Algèbre et théorie des nombres

Corrigé - Examen partiel du 12 novembre 2009

I - Arithmétique

1. Résoudre le système suivant dans $\mathbb{Z}$:

$$\begin{cases} 2x & \equiv & 4 & (\text{mod } 5) \\ 6x & \equiv & 4 & (\text{mod } 8) \end{cases}$$

Le nombre 3 *est l'inverse de* 2 *dans* $\mathbb{Z}/5\mathbb{Z}$ *donc en multipliant par* 3, *la première équation est équivalente à* $x \equiv 12 \equiv 2 \pmod 5$. *La seconde équation est équivalente à* $3x \equiv 2 \pmod 4$, *qui est équivalente à* $x \equiv -2 \equiv 2 \pmod 4$. *Comme* 5 *et* 4 *sont premiers entre-eux, par le théorème des restes Chinois les deux équations sont équivalentes à* $x \equiv 2 \pmod{20}$. *L'ensemble des solutions est donc*

$$\{2 + 20k : k \in \mathbb{Z}\}.$$

2. Montrer qu'un entier de la forme $8k - 1$ n'est pas la somme de trois carrés.
Tout carré est congru modulo 8 *à* 0, 1 *ou* 4. *Il suit que la somme de trois carrés ne peut être congru modulo* 8 *à* -1 *et donc ne peut être de la forme* $8k - 1$.

II - Groupe symétrique.

On considère les deux permutations dans S_8 :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 4 & 1 & 7 & 5 & 2 & 6 & 3 \end{pmatrix} \text{ et } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 7 & 5 & 1 & 6 & 3 & 4 \end{pmatrix}.$$

1. Donner les décompositions en cycles disjoints de σ et τ.
$\sigma = (1\ 8\ 3)(2\ 4\ 7\ 6)$ *et* $\tau = (1\ 8\ 4\ 5)(3\ 7)$
2. Calculer leurs signatures.
$sgn(\sigma) = (-1)^{3-1}(-1)^{4-1} = -1$ *et* $sgn(\tau) = (-1)^{4-1}(-1)^{2-1} = 1$
3. Les permutations σ et $\tau\sigma^{-1}$ sont elles conjuguées ?
$\tau\sigma^{-1} = (1\ 7\ 5)(2\ 6\ 3\ 4)$. *Les longueurs des cycles dans les décompositions canoniques de* σ *et de* $\tau\sigma^{-1}$ *se correspondent donc ces deux permutations sont conjuguées.*
4. Combien y-a-t-il de permutations dans S_8 conjuguées à σ ?
Il s'agit de dénombre le nombre de permutations qui sont produits d'un 3*-cycle et d'un* 4*-cycle à support disjoint. Pour commencer, il y a* $2 \times \binom{8}{3}$ *choix pour le* 3*-cycle, puis il reste* $3! \times \binom{5}{4}$ *choix pour un* 4*-cylce à support disjoint du* 3*-cycle déjà choisi. Il y a donc*

$$3360 = 2 \times \binom{8}{3} \times 3! \times \binom{5}{4}$$

permutations dans S_8 *conjuguées à* σ.

III - Groupes - Questions de cours

1. Soit G un groupe. Montrer que le centre de G,

$$Z(G) = \{g \in G : \forall x \in G, gx = xg\},$$

est un sous-groupe de G qui est commutatif et normal dans G.

$Z(G)$ est non vide car il contient e. Soient g_1 et g_2 deux éléments de $Z(G)$. Soit $x \in G$. Alors $g_1 g_2 x = g_1 x g_2 = x g_1 g_2$ et $g_1^{-1} x = (x^{-1} g_1)^{-1} = (g_1 x^{-1})^{-1} = x g_1^{-1}$. Donc $g_1 g_2$ et g_1^{-1} sont des éléments de $Z(G)$. L'ensemble $Z(G)$ est donc un sous-groupe de G. De plus deux éléments de $Z(G)$ commutent entre-eux car tout élément de $Z(G)$ commute avec tout élément de G. Donc $Z(G)$ est commutatif. Soient $g \in Z(G)$ et $h \in G$. Alors $hgh^{-1} = ghh^{-1} = g$. Donc $Z(G)$ est normal dans G.

2. Soit ϕ un morphisme d'un groupe G vers un groupe G'. Montrer que si H' est un sous-groupe de G' alors $\phi^{-1}(H')$ est un sous-groupe de G. Montrer que si de plus H' est normal dans G' alors $\phi^{-1}(H')$ est normal dans G.

L'ensemble $\phi^{-1}(H')$ contient 1_G. Soient $h_1, h_2 \in \phi^{-1}(H')$. Alors $\phi(h_1 h_2^{-1}) = \phi(h_1)\phi(h_2^{-1}) = \phi(h_1)\phi(h_2)^{-1}$. Comme H' est un sous-groupe, on en déduit que $\phi(h_1 h_2^{-1}) \in H'$ et donc que $h_1 h_2^{-1} \in \phi^{-1}(H')$. On a montré que $\phi^{-1}(H')$ était un sous-groupe de G.

