Exercices complémentaires

I Soient H et K deux sous-groupes d'un groupe G. On note $HK = \{hk / h \in H \text{ et } k \in K\}$. Montrer que HK est un sous-groupe de G ssi $HK = KH$. Soit $K \lhd G$ et H un sous-groupe de G. Montrer que :

(i) $H \cap K \lhd H$;

(ii) HK est un sous-groupe de G;

(iii) $H/H\cap K$ est isomorphe à HK/K. (considérer le morphisme de groupes φ de H dans HK/K qui à h associe $\bar{h}$; montrer que φ est surjectif et passer φ au quotient).

II Soient H et K deux sous-groupes distingués de G. Montrer que si $HK = G$ et si $H\cap K = \{e\}$ alors $\forall h \in H$, $\forall k \in K$ on a : $hk = kh$ et G est isomorphe à $H\times K$. (considérer le morphisme de groupes φ de $H\times K$ dans $G = HK$ qui à (h, k) associe hk).

En déduire que si G est un groupe fini, H et K deux sous-groupes distingués de G tels que $|H|\times|K| = |G|$ et si : $H\cap K = \{e\}$ ou $HK = G$ alors G est isomorphe à $H\times K$.

Application : Montrer que $(\mathbb{Z}/16\mathbb{Z})^*$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$.

III Soit G un groupe fini distinct de $\{e\}$ tel que : $\forall a \in G : a^2 = e$.

1°/ Montrer que G est commutatif.

2°/ Montrer que le cardinal de G est pair (utiliser le théorème de Lagrange).

3°/ Montrer que G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^p$ (et donc $|G| = 2^p$).

IV Soit H un sous-groupe distingué de G. Montrer que qu'il existe une bijection entre les sous-groupes de G contenant H et les sous-groupes de G/H. Par cette bijection les sous-groupes distingués se correspondent.

(La projection canonique $\pi : G \to G/H$ induit cette bijection).

V Soit H un sous-groupe de G tel que $[G:H] = 2$. Montrer que H est distingué dans G.

(noter que les deux éléments de $(G/H)_g$ sont H et $C_G H$ puisque les éléments de $(G/H)_g$ forment une partition de G: donc $aH = C_G H$ si $a \notin H$; de même pour les classes à droite).

VI Décrire le groupe des isométries du plan invariant un polygone régulier à n côtés (appelé groupe diédral et noté D_n).

VII *Fonction indicatrice d'Euler*

On rappelle que $(\mathbb{Z}/n\mathbb{Z})^*$ désigne le groupe des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

1°/ Montrer que $\bar{p} \in (\mathbb{Z}/n\mathbb{Z})^* \Leftrightarrow p\wedge n = 1$ (utiliser la relation de Bezout).

On a donc : $|(\mathbb{Z}/n\mathbb{Z})^*| = \text{Card}\{p \in \mathbb{N}^* / p < n \text{ et } p\wedge n = 1\}$. Cet entier se note $\varphi(n)$ et l'application φ de $\mathbb{N}^*$ dans $\mathbb{N}^*$ qui à n associe $\varphi(n)$ s'appelle *fonction indicatrice d'Euler* Calculer $\varphi(15)$.

2°/ Calculer $\varphi(p^\alpha)$ pour p premier et $\alpha \in \mathbb{N}^*$ (on trouve $p^\alpha - p^{\alpha-1}$) $= p^\alpha\left(1 - \frac{1}{p}\right)$).

3°/ Soient m et n deux entiers naturels non nuls premiers entre eux. Montrer que l'application Ψ de $(\mathbb{Z}/mn\mathbb{Z})^*$ dans $(\mathbb{Z}/n\mathbb{Z})^*\times(\mathbb{Z}/m\mathbb{Z})^*$ qui à $\bar{x}^{mn}$ associe $(\bar{x}^n ; \bar{x}^m)$ est un isomorphisme de groupes (considérer l'application Ψ de $(\mathbb{Z}/mn\mathbb{Z})$ dans $(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/m\mathbb{Z})$ qui à $\bar{x}^{mn}$ associe $(\bar{x}^n ; \bar{x}^m)$; montrer que c'est un isomorphisme de groupes en montrant qu'elle est injective puis remarquer que $[(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/m\mathbb{Z})]^* = (\mathbb{Z}/n\mathbb{Z})^*\times(\mathbb{Z}/m\mathbb{Z})^*$).

En déduire que $\varphi(mn) = \varphi(m)\varphi(n)$.

4°/ Soit $n = \prod_{i=1}^{q} p_i^{\alpha_i}$ la décomposition de n en produit de facteurs premiers; calculer $\varphi(n)$.

5°/ Montrer que : $\forall n \in \mathbb{N}^* : n = \sum_{d/n} \varphi(d)$ (utiliser 4°/ ou alors raisonner dans $\mathbb{Z}/n\mathbb{Z}$ et montrer que si Γ_d est l'ensemble des éléments d'ordre d, la famille $\{\Gamma_d / d/n\}$ est une partition de $\mathbb{Z}/n\mathbb{Z}$ en utilisant le théorème 2 du 3.2).

