est un sous-groupe distingué de $G$.*

**Correction**: Notons $\mathcal{H}_p$ l'ensemble des éléments de $G$ d'ordre $p$. Pour tout $g \in G$, la conjugaison $x \to gxg^{-1}$ étant un automorphisme de $G$, on a $g\mathcal{H}_p g^{-1} = \mathcal{H}_p$. En combinant $g\langle\mathcal{H}_p\rangle g^{-1} = \langle g\mathcal{H}_p g^{-1}\rangle$ et $\langle\mathcal{H}_p\rangle = H_p$, on obtient $gH_pg^{-1} = H_p$. Comme $g \in G$ est quelconque, on obtient que $H_p$ est distingué dans $G$.

(b) *Démontrer que pour tout $g \in G$, si $g$ est d'ordre $p^u m$ avec $u, m \in \mathbb{N}$ et $p$ ne divisant pas $m$, alors $g^{p^u} \in H_p$.*

**Correction**: Soit $g$ d'ordre $p^u m$ avec $u, m \in \mathbb{N}$ et $p$ ne divisant pas $m$. Alors $g^{p^u}$ est clairement d'ordre $m$. Comme $p$ ne divise pas $m$, $g^{p^u} \in H_p$.

(c) *En déduire que tous les éléments de $G/H_p$ sont d'ordre une puissance de $p$.*

**Correction**: Soit $gH_p \in G/H_p$ avec $g \in G$. L'ordre de $g$ dans $G$ peut s'écrire $p^u m$ avec $u, m \in \mathbb{N}$ et $p$ ne divisant pas $m$. D'après (b), $g^{p^u} \in H_p$, et donc $(gH_p)^{p^u} = g^{p^u}H_p = H_p$. On obtient que l'ordre de $gH_p$ dans $G/H_p$ divise $p^u$, et est donc une puissance de $p$.

(d) *En déduire que le groupe quotient $G/H_p$ est un $p$-groupe.*

**Correction**: Si $G/H_p$ n'est pas un $p$-groupe, alors il existe un nombre premier $q \neq p$ divisant $|G/H_p|$. D'après le théorème de Cauchy, il existe alors un élément de $G/H_p$ d'ordre $q$, ce qui contredit (c).

(e) *Démontrer que si $G$ n'est pas engendré par ses éléments d'ordre premier à $p$, alors il existe un sous-groupe $V$ distingué dans $G$ tel que $G/V$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

**Correction**: D'après (a) et (d), $H_p$ est un sous-groupe distingué de $G$ et $G/H_p$ est un $p$-groupe. Si $G$ n'est pas engendré par ses éléments d'ordre premier à $p$, alors $G \neq H_p$ et $G/H_p$ est d'ordre $p^r$ avec $r \geq 1$. D'après la question de cours (b), $G/H_p$ a un sous-groupe distingué $\mathcal{U}$ tel que le quotient $(G/H_p)/\mathcal{U}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. D'après la question de cours (a), ce quotient $(G/H_p)/\mathcal{U}$ est isomorphe à un groupe quotient de $G$ par un sous-groupe distingué $V$ de $G$. On obtient $G/V \simeq \mathbb{Z}/p\mathbb{Z}$; $V$ répond à la question.

## PARTIE II

**Exercice 3 [5 pts]**: *On note $j$ le nombre complexe $j = e^{2i\pi/3}$ et $\mathbb{Z}[j]$ l'ensemble des nombres complexes de la forme $m + jn$ avec $m, n \in \mathbb{Z}$. On rappelle que $1 + j + j^2 = 0$.*

(a) *Montrer que $\mathbb{Z}[j]$ est le plus petit sous-anneau de $\mathbb{C}$ contenant $\mathbb{Z}$ et $j$.*

**Correction**: Si $m + jn$ et $m' + jn'$ sont deux éléments de $\mathbb{Z}[j]$ (où $m, n, m', n' \in \mathbb{Z}$), alors leur différence $(m - m') + j(n - n')$ et leur produit $mm' + (mn' + m'n)j + nn'j^2$, lequel se réécrit $(mm' - nn') + (mn' + m'n - nn')j$ (puisque $j^2 = -1 - j$), sont également dans $\mathbb{Z}[j]$. Comme de plus $1 \in \mathbb{Z}[j]$, $\mathbb{Z}[j]$ est un sous-anneau de $\mathbb{C}$. D'autre part, il est clair que si un sous-anneau $A$ de $\mathbb{C}$ contient $\mathbb{Z}$ et $j$, alors il contient $\mathbb{Z}[j]$, qui est donc bien le plus petit sous-anneau de $\mathbb{C}$ contenant $\mathbb{Z}$ et $j$.

(b) *Montrer que*
(b-1) *pour tous $c, d \in \mathbb{R}$, $|\, c + jd\,|^2 = c^2 + d^2 - cd = (c - d)^2 + cd$,*

**Correction**: $|\, c+jd\,|^2 = (c+jd)(c+\bar{j}d) = c^2+d^2|j|+2cd\,\mathrm{Re}(j)$. Comme $\mathrm{Re}(j) = -1/2$, on a bien la première égalité. La seconde est évidente.
(b-2) *pour tous $\alpha, \beta \in \mathbb{R}$, il existe $m, n \in \mathbb{Z}$ tel que le nombre complexe $(\alpha - m) + j(\beta - n)$ soit de module $< 1$.*

**Correction**: Soient $\alpha, \beta \in \mathbb{R}$. Il existe $m, n \in \mathbb{Z}$ tels que $|\alpha - m| \leq 1/2$ et $|\beta - n| \leq 1/2$. On a alors $|(\alpha - m) + j(\beta - n)|^2 \leq (\alpha - m)^2 + (\beta - n)^2 + |\alpha - m||\beta - n| \leq 3/4 < 1$.

(c) *Montrer qu'un élément $c + jd \in \mathbb{Z}[j]$ est inversible si et seulement si $| c + jd |^2 = 1$. Puis en déduire que $\mathbb{Z}[j]^\times = \{\pm 1, \pm j, \pm j^2\}$.*

**Correction**: Soit $c+jd \in \mathbb{Z}[j]$. Si $c+jd$ est inversible dans $\mathbb{Z}[j]$, alors il existe $c', d' \in \mathbb{Z}$ tel que $(c+jd)(c'+jd') = 1$. On en déduit $|c+jd|^2|c'+jd'|^2 = 1$, et donc que $|c+jd|^2 = 1$ puisque $|c+jd|^2$ et $|c'+jd'|^2$ sont des entiers positifs. Réciproquement, si $|c+jd|^2 = 1$ alors $c + \bar{j}d = (c-d) - jd$ est l'inverse de $c+jd$ dans $\mathbb{Z}[j]$.

Trouver les inversibles de $\mathbb{Z}[j]$ revient à résoudre l'édquation $|c+jd|^2 = 1$ avec $c, d \in \mathbb{Z}$. On utilise la question (b-1). Si $cd > 0$, l'équation $(c-d)^2 + cd = 1$ n'est possible que si $c = d = \pm 1$, ce qui donne $c + jd = \pm(1+j) = \pm j^2$, lequel est bien inversible d'inverse $\pm j$. Si $cd \leq 0$, l'équation $c^2 + d^2 - cd = 1$ n'est possible que si $c = 0$ ou $d = 0$, auquel cas on doit avoir respectivement $d = \pm 1$ et $c = \pm 1$; on obtient dans ce cas $c + jd = \pm 1, \pm j$, qui sont bien inversibles.

(d) *Montrer que pour tout $a, b \in \mathbb{Z}[j]$ avec $b \neq 0$, il existe $q, r \in \mathbb{Z}[j]$ tels que $a = bq + r$ avec $|r| < |b|$.*

**Correction**: Posons $a = u + jv$ et $b = r + js$ avec $u, v, r, s \in \mathbb{Z}$. Dans $\mathbb{C}$, on a

$$\frac{a}{b} = \frac{u+jv}{r+js} = \frac{(u+jv)(r+\bar{j}s)}{r^2+s^2-rs}$$

et le nombre complexe $a/b$ peut donc être mis sous la forme $\alpha + j\beta$ avec $\alpha, \beta \in \mathbb{Q}$. D'après la question (b-2), il existe $m, n \in \mathbb{Z}$ tel que $(\alpha - m) + j(\beta - n)$ soit de module $< 1$, c'est-à-dire $|(a/b) - (m+jn)| < 1$. Posons $\rho = (a/b) - (m+jn)$ et $r = \rho b$. Par construction, on a alors $|r| < |b|$ et $a = b(m+jn) + r$. Comme $q = m + nj$ et $r = a - (m+jn)b$ sont dans $\mathbb{Z}[j]$, les deux nombres $q$ et $r$ répondent à la question.

(e) *Montrer que l'anneau $\mathbb{Z}[j]$ est principal.*

**Correction**: La question précédente montre que l'anneau $\mathbb{Z}[j]$ est un anneau euclidien, ce dont on sait impliquer qu'il est principal.

**Exercice 4 [5 pts]**: *On considère l'anneau $\mathbb{Z}[j] = \{m + jn | m, n \in \mathbb{Z}\}$ de l'exercice précédent (mais ce nouvel exercice peut être traité de façon indépendante).*

**Correction**:

(a) *Montrer que le polynôme $X^2 + X + 1$ est irréductible dans $\mathbb{Q}[X]$ et dans $\mathbb{Z}[X]$.*

**Correction**: Le polynôme $X^2 + X + 1$ n'a pas de racine dans $\mathbb{Q}$ (ses deux seules racines dans $\mathbb{C}$ sont $j$ et $\bar{j}$). Comme il est de degré 2, on peut en déduire qu'il est irréductible dans $\mathbb{Q}[X]$. Comme de plus il est primitif, il est irréductible dans $\mathbb{Z}[X]$.

(b) *Montrer que pour tout polynôme $f \in \mathbb{Z}[X]$, il existe un polynôme $Q \in \mathbb{Z}[X]$ et deux entiers $u, v \in \mathbb{Z}$ tels que $f(X) = (X^2 + X + 1)Q(X) + uX + v$.*

**Correction**: Le coefficient dominant de $X^2 + X + 1$, à savoir 1, est inversible dans $\mathbb{Z}$. Cela garantit l'existence de la division euclidienne de tout polynôme $f \in \mathbb{Z}[X]$ par $X^2 + X + 1$: il existe $Q, R \in \mathbb{Z}[X]$ tels que $f = (X^2 + X + 1)Q + R$ avec $R = 0$ ou $\deg(R) < 2$. Le polynôme $R$ s'écrit $R = uX + v$ avec $u, v \in \mathbb{Z}$.

