DS n°1

mercredi 17 septembre 2014 (durée 4 heures)

Toute calculatrice interdite

Rappel : Bien traiter quelques questions rapporte des points, les bâcler toutes n'en rapporte aucun.

Problème 1

Soit α un complexe. On note $\mathbb{Z}[\alpha] = \{a + b\alpha/(a,b) \in \mathbb{Z}^2\}$

Préliminaire

Montrer que $\mathbb{Z}[\alpha]$ est un anneau si et seulement si α est racine d'un polynôme unitaire (i.e. de coefficient dominant égal à 1), de degré égal à 2 et à coefficients dans $\mathbb{Z}$.

L'anneau $\mathbb{Z}[\sqrt{n}]$

Soit n un entier naturel qui n'est pas le carré d'un entier.

1. Justifier rapidement que $\mathbb{Z}[\sqrt{n}]$ est un anneau. Est-il intègre ?
2. Montrer que l'application $\begin{cases} \mathbb{Z}^2 & \to \mathbb{Z}[\sqrt{n}] \\ (a,b) & \to a + b\sqrt{n} \end{cases}$ est bijective.
3. Soit $x \in \mathbb{Z}[\sqrt{n}]$. Pour $x = a + b\sqrt{n}$ avec $(a,b) \in \mathbb{Z}^2$, on note $\hat{x}$ l'élément $\hat{x} = a - b\sqrt{n}$.
   Montrer que l'application $f : \begin{cases} \mathbb{Z}[\sqrt{n}] & \to \mathbb{Z}[\sqrt{n}] \\ x & \to \hat{x} \end{cases}$ est un automorphisme d'anneaux involutif (Rappel : une application f est dite involutive lorsqu'elle vérifie $f^{-1} = f$).
4. Pour $x \in \mathbb{Z}[\sqrt{n}]$ on pose $N(x) = x\hat{x}$. Montrer que :
   (a) $\forall x \in \mathbb{Z}[\sqrt{n}],\ N(x) = 0 \iff x = 0$
   (b) $\forall (x,y) \in \mathbb{Z}[\sqrt{n}]^2,\ N(xy) = N(x)N(y)$
5. Montrer que x est inversible dans $\mathbb{Z}[\sqrt{n}]$ si et seulement si $|N(x)| = 1$.
6. Dans cette question on pose $n = 7$.
   (a) Montrer que $8 + 3\sqrt{7}$ est inversible et donner son inverse.
   (b) Montrer qu'il existe une infinité d'éléments inversibles dans $\mathbb{Z}[\sqrt{7}]$.
7. On revient au cas général sur n.
   On note G l'ensemble des éléments inversibles de $\mathbb{Z}[\sqrt{n}]$ et G^+ l'ensemble des éléments inversibles positifs de $\mathbb{Z}[\sqrt{n}]$.
   (a) Montrer rapidement que $(G^+, \times)$ est un groupe.
   (b) Soit $x \in G : x = a + b\sqrt{n}$ avec $(a,b) \in \mathbb{Z}^2$. Montrer que $x \geqslant 1 \iff (a \geqslant 1 \text{ et } b \geqslant 0)$
   (c) Montrer que $\forall M \geqslant 1,\ G \cap [1, M]$ est fini.
   (d) Montrer que $(G^+, \times)$ est monogène.

Problème 2

On admettra le **théorème de Lagrange** (déjà prouvé en Td) qui dit que si un groupe G est fini, alors tout sous-groupe de G a un cardinal que divise le cardinal de G.
Si G est un groupe, on appelle centre du groupe G l'ensemble des éléments de G qui commutent avec tout élément de G. On le note $Z(G)$

Dans tout le problème, G est un groupe fini dont la loi est notée multiplicativement. On notera e son élément neutre.

Partie I

1. Dans cette question, G est de cardinal p premier. Montrer que G est cyclique.
   Quel est le centre de G ?
2. On considère la relation $\mathcal{R}$ définie sur G par : $a\mathcal{R}b \iff \exists g \in G/\ b = g.a.g^{-1}$
   Pour tout élément a de G on pose $H_a = \{g \in G/g.a.g^{-1} = a\}$.
   (a) Montrer que $\mathcal{R}$ est une relation d'équivalence sur G. On notera $cl(a)$ la classe de a pour $\mathcal{R}$.
   (b) Déterminer $cl(a)$ lorsque $a \in Z(G)$. Montrer la réciproque.
   (c) Montrer que H_a est un sous-groupe de G.
   (d) Soit $h \in G$ et $b = h.a.h^{-1}$. On considère l'application $\varphi : g \to h.g.h^{-1}$. Montrer que φ définit une bijection de H_a sur H_b.
   En déduire $cl(a) = cl(b) \Longrightarrow Card(H_a) = Card(H_b)$
3. Soit $a \in G$. En introduisant l'application $f : G \to cl(a)$ définie par $f(g) = g.a.g^{-1}$ montrer que $Card(G) = Card(H_a) \times Card(cl(a))$.

Partie II

Soit H un sous-groupe de G. On dira que H est distingué si et seulement si $\forall x \in G,\ \forall h \in H,\ x.h.x^{-1} \in H$.

1. Quels sont les sous groupes distingués de G dans le cas où G est abélien ?
2. (a) Montrer que $\mathbb{Z}(G)$ est distingué.
   (b) Soit f un morphisme d'un groupe G vers un groupe G'. Montrer que le noyau de f est distingué.
3. Soit H un sous-groupe distingué de G, et soit $\mathcal{S}$ la relation définie sur G par : $x\mathcal{S}y \iff x.y^{-1} \in H$. On notera $\overline{x}$ la classe de x par $\mathcal{S}$ (on sait que S est une relation d'équivalence ; on ne demande pas de le redémontrer)
   (a) Montrer que $\forall x, x', y, y' \in G,\ \left\{ \begin{array}{l} \overline{x} = \overline{x'} \\ \overline{y} = \overline{y'} \end{array} \right. \Longrightarrow \overline{x.y} = \overline{x'.y'}$
   (b) Ceci nous autorise à écrire $\forall \overline{x}, \overline{y} \in G/H,\ \overline{x}.\overline{y} = \overline{xy}$ car la classe de xy est indépendante du choix du représentant de $\overline{x}$ et de celui de $\overline{y}$.
   On définit ainsi une loi de composition interne sur G/H. Montrer que G/H muni de cette loi est un groupe.
4. On prend ici $H = Z(G)$. On suppose en outre que G/H est cyclique. Soit alors y un élément de G tel que $\overline{y}$ engendre G/H.
   (a) Montrer que $\forall g \in G,\ \exists \alpha \in \mathbb{N},\ \exists z \in Z(G),\ g = z.y^{\alpha}$
   (b) Montrer que G est abélien.

Partie III

On suppose que G est de cardinal p^2 avec p premier.

(a) Montrer que si on suppose que $Card(Z(G)) = p$ alors $G/Z(G)$ est cyclique.
Montrer alors une contradiction.
(b) On suppose que $Card(Z(G)) = 1$. Montrer en utilisant la relation $\mathcal{R}$ de la partie I. qu'il existe $\ell \in \mathbb{N}$ tel que $Card(G) = 1 + p\ell$.
(c) Montrer que G est nécessairement commutatif.