6°/ Soient a et n deux entiers premiers entre eux. Montrer que :

$a^{\varphi(n)} \equiv 1\ (n)$ (*formule d'Euler* généralisant le théorème de Fermat).

7°/ Montrer qu'à similitude près il y-a $\varphi(n)/2$ polygones réguliers à n côtés ($n \geq 3$).

8°/ <u>Application à la cryptographie</u> : supposons qu'on veuille envoyer un message codé à un individu *I*. On lui attribut couple de nombres premiers distincts (p , q) , et, si $n = pq$, un entier c premier avec $\varphi(n) = (p - 1)(q - 1)$. Soul *I* connaît la factorisation de n (i.e. p ou q) et donc peut connaître l'inverse d de c modulo $\varphi(n)$. Les nombre n et c par contre sont publics. Chaque caractère étant codé par un entier, un message est un entier M (dont la taille est strictement inférieure à n) obtenu par concaténation de ces nombres.

Pour adresser le message M à *I* on lui envoie $M_1 \equiv M^c\ (n)$. Pour que *I* décrypte le message il lui suffit de calculer M_1^d .

Montrer qu'en effet $M_1^d = M^{cd} \equiv M\ (n)$.

<u>Remarques</u> : 1/ le succès de la confidentialité repose sur le fait qu'en l'état actuel des moyens de calcul on peut facilement fabriquer de grands nombres premiers mais qu'il est très difficile de factoriser un grand nombre, donc de retrouver p_i et q_i à partir de n_i. A l'heure actuelle on peut considérer que des nombres premier de l'ordre de 10^{100} sont grand en ce sens.

2/ le calcul de d_i se fait à l'aide de l'algorithme d'Euclide.

VIII *Structure de $(\mathbb{Z}/n\mathbb{Z})^*$*

1°/ Montrer que $(\mathbb{Z}/2\mathbb{Z})^* = \{\overline{1}\}$ et que $(\mathbb{Z}/4\mathbb{Z})^* \approx \mathbb{Z}/2\mathbb{Z}$ (i.e : isomorphe à $\mathbb{Z}/2\mathbb{Z}$**)**.

On admet que si p est premier le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique (voir exercice XIII « anneaux et corps ») donc isomorphe à $\mathbb{Z}/p^{\alpha-1}(p-1)\ \mathbb{Z}$ (voir exercice VIII)..

2°/ Soit p un nombre premier ≥ 3 et α un entier ≥ 2.

a/ Montrer que pour tout entier $k \geq 1$ on a :

$(1+p)^{p^k} = 1 + \lambda p^{k+1}$ avec $\lambda \wedge p = 1$ (récurrence sur k).

En déduire que $\overline{(1+p)}$ est d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$.

b/ Soit l'homomorphisme de groupes Ψ de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ dans $(\mathbb{Z}/p\mathbb{Z})^*$ qui à $\overline{x}^{p^\alpha}$ associe $\overline{x}^p$. Soit $x \in (\mathbb{Z}/p^\alpha\mathbb{Z})^*$ tel que $\Psi(x)$ engendre $(\mathbb{Z}/p\mathbb{Z})^*$. Que peut-on dire de l'ordre de x ? Montrer que l'on peut trouver dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ un élément d'ordre $p^{\alpha-1}(p-1)$. En déduire que :

$(\mathbb{Z}/p^\alpha\mathbb{Z})^* \approx \mathbb{Z}/\varphi(p)\ \mathbb{Z} = \mathbb{Z}/p^{\alpha-1}(p-1)\ \mathbb{Z}$.

3°/ On s'intéresse maintenant au cas $p = 2$.

a/ Montrer que pour tout entier $k \geq 1$ on a :

$5^{2^k} = 1 + \lambda.2^{k+2}$ avec λ impair (récurrence sur k).

En déduire que $\overline{5}$ est d'ordre $2^{\alpha-2}$ dans $(\mathbb{Z}/2\mathbb{Z})$**)**

b/ Soit l'homomorphisme de groupes Φ de $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ dans $(\mathbb{Z}/4\mathbb{Z})^*$ qui à $\overline{x}^{2^\alpha}$ associe $\overline{x}^4$ et N son noyau. Montrer que : $|N| = 2^{\alpha-2}$ (passer Φ au quotient) puis que $N \approx \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$ (utiliser a).

c/ Montrer que $H = \{\overline{1};-\overline{1}\}$ est un sous-groupe de $(\mathbb{Z}/2^\alpha)^*$. En utilisant l'exercice III en déduire que :

$(\mathbb{Z}/2^\alpha\mathbb{Z})^* \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$ (pour $\alpha \geq 2$).

4°/ Caractériser les entiers naturels n tels que le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ soit cyclique (utiliser l'exercice VIII 3°/).