(c) *Montrer que $\mathbb{Z}[j]$ est isomorphe à l'anneau $\mathbb{Z}[X]/\langle X^2 + X + 1 \rangle$,*

**Correction**: Considérons le morphisme $v_j : \mathbb{Z}[X] \to \mathbb{Z}[j]$ d'évaluation en $j$: si $f \in \mathbb{Z}[X]$, $v_j(f) = f(j)$. Ce morphisme est surjectif puisque pour tout $m + jn \in \mathbb{Z}[j]$, on a $m + jn = v_j(m + nX)$. Cherchons le noyau $\ker(v_j)$. Pour $f \in \mathbb{Z}[X]$, notons, comme en (b), $f(X) = (X^2 + X + 1)Q(X) + uX + v$ la division euclidienne de $f$ par $X^2 + X + 1$. Si

$f \in \ker(v_j)$, alors $f(j) = uj + v = 0$. Comme $j \notin \mathbb{Q}$, cela n'est possible que $u = v = 0$. D'où $uX + v = 0$, c'est-à-dire, $X^2 + X + 1$ divise $f$ dans $\mathbb{Z}[X]$. Cela montre que $\ker(v_j) \subset \langle X^2 + X + 1\rangle$. L'inclusion inverse étant évidente, on a $\ker(v_\alpha) = \langle X^2 + X + 1\rangle$. Les théorèmes d'isomorphisme classiques fournissent $\mathbb{Z}[X]/\langle X^2 + X + 1\rangle \simeq \mathbb{Z}[j]$.

(d) *Montrer que pour tout nombre premier $p \in \mathbb{N}$, on a*

$$\mathbb{Z}[j]/\langle p\rangle \simeq \mathbb{Z}[X]/\langle p, X^2 + X + 1\rangle \simeq (\mathbb{Z}/p\mathbb{Z})[X]/\langle X^2 + X + \overline{1}\rangle$$

*où on désigne par $\overline{1}$ la classe de 1 modulo p. (On justifiera soigneusement les différentes étapes du raisonnement en rappelant les résultats du cours utilisés).*

**Correction**: *Via* l'isomorphisme $\mathbb{Z}[X]/\langle X^2 + X + 1\rangle \simeq \mathbb{Z}[j]$ de la question (c), l'idéal $\langle p\rangle \subset \mathbb{Z}[j]$ correspond à l'idéal engendré dans $\mathbb{Z}[X]/\langle X^2+X+1\rangle$ par la classe de $p \in \mathbb{Z}[X]$ modulo $\langle X^2 + X + 1\rangle$, c'est-à-dire l'idéal $\langle s(p)\rangle$ si $s : \mathbb{Z}[X] \to \mathbb{Z}[X]/\langle X^2 + X + 1\rangle$ désigne la surjection canonique. On obtient ainsi l'isomorphisme

$$\frac{\mathbb{Z}[X]}{\langle X^2 + X + 1\rangle} \Big/ \langle s(p)\rangle \;\simeq\; \mathbb{Z}[j]/\langle p\rangle$$

Les théorèmes d'isomorphisme du cours permettent ensuite d'écrire

$$\frac{\mathbb{Z}[X]}{\langle X^2 + X + 1\rangle} \Big/ \langle s(p)\rangle \simeq \mathbb{Z}[X]/\langle p, X^2 + X + 1\rangle \simeq \frac{\mathbb{Z}[X]}{\langle p\rangle} \Big/ \sigma(\langle X^2 + X + 1\rangle)$$

avec $\sigma : \mathbb{Z}[X] \to \mathbb{Z}[X]/\langle p\rangle$ la surjection canonique. On sait aussi que l'anneau du haut du dernier terme est isomorphe à $(\mathbb{Z}/p\mathbb{Z})[X]$. On en déduit que le dernier terme est isomorphe à $(\mathbb{Z}/p\mathbb{Z})[X]/\langle X^2 + X + \overline{1}\rangle$. On a bien montré le résultat souhaité.

(e) *On prend ici $p = 7$. Montrer que*

(e-1) $X^2 + X + \overline{1}$ *a une racine dans* $\mathbb{Z}/7\mathbb{Z}$,

**Correction**: On vérifie que $\overline{2}$ (classe de 2 modulo 7) est racine de $X^2 + X + \overline{1}$ dans $\mathbb{Z}/7\mathbb{Z}$.

(e-2) *L'idéal $\langle 7\rangle$ engendré par 7 dans $\mathbb{Z}[j]$ n'est pas premier.*

**Correction**: Supposons que $\langle 7\rangle$ soit un idéal premier de $\mathbb{Z}[j]$. L'anneau quotient $\mathbb{Z}[\alpha]/\langle 7\rangle$ est alors intègre. D'après la question (d), l'anneau $(\mathbb{Z}/7\mathbb{Z})[X]/\langle X^2+X+\overline{1}\rangle$ l'est également, ou, de façon équivalente, $\langle X^2 + X + \overline{1}\rangle$ est un idéal premier de $(\mathbb{Z}/7\mathbb{Z})[X]$. Mais cela entraîne que le polynôme $X^2 + X + \overline{1}$ est irréductible dans $(\mathbb{Z}/7\mathbb{Z})[X]$, ce qui est absurde puisque ce polynôme a une racine dans $\mathbb{Z}/7\mathbb{Z}$ et qu'il est de degré $> 1$.

# UNIVERSITÉ DE LILLE

Enseignant responsable: **PIERRE DÈBES**
Filière: **Licence 5ème Semestre**
Matière: **M51**
Année universitaire: **2020/2021**
Date, heure et lieu: **lundi 18 Janvier 2020 à 8h au Bâtiment A5**
Durée de l'épreuve: **3 heures**

---

**Chacune des deux parties devra être rédigée sur une copie différente.**
**Ni calculatrice ni documents.**
**Le barême est donné à titre indicatif.**
**Une attention particulière sera portée à la rédaction.**

---

## PARTIE I

**Exercice 1 [6 pts]:** On définit l'ensemble $\mathbb{Z}[i\sqrt{7}]$ et l'application $N : \mathbb{Z}[i\sqrt{7}] \to \mathbb{Z}$ par:

$$\mathbb{Z}[i\sqrt{7}] = \{a + ib\sqrt{7} \in \mathbb{C} \mid a, b \in \mathbb{Z}\} \quad \text{et} \quad N(a + ib\sqrt{7}) = a^2 + 7b^2.$$

(a) Montrer que $(\mathbb{Z}[i\sqrt{7}], +, \times)$ est un anneau commutatif unitaire,
et que pour tous $z, z' \in \mathbb{Z}[i\sqrt{7}]$, on a $N(zz') = N(z)N(z')$.

(b) Montrer que les seuls éléments inversibles de l'anneau $\mathbb{Z}[i\sqrt{7}]$ sont 1 et $-1$.

(c) Montrer que 2, 3 et 5 sont des irréductibles de l'anneau $\mathbb{Z}[i\sqrt{7}]$.

(d) Montrer que ni 7 ni 11 ne sont des irréductibles de l'anneau $\mathbb{Z}[i\sqrt{7}]$.

(e) Vérifier que $(1 + i\sqrt{7})(1 - i\sqrt{7}) = 8$ et en déduire que $\mathbb{Z}[i\sqrt{7}]$ n'est pas principal.

**Exercice 2 [4 pts]:** Pour tout entier $n \geq 1$, on note $S_n$ l'ensemble des bijections de $\{1, \ldots, n\}$ dans $\{1, \ldots, n\}$. Soit $G$ un groupe fini et $\rho : G \to S_n$ une action de $G$ sur l'ensemble $\{1, \ldots, n\}$. On suppose que l'action $\rho$ est transitive, c'est-à-dire, qu'elle ne possède qu'une seule orbite. Pour tout $i \in \{1, \ldots, n\}$, on note $\mathrm{Stab}_G(i)$ le stabilisateur de $i$ sous l'action de $G$

(a) Montrer que pour tout $i \in \{1, \ldots, n\}$, on a $|\mathrm{Stab}_G(i)| = |G|/n$.

(b) Soit $U$ la réunion des ensembles $\mathrm{Stab}_G(i) \setminus \{1\}$ pour $i$ variant de 1 à $n$. Montrer que

$$|U| \leq |G| - n.$$

(c) Montrer que si $n \geq 2$, il existe $g \in G$ tel que pour tout $i \in \{1, \ldots, n\}$, on a $\rho(g)(i) \neq i$.
(Indication: on pourra raisonner par l'absurde).

**T.S.V.P.**

# PARTIE II

Dans les exercices 3 et 4, on note $(\mathbb{Z}/p\mathbb{Z})^*$ l'ensemble $(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$.

**Exercice 3 [4 pts]:** Soit $p$ un nombre premier. On note $\mathcal{C}_3(p)$ l'ensemble des cubes des éléments de $\mathbb{Z}/p\mathbb{Z}$, c'est-à-dire:

$$\mathcal{C}_3(p) = \{y^3 \mid y \in \mathbb{Z}/p\mathbb{Z}\}, \text{ et } \mathcal{C}_3(p)^* = \mathcal{C}_3(p) \setminus \{0\}.$$

(a) Montrer que l'application $\varphi$ envoyant $x$ sur $x^3$ est un morphisme du groupe $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ sur lui-même et que son noyau $\ker(\varphi)$ est d'ordre $\leq 3$.

(b) Montrer que si $p \not\equiv 1$ [mod 3] alors $|\ker(\varphi)| = 1$, et si $p \equiv 1$ [mod 3] alors $|\ker(\varphi)| = 3$. (Indication: pour le cas où $p \equiv 1$ [mod 3], on pourra utiliser sans le redémontrer le lemme selon lequel dans un groupe abélien fini d'ordre divisible par 3, il existe un élément d'ordre 3).

(c) Montrer que si $p \equiv 1$ [mod 3], alors $\mathcal{C}_3(p)^*$ est l'ensemble des éléments $x \in \mathbb{Z}/p\mathbb{Z}$ tels que $x^{(p-1)/3} = 1$.

(d) Quel est l'ensemble $\mathcal{C}_3(p)^*$ si $p \not\equiv 1$ [mod 3]?

**Exercice 4 [6 pts]:** (a) Trouver les factorisations en irréductibles du polynôme $X^6 - 1$ dans l'anneau $\mathbb{C}[X]$ et dans l'anneau $\mathbb{R}[X]$.

(b) Montrer que chacun des deux polynômes $(X^2-X+1)(X^2-1)$ et $(X^2-X+1)(X^3-1)$ divise $X^6 - 1$ dans l'anneau $\mathbb{Z}[X]$.

Soient $p$ un nombre premier et $\mu$ un élément de $\mathbb{Z}/p\mathbb{Z}$ tel que $\mu^2 - \mu + 1 = 0$.

(c) Montrer que $\mu$ est une racine du polynôme $X^6 - 1$ dans $\mathbb{Z}/p\mathbb{Z}$, et que, si $\mu^2 = 1$ ou bien $\mu^3 = 1$, alors $\mu$ est une racine d'ordre au moins deux de ce polynôme.

(d) Montrer que si $p \neq 2$ et $p \neq 3$ alors $\mu$ est d'ordre 6 dans le groupe $((\mathbb{Z}/p\mathbb{Z})^*, \times)$. (Indication: On pourra le déduire de la question (c) en utilisant, en la rappelant, la caractérisation donnée dans le cours des racines d'ordre multiple d'un polynôme).

(e) Montrer que pour tout entier $m$ multiple de 6, si $p$ est un diviseur premier de $m^2 - m + 1$, alors on a $p \equiv 1$ [mod 6].

