Contrôle 1, vendredi 18 octobre 2024, 15h30-17h

Les documents et calculatrices sont interdits.

Les téléphones portables doivent être éteints et rangés dans les sacs.

Les réponses doivent être justifiées.

Barème approximatif : 4 + 3 + 3 + 3 + 8

Exercice 1. Question de cours.

Soient x, y deux éléments d'un groupe G, d'ordres respectifs m et n. On suppose que $xy = yx$ et que $< x > \cap < y >= \{e\}$. Montrer que l'ordre de xy est égal à $ppcm(m, n)$.

Correction. On va montrer que $o(xy) = ppcm(m, n)$. On remarque que, comme x et y commutent et que m et n divisent $ppcm(m, n)$:

$$(xy)^{ppcm(m,n)} = x^{ppcm(m,n)}y^{ppcm(m,n)} = 1.$$

Ainsi $o(xy)|ppcm(m, n)$.

Soit $k > 0$ tel que $(xy)^k = 1$. En particulier, $x^k y^k = 1$, donc $x^k = y^{-k}$. Ainsi $x^k \in \langle x\rangle \cap \langle y\rangle$ et donc $x^k = 1$. De même $y^k = 1$, et il vient $m|k$ et $n|k$ ce qui implique que $ppcm(m, n)|k$. Finalement on a bien montré que $o(xy) = ppcm(m, n)$.

Exercice 2. Soit G un groupe et soit H un sous-groupe distingué de G d'ordre n et d'indice m.

1. Montrer que $g^m \in H$ pour tout $g \in G$.
2. On suppose que m et n sont premiers entre eux. Montrer que H est l'unique sous-groupe de G d'ordre n. *Indication : on pourra appliquer le Théorème de Bezout aux entiers m et n.*

Correction.

1. Comme H est distingué, et par définition de m, le groupe G/H est bien défini et est d'ordre m. Ainsi, avec $\pi : G \longrightarrow G/H$ le morphisme quotient, pour tout $g \in G$, on a $\pi(g)^m = \pi(e)$, soit encore $g^m H = H$. Cela prouve bien que pour tout $g \in G$, $g^m \in H$.

2. Soit K un sous-groupe de G d'ordre n, montrons que $K = H$. Soit $k \in K$, alors $k^n = e$. Puisque m et n sont premiers entre eux, par le théorème de Bezout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $um + vn = 1$. Ainsi, on a :

$$k = k^{um+vn} = (k^m)^u(k^n)^v = (k^m)^u.$$

Par la question précédente, $k^m \in H$, donc $(k^m)^u = k \in H$. Ainsi, $K \subset H$, et par égalité des cardinaux, il vient $K = H$.

Exercice 3.

1. Soient G et H deux groupes finis et soit $f : G \to H$ un morphisme de groupe. Vérifier que pour tout $x \in G$, l'ordre de $f(x)$ divise l'ordre de x.
2. Donner tous les morphismes de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/4\mathbb{Z}$.
3. Donner tous les morphismes de $\mathbb{Z}/6\mathbb{Z}$ dans $\mathbb{Z}/8\mathbb{Z}$.

Correction.

1. Pour $x \in G$, on a :
$$f(x)^{o(x)} = f\left(x^{o(x)}\right) = f(e_G) = e_H.$$
Ainsi, l'ordre de $f(x)$ divise bien l'ordre de x.

2. Un morphisme $\varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z}$ est entièrement déterminé par $\varphi(\overline{1}^3)$, car $\overline{1}^3$ engendre $\mathbb{Z}/3\mathbb{Z}$. Or, $\overline{1}^3$ est d'ordre 3, et l'ordre de $\varphi(\overline{1}^3)$ divise 4 (l'ordre de $\mathbb{Z}/4\mathbb{Z}$), et 3 par la question précédente. L'ordre de $\varphi(\overline{1}^3)$ est donc 1, et on peut conclure qu'il existe un unique morphisme $\varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z}$: le morphisme trivial.

