Université Pierre & Marie Curie — Année 2008-2009
Master de Mathématiques — MM014 Théorie des groupes
Professeur: J.F. Dat — A. Guilloux

Feuille 2

Corrigé

Groupes abéliens

Solution 1 *Les groupes abéliens finis sont déterminés à isomorphisme près par leurs facteurs invariants, donc il faut juste étudier les décompositions possibles de 15 et 48.*

On a $15 = 3 \times 5$*, donc le seul facteur invariant possible d'un groupe abélien d'ordre 15 est 15. Donc* $\mathbb{Z}/15\mathbb{Z}$ *est le seul groupe abélien d'ordre 15.*

On a

$$\begin{array}{rcll} 48 & = & (2 \times 2 \times 2 \times 2 \times 3) & \text{et le groupe est } \mathbb{Z}/48\mathbb{Z} \\ & = & (2) \times (2 \times 2 \times 2 \times 3) & \text{et le groupe est } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24 \\ & = & (2 \times 2) \times (2 \times 2 \times 3) & \text{et le groupe est } \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12 \\ & = & (2) \times (2) \times (2 \times 2 \times 3) & \text{et le groupe est } \left(\mathbb{Z}/2\mathbb{Z}\right)^2 \times \mathbb{Z}/12 \\ & = & (2) \times (2) \times (2) \times (2 \times 3) & \text{et le groupe est } \left(\mathbb{Z}/2\mathbb{Z}\right)^3 \times \mathbb{Z}/6 \end{array}$$

Solution 2

a)On a

$$\begin{array}{rcl} G & = & (\mathbb{Z}/4\mathbb{Z})^3 \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z} \\ & = & (\mathbb{Z}/4\mathbb{Z})^4 \times \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^3 \times (\mathbb{Z}/5\mathbb{Z})^2 \times \mathbb{Z}/7\mathbb{Z} \\ & = & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/3 \times 4\mathbb{Z}) \times (\mathbb{Z}/3 \times 4 \times 5\mathbb{Z}) \times (\mathbb{Z}/3 \times 4 \times 5 \times 7\mathbb{Z}) \end{array}$$

et les facteurs invariants de G *sont* $2, 4, 3 \times 4 = 12, 3 \times 4 \times 5 = 60$ *et* $3 \times 4 \times 5 \times 7 = 420$*.*

b)On a

$$\begin{array}{rcl} (\mathbb{Z}/55\mathbb{Z})^* & = & (\mathbb{Z}/11\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^* \\ & = & (\mathbb{Z}/10\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \\ & = & (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \\ & = & (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/20\mathbb{Z}) \end{array}$$

et les facteurs invariants de $(\mathbb{Z}/55\mathbb{Z})^*$ *sont 2 et 20.*

Solution 3 *1. Notons x un élément de G dont la classe modulo $Z(G)$ engendre le groupe $G/Z(G)$. Donc pour tout $g \in G$, il existe z_g dans $Z(G)$ et k_g dans $\mathbb{N}$ tel que $g = z_g x^{k_g}$. Donc pour tout g et h dans G,*

$$gh = z_g x^{k_g} z_h x^{k_h} = z_h x^{k_h} z_g x^{k_g} = hg.$$

Donc G est commutatif.

2. *Les éléments g de G dont la classe de conjugaison est réduite à g forment précisément le centre $Z(G)$ de G. On note $O_1, \dots O_k$ les classes de conjugaison de G qui ne sont pas réduites à 1 élément. La formule des classes nous donne*

$$|G| = |Z(G)| + \sum_{i=1}^{k} |O_i|.$$

Comme $|O_i| \backslash |G|$ et $|O_i| > 1$, on a forcément $p \backslash |O_i|$. Comme $p \backslash |G|$, on a alors $p \setminus |Z(G)|$. Comme $Z(G)$ contient e, on en déduit $|Z(G)| \geq p$

3. *Supposons G d'ordre p^2 et non commutatif. Donc $|Z(G)| = 1$ ou p. D'après l'exercice précédent, G a un centre non trivial, donc $|Z(G)| = p$. Donc $G/Z(G) = \mathbb{Z}/p\mathbb{Z}$ est cyclique et d'après la question précédente, G est commutatif ce qui est une contradiction.*

4. *Supposons que G n'est pas isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$. ALors tous les éléments de G autre que 1 sont d'ordre p. Soit x un tel élément, et y un élément de $G \backslash < x >$. Comme $< x > \cap < y >$ est une sous groupe de G, on a forcément $< x > \cap < y >= \{1\}$. On définit le morphisme de groupe suivant*

$$\begin{array}{rccc} \varphi : & \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} & \longrightarrow & G \\ & (a,b) & \longmapsto & x^a y^b \end{array}.$$

On a $\varphi(a,b) = 1 \Leftrightarrow x^a = y^{-b} \Leftrightarrow x^a = y^{-b} = 1 \Leftrightarrow a = b = 0$ donc φ est injective, et c'est donc un isomorphisme de groupes.