# UNIVERSITÉ DE LILLE

Enseignant responsable: **Pierre DÈBES**
Filière: **Licence 5ème Semestre**
Matière: **M51**
Année universitaire: **2020/2021 - Session 2**
Date, heure et lieu: **Mercredi 9 Juin à 14h, Halles Grémeaux**
Durée de l'épreuve: **3 heures**

---

**Chacune des deux parties devra être rédigée sur une copie différente.**
**Ni calculatrice ni documents.**
**Le barême est donné à titre indicatif.**
**Une attention particulière sera portée à la rédaction.**

---

## PARTIE I (copie blanche)

**Exercice 1 [6 pts]:** On définit l'ensemble $\mathbb{Z}[i\sqrt{11}]$ et l'application $N : \mathbb{Z}[i\sqrt{11}] \to \mathbb{Z}$ par:

$$\mathbb{Z}[i\sqrt{11}] = \{a + ib\sqrt{11} \in \mathbb{C} \mid a, b \in \mathbb{Z}\} \quad \text{et} \quad N(a + ib\sqrt{11}) = a^2 + 11b^2.$$

(a) Montrer que $(\mathbb{Z}[i\sqrt{11}], +, \times)$ est un anneau commutatif unitaire,
et que pour tous $z, z' \in \mathbb{Z}[i\sqrt{11}]$, on a $N(zz') = N(z)N(z')$.

(b) Montrer que les seuls éléments inversibles de l'anneau $\mathbb{Z}[i\sqrt{11}]$ sont 1 et $-1$.

(c) Montrer que 2, 3, 5, 7 sont des irréductibles de l'anneau $\mathbb{Z}[i\sqrt{11}]$.

(d) Montrer que ni 9 ni 11 ni 47 ne sont des irréductibles de l'anneau $\mathbb{Z}[i\sqrt{11}]$.

(e) Vérifier que $(1 + i\sqrt{11})(1 - i\sqrt{11}) = 12$ et en déduire que $\mathbb{Z}[i\sqrt{11}]$ n'est pas principal.

**Exercice 2 [4 pts]:** Soient $G$ un groupe fini et $p$ un nombre premier divisant l'ordre de $G$. Soit $X$ l'ensemble des $p$-uplets $(g_1, \ldots, g_p) \in G^p$ tels que le produit $g_1 \cdots g_p$ vaut 1 (l'élément neutre de $G$). On note $\sigma$ le $p$-cycle $(1\,2\,\ldots\,p)$ et $\rho : \langle\sigma\rangle \to \mathrm{Bij}(X)$ l'action du groupe engendré par $\sigma$ (dans le groupe symétrique $S_p$) sur l'ensemble $X$ définie par

$$\rho(\sigma)(g_1, \ldots, g_p) = (g_{\sigma(1)}, \ldots, g_{\sigma(p)}) \text{ pour } \sigma \in S_p \text{ et } (g_1, \ldots, g_p) \in X.$$

(a) Montrer que l'application $f : X \to G^{p-1}$ définie par $f(g_1, \ldots, g_p) = (g_1, \ldots, g_{p-1})$ est une bijection et en déduire $\mathrm{card}(X)$.

(b) Montrer que les points fixes de l'action $\rho$ sont exactement les $p$-uplets de la forme $(g, \ldots, g)$ avec $g \in G$ tel que $g^p = 1$.

(c) Ecrire la formule des classes pour l'action $\rho$.

(d) Montrer que $G$ possède un élément d'ordre $p$.

**T.S.V.P.**

# PARTIE II (copie bleue)

Dans les exercices 3 et 4, on note $(\mathbb{Z}/p\mathbb{Z})^*$ l'ensemble $(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$.

**Exercice 3 [6 pts]:** Soit $p$ un nombre premier. On note $\mathcal{C}_5(p)$ l'ensemble des puissances 5-èmes des éléments de $\mathbb{Z}/p\mathbb{Z}$, c'est-à-dire:

$$\mathcal{C}_5(p) = \{x^5 \mid x \in \mathbb{Z}/p\mathbb{Z}\}, \text{ et } \mathcal{C}_5(p)^* = \mathcal{C}_5(p) \setminus \{0\}.$$

(a) Montrer que l'application $\varphi : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ définie par $\varphi(x) = x^5$ est un morphisme du groupe $((\mathbb{Z}/p\mathbb{Z})^*, \times)$, que son groupe image est $\mathcal{C}_5(p)^*$ et que son noyau $\ker(\varphi)$ est d'ordre $\leq 5$.

(b) Montrer que si $p \not\equiv 1$ [mod 5] alors $|\ker(\varphi)| = 1$.

(c) Montrer que si $p \equiv 1$ [mod 5] alors $|\ker(\varphi)| = 5$. (Indication: on pourra utiliser la question (d) de l'exercice 2).

(d) Montrer que si $p \equiv 1$ [mod 5], alors $\mathcal{C}_5(p)^*$ est l'ensemble des éléments $x \in \mathbb{Z}/p\mathbb{Z}$ tels que $x^{(p-1)/5} = 1$.

(e) Quel est l'ensemble $\mathcal{C}_5(p)^*$ si $p \not\equiv 1$ [mod 5]?

**Exercice 4 [4 pts]:** Soient $p$ un nombre premier et $\mu \in \mathbb{Z}$ un entier tel que $p$ divise $\mu^4 + 1$. On note $\overline{\mu}$ la classe de $\mu$ modulo $p$.

(a) Montrer que $\overline{\mu}$ est d'ordre au plus 8 dans le groupe $((\mathbb{Z}/p\mathbb{Z})^*, \times)$.

(b) Montrer que si $p \neq 2$, alors $\overline{\mu}$ est d'ordre égal à 8 dans le groupe $((\mathbb{Z}/p\mathbb{Z})^*, \times)$.

(c) Montrer que pour tout entier pair $m$, si $p$ est un diviseur premier de $m^4 + 1$, alors on a $p \equiv 1$ [mod 8].

# UNIVERSITÉ DE LILLE

Enseignant responsable: **Pierre DÈBES**
Filière: **Licence 5ème Semestre**
Matière: **M51**
Année universitaire: **2021/2022**
Date, heure et lieu: **vendredi 19 novembre 2021 à 9h au Bâtiment A5**
Durée de l'épreuve: **2 heures**

---

**Chacune des deux parties devra être rédigée sur une copie différente.**
**Ni calculatrice ni documents.**
**Le barême est donné à titre indicatif.**

**UNE ATTENTION PARTICULIÈRE SERA PORTÉE À LA RIGUEUR ET LA PRÉCISION DE LA RÉDACTION.**

---

## PARTIE I (cours)

**Question 1 [1,5 pts]:** Donner la définition
(a) d'un ensemble infini,
(b) d'un ensemble dénombrable.

**Question 2 [3,5 pts]:** Soient $G$ un groupe et $H$ un sous-groupe de G

(a) Donner la définition de la relation de congruence à gauche sur $G$ modulo $H$.

(b) Sans justifier que cette relation est une relation d'équivalence sur $G$, montrer que toutes ses classes d'équivalence sont des ensembles équipotents à $H$.
(c) *Application*: énoncer et démontrer le théorème de Lagrange pour un groupe $G$ fini.

**Question 3 [3,5 pts]:** (a) Donner

(a-1) la définition de l'action d'un groupe $G$ sur un ensemble $X$,

(a-2) pour $x \in X$, les définitions de l'orbite de $x$ et du stabilisateur de $x$ sous l'action de $G$.

(b) Supposant $G$ et $X$ finis, donner et démontrer la formule liant, pour $x \in X$ donné, les cardinaux du groupe $G$, de l'orbite de $x$ et du stabilisateur de $x$ sous l'action de $G$.

**Question 4 [1,5 pts]:** Enoncer un des trois "théorèmes d'isomorphisme" de la théorie des groupes.

**T.S.V.P.**

# PARTIE II (exercices)

**Exercice 1 [3,5 pts]:** Soient $G$ un groupe fini et $p$ un nombre premier divisant l'ordre de $G$. Soit $X$ l'ensemble des $p$-uplets $(g_1, \ldots, g_p) \in G^p$ tels que le produit $g_1 \cdots g_p$ vaut 1 (l'élément neutre de $G$). On note $\sigma$ le $p$-cycle $(1\,2\,\ldots\,p)$ et $\rho : \langle\sigma\rangle \to \mathrm{Bij}(X)$ l'action du groupe engendré par $\sigma$ (dans le groupe symétrique $S_p$) sur l'ensemble $X$ définie par

$$\rho(\sigma^k)(g_1, \ldots, g_p) = (g_{\sigma^k(1)}, \ldots, g_{\sigma^k(p)}) \quad ((g_1, \ldots, g_p) \in X,\, k \in \mathbb{Z}).$$

(a) Déterminer le cardinal de $X$ en fonction de $p$.

(b) Quels sont les points fixes de l'action $\rho$?

(c) Montrer que $G$ possède un élément d'ordre $p$.

**Exercice 2 [3 pts]:** Soit $G$ un groupe. On note $\varphi : G \to \mathrm{Aut}(G)$ le morphisme de conjugaison sur $G$, qui, à tout élément $g \in G$ associe l'automorphisme $\varphi_g : G \to G$ défini par $\varphi_g(x) = gxg^{-1}$ $(x \in G)$.

(a) Quel est le noyau $\ker(\varphi)$ du morphisme $\varphi$?

(b) Montrer que le centre $Z(G)$ du groupe $G$ est un sous-groupe distingué de $G$.
(On rappelle que $Z(G) = \{x \in G \mid xy = yx \text{ pour tout } y \in G\}$).

(c) Montrer que si le groupe quotient $G/Z(G)$ est monogène, alors le groupe $G$ est abélien.

**Exercice 3 [3,5 pts]:** Soient $G$ un groupe et $\mathcal{S}$ le sous-ensemble de $G$ constitué des éléments d'ordre 2.

(a) Montrer que le sous-groupe $\langle\mathcal{S}\rangle \subset G$ engendré par $\mathcal{S}$ est distingué. (Indication: on montrera d'abord que l'ensemble $\mathcal{S}$ est stable par conjugaison, puis on le montrera pour le groupe $\langle\mathcal{S}\rangle$).

(b) Montrer que si $G$ est d'ordre pair, alors $\mathcal{S} \neq \emptyset$.

(c) On suppose ici que le groupe $G$ est d'ordre pair et est un groupe simple. Montrer que $G$ est engendré par ses éléments d'ordre 2.

# UNIVERSITÉ LILLE 1

Enseignants: **P. DÈBES, E. DUCLOS, H. ZHANG**
Filière: **Licence - Semestre 5**
Matière: **M51**
Année universitaire: **2021/2022**
Épreuve: **Devoir à la maison**

---

**à rendre en TD la semaine du 29 novembre 2021.**

**UNE ATTENTION PARTICULIÈRE SERA PORTÉE À LA RIGUEUR ET LA PRÉCISION DE LA RÉDACTION.**

---

**Exercice 1 [5 pts]:** Etant donnés deux nombres premiers distincts $p$ et $q$, on considère les trois groupes suivants:

$G_1 = \mathbb{Z}/p^n\mathbb{Z}$ ($n \geq 1$ entier), $G_2 = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ et $G_3 = \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

(a) Pour chacun de ces trois groupes, déterminer l'ensemble de ses sous-groupes.
(On justifiera sa réponse).

