N1MA4M11 Algèbre 3

DS

21 Mars 2014, durée 1h20, documents interdits

Exercice 1 :

1. Dans cette question on considère le groupe $G = (\mathbb{Z}/23\mathbb{Z})^*$ muni de la multiplication modulo 23.

   1a. Quel est l'ordre de G ?

   23 étant un nombre premier, l'ordre de $(\mathbb{Z}/23\mathbb{Z})^*$ *est* $23 - 1 = 22$.

   1b. Que peuvent valoir les ordres des éléments de G d'après le théorème de Lagrange ?

   D'après le théorème de Lagrange, l'ordre d'un élément de G *divise l'ordre de* G *qui vaut* 22 *donc les possibilités sont :* $1, 2, 11, 22$.

   1c. Quels sont les ordres des éléments suivants de G : $-1 \bmod 23$, $2 \bmod 23$, $-2 \bmod 23$?

   Soit $x = -1 \bmod 23$, *on a* $x^2 = (-1)^2 = 1 \bmod 23$ *et* $x \neq 1 \bmod 23$ *donc* x *est d'ordre* 2. *Soit* $x = 2 \bmod 23$. *On calcule* $2^{11} = 1 \bmod 23$, *ce qui montre que l'ordre de* x *divise* 11, *et comme* $x \neq 1 \bmod 23$, *on conclut que* x *est d'ordre* 11. *Soit* $x = -2 \bmod 23$. *Il est clair que* x *n'est ni d'ordre* 1 *ni d'ordre* 2. *Comme* $x^{11} = (-2)^{11} = -1 \bmod 23$, x *n'est pas non plus d'ordre* 11, *donc il est nécessairement d'ordre* 22 *d'après la question précédente.*

   1d. Montrez que G est cyclique.

   On a $\langle -2 \bmod 23 \rangle \subset G$ *et, d'après la question précédente,* $-2 \bmod 23$ *est d'ordre* 22. *Donc,* $\langle -2 \bmod 23 \rangle$ *est d'ordre* 22 *comme* G, *donc ils sont égaux et* $G = \langle -2 \bmod 23 \rangle$ *est cyclique.*

2. Dans cette question, p et q sont deux nombres premiers impairs tels que $p = 1 + 2q$. Soit G le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ muni de la multiplication modulo p.

   2a. Quel est l'ordre de G ?

   p *est un nombre premier donc l'ordre de* $(\mathbb{Z}/p\mathbb{Z})^*$ *est* $p - 1$.

   2b. Que peuvent valoir les ordres des éléments de G d'après le théorème de Lagrange ?

   D'après le théorème de Lagrange, l'ordre d'un élément de G *divise l'ordre de* G *qui vaut* $(p - 1) = 2q$ *; comme* q *est premier, les possibilités sont :* $1, 2, q, 2q$.

   2c. Montrez que $-1 \bmod p$ est l'unique élément d'ordre 2 de G (indication : pensez à utiliser : $a^2 - 1 = (a - 1)(a + 1)$).

   Il est clair que $-1 \bmod p$ *est d'ordre* 2 *parce que* $(-1 \bmod p)^2 = (-1)^2 \bmod p = 1 \bmod p$. *Soit* $x = a \bmod p$ *un élément d'ordre* 2 *de* G. *Alors,* $x^2 = a^2 = 1 \bmod p$, *ce qui signifie que* p *divise* $a^2 - 1$. *Comme* $a^2 - 1 = (a - 1)(a + 1)$ *et que* p *est premier,* p *divise* $(a - 1)$ *ou* p *divise* $(a + 1)$. *En revenant aux congruences, on a :* $a = 1 \bmod p$ *ou* $a = -1 \bmod p$. *Comme* $1 \bmod p$ *est d'ordre* 1, *on conclut que seul* $-1 \bmod p$ *est d'ordre* 2.

2d. Montrez que, si $a \bmod p$ est d'ordre q dans G, alors $-a \bmod p$ est d'ordre $2q$ dans G.
On a : $(-a \bmod p)^q = (-a)^q = (-1)^q a^q = -1 \bmod p$ car q est impair et a est d'ordre q modulo p, donc l'ordre de $-a \bmod p$ ne divise pas q. D'autre part l'ordre de $-a \bmod p$ ne peut pas être 2 car $(-a \bmod p)^2 = (-a)^2 = a^2 \bmod p$ donc si c'était le cas a serait aussi d'ordre 2. Donc, d'après la question 2b., la seule possibilité est que l'ordre de $-a \bmod p$ soit $2q$.

2e. Déduire de ce qui précède que G est cyclique.
G contient un élément d'ordre $2q = (p-1) = |G|$ par la question précédente donc il est cyclique.

Exercice 2 : Soit G un groupe, et soit H et K deux sous-groupes de G. On note

$$HK := \{hk \mid h \in H \text{ et } k \in K\}.$$

1. Dans cette question on prend $G = S_3$, et on pose $H = \langle (1,2) \rangle$, $K = \langle (2,3) \rangle$, $L = \langle (1,2,3) \rangle$.