IX *Simplicité de $O_+(E)$ (dimE = 3)*

Soit E un espace vectoriel euclidien de dimension 3 et Γ un sous-groupe distingué de $O_+(E)$ non réduit à $\{Id_E\}$ et soit u élément de Γ distinct de Id_E.

1°/ Montrer qu'il existe ρ appartenant à Γ d'angle θ tel que $\cos(\theta) < 0$ (chercher ρ sous la forme u^k avec k entier naturel). En déduire qu'il existe $x \in E - \{0\}$ tel que $\rho(x)$ soit orthogonal à x. Soit t le demi-tour d'axe engendré par x. Montrer que $r = t\ o\ \rho\ o\ t^{-1} o\ \rho^{-1}$ est un demi-tour appartenant à Γ.

2°/ Soit f un élément quelconque de $O_+(E)$. Montrer que $f\ o\ r\ o\ f^{-1}$ est un retournement d'axe engendré par $f(x)$. En déduire que Γ contient tous les retournements et conclure que $\Gamma = O_+(E)$ (autrement dit $O_+(E)$ est un groupe simple).

X *Produits semi-directs*

1°/ Exemple du groupe diédral (voir exercice complémentaire VI/). Soit D_n le groupe des isométries du plan invariant un polygone régulier à n côtés, $D_n^+ = D_n \cap O^+(P)$ et s une réflexion appartenant à D_n. Montrer que tout élément f de D_n s'écrit de façon unique $f = r \circ \varepsilon$ avec $r \in D_n^+$ et $\varepsilon \in \{\mathrm{Id}_P, s\}$.

On peut donc considérer la bijection φ de D_n dans $D_n^+ \times \{\mathrm{Id}_P, s\}$ qui à f associe (r, ε). Montrer que φ est un isomorphisme de groupes sii on munit $D_n^+ \times \{\mathrm{Id}_P, s\}$ de la loi $(r, \varepsilon)(r', \varepsilon') = (r\varepsilon r'\varepsilon, \varepsilon\varepsilon')$.

Le groupe $D_n^+ \times \{\mathrm{Id}_P, s\}$ muni de cette loi s'appelle *produit semi-direct* des groupes D_n^+ et $\{\mathrm{Id}_P, s\}$. On la note $D_n^+ \ltimes \{\mathrm{Id}_P, s\}$. Comme le groupe $\{\mathrm{Id}_P, s\}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ on a donc $D_n \approx D_n^+ \ltimes \mathbb{Z}/2\mathbb{Z}$.

2°/ Cas général : soient H et K deux groupes et σ un morphisme de groupes de K dans $\mathrm{Aut}(H)$. On définit un *produit semi-direct* dans $H \times K$ en posant $\forall (h, k) \in H \times K,\ \forall (h', k') \in H \times K\ :\ (h, k).(h', k') = (h\sigma_k(h'), kk')$.

a/ Montrer que $H \times K$ munit de ce produit est un groupe. Ce groupe est appelé *produit semi-direct* des groupes H et K. On le note $H \times_\sigma K$.

b/ Montrer que l'on a une *suite exacte* : $e \to H \xrightarrow{i} H \times_\sigma K \xrightarrow{p} K \to e$' (c'est à dire que les applications sont des morphismes de groupes, i est injective, p surjective et Im i = Ker p), avec i et p définies par $i(h) = (h, e)$ et $p(h, k) = k$.

De plus, si on identifie H à un sous-groupe de $H \times_\sigma K$ par l'injection i, alors H est un sous-groupe distingué de $H \times_\sigma K$ et si on identifie K à un sous-groupe de $H \times_\sigma K$ par l'injection $k \mapsto (e, k)$ alors K est un sous-groupe de $H \times_\sigma K$.

3°/ a/ Soient H et K deux sous-groupes d'un groupe G tels que H soit distingué dans G, $H \cap K = \{e\}$ et $HK = G$ (avec $HK = \{hk \,/\, h \in H \text{ et } k \in K\}$. Montrer que G est isomorphe au produit semi-direct $H \times_\sigma K$ avec σ est défini par : $\forall\ k \in K,\ \forall h \in H,\ \sigma_k(h) = khk^{-1}$.

b/ Soit $e \to H \xrightarrow{i} G \xrightarrow{p} K \to e$' une suite exacte de groupes telle qu'il existe un morphisme de groupes $s : K \longrightarrow G$ avec $p \circ s = \mathrm{Id}_K$ (on dit que s est une *section* de p). Montrer que G est isomorphe au produit semi-direct $H \times_\sigma K$. Si on identifie H à un sous-groupe de G par l'injection i, et si on identifie K à un sous-groupe de G par l'injection s alors σ est définit par : $\forall\ k \in K,\ \forall h \in H,\ \sigma_k(h) = khk^{-1}$.

4°/ Exemple : le groupe symétrique S_n est isomorphe au produit semi-direct $A_n \times_\sigma \mathbb{Z}/2\mathbb{Z}$.