Etant donné un groupe $G$, on s'intéresse ci-dessous aux *sous-groupes $H \subset G$ maximaux parmi les sous-groupes distincts de $G$*, c'est-à-dire ceux pour lesquels tout sous-groupe $H' \subset G$ contenant strictement $H$ est nécessairement égal à $G$.

On note $\Phi(G)$ l'intersection des sous-groupes $H \subset G$ maximaux parmi les sous-groupes distincts de $G$.

(b) Pour $i = 1, 2, 3$, déterminer le groupe $\Phi(G_i)$.

(c) Pour un groupe $G$ arbitraire, montrer que $\Phi(G)$ est un sous-groupe distingué de $G$ et qu'il a la propriété suivante:
(*) si $H$ est un sous-groupe de $G$ tel que $H\Phi(G) = G$, alors $H = G$.

**Exercice 2 [6 pts]:** Soit $G$ un groupe d'ordre $p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ où $p_1, \ldots, p_n$ sont $n$ nombres premiers tels que $p_1 < \ldots < p_n$ et $\alpha_i > 0$, $i = 1, \ldots, n$ ($n \geq 1$).

Soit $U$ un sous-groupe de $G$ d'indice $p_1$.

(a) Montrer que le pgcd de $p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ et de $p_1!$ est $p_1$.

On note $G/\cdot U$ l'ensemble des classes à gauche $xU$ de $G$ modulo $U$ ($x \in G$).

(b) Montrer que la formule: $\gamma(g)(xU) = gxU$ ($g, x \in G$) définit une action

$$\gamma : G \to \mathrm{Bij}(G/\cdot U)$$

du groupe $G$ sur l'ensemble $G/\cdot U$.

(c) Montrer que $|G/\ker(\gamma)| = p_1$.

(d) Montrer que $\ker(\gamma) = U$ et conclure que $U$ est distingué dans $G$.

**T.S.V.P.**

**Exercice 3 [9 pts]:** Le but de cet exercice est de montrer que tout nombre premier congru à 1 modulo 4 est somme de deux carrés.

**Première partie:** Soient $Y$ un ensemble fini et $\rho$ une involution sur $Y$, c'est-à-dire, une application $\rho : Y \longrightarrow Y$ telle que $\rho \circ \rho = \mathrm{Id}_Y$. Posons

$$Y^\rho := \{y \in Y \mid \rho(y) = y\}.$$

Montrer que $\mathrm{card}(Y)$ et $\mathrm{card}(Y^\rho)$ ont la même parité.

**Seconde partie:** On fixe un nombre premier $p$ congru à 1 modulo 4. On définit

$$X := \{(x, y, z) \in \mathbb{N}^3 \mid p = x^2 + 4yz\}.$$

(a) Montrer que $X$ est non vide et fini.

(b) Montrer que l'application $f : \mathbb{N}^3 \to \mathbb{N}^3$ définie par $f(x, y, z) = (x, z, y)$ se restreint en une involution sur $X$, notée $\sigma : X \to X$.

(c) Montrer que si $X^\sigma$ est non vide, alors $p$ est somme de deux carrés.

(d) Soit $(x, y, z) \in X$. Vérifier les trois inégalités suivantes:

$$y - z < 2y, \quad x \neq y - z, \quad x \neq 2y.$$

(e) Soit $g : X \to \mathbb{Z}^3$ l'application définie par

$$g(x, y, z) := \begin{cases} (x + 2z,\ z,\ y - x - z) & \text{si } x < y - z, \\ (2y - x,\ y,\ x - y + z) & \text{si } y - z < x < 2y, \\ (x - 2y,\ x - y + z,\ y) & \text{si } x > 2y. \end{cases}$$

Montrer que $g$ se restreint en une involution sur $X$, notée $\tau : X \longrightarrow X$.

(f) Décrire l'ensemble $X^\tau$. (Indication: penser à $(1, 1, k)$ pour $p = 4k + 1$.)

(g) Déduire de la première partie que les cardinaux des trois ensembles $X^\tau$, $X$ et $X^\sigma$ sont tous impairs. Conclure par la question (c).

# UNIVERSITÉ DE LILLE

Enseignants: **P. DÈBES, E. DUCLOS, H. ZHANG**
Filière: **Licence 3ème année, semestre 5**
Matière: **M51**
Année universitaire: **2021/2022 - Session 1**
Date, heure et lieu: **Lundi 3 Janvier 2022 à 14h, Bâtiment A5**
Durée de l'épreuve: **3 heures**

---

**Chacune des deux parties devra être rédigée sur une copie différente.**
**Ni calculatrice ni documents.**
**Le barême est donné à titre indicatif.**
**Une attention particulière sera portée à la rédaction.**

---

## PARTIE I (copie blanche)

**Exercice 1 [7 pts]:** On définit l'ensemble $\mathbb{Z}[i\sqrt{11}]$ et l'application $N : \mathbb{Z}[i\sqrt{11}] \to \mathbb{Z}$ par:

$$\mathbb{Z}[i\sqrt{11}] = \{a + ib\sqrt{11} \in \mathbb{C} \mid a, b \in \mathbb{Z}\} \quad \text{et} \quad N(a + ib\sqrt{11}) = a^2 + 11b^2.$$

(a) Montrer que $(\mathbb{Z}[i\sqrt{11}], +, \times)$ est un anneau commutatif unitaire,
et que pour tous $z, z' \in \mathbb{Z}[i\sqrt{11}]$, on a $N(zz') = N(z)N(z')$.

(b) Déterminer les éléments inversibles de l'anneau $\mathbb{Z}[i\sqrt{11}]$.

(c) Donner la définition d'un irréductible de l'anneau $\mathbb{Z}[i\sqrt{11}]$.

(d) Montrer que 2, 3, 5, 7 sont des irréductibles de l'anneau $\mathbb{Z}[i\sqrt{11}]$.

(e) Montrer que ni 9 ni 11 ni 47 ne sont des irréductibles de l'anneau $\mathbb{Z}[i\sqrt{11}]$.

(f) Vérifier que $(1 + i\sqrt{11})(1 - i\sqrt{11}) = 12$ et en déduire que $\mathbb{Z}[i\sqrt{11}]$ n'est pas principal.

**Exercice 2 [3 pts]:** Soit $G$ un groupe d'ordre $p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ où $p_1, \ldots, p_n$ sont $n$ nombres premiers tels que $0 < p_1 < \ldots < p_n$ et $\alpha_i > 0$, $i = 1, \ldots, n$ $(n \geq 1)$.

Soit $N$ un sous-groupe distingué de $G$ d'ordre $p_1$.

(a) Montrer que si $N \cap Z(G) \neq \{1\}$ alors $N \subset Z(G)$.

(b) En utilisant l'action de $G$ par conjugaison sur $N$, montrer que cette action n'a aucune orbite de cardinal $> 1$.

(c) Montrer que $N \subset Z(G)$.

**T.S.V.P.**

# PARTIE II (copie bleue)

Dans les exercices 3 et 4, étant donné un nombre premier $p$, on note

- $\mathbb{Z}/p\mathbb{Z}$ l'anneau des classes de congruence modulo $p$,
- $(\mathbb{Z}/p\mathbb{Z})^*$ l'ensemble $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$.

**Exercice 3 [7 pts]:** Soit $p$ un nombre premier.

(a) Montrer que l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps, et que pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^*$, on a $x^{p-1} = 1$.

(b) Enoncer le théorème donnant une majoration du nombre de racines d'un polynôme d'une variable à coefficients dans un corps.

(c) Montrer que l'application $\varphi : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ définie par $\varphi(x) = x^5$ est un morphisme du groupe $((\mathbb{Z}/p\mathbb{Z})^*, \times)$.

(d) Rappeler la définition du noyau $\ker(\varphi)$ et montrer que $\ker(\varphi)$ est de cardinal $\leq 5$.

(e) Montrer que si 5 ne divise pas $p-1$, alors $|\ker(\varphi)| = 1$. (Indication: pour $x \in \ker(\varphi)$, on pourra combiner la condition "$x \in \ker(\varphi)$" et l'égalité de la question (a)).

(f) Montrer que si 5 divise $p-1$, alors $|\ker(\varphi)| = 5$. (Indication: on pourra utiliser le théorème de Cauchy selon lequel si $p$ est un nombre premier divisant l'ordre d'un groupe fini $G$, alors $G$ possède un élément d'ordre $p$).

(g) Montrer que si 5 divise $p-1$, alors le groupe image $\mathrm{Im}(\varphi)$ de $\varphi$ est égal à l'ensemble

$$\mathcal{D} = \{x \in \mathbb{Z}/p\mathbb{Z} \mid x^{(p-1)/5} = 1\}.$$

**Exercice 4 [3 pts]:** Soient $p$ un nombre premier et $\mu \in \mathbb{Z}$ un entier tel que $p$ divise $\mu^4 + \mu^3 + \mu^2 + \mu + 1$. On note $\overline{\mu}$ la classe de $\mu$ modulo $p$.

(a) Montrer que $\overline{\mu}$ est d'ordre divisant 5 dans le groupe $((\mathbb{Z}/p\mathbb{Z})^*, \times)$.

(b) Montrer que si $p \neq 5$, alors $\overline{\mu}$ est d'ordre égal à 5 dans le groupe $((\mathbb{Z}/p\mathbb{Z})^*, \times)$.

(c) Montrer que pour tout entier $m$ multiple de 5, si $p$ est un diviseur premier de $m^4 + m^3 + m^2 + m + 1$, alors on a $p \equiv 1$ [mod 5]. Le vérifier sur un exemple.

# CORRIGÉ DU DS2

Enseignants: **P. DÈBES, E. DUCLOS, H. ZHANG**
Filière: **Licence 3ème année, semestre 5**
Matière: **M51**
Année universitaire: **2021/2022 - Session 1**
Date, heure et lieu: **Lundi 3 Janvier 2022 à 14h, Bâtiment A5**
Durée de l'épreuve: **3 heures**

---

## PARTIE I (copie blanche)

**Exercice 1 [7 pts]:** On définit l'ensemble $\mathbb{Z}[i\sqrt{11}]$ et l'application $N : \mathbb{Z}[i\sqrt{11}] \to \mathbb{Z}$ par:

$$\mathbb{Z}[i\sqrt{11}] = \{a + ib\sqrt{11} \in \mathbb{C} \mid a, b \in \mathbb{Z}\} \quad \text{et} \quad N(a + ib\sqrt{11}) = a^2 + 11b^2.$$

(a) Montrer que $(\mathbb{Z}[i\sqrt{11}], +, \times)$ est un anneau commutatif unitaire,
et que pour tous $z, z' \in \mathbb{Z}[i\sqrt{11}]$, on a $N(zz') = N(z)N(z')$.