3. Un morphisme $\varphi : \mathbb{Z}/6\mathbb{Z} \longrightarrow \mathbb{Z}/8\mathbb{Z}$ est entièrement déterminé par $\varphi(\overline{1}^6)$, car $\overline{1}^6$ engendre $\mathbb{Z}/6\mathbb{Z}$. Or, $\overline{1}^6$ est d'ordre 6, et l'ordre de $\varphi(\overline{1}^6)$ divise 8 (l'ordre de $\mathbb{Z}/8\mathbb{Z}$), et 6 par la question 1. L'ordre de $\varphi(\overline{1}^6)$ est donc soit 1, soit 2. Il existe un unique élément d'ordre 2 dans $\mathbb{Z}/8\mathbb{Z}$: $\overline{4}^8$. On vérifie aisément que si $\varphi(\overline{1}^6) = \overline{4}^8$, φ est bien un morphisme de groupe : c'est le morphisme $\overline{k}^6 \mapsto \begin{cases} \overline{0}^8 & \text{si } k \text{ est pair} \\ \overline{4}^8 & \text{sinon} \end{cases}$ (c'est la multiplication par 4 !). Ainsi, il existe exactement deux morphismes de $\mathbb{Z}/6\mathbb{Z}$ dans $\mathbb{Z}/8\mathbb{Z}$: le morphisme trivial et le morphisme $\overline{k}^6 \mapsto \begin{cases} \overline{0}^8 & \text{si } k \text{ est pair} \\ \overline{4}^8 & \text{sinon} \end{cases}$.

Exercice 4. Soit $n \geq 1$. Montrer que n divise $\varphi(2^n - 1)$, où φ est l'indicatrice d'Euler.

Indication : observer que $2^n = 1$ modulo $2^n - 1$ puis étudier l'ordre de 2 modulo $2^n - 1$.

Correction. Comme $2^n - 1 \equiv 0[2^n - 1]$, on remarque que $2^n \equiv 1[2^n - 1]$. Ainsi, 2 est inversible modulo $2^n - 1$. Soit m l'ordre de $\overline{2} \in ((\mathbb{Z}/(2^n - 1)\mathbb{Z})^*, \times)$.

Comme $\overline{2}^n = \overline{1}$, on a $m \mid n$.

Pour $k \in \mathbb{N}$, $0 < k < n$, on a $1 < 2^k < 2^n - 1$, donc en particulier $\overline{2}^k \neq \overline{1}$, et donc $m > n - 1$. On a donc $m = n$.

Par le théorème de Lagrange, il vient bien : n divise $\#\,(\mathbb{Z}/(2^n - 1)\mathbb{Z})^* = \varphi(2^n - 1)$.

Exercice 5. Soit G un groupe, soient K, H deux sous groupes de G.

1. Montrer que KH est un sous-groupe de G si et seulement si $KH = HK$

   Dans toute la suite de l'exercice, on suppose que H est un sous-groupe distingué de G.

2. Vérifier que KH est un sous-groupe de G.

3. Montrer que H est un sous-groupe distingué de KH.

4. Montrer que $K \cap H$ est un sous-groupe distingué de K.

5. Montrer que les groupes $K/(K \cap H)$ et KH/H sont isomorphes.

   Nous avons démontré le second Théorème d'isomorphisme.

6. Soit V le sous-groupe de S_4 donné par $\{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. Vérifier que V est un sous-groupe distingué de S_4, puis montrer que S_4/V est isomorphe à S_3 (on pourra introduire le sous-groupe H de S_4, isomorphe à S_3, formé des permutations fixant 4).

7. Donner une condition portant sur K, H et G, plus faible que la condition "H est un sous-groupe distingué de G", pour laquelle ce Théorème reste vrai.

Correction.

1. Supposons que KH soit un sous-groupe de G, et considérons l'application "inverse" $\varphi : \begin{pmatrix} K \times H & \longrightarrow & HK \\ (k,h) & \longmapsto & h^{-1}k^{-1} = (kh)^{-1} \end{pmatrix}$. Comme KH est un groupe, l'application inverse $\begin{pmatrix} G & \longrightarrow & G \\ x & \longmapsto & x^{-1} \end{pmatrix}$ restreinte à KH est une bijection de KH, donc $Im(\varphi) = KH$. De plus, on voit que pour $hk \in HK$, (k^{-1}, h^{-1}) est un antécédent de hk par φ, donc φ est surjective : $Im(\varphi) = HK$. Il vient donc bien : $HK = Im(\varphi) = KH$.