Produits semi-directs

Solution 4

a) Dans les trois cas, le sous-groupe H de gauche est d'indice 2, donc distingué. Il suffit donc de montrer qu'il existe un sous-groupe K d'ordre 2 qui n'est pas inclus dans H. Dans le groupe diédral, on peut prendre n'importe quel élément qui n'est pas dans le groupe cyclique, puisqu'ils sont tous d'ordre 2. Dans $\mathcal{S}_n$ (pour $n \geq 2$), il y a des transpositions, qui sont d'ordre 2 et ne sont pas dans $\mathcal{A}_n$. Enfin, une symétrie orthogonale par rapport à un hyperplan est toujours d'ordre 2 et n'est jamais une rotation. On remarque que si n est impair, le scalaire -1 a la même propriété, ce qui fait que l'on a même un produit direct :

$$O_n(\mathbb{R}) \simeq SO_n(\mathbb{R}) \times \{\pm 1\}.$$

b) Le groupe H_8 admet 4 sous-groupes non triviaux, et ils sont tous distingués. Toutefois, ils contiennent tous le centre $\{\pm 1\}$ de H_8, ce qui fait que la condition $H \cap K = \{1\}$ n'est satisfaite que si H ou K est trivial.

Solution 5 *1. On pose*

$$\begin{array}{rccc} \rho: & H \rtimes_\varphi K & \longrightarrow & H \rtimes_{\varphi'} K \\ & (h,k) & \longmapsto & (h, \sigma^{-1}(k)) \end{array}$$

Puisque σ est un isomorphisme de groupes, il est clair que ρ est une bijection. Il reste à montrer que c'est un morphisme de groupes. On a

$$\begin{array}{rcl} \rho\big((h,k)(h',k')\big) & = & \rho\big((h\varphi(k)(h'), kk')\big) \\ & = & (h\varphi(k)(h'), \sigma^{-1}(kk')) \\ & = & (h\varphi(k)(h'), \sigma^{-1}(k)\sigma^{-1}(k')) \\ & = & (h\varphi'(\sigma^{-1}(k))(h'), \sigma^{-1}(k)\sigma^{-1}(k')) \\ & = & (h, \sigma^{-1}(k))(h', \sigma^{-1}(k')) \\ & = & \rho\big((h,k)\big)\rho\big((h',k')\big) \end{array}$$

donc ρ est bien un morphisme de groupe.

2. On pose

$$\begin{array}{rccc} \rho: & H \rtimes_\varphi K & \longrightarrow & H \rtimes_{\varphi'} K \\ & (h,k) & \longmapsto & (\sigma(h), k) \end{array}$$

Puisque σ est un isomorphisme de groupes, il est clair que ρ est une bijection. Il reste à montrer que c'est un morphisme de groupes. On a

$$\begin{array}{rcl} \rho\big((h,k)(h',k')\big) & = & \rho\big((h\varphi(k)(h'), kk')\big) \\ & = & (\sigma(h)\sigma(\varphi(k)(h')), kk') \\ & = & (\sigma(h)\varphi'(k)(\sigma(h')), kk') \\ & = & (\sigma(h), k)(\sigma(h'), k') \\ & = & \rho\big((h,k)\big)\rho\big((h',k')\big) \end{array}$$

donc ρ est bien un morphisme de groupe.

Solution 6 *Si H et K sont donnés, décrire les produits semi-directs (non directs) $H \rtimes K$, c'est énumérer les homomorphismes (non triviaux) de K dans $Aut(H)$ et éliminer les produits qui sont isomorphes entre eux.*

a) Comme $Aut(\mathbb{Z}/4\mathbb{Z}) = (\mathbb{Z}/4\mathbb{Z})^* = \{\pm 1\}$ il y a un seul morphisme non trivial, donc un seul produit semi-direct, qui est le groupe diédral D_4.

b) Ici, il n'y a pas d'homomorphisme non trivial de $\mathbb{Z}/3\mathbb{Z}$ dans $\{\pm 1\}$, donc pas de produit semi-direct non direct.