**Correction:** On vérifie que $(\mathbb{Z}[i\sqrt{11}], +, \times)$ est un sous-anneau de $(\mathbb{C}, +, \times)$, c'est-à-dire: que pour tous $z, z' \in \mathbb{Z}[i\sqrt{11}]$, on a $z - z' \in \mathbb{Z}[i\sqrt{11}]$ et $z \cdot z' \in \mathbb{Z}[i\sqrt{11}]$, et que $0 \in \mathbb{Z}[i\sqrt{11}]$ (détails laissés au lecteur). La commutativité de la loi $\times$ est vraie sur $\mathbb{C}$, donc aussi sur $\mathbb{Z}[i\sqrt{11}]$. Comme $1 \in \mathbb{Z}[i\sqrt{11}]$, l'anneau commutatif $(\mathbb{Z}[i\sqrt{11}], +, \times)$ est également unitaire. En désignant par $\overline{u}$ le conjugué d'un nombre complexe $u$, pour tous $z, z' \in \mathbb{Z}[i\sqrt{11}]$, on a: $N(zz') = (zz') \cdot \overline{zz'} = z \cdot z' \cdot \overline{z} \cdot \overline{z'} = z \cdot \overline{z} \cdot z' \cdot \overline{z'} = N(z)N(z')$.

(b) Déterminer les éléments inversibles de l'anneau $\mathbb{Z}[i\sqrt{11}]$.

**Correction:** Si un élément $z \in \mathbb{Z}[i\sqrt{11}]$ est inversible, et que $z^{-1}$ désigne son inverse, on a $z \cdot z^{-1} = 1$, et donc en utilisant (a), que $N(z)N(z') = N(1) = 1$. En écrivant $z = a + ib\sqrt{11}$ avec $a, b \in \mathbb{Z}$, on voit que $N(z) = a^2 + 11b^2$ ne peut être égal à 1 que pour $a = \pm 1$ et $b = 0$, ce qui donne $z = \pm 1$. Réciproquement 1 et $-1$ sont inversibles, égaux à leurs inverses. Les inversibles de $\mathbb{Z}[i\sqrt{11}]$ sont donc 1 et $-1$.

(c) Donner la définition d'un irréductible de l'anneau $\mathbb{Z}[i\sqrt{11}]$.

**Correction:** Voir la Définition 54 du poly.

(d) Montrer que 2, 3, 5, 7 sont des irréductibles de l'anneau $\mathbb{Z}[i\sqrt{11}]$.

**Correction:** Notons $p$ l'un quelconque des quatre nombres 2, 3, 5, 7. Supposons que $p = zz'$ avec $z, z' \in \mathbb{Z}[i\sqrt{11}]$. Par (b), on a $N(p) = p^2 = N(z)N(z')$. Comme $p$ est premier et que $N(z)$, $N(z')$ sont des entiers positifs, $N(z)$ ne peut valoir que 1, $p$ ou $p^2$. On vérifie aisément que pour chacun des quatre nombres 2, 3, 5, 7, l'équation $N(z) = p$ n'a pas de solution dans $\mathbb{Z}[i\sqrt{11}]$ (détails laissés au lecteur). On a donc: ou bien $N(z) = 1$ auquel cas $z$ est inversible, ou bien $N(z) = p^2$ et alors $N(z') = 1$, auquel cas $z'$ est inversible. On a montré que $p$ est irréductible.

(e) Montrer que ni 9 ni 11 ni 47 ne sont des irréductibles de l'anneau $\mathbb{Z}[i\sqrt{11}]$.

**Correction:** 9 n'est pas irréductible car $9 = 3 \cdot 3$ et que 3 n'est pas inversible. Similairement, 11 n'est pas irréductible car $11 = \sqrt{11} \cdot \sqrt{11}$ et que l'élément $\sqrt{11} \in \mathbb{Z}[i\sqrt{11}]$ n'est pas inversible. Enfin 47 n'est pas irréductible car $47 = (6 + i\sqrt{11}) \cdot (6 - i\sqrt{11})$ et que ni $6 + i\sqrt{11}$ ni $6 - i\sqrt{11}$ ne sont des inversibles de $\mathbb{Z}[i\sqrt{11}]$.

(f) Vérifier que $(1 + i\sqrt{11})(1 - i\sqrt{11}) = 12$ et en déduire que $\mathbb{Z}[i\sqrt{11}]$ n'est pas principal.

**Correction:** La vérification est immédiate et donne que $(1+i\sqrt{11})(1-i\sqrt{11}) = 2^2 \cdot 3$. D'après (d), 3 est un irréductible, et il divise le produit $(1+i\sqrt{11})(1-i\sqrt{11})$. Si l'anneau $\mathbb{Z}[i\sqrt{11}]$ était principal, par le lemme de Gauss, on devrait avoir que ou bien 3 divise $1+i\sqrt{11}$ ou bien 3 divise $1-i\sqrt{11}$. Comme ce n'est pas vrai (puisque 3 ne divise pas 1 dans $\mathbb{Z}$), on peut conclure que $\mathbb{Z}[i\sqrt{11}]$ n'est pas principal.

**Exercice 2 [3 pts]:** Soit $G$ un groupe d'ordre $p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ où $p_1, \ldots, p_n$ sont $n$ nombres premiers tels que $0 < p_1 < \ldots < p_n$ et $\alpha_i > 0$, $i = 1, \ldots, n$ $(n \geq 1)$.

Soit $N$ un sous-groupe distingué de $G$ d'ordre $p_1$.

(a) Montrer que si $N \cap Z(G) \neq \{1\}$ alors $N \subset Z(G)$.

**Correction:** Supposons que $N \cap Z(G) \neq \{1\}$. Soit $x \in N \cap Z(G)$, $x \neq 1$. Comme $N \cap Z(G)$ est un groupe, il contient le groupe $\langle x \rangle$ engendré par $x$. Comme $N$ est d'ordre premier $p_1$, on a $\langle x \rangle = N$. On a donc $N \subset N \cap Z(G)$, et donc $N \subset Z(G)$.

(b) En utilisant l'action de $G$ par conjugaison sur $N$, montrer que cette action n'a aucune orbite de cardinal $> 1$.

**Correction:** L'action par conjugaison de $G$ sur $N$ est bien définie parce que $N$ est distingué dans $G$. Supposons qu'une orbite $\mathcal{O}$ de cette action soit de cardinal $> 1$. Comme $\mathrm{card}(\mathcal{O})$ divise $|G|$, on a $\mathrm{card}(\mathcal{O}) \geq p_1$ (puisque $p_1$ est le plus petit diviseur positif différent de 1 de $|G|$). Mais l'action a aussi une orbite de cardinal 1, à savoir celle de l'élément neutre de $G$. On obtient une contradiction puisque la réunion (disjointe) de ces deux orbites est de cardinal $p_1 + 1$ alors que la réunion de toutes les orbites est égale à $N$ (d'ordre $p_1$).

(c) Montrer que $N \subset Z(G)$.

**Correction:** D'après (b), toutes les orbites sont de cardinal 1. Autrement dit, tous les points de $N$ sont fixes. Pour l'action considérée, cela signifie que $N \subset Z(G)$.

## PARTIE II (copie bleue)

Dans les exercices 3 et 4, étant donné un nombre premier $p$, on note

- $\mathbb{Z}/p\mathbb{Z}$ l'anneau des classes de congruence modulo $p$,
- $(\mathbb{Z}/p\mathbb{Z})^*$ l'ensemble $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$.

**Exercice 3 [7 pts]:** Soit $p$ un nombre premier.

(a) Montrer que l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps, et que pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^*$, on a $x^{p-1} = 1$.

**Correction:** Soit $\overline{n} \in \mathbb{Z}/p\mathbb{Z}$ la classe modulo $p$ d'un entier $n \in \mathbb{Z}$. Si $\overline{n} \neq 0$, alors $p$ ne diivise pas $n$ et donc $p$ et $n$ sont premiers entre eux (puisque $p$ est premier). D'après Bézout, il existe $a, b \in \mathbb{Z}$ tels que $ap + bn = 1$, ce qui donne $\overline{b}\,\overline{n} = \overline{1}$. Ainsi $\overline{n}$ est inversible pour tout $\overline{n} \in \mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$; cela montre que l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps. Le groupe multiplicatif $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ est d'ordre $p-1$. D'après une conséquence classique du théorème de Lagrange, on a $x^{p-1} = 1$ pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^*$.

(b) Enoncer le théorème donnant une majoration du nombre de racines d'un polynôme d'une variable à coefficients dans un corps.

**Correction:** Voir le Corollaire 17 du poly.

(c) Montrer que l'application $\varphi : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ définie par $\varphi(x) = x^5$ est un morphisme du groupe $((\mathbb{Z}/p\mathbb{Z})^*, \times)$.

**Correction:** Il s'agit de voir que $\varphi(xy) = (xy)^5 = x^5y^5 = \varphi(x)\varphi(y)$ si $x, y \in (\mathbb{Z}/p\mathbb{Z})^*$.

(d) Rappeler la définition du noyau $\ker(\varphi)$ et montrer que $\ker(\varphi)$ est de cardinal $\leq 5$.

**Correction:** Le noyau $\ker(\varphi)$ est l'ensemble des $x \in (\mathbb{Z}/p\mathbb{Z})^*$ tels que $x^5 = 1$. D'après le théorème rappelé en (b), au plus 5 éléments du corps $\mathbb{Z}/p\mathbb{Z}$ satisfont cette équation.

(e) Montrer que si 5 ne divise pas $p-1$, alors $|\ker(\varphi)| = 1$. (Indication: pour $x \in \ker(\varphi)$, on pourra combiner la condition "$x \in \ker(\varphi)$" et l'égalité de la question (a)).

**Correction:** Soit $x \in \ker(\varphi)$. On a donc $x^5 = 1$ et, d'après l'égalité de la question (a), on a aussi $x^{p-1} = 1$. Comme 5 ne divise pas $p-1$ et que 5 est premier, 5 et $p-1$ sont premiers entre eux. D'après Bézout, il existe $a, b \in \mathbb{Z}$ tels que $a(p-1)+5b = 1$. On déduit $x = (x^{p-1})^a(x^5)^b = 1$. D'où $\ker(\varphi) \subset \{1\}$ et donc $\ker(\varphi) = \{1\}$ puisque $1 \in \ker(\varphi)$.

(f) Montrer que si 5 divise $p-1$, alors $|\ker(\varphi)| = 5$. (Indication: on pourra utiliser le théorème de Cauchy selon lequel si $p$ est un nombre premier divisant l'ordre d'un groupe fini $G$, alors $G$ possède un élément d'ordre $p$).

**Correction:** D'après le théorème de Cauchy, le groupe $(\mathbb{Z}/p\mathbb{Z})^*$, qui est d'ordre $p-1$ supposé divisible par 5, possède un élément $\alpha$ d'ordre 5. Les 5 éléments $1, \alpha, \ldots, \alpha^4$ sont dans $\ker(\varphi)$, qui est donc d'ordre $\geq 5$. Combiné à (d), cela donne $|\ker(\varphi)| = 5$.