   Supposons maintenant que $KH = HK$. Comme $e \in K \cap H$, $e \in KH$. Soit $(kh, k'h') \in KH$. Alors $kh(k'h')^{-1} = khh'^{-1}k'^{-1} \in KHK = K(HK) = K(KH) = KH$, donc KH est bien un sous-groupe de G.

2. Comme H est supposé distingué, pour tout $g \in G$, $gHg^{-1} = H$. En particulier, pour tout $k \in K$, $kH = Hk$. Ceci montre bien que $KH = HK$, et on peut conclure avec la question 1.

3. On a immédiatement $H = eH < KH$. De plus, pour $(h,k) \in H \times K$, on a : $khH(kh)^{-1} = khHh^{-1}k^{-1} = kHk^{-1} = H$, car H est distingué dans G, d'où le résultat.

4. Pour $k \in K$, $kHk^{-1} = H$ car H est distingué dans G, et $kKk^{-1} = K$ (K est distingué dans lui-même). Ainsi, $k(K \cap H)k^{-1} \subset kKk^{-1} \cap kHk^{-1} = K \cap H$.

5. Par les questions précédentes, les groupes considérés sont bien définis. On considère le morphisme $\varphi : \begin{pmatrix} K & \longrightarrow & KH/H \\ k & \longmapsto & kH \end{pmatrix}$. Ce morphisme est clairement surjectif, et de noyau $K \cap H$, donc le premier théorème d'isomorphisme permet de conclure.

6. Soit $\sigma \in S_4$ et $(a\ b)(c\ d)$ un élément de $V \backslash \{e\}$. On a :

$$\sigma(a\ b)(c\ d)\sigma^{-1} = (\sigma(a)\ \sigma(b))(\sigma(c)\ \sigma(d)).$$

Ainsi, comme σ est une bijection de $[\![1,4]\!]$ et que $\#\{a,b,c,d\}=4$, il est clair que l'élément ci-dessus est dans $V\backslash\{e\}$ (le type de la permutation est préservé). Comme $\sigma e\sigma^{-1}=e$, on a bien $\sigma V\sigma^{-1}=V$ pour tout $\sigma\in S_4$, ce qui montre que V est distingué dans S_4.

Remarque : On pouvait aussi vérifier que $\sigma V\sigma^{-1}=V$ pour σ parcourant un ensemble générateur de S_4. On sait que S_4 est engendré par $(1,2)$ et $(1,2,3,4)$. On a bien :

$$(1,2)V(1,2)=\{e,(3,4)(1,2),(1,4)(2,3),(1,3)(2,4)\}=V$$

et

$$(1,2,3,4)V(1,2,3,4)=\{e,(3,4)(1,2),(1,4)(2,3),(1,3)(2,4)\}=V.$$

Comme proposé, soit $H<S_4$ composé des permutations fixant 4. Il est bien isomorphe à S_3. On remarque que $H\cap V=\{e\}$. Par le second théorème d'isomorphisme, on a donc :

$$S_3\simeq H\simeq H/(H\cap V)\simeq HV/V.$$

Il ne reste qu'à montrer que $HV=S_4$ pour conclure. Il suffit de montrer que $(1,2)$ et $(1,2,3,4)$ sont dans HV. On a bien :

$$(1,2)=\underbrace{(1,2)}_{\in H}\underbrace{e}_{\in V},$$

et

$$(1,2,3,4)=(1,2)(2,3)(3,4)=\underbrace{(1,2)(2,3)(1,2)}_{\in H}\underbrace{(1,2)(3,4)}_{\in V}.$$

7. On voit que dans les questions précédentes (2 à 4), plutôt qu'utiliser le fait que H est distingué dans G, on a utilisé le fait que pour tout $k\in K$, $kHk^{-1}=H$. La condition plus faible est donc : $K<N_G(H):=\{g\in G,gH=Hg\}$ (c'est le normalisateur de H dans G).