Supposons que H' soit normal dans G'. Soient $h \in \phi^{-1}(H')$ et $g \in G$. Alors $\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1}$. Donc $\phi(ghg^{-1}) \in H'$ et $ghg^{-1} \in \phi^{-1}(H')$. Le groupe $\phi^{-1}(H')$ est par conséquent normal dans G.

3. Soit G un groupe et $D(G)$ le sous-groupe engendré par les commutateurs :

$$D(G) = \langle ghg^{-1}h^{-1} : g, h \in G \rangle.$$

   (a) Montrer que $D(G)$ est normal dans G.

   Il suffit de montrer que le conjugué d'un commutateur est toujours dans $D(G)$. Soient $ghg^{-1}h^{-1}$ un commutateur et k un élément de G quelconques. Alors

$$kghg^{-1}h^{-1}k^{-1} = kgk^{-1}khk^{-1}kg^{-1}k^{-1}kh^{-1}k^{-1} = (kgk^{-1})(khk^{-1})(kgk^{-1})^{-1}(khk^{-1})^{-1}.$$

   Il suit que le conjugué d'un commuatteur est lui-même un commutateur donc $D(G)$ est normal dans G.

   (b) Montrer que le groupe quotient $G/D(G)$ est abélien.

   Soient $a, b \in G$. Alors $aD(G) \cdot bD(G) \cdot a^{-1}D(G) \cdot b^{-1}D(G) = aba^{-1}b^{-1}D(G) = D(G)$. Donc $aD(G) \cdot bD(G) = bD(G) \cdot aD(G)$. Le groupe quotient $G/D(G)$ est donc abélien.

IV - Groupes à 9 éléments .

1. Donnez deux exemples de groupes à 9 éléments non isomorphes.

Les groupes $\mathbb{Z}/9\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ sont d'ordres 9 et non isomorphes ; le premier étant cyclique, l'autre non.

2. Soit G un groupe d'ordre 9 non cyclique.

   (a) Quels sont les ordres des éléments de G.

   Par le théorème de Lagrange et du fait que G n'est pas cyclique, tous les éléments sont d'ordre 3 à l'exception de l'élément neutre

(b) Montrer que G est engendré par deux éléments a et b.

Prenons un élément a différent de l'élément neutre et un élément $b \notin \langle a \rangle$. Alors $\langle a, b \rangle$ est un sous-groupe de G contenant au moins 4 éléments. Comme G est d'ordre 9, ce sous-groupe est nécessairement d'ordre 9, c'est-à-dire a et b engendre G.

(c) Montrer que

$$G = \{1, a, b, a^2, b^2, ab, ab^2, a^2b, a^2b^2\}.$$

Par (a) tout élément g de G a pour inverse g^2 (car $g^3 = 1$). Il suit que $\langle a \rangle \cap \langle b \rangle = \{1\}$. Les éléments $1, a, b, a^2, b^2$ sont donc distincts. On en déduit facilement que les éléments $1, a, b, a^2, b^2, ab, ab^2, a^2b, a^2b^2$ sont 9 éléments distincts et donc $G = \{1, a, b, a^2, b^2, ab, ab^2, a^2b, a^2b^2\}$.

(d) Montrer que $ba \in \{ab, ab^2, a^2b, a^2b^2\}$.

De même comme $1, a, b, a^2, b^2$ sont distincts, on vérifie facilement que $ba \notin \{1, a, b, a^2, b^2\}$. D'où $ba \in \{ab, ab^2, a^2b, a^2b^2\}$.

(e) Montrer que $(ba)^2 = a^2b^2$.

$(ba)^2 = (ba)^{-1} = a^{-1}b^{-1} = a^2b^2$

(f) Déduire des questions précédentes que $ba = ab$.

$a^2b^2 \neq (ab^2)^2$ car $1 \neq b^2$, $a^2b^2 \neq (a^2b)^2$ car $1 \neq a^2$ et $a^2b^2 \neq (a^2b^2)^2$ car $1 \neq a^2b^2$. Donc la seule possibilité est $ba = ab$.

(g) En déduire que G est commutatif et que G est isomorphe à $\langle a \rangle \times \langle b \rangle$.

Les éléments a et b commutent entre-eux et engendrent G donc G est commutatif. De plus $\langle a \rangle \cap \langle b \rangle = \{1\}$ donc G est isomorphe à $\langle a \rangle \times \langle b \rangle$.

3. Conclure.

Tout groupe d'ordre 9 est isomorphe à $\mathbb{Z}/9\mathbb{Z}$ ou à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.