1a. Montrez que $HK = \{\mathrm{Id}, (1,2), (2,3), (1,2,3)\}$ et que HK n'est pas un sous-groupe de G.
On a $H = \{\mathrm{Id}, (1,2)\}$ car la transposition $(1,2)$ est d'ordre 2, et de même $K = \{\mathrm{Id}, (2,3)\}$ donc, d'après la définition de HK, $HK = \{\mathrm{Id}, (1,2), (2,3), (1,2)(2,3)\}$. On calcule les images de $1,2,3$ par $\sigma = (1,2)(2,3)$, et on trouve $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$ donc $\sigma = (1,2,3)$.
Le produit $(2,3)(1,2)$ n'appartient pas à HK car $(2,3)(1,2) = (1,3,2)$. L'ensemble HK n'est pas stable par la loi du groupe donc ce n'est pas un sous-groupe. (Autre argument plus sophistiqué : 4 ne divise pas $6 = |S_3|$ donc si HK était un sous-groupe de G il contredirait le théorème de Lagrange).

1b. Montrez que ni H ni K n'est distingué dans G.
On a $(2,3)(1,2)(2,3)^{-1} = (2,3)(1,2)(2,3) = (1,3) \notin H$ donc H n'est pas distingué dans G et de même $(1,2)(2,3)(1,2)^{-1} = (1,3)$ donc K n'est pas distingué dans G.

1c. Montrez que L est distingué dans G.
Pour montrer que L est distingué dans G, il faut montrer que $xyx^{-1} \in L$ pour tout $x \in G$ et $y \in L$. Listons d'abord les éléments de L et G : en notant $\sigma = (1,2,3)$, $\tau_3 = (1,2)$, $\tau_2 = (1,3)$, $\tau_1 = (2,3)$,

$$L = \{\mathrm{Id}, \sigma, \sigma^2\} \quad G = \{\mathrm{Id}, \sigma, \sigma^2, \tau_1, \tau_2, \tau_3\}.$$

Afin de minimiser les vérifications à faire, on remarque que :

i. On peut se restreindre à $y = \sigma$, car : si $y = \mathrm{Id}$, $xyx^{-1} = \mathrm{Id}$; si $y = \sigma^2$, $xyx^{-1} = x\sigma^2x^{-1} = (x\sigma x^{-1})^2$.

ii. Si $x = \mathrm{Id}, \sigma, \sigma^2$, c'est trivial car les puissances de σ commutent entre elles.

Il reste donc à vérifier que $\tau_i \sigma \tau_i^{-1} \in L$ pour $i = 1,2,3$. On vérifie que $\tau_i \sigma \tau_i^{-1} = \sigma^2$ pour tout $i = 1,2,3$.

1d. Montrez que $LK = G$.
On a : $LK = \{\mathrm{Id}, \sigma, \sigma^2, \tau_1, \sigma\tau_1, \sigma^2\tau_1\}$. On vérifie que $\sigma\tau_1 = (1,2,3)(2,3) = (1,2) = \tau_3$ et que $\sigma^2\tau_1 = (1,3,2)(2,3) = (1,3) = \tau_2$.

2. On retourne au cas général, et on considère l'application :

$$\begin{aligned} f : H \times K &\to HK \\ (h,k) &\mapsto hk \end{aligned}$$

2a. Montrez que, si $x = f(h,k)$, alors l'ensemble des antécédents de x par f est l'ensemble $\{(hg, g^{-1}k) \mid g \in H \cap K\}$ et que celui-ci est de cardinal $|H \cap K|$.
Soit (h',k') tel que $f(h',k') = x$. Alors, $h'k' = hk$ donc $h^{-1}h' = kk'^{-1}$. Posons $g := h^{-1}h' = kk'^{-1}$. On a $g \in H \cap K$ puisque g est d'un part un produit d'éléments de H et d'autre part un produit d'éléments de K. On peut écrire $(h',k') = (hg, g^{-1}k)$ donc tout antécédent de x est bien de la forme annoncée. Réciproquement, si $(h',k') = (hg, g^{-1}k)$, alors $f(h',k') = hgg^{-1}k = hk = x$ donc tout élément de cette forme est bien antécédent de x. Il reste à montrer que deux éléments g appartenant à $H \cap K$ donnent naissance à des antécédents distincts de x. En effet, si $((hg, g^{-1}k) = (hg_1, g_1^{-1}k)$, alors $hg = hg_1$ donc $g = g_1$. On a bien montré que l'ensemble des antécédents de x est de cardinal $|H \cap K|$.

2b. En déduire que le cardinal de l'ensemble HK est égal à $|H||K|/|H \cap K|$.
L'application f est claireent surjective, et tout élément de HK possède $|H \cap K|$ antécédents donc on a bien l'égalité annoncée.

2c. Montrez que, si H est distingué dans G, alors HK est un sous-groupe de G.
Il est clair que HK est non vide puisque $e.e = e \in HK$. Soit $x = hk \in HK$ et $y = h'k' \in HK$ et montrons que $xy^{-1} \in HK$. On a : $xy^{-1} = hk(h'k')^{-1} = hkk'^{-1}h'^{-1}$. On écrit :

$$\begin{aligned} hkk'^{-1}h'^{-1} &= h(kk'^{-1})h'^{-1}(k'k^{-1})(kk'^{-1}) \\ &= h(kk'^{-1})h'^{-1}(kk'^{-1})^{-1}(kk'^{-1}). \end{aligned}$$

Comme H est distingué dans G, $h'' := (kk'^{-1})h'^{-1}(kk'^{-1})^{-1}$ est élément de H. On a donc $xy^{-1} = hh''(kk'^{-1})$ qui appartient bien à HK.