MT10/P11 - Examen médian

Exercice 1 (groupes, sous-groupes, groupe dérivé) (10 points)
Soient deux groupes, $(G, *, e)$ et $(G', *', e')$, et un morphisme $f : G \to G'$.

1. Soit H un sous-groupe de G. Montrer que $f(H) \overset{\text{déf}}{=} \{f(h) \ : \ h \in H\}$ est un sous-groupe de G'.
2. Soit H' un sous-groupe de G'.
   (a) Montrer que $f^{-1}(H') \overset{\text{déf}}{=} \{x \in G \ : \ f(x) \in H'\}$ est un sous-groupe de G.
   (b) On suppose de plus que H' est distingué dans G'. Montrer que $f^{-1}(H')$ est distingué dans G.
3. **(commutateurs et groupe dérivé en général)**
   On rappelle que si $x, y \in G$, leur commutateur est défini par $[x, y] \overset{\text{déf}}{=} x * y * (y * x)^{-1}$ et que le groupe dérivé de G, noté $D(G)$, est le sous-groupe de G engendré par les commutateurs.
   (a) Dans le cas où G serait commutatif, calculer $[x, y]$ pour $x, y \in G$ quelconques, puis $D(G)$.
   Dans la suite, on ne supposera plus que G est commutatif.
   (b) Calculer $[x, y]^{-1}$ (et voir que c'est un commutateur de G).
   (c) Calculer $f([x, y])$ (et voir que c'est un commutateur de G').
   (d) Calculer $g * [x, y] * g^{-1}$ (et voir que c'est un commutateur de G).
   (e) Montrer que $D(G)$ est un sous-groupe distingué de G.
   (f) Montrer que $f(D(G)) \subset D(G')$.
   (g) On suppose de plus que f est surjectif. Montrer que $f(D(G)) = D(G')$.
4. **(commutateurs et groupe dérivé dans $\mathfrak{S}_3$)**
   On adoptera la notation des cycles pour désigner les éléments de $\mathfrak{S}_3$, le groupe des bijections de $\{1; 2; 3\}$ dans lui-même, de sorte que :
   $$\mathfrak{S}_3 = \{\mathrm{Id}; (1\ 2); (1\ 3); (2\ 3); (1\ 2\ 3); (1\ 3\ 2)\}$$
   (a) Quel est $< (1\ 2) >$, le sous-groupe de $\mathfrak{S}_3$ engendré par la permutation $(1\ 2)$?
   (b) Quel est $< (1\ 2\ 3) >$, le sous-groupe de $\mathfrak{S}_3$ engendré par le cycle $(1\ 2\ 3)$?
   (c) Quel est $< (1\ 2), (1\ 2\ 3) >$, le sous-groupe de $\mathfrak{S}_3$ engendré par $(1\ 2)$ et $(1\ 2\ 3)$?
   (d) Calculer le commutateur $[(1\ 2), (1\ 3)]$.
   (e) Calculer le commutateur $[(1\ 2), (1\ 2\ 3)]$.
   (f) Calculer le groupe dérivé $D(\mathfrak{S}_3)$.

Exercice 2 (Le groupe des quaternions) (5 points)
scolie : *On sait qu'un groupe commutatif a tous ses sous-groupes qui sont distingués. Question naturelle : est-ce qu'un groupe dont tous les sous-groupes sont distingués est commutatif ? Réponse : pas forcément, comme on va le voir avec un groupe à 8 éléments, dit groupe des quaternions ...*
On munit l'ensemble à 8 éléments

$$\mathbb{H}_8 = \{1; -1; i; -i; j; -j; k; -k\}$$

d'une loi interne (notée $*$) de sorte que 1 soit l'élément neutre, que la "règle des signes" soit satisfaite (*i.e.* $(-1)*(-1) = 1$, $(-1)*i = i*(-1) = -i$, $(-1)*j = j*(-1) = -j$ et $(-1)*k = k*(-1) = -k$) et telle que

$$\begin{array}{rclcrcl} i*j &=& k & \quad & j*i &=& -k \\ j*k &=& i & & k*j &=& -i \\ k*i &=& j & & i*k &=& -j \end{array}$$

On complète la définition de $*$ de sorte que $(\mathbb{H}_8, *, 1)$ soit un groupe. Ce groupe s'appelle le groupe des quaternions [1].

1. Montrer que $i*i = -1$.
2. Donner la table complète de $*$.
3. Quels sont les symétriques de i, j, k ?
4. Donner tous les sous-groupes non triviaux de $\mathbb{H}_8$.
5. Montrer qu'ils sont tous distingués, bien que $\mathbb{H}_8$ ne soit pas commutatif.

Exercice 3 (arithmétique variée) (5 points)

1. 2 est-il inversible dans l'anneau $\mathbb{Z}/27\mathbb{Z}$? Si oui, calculer son inverse.
2. 12^{2011} est-il multiple de 11 ?
3. Montrer que, pour tout $n \in \mathbb{N}$, $3^{2n} - 2^n$ est divisible par 7.
4. **Une faille bien connue de RSA** :
   Alice et Bob utilisent le système RSA avec le modulo N (produit de deux très grands nombres premiers p et q), et les clefs, publiques et privées, respectives (e_A, d_A) et (e_B, d_B). Supposons que Candide doive envoyer le même message secret m à ses amis Alice et Bob. Précisément, Candide calcule $m_A = m^{e_A} \quad [N]$ et $m_B = m^{e_B} \quad [N]$, puis envoie m_A et m_B à Alice et Bob respectivement.
   Raoul, qui espionne la ligne de transmission, réussit à intercepter les messages cryptés m_A et m_B. Remarquant que les clefs publiques e_A et e_B sont premières entre elles, (et ayant quelques souvenirs d'une certaine UV réputée à l'UTC), reconstitue sans problème le message clair m.
   Question : Expliquer comment Raoul a pu procéder.

1. Ne pas confondre avec le corps des quaternions, qui est un corps infini (non commutatif). Il y a cependant un lien entre le groupe $\mathbb{H}_8$ et le corps des quaternions, mais ceci est une autre histoire ...