(g) Montrer que si 5 divise $p-1$, alors le groupe image $\mathrm{Im}(\varphi)$ de $\varphi$ est égal à l'ensemble

$$\mathcal{D} = \{x \in \mathbb{Z}/p\mathbb{Z} \,|\, x^{(p-1)/5} = 1\}.$$

**Correction:** On sait que le groupe quotient $(\mathbb{Z}/p\mathbb{Z})^*/\ker(\varphi)$ est isomorphe au groupe image $\mathrm{Im}(\varphi)$. Cela donne $|\mathrm{Im}(\varphi)| = (p-1)/5$ (en utilisant (f)). On a aussi $\mathrm{Im}(\varphi) \subset \mathcal{D}$: en effet, pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^*$, on a: $\varphi(x)^{(p-1)/5} = (x^5)^{(p-1)/5} = x^{p-1} = 1$. Enfin, d'après le théorème rappelé en (b), on a $\mathrm{card}(\mathcal{D}) \leq (p-1)/5$. Ces trois faits donnent que $\mathrm{card}(\mathcal{D}) = (p-1)/5$ et $\mathcal{D} = \mathrm{Im}(\varphi)$.

**Exercice 4 [3 pts]:** Soient $p$ un nombre premier et $\mu \in \mathbb{Z}$ un entier tel que $p$ divise $\mu^4 + \mu^3 + \mu^2 + \mu + 1$. On note $\overline{\mu}$ la classe de $\mu$ modulo $p$.

(a) Montrer que $\overline{\mu}$ est d'ordre divisant 5 dans le groupe $((\mathbb{Z}/p\mathbb{Z})^*, \times)$.

**Correction:** Par définition de l'ordre, il s'agit de vérifier que $\overline{\mu}^5 = \overline{1}$. Or on a

$$(\overline{\mu}^5 - \overline{1}) = (\overline{\mu}^4 + \overline{\mu}^3 + \overline{\mu}^2 + \overline{\mu} + \overline{1})(\overline{\mu} - \overline{1}) = \overline{(\mu^4 + \mu^3 + \mu^2 + \mu + 1)}(\overline{\mu} - \overline{1}) = \overline{0} \cdot (\overline{\mu} - \overline{1}) = \overline{0}.$$

(b) Montrer que si $p \neq 5$, alors $\overline{\mu}$ est d'ordre égal à 5 dans le groupe $((\mathbb{Z}/p\mathbb{Z})^*, \times)$.

**Correction:** D'après la question précédente, $\overline{\mu}$ est d'ordre égal à 1 ou à 5. S'il était d'ordre 1, on aurait $\overline{\mu} = \overline{1}$. Cela entraînerait $\overline{\mu}^4 + \overline{\mu}^3 + \overline{\mu}^2 + \overline{\mu} + \overline{1} = \overline{5} = \overline{0}$, et donc $p = 5$, ce qui est exclus. Conclusion: $\overline{\mu}$ est d'ordre 5.

(c) Montrer que pour tout entier $m$ multiple de 5, si $p$ est un diviseur premier de $m^4 + m^3 + m^2 + m + 1$, alors on a $p \equiv 1$ [mod 5]. Le vérifier sur un exemple.

**Correction:** On applique ce qui précède avec $\mu = m$. Le nombre premier $p$ est bien un diviseur de $\mu^4+\mu^3+\mu^2+\mu+1$. De plus $p \neq 5$ car, $\mu = m$ étant supposé divisible par 5, on a que 5 divise chacun des nombres $\mu^4, \mu^3, \mu^2, \mu$ et donc ne divise pas $\mu^4+\mu^3+\mu^2+\mu+1$. D'après la question (b), $\overline{\mu}$ est d'ordre égal à 5 dans le groupe $((\mathbb{Z}/p\mathbb{Z})^*, \times)$. D'après le théorème de Lagrange, 5 divise l'ordre du groupe $(\mathbb{Z}/p\mathbb{Z})^*$, c'est-à-dire, 5 divise $p-1$, ou, de façon équivalente, $p \equiv 1$ [mod 5]. Par exemple, pour $m = 5$, on a $m^4+m^3+m^2+m+1 = 781 = 11 \cdot 71$. Les deux facteurs premiers 11 et 71 sont bien congrus à 1 modulo 5.

# UNIVERSITÉ DE LILLE

Enseignants: **P. DÈBES, E. DUCLOS, H. ZHANG**
Filière: **Licence 3ème année, semestre 5**
Matière: **M51**
Année universitaire: **2021/2022 - Session de substitution**
Date et heure: **le jeudi 10 février 2022 de 16h30 à 18h30**
Durée de l'épreuve: **2 heures**

---

**Ni calculatrice ni documents.**
**Le barême est donné à titre indicatif.**
**Une attention particulière sera portée à la rédaction.**

---

Dans la suite, on utilise les notations suivantes:

- si $p$ est un nombre premier, $\mathbb{Z}/p\mathbb{Z}$ désigne l'anneau des classes de congruence modulo $p$,
- si $A$ est un anneau commutatif unitaire, $A[X]$ désigne l'anneau des polynômes en une indéterminée à coefficients dans $A$,
- si $A$ est un anneau commutatif unitaire et $a \in A$, l'idéal engendré par $a$ est noté $(a)$.

**Exercice 1 [8 pts]:** On définit l'ensemble $\mathbb{Z}[i]$ et l'application $N : \mathbb{Z}[i] \to \mathbb{N}$ par:

$$\mathbb{Z}[i] = \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\} \quad \text{et} \quad N(a + ib) = a^2 + b^2.$$

(a) Montrer que $(\mathbb{Z}[i], +, \times)$ est un anneau commutatif unitaire,
et que pour tous $z, z' \in \mathbb{Z}[i]$, on a $N(zz') = N(z)N(z')$.

(b) Déterminer les éléments inversibles de l'anneau $\mathbb{Z}[i]$.

(c) Donner la définition d'un irréductible de l'anneau $\mathbb{Z}[i]$.

(d) Montrer que 3 et 7 sont des irréductibles de l'anneau $\mathbb{Z}[i]$.

(e) Montrer que ni 2 ni 5 ni 37 ne sont des irréductibles de l'anneau $\mathbb{Z}[i]$.

**Exercice 2 [5 pts]:** On conserve les notations de l'exercice 1.

(a) Montrer que $\mathbb{Z}[i]$ et $\mathbb{Z}[X]/(X^2 + 1)$ sont des anneaux isomorphes.

(b) Montrer que les anneaux $\mathbb{Z}[i]/(p)$ et $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2 + \overline{1})$ sont isomorphes (où $\overline{1}$ désigne la classe de 1 modulo $p$).
(Indication: on pourra combiner la question (a) au théorème d'isomorphisme selon lequel *si $A$ est un anneau commutatif unitaire, $I$ et $J$ sont deux idéaux de $A$ et $s : A \to A/I$ est la surjection canonique, alors on a un isomorphisme d'anneau*

$$A/(I + J) \simeq (A/I)/(s(J)/I).$$

**Exercice 3 [7 pts]:** On conserve les notations des exercices 1 et 2. On admettra que $\mathbb{Z}[i]$ est un anneau euclidien (ce qui figure dans le cours).

On fixe un nombre premier $p$ tel que $-\overline{1}$ est le carré d'un élément de $\mathbb{Z}/p\mathbb{Z}$.

(a) Expliciter l'hypothèse faite sur $p$ en termes de divisibilité d'entiers et donner un exemple de nombre premier $p$ satisfaisant cette hypothèse.

(b) Montrer que $p$ n'est pas irréductible dans $\mathbb{Z}[i]$, et en déduire que $p$ est le produit d'un nombre $r \geq 2$ d'irréductibles $P_1, \ldots, P_r$ de $\mathbb{Z}[i]$. (On précisera bien les propriétés de l'anneau $\mathbb{Z}[i]$ utilisées dans les arguments).

(c) Montrer qu'il existe $i \in \{1, \ldots, r\}$ tel que $N(P_i) = p$ et conclure que $p$ est somme de deux carrés d'entiers. Le vérifier sur un exemple de nombre premier $p$.

# UNIVERSITÉ DE LILLE

Enseignants: **P. DÈBES, E. DUCLOS, H. ZHANG**
Filière: **Licence 3ème année, semestre 5**
Matière: **M51**
Année universitaire: **2021/2022 - Session 2**
Date, heure et lieu: **mercredi 8 Juin 2022 à 8h en Halle Vallin**
Durée de l'épreuve: **3 heures**

---

**Ni calculatrice ni documents.**
**Le barême est donné à titre indicatif.**
**Une attention particulière sera portée à la rédaction.**

---

Dans la suite, on utilise les notations suivantes:

- si $p$ est un nombre premier, $\mathbb{Z}/p\mathbb{Z}$ désigne l'anneau des classes de congruence modulo $p$,
- si $A$ est un anneau commutatif unitaire, $A[X]$ désigne l'anneau des polynômes en l'indéterminée $X$ et à coefficients dans $A$,
- si $A$ est un anneau commutatif unitaire et $a \in A$, l'idéal engendré par $a$ est noté $(a)$.
- si $n \geq 1$ est un entier, $S_n$ désigne le groupe symétrique de degré $n$.

**Exercice 1 [5 pts]:** Soit $G$ un groupe fini.

(a) Donner la définition de l'ordre d'un élément $g$ de $G$.

(b) Montrer que si le cardinal de $G$ est un nombre premier, alors tout élément $g \in G$ différent de l'élément neutre engendre $G$. (L'argument sera détaillé avec soin en précisant bien les résultats utilisés).

Soit $n \geq 3$ un entier.

(c) Montrer que tout 3-cycle $\gamma \in S_n$ peut s'écrire $\gamma = \omega^2$ avec $\omega \in S_n$.

(d) Montrer que le seul groupe $H \subset S_n$ d'indice 2 est le groupe alterné $A_n$ (Indication: on rappelle que $A_n$ est engendré par les 3-cycles).

**Exercice 2 [5 pts]:** On définit l'ensemble $\mathbb{Z}[i\sqrt{2}]$ et l'application $N : \mathbb{Z}[i\sqrt{2}] \to \mathbb{Z}$ par:

$$\mathbb{Z}[i\sqrt{2}] = \{a + ib\sqrt{2} \in \mathbb{C} \mid a, b \in \mathbb{Z}\} \quad \text{et} \quad N(a + ib\sqrt{2}) = a^2 + 2b^2.$$

(a) Montrer que $(\mathbb{Z}[i\sqrt{2}], +, \times)$ est un anneau commutatif unitaire,
et que pour tous $z, z' \in \mathbb{Z}[i\sqrt{2}]$, on a $N(zz') = N(z)N(z')$.

(b) Déterminer les éléments inversibles de l'anneau $\mathbb{Z}[i\sqrt{2}]$.

(c) Pour un élément non nul $\alpha \in \mathbb{Z}[i\sqrt{2}]$, donner la définition de chacune des deux conditions suivantes:

(i) $\alpha$ est irréductible dans $\mathbb{Z}[i\sqrt{2}]$.

(ii) L'idéal $(\alpha)$ est un idéal premier de $\mathbb{Z}[i\sqrt{2}]$.

**Exercice 3 [4,5 pts]:** On conserve les notations de l'exercice 2. Soient $\alpha = a + ib\sqrt{2}$ et $\beta = a' + ib'\sqrt{2}$ deux éléments de $\mathbb{Z}[i\sqrt{2}]$, avec $\beta \neq 0$.

(a) Montrer qu'on peut écrire $\dfrac{\alpha}{\beta} = u + iv\sqrt{2}$ avec $u, v \in \mathbb{Q}$.

(b) Soient $c$ et $d$ deux entiers tels que $|u - c| \leq 1/2$ et $|v - d| \leq 1/2$ ($c$ et $d$ sont les éléments de $\mathbb{Z}$ les plus proches de $u$ et $v$ respectivement). Montrer que

$$\alpha = \beta(c + id\sqrt{2}) + r,$$

$$\text{où} \quad \begin{cases} (c + id\sqrt{2}) \in \mathbb{Z}[i\sqrt{2}], \\ r = \beta\left[(u - c) + i\sqrt{2}(v - d)\right], \\ r \in \mathbb{Z}[i\sqrt{2}], \\ N(r) < N(\beta). \end{cases}$$

(c) Quelle propriété de l'anneau $\mathbb{Z}[i\sqrt{2}]$ montre la question (b)? Quelle conséquence a cette propriété sur les conditions (i) et (ii) de la question (c) de l'exercice 2?

**Exercice 4 [5,5 pts]:** On conserve les notations des exercices 2 et 3. On admettra que $\mathbb{Z}[i\sqrt{2}]$ est un anneau principal.

On fixe un nombre premier $p \neq 2$ tel que la classe de $-2$ modulo $p$ soit le carré d'un élément de $\mathbb{Z}/p\mathbb{Z}$.

(a) Expliciter l'hypothèse faite sur $p$ en termes de divisibilité d'entiers et montrer que $p = 11$ et $p = 17$ vérifient cette hypothèse tandis que 7 ne la vérifie pas.

(b) Montrer que $p$ n'est pas irréductible dans $\mathbb{Z}[i\sqrt{2}]$. (Indication: on pourra le déduire de l'hypothèse sur $p$).

(c) Déduire de (b) que $p$ est le produit d'un nombre $r \geq 2$ d'irréductibles $P_1, \ldots, P_r$ de l'anneau $\mathbb{Z}[i\sqrt{2}]$.

(d) Montrer qu'il existe $i \in \{1, \ldots, r\}$ tel que $N(P_i) = p$ et conclure qu'on peut écrire $p = a^2 + 2b^2$ avec $a, b \in \mathbb{Z}$. Le vérifier sur deux exemples de nombres premiers $p$.

# UNIVERSITÉ DE LILLE

Enseignants: **P. DÈBES**, **M. DIMITROV**, **D. MARKOUCHEVITCH**, **H. ZHANG**
Filière: **Licence 5ème Semestre**
Matière: **M51**
Année universitaire: **2022/2023**
Date, heure et lieu: **lundi 7 novembre 2022 à 8h au Bâtiment A5**
Durée de l'épreuve: **2 heures**

---

**Chacune des deux parties devra être rédigée sur une copie différente.**
**Ni calculatrice ni documents.**
**Le barême est donné à titre indicatif.**

**UNE ATTENTION PARTICULIÈRE SERA PORTÉE À LA RIGUEUR ET LA PRÉCISION DE LA RÉDACTION.**

---

## PARTIE I (cours)

**Question 1 [3 pts]:** Soient $G$ un groupe et $H$ un sous-groupe de $G$. Montrer que si $H$ est d'indice 2 dans $G$ alors le sous-groupe $H$ est distingué dans $G$. (On précisera le sens de l'hypothèse et celui de la conclusion au sein de la preuve).

**Question 2 [3,5 pts]:**

(a) Étant donnés un groupe $G$ et un sous-ensemble $S \subset G$, donner la définition du *sous-groupe* $\langle S \rangle$ *de* $G$ *engendré par* $S$. Que peut-on dire de $\langle S \rangle$ quand $S = \{g\}$ est un singleton? On justifiera la réponse.

(b) Montrer que si $G$ est un groupe cyclique d'ordre $n$ ($n \in \mathbb{N}^*$), alors $G$ est isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

**Question 3 [3,5 pts]:**

(a) Donner la définition de *l'action d'un groupe* $G$ *sur un ensemble* $X$ et énoncer *l'équation aux classes* (en précisant bien les termes qui y apparaissent).

(b) Soit $G$ un groupe d'ordre égal à une puissance $p^r$ d'un nombre premier $p$ avec $r \geq 1$. Rappeler la définition de *l'action par conjugaison de* $G$ *sur lui-même* et démontrer que le centre de $G$ possède au moins un élément différent de l'élément neutre de $G$.

**T.S.V.P.**

# PARTIE II (exercices)

**Exercice 1 [3 pts]:** Soient $A$ une partie de $E$ et $\mathcal{R}$ la relation définie sur l'ensemble $\mathcal{P}(E)$ des parties de $E$ par: pour $X, Y \in \mathcal{P}(E)$, on a $X \mathcal{R} Y$ si $X \cap A = Y \cap A$.

(a) Montrer que $\mathcal{R}$ est une relation d'équivalence.

(b) Montrer que l'ensemble quotient $\mathcal{P}(E)/\mathcal{R}$ est équipotent à $\mathcal{P}(A)$.

(c) On suppose $E$ fini. On note $\chi_A : E \to \{0,1\}$ la fonction caractéristique de $A$, définie par $\chi_A(x) = 1$ si $x \in A$ et $\chi_A(x) = 0$ si $x \notin A$. Montrer que l'application

$$f : \begin{cases} \mathcal{P}(E) & \to & \mathbb{N} \\ X & \mapsto & f(X) = \sum_{x \in X} \chi_A(x) \end{cases}$$

est compatible avec la relation d'équivalence $\mathcal{R}$.

**Exercice 2 [3 pts]**: On note 1, $I$, $J$, $K$ les matrices $2 \times 2$ à coefficients complexes

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \ , \ I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \ , \ J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \ K = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

(avec $i \in \mathbb{C}$ tel que $i^2 = -1$)

et on considère le groupe $\mathbb{H}_8$ composé des 8 éléments $\pm 1, \pm I, \pm J, \pm K$ et dont la table de multiplication est déterminée par les relations $I^2 = J^2 = K^2 = -1$, $IJ = -JI = K$, $JK = -KJ = I$ et $KI = -IK = J$.

(a) Montrer que tous les sous-groupes de $\mathbb{H}_8$ sont distingués.

(b) Le groupe quotient $\mathbb{H}_8/\langle -1 \rangle$ est-il cyclique? Justifier la réponse.

**Exercice 3 [4 pts] :** On note $I = \{1,2,3,4\}$, $J = \{5,6,7\}$ et $G$ le sous-groupe du groupe symétrique $S_7$ des permutations $\sigma$ de $\{1, \ldots, 7\}$ qui vérifient $\sigma(I) \subset I$.

Soit $\sigma \in S_7$ n'appartenant pas au sous-groupe $G$.

(a) Montrer qu'il existe $a \in I$ tels que $\sigma(a) \in I$.

(b) Montrer qu'il existe $b \in I$ tels que $\sigma(b) \in J$.

On pose $\sigma(a) = a'$ et $\sigma(b) = b'$; on a $a' \in I$ et $b' \in J$.

(c) Pour $i \in I$ et $j \in J$, on note $\tau$ la permutation

$$\tau = (a'\ i) \cdot (b'\ j) \cdot \sigma$$

(où on convient que $(a'\ i) = \mathrm{Id}$ si $a' = i$ et $(b'\ j) = \mathrm{Id}$ si $b' = j$). Calculer le produit

$$\tau \cdot (a\ b) \cdot \tau^{-1}$$

(d) Montrer que le groupe $\langle G, \sigma \rangle$ engendré par $G$ et $\sigma$ contient toutes les transpositions de $S_7$. Que peut-on en déduire?

# UNIVERSITÉ DE LILLE

Enseignant: **P. DÈBES**
Filière: **Licence 5ème Semestre**
Matière: **M51**
Année universitaire: **2022/2023**
Epreuve: **Devoir à la maison - 1ère partie**
Date: **à rendre le vendredi 21 cctobre 2022**

---

**UNE ATTENTION PARTICULIÈRE SERA PORTÉE À LA RIGUEUR ET LA PRÉCISION DE LA RÉDACTION.**

---

Le but du problème est de déterminer les sous-groupes du groupe $(\mathbb{Z}^2, +)$.

On note $p_1 : \mathbb{Z}^2 \to \mathbb{Z}$ et $p_2 : \mathbb{Z}^2 \to \mathbb{Z}$ les deux projections, qui à un couple $(z_1, z_2) \in \mathbb{Z}^2$ associent respectivement $p_1(z_1, z_2) = z_1$ et $p_2(z_1, z_2) = z_2$.

Soit $H$ un sous-groupe du groupe $(\mathbb{Z}^2, +)$.

(a) Montrer qu'il existe deux entiers $n_1, n_2 \in \mathbb{N}$ tels que:

$$p_1(H) = n_1\mathbb{Z} \quad \text{et} \quad p_2(H \cap (\{0\} \times \mathbb{Z})) = n_2\mathbb{Z}.$$

(b) Montrer qu'il existe $\mathbf{u}_1 \in H$ et $\mathbf{u}_2 \in H \cap (\{0\} \times \mathbb{Z})$ tels que $p_1(\mathbf{u}_1) = n_1$ et $p_2(\mathbf{u}_2) = n_2$, et qu'alors $H = \mathbb{Z}\mathbf{u}_1 + \mathbb{Z}\mathbf{u}_2$.

(c) Montrer plus généralement que si $H$ est un sous-groupe du groupe $(\mathbb{Z}^n, +)$ $(n \geq 1)$, alors il existe $\mathbf{u}_1, \ldots, \mathbf{u}_n \in H$ tels que $H = \mathbb{Z}\mathbf{u}_1 + \cdots + \mathbb{Z}\mathbf{u}_n$.

On revient au cas $n = 2$.

(d) Montrer que si $n_1 = 0$ alors on peut prendre $\mathbf{u}_1 = (0, 0)$ et alors $H = \mathbb{Z}\mathbf{u}_2$, et que si $n_2 = 0$, alors $H = \mathbb{Z}\mathbf{u}_1$.

(e) Montrer que si $n_1 n_2 \neq 0$, alors on a $n_1 n_2 \mathbb{Z}^2 \subset \mathbb{Z}\mathbf{u}_1 + \mathbb{Z}\mathbf{u}_2 = H$ et en déduire un morphisme surjectif $(\mathbb{Z}/n_1 n_2 \mathbb{Z})^2 \to \mathbb{Z}^2/H$. Conclure que $H$ est d'indice fini dans $\mathbb{Z}^2$.

(f) Montrer que dans chacun des deux cas $n_1 = 0$ ou $n_2 = 0$, le sous-groupe $H$ n'est pas d'indice fini dans $\mathbb{Z}^2$.

# UNIVERSITÉ DE LILLE

Enseignant: **P. DÈBES**
Filière: **Licence 5ème Semestre**
Matière: **M51**
Année universitaire: **2022/2023**
Epreuve: **Devoir à la maison - 2ème partie**
Date: **à rendre le vendredi 9 décembre 2022**

---

**UNE ATTENTION PARTICULIÈRE SERA PORTÉE À LA RIGUEUR ET LA PRÉCISION DE LA RÉDACTION.**

---

**Problème:** Etant donné un entier $m \geq 1$, le but du problème est de montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo $m$. Cela constitue un cas particulier du théorème de Dirichlet affirmant l'existence d'une infinité de nombres premiers dans toute progression arithmétique $(a\ell + b)_{\ell \in \mathbb{Z}}$ avec $a$ et $b$ deux entiers premiers entre eux.

(a) Montrer que, pour tout entier $m \geq 1$, la correspondance $\overline{k} \mapsto \exp(2ik\pi/m)$ définit un morphisme injectif $\varepsilon_m : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}^\times$ entre le groupe $(\mathbb{Z}/m\mathbb{Z}, +)$ et le groupe $(\mathbb{C}^\times, \times)$. Quel est le groupe image $\mu_m = \varepsilon_m(\mathbb{Z}/m\mathbb{Z})$?

Pour tout entier $d \geq 1$, on note $\Gamma_d$ l'ensemble des racines primitives $d$-ièmes de l'unité, c'est-à-dire des racines $d$-ièmes de l'unité qui ne sont pas des racines $k$-ièmes de l'unité pour un entier $1 \leq k < d$. Pour tout diviseur $d \geq 1$ d'un entier $m \geq 1$, on note $\mathcal{G}_{m,d}$ l'ensemble des éléments d'ordre $d$ du groupe $(\mathbb{Z}/m\mathbb{Z}, +)$.

(b) Montrer que pour tout entier $d \geq 1$ et tout multiple $m$ de $d$, on a

$$\varepsilon_m(\mathcal{G}_{m,d}) = \Gamma_d.$$

On définit le $d$-ième polynôme cyclotomique $\Phi_d$ par

$$\Phi_d(X) = \prod_{\zeta \in \Gamma_d} (X - \zeta).$$

(c) Montrer que pour tout $m \geq 1$, on a $X^m - 1 = \prod_{d|m} \Phi_d(X)$.

(d) Montrer que, pour tout $m \geq 1$, on a

(i) $\Phi_m(X) \in \mathbb{Z}[X]$.

(ii) Si $d|m$ et $d \neq m$, alors $(X^d - 1)\Phi_m(X)$ divise $X^m - 1$ dans $\mathbb{Z}[X]$.

(iii) $|\Phi_m(x)| \geq x - 1$ pour tout nombre réel $x \geq 2$.

On fixe un entier $m \geq 1$.

(e) Soient $n \in \mathbb{Z}$ et $p$ un diviseur premier de $\Phi_m(n)$. Montrer que $p$ divise $m$ ou que $p$ est congru à 1 modulo $m$.

Indication: on pourra préalablement montrer que, pour $\bar{n}$ la classe de $n$ modulo $p$, on a:

(i) $\bar{n}^m = 1$ dans $\mathbb{Z}/p\mathbb{Z}$,

(ii) si $p$ ne divise pas $m$, alors $\bar{n}$ est d'ordre $m$ dans le groupe $((\mathbb{Z}/p\mathbb{Z})^\times, \times)$.

(f) Montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo $m$.

# UNIVERSITÉ DE LILLE

Enseignants: **P. DÈBES**, **M. DIMITROV**, **D. MARKOUCHEVITCH**, **H. ZHANG**
Filière: **Licence 5ème Semestre**
Matière: **M51**
Année universitaire: **2022/2023**
Date, heure et lieu: **mardi 3 janvier 2023 à 8h**
Lieu: **amphithéâtre Painlevé au Bâtiment M1**
Durée de l'épreuve: **3 heures**

---

**Chacune des deux parties devra être rédigée sur une copie différente.**
**Ni calculatrice ni documents.**
**Le barême est donné à titre indicatif.**

—

**Une attention particulière sera portée à la rédaction: on précisera le rôle des hypothèses, les énoncés du cours invoqués et les conclusions obtenues.**

---

## PARTIE I

**Exercice 1 [4 pts] :** Dans le groupe symétrique $S_9$, on considère les permutations

$$\begin{cases} \omega_1 = (1\,2\,3) \\ \omega_2 = (4\,5\,6) \\ \omega_3 = (7\,8\,9) \end{cases}$$

(a) Montrer que l'application

$$\Phi : \left\{ \begin{array}{ccc} \mathbb{Z}^3 & \longrightarrow & S_9 \\ (n_1, n_2, n_3) & \mapsto & \omega_1^{n_1}\omega_2^{n_2}\omega_3^{n_3} \end{array} \right.$$

est un morphisme de groupes.

(b) Déterminer l'image et le noyau de $\Phi$. En déduire que le sous-groupe $\langle \omega_1, \omega_2, \omega_3 \rangle \subset S_9$ engendré par $\omega_1, \omega_2, \omega_3$ est isomorphe au groupe $((\mathbb{Z}/3\mathbb{Z})^3, +)$.

On considère la permutation $\tau = (1\,4\,7)(2\,5\,8)(3\,6\,9)$.

(c) Montrer que pour tout triplet $(n_1, n_2, n_3) \in \mathbb{Z}^3$, on a:

$$\tau\,(\omega_1^{n_1}\omega_2^{n_2}\omega_3^{n_3})\,\tau^{-1} = \omega_2^{n_1}\omega_3^{n_2}\omega_1^{n_3}.$$

**Exercice 2 [6 pts]:** On considère les ensembles:

$$\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} \in \mathbb{R} \mid a, b \in \mathbb{Q}\} \quad \text{et} \quad \mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \in \mathbb{R} \mid a, b \in \mathbb{Z}\}.$$

(a) Montrer que :
- tout élément de $\mathbb{Q}[\sqrt{3}]$ s'écrit de façon unique sous la forme $a + b\sqrt{3}$, avec $a, b \in \mathbb{Q}$,
- $(\mathbb{Z}[\sqrt{3}], +, \times)$ est un anneau commutatif unitaire.

(b) Montrer que l'application $N : \mathbb{Q}[\sqrt{3}] \to \mathbb{Q}$ définie par $N(a + b\sqrt{3}) = a^2 - 3b^2$ vérifie:

$$N(zz') = N(z)N(z') \text{ pour tous } z, z' \in \mathbb{Q}[\sqrt{3}] \quad \text{et} \quad N(\mathbb{Z}[\sqrt{3}]) \subset \mathbb{Z}.$$

(c) Montrer que $2-\sqrt{3}$ est un élément inversible de l'anneau $\mathbb{Z}[\sqrt{3}]$.

(d) Trouver 3 couples $(a,b) \in \mathbb{N}^2$ solutions de l'équation $a^2 - 3b^2 = 1$.

(e) Etant donnés $\alpha = a + b\sqrt{3}$ et $\beta = a' + b'\sqrt{3}$ dans $\mathbb{Z}[\sqrt{3}]$, avec $\beta \neq 0$, montrer que:
- on peut écrire $\dfrac{\alpha}{\beta} = u + v\sqrt{3}$ avec $u, v \in \mathbb{Q}$,
- si $c$ et $d$ sont deux entiers tels que $|u-c| \leq 1/2$ et $|v-d| \leq 1/2$, on a:

$$\alpha = \beta(c + d\sqrt{3}) + r,$$

$$\text{où} \quad \begin{cases} c + d\sqrt{3} \in \mathbb{Z}[\sqrt{3}], \\ r = \beta\left[(u-c) + \sqrt{3}(v-d)\right], \\ r \in \mathbb{Z}[\sqrt{3}], \\ |N(r)| < |N(\beta)|. \end{cases}$$

(f) Quelle propriété de l'anneau $\mathbb{Z}[\sqrt{3}]$ montre la question (d)?

## PARTIE II

**Exercice 3 [5 pts]:** On conserve les notations de l'exercice 2. Les exercices 2 et 3 sont reliés mais peuvent être traités de façon indépendante.

On admettra que $\mathbb{Z}[\sqrt{3}]$ est un anneau principal.

On fixe un nombre premier $p \neq 3$ tel que la classe de 3 modulo $p$ soit le carré d'un élément de $\mathbb{Z}/p\mathbb{Z}$.

(a) Expliciter l'hypothèse faite sur $p$ en termes de divisibilité d'entiers et montrer que $p = 11$ et $p = 13$ vérifient cette hypothèse tandis que 7 ne la vérifie pas.

(b) Montrer que $p$ n'est pas irréductible dans $\mathbb{Z}[\sqrt{3}]$. (Indication: on pourra le déduire de l'hypothèse sur $p$ (en précisant bien les propriétés de l'anneau $\mathbb{Z}[\sqrt{3}]$ utilisées)).

(c) Montrer que $p$ est le produit d'un nombre $r \geq 2$ d'irréductibles $P_1, \ldots, P_r$ de l'anneau $\mathbb{Z}[\sqrt{3}]$. (On précisera bien les propriétés de l'anneau $\mathbb{Z}[\sqrt{3}]$ utilisées).

(d) Montrer qu'il existe $i \in \{1, \ldots, r\}$ tel que $N(P_i) = \pm p$ et conclure qu'on peut écrire $p$ sous la forme $p = a^2 - 3b^2$ ou $p = 3b^2 - a^2$ avec $a, b \in \mathbb{Z}$. Le vérifier sur deux exemples de nombres premiers $p$.

**Exercice 4 [5 pts]**: Soit $P \in \mathbb{Z}[X]$ le polynôme défini par

$$P = X^4 + X^3 + X^2 + X + 1 = \frac{X^5 - 1}{X - 1}.$$

(a) Déterminer la décomposition en produit de facteurs irréductibles de $P$ dans l'anneau $\mathbb{C}[X]$, puis dans l'anneau $\mathbb{R}[X]$, enfin dans l'anneau $\mathbb{Q}[X]$. Pour la question dans $\mathbb{Q}[X]$, on admettra que $\cos(2\pi/5) \notin \mathbb{Q}$.

(b) Que peut-on déduire de l'idéal $(P)$ engendré par $P$ dans l'anneau $\mathbb{Q}[X]$?

On note $E : \mathbb{Q}[X] \to \mathbb{C}$ le morphisme d'évaluation qui envoie $X$ sur $e^{2i\pi/5}$
et $\mathbb{Q}[e^{2i\pi/5}]$ l'image du morphisme $E$.

(c) Montrer que $\mathbb{Q}[e^{2i\pi/5}]$ est un sous-anneau de $\mathbb{C}$ contenant le corps $\mathbb{Q}$ et $e^{2i\pi/5}$.

(d) Montrer que $\ker(E) = (P)$ et que $\mathbb{Q}[e^{2i\pi/5}]$ est un corps.