c) Le groupe $Aut(\mathbb{Z}/q\mathbb{Z}) = (\mathbb{Z}/q\mathbb{Z})^*$ est cyclique d'ordre $q-1$. Il existe un homomorphisme non trivial de $\mathbb{Z}/p\mathbb{Z}$ dans ce groupe si et seulement si p divise $q-1$. Deux tels homomorphismes diffèrent par composition par un automorphisme de $\mathbb{Z}/p\mathbb{Z}$. Donc d'après la question 1 de l'exercice 7, il y a

dans ce cas un seul groupe semi-direct, qui est un sous-groupe du groupe métacyclique *des similitudes du corps* $\mathbb{Z}/q\mathbb{Z}$

$$G_q = (\mathbb{Z}/q\mathbb{Z}) \rtimes (\mathbb{Z}/q\mathbb{Z})^*$$

où le couple (a, b) *représente la similitude* $x \mapsto a + bx$.

d) Le groupe

$$Aut(\mathbb{Z}/15\mathbb{Z}) = (\mathbb{Z}/15\mathbb{Z})^* = \{1, 2, 4, 7, 8, 11, 13, 14\} = (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$$

a trois éléments d'ordre 2, c'est à dire 4, 11, et 14, ou $(1, -1)$, $(-1, 1)$ *et* $(-1, -1)$ *dans* $(\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$. *Il y a donc trois produits semi-directs possibles qui sont respectivment* $\mathbb{Z}/3\mathbb{Z} \times D_5$, $\mathbb{Z}/5\mathbb{Z} \times D_3$ *et* D_{15}.

e) Le groupe cyclique $Aut(\mathbb{Z}/p^2\mathbb{Z}) = (\mathbb{Z}/p^2\mathbb{Z})^*$ *a un sous-groupe d'ordre* p *engendré par* $1 + p$. *On en déduit comme au c) un seul groupe semi-direct non trivial formé des couples* (a, b) *dans* $\mathbb{Z}/p^2\mathbb{Z}$ *avec* $b \equiv 1 \pmod{p}$, *munis de la loi*

$$(a, b).(a', b') = (a + ba', bb').$$

f) Toute permutation des 3 éléments non nuls de V *est un automorphisme, donc* $Aut(V) \simeq \mathcal{S}_3$ *et il y a deux homorphismes non triviaux de* $\mathbb{Z}/3\mathbb{Z}$ *dans* $Aut(V)$. *Comme l'un est composé de l'autre par l'automorphisme non trivial de* $\mathbb{Z}/3\mathbb{Z}$, *ils donnent naissance au même produit semi-direct. Comme* $\mathcal{A}_4$ *admet* V *comme sous-groupe distingué, le groupe cherché est* $\mathcal{A}_4$.

g) De même, il y a 3 homomorphismes non triviaux de V *dans* $\{\pm 1\} = Aut(\mathbb{Z}/3\mathbb{Z})$, *et ils se déduisent l'un de l'autre par composition avec un automorphisme de* V. *On en déduit un produit semi-direct* $(\mathbb{Z}/3\mathbb{Z}) \rtimes V$ *et un seul :*

$$D_3 \times \{\pm 1\}.$$

Solution 7 *1. Soit* G *un groupe d'ordre* p^2. *Si il existe un élément d'ordre* p^2, *alors* $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ *est cyclique et donc abélien. Sinon, soit* $x \in G \setminus \{e\}$. *Comme* x *est d'ordre* p, *il existe* $y \in G \setminus < x >$, *et* y *est aussi d'ordre* p. *Le sous groupe* $< x >$ *est d'indice* p *dans* G, *et* p *est le plus petit facteur premier de* G, *donc* $< x >$ *est distingué dans* G. *De plus, on* $a < x > \cap < y > = \{e\}$ *et* $| < x > || < y > | = p^2$, *donc le groupe* G *est le produit semi direct de* $< y >$ *par* $< x >$. *Or,* $< x > \simeq < y > \simeq \mathbb{Z}/p\mathbb{Z}$, *donc il n'y a pas de morphisme non trivial* $\mathbb{Z}/p\mathbb{Z} = < x > \to \mathbb{Z}/(p-1)\mathbb{Z} = Aut(< y >)$ *(car* p *ne divise pas* $p - 1$*). C'est à dire que le produit semi direct est en fait direct, et* $G \simeq < x > \times < y > \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. *En particulier,* G *est abélien.*

2. Soient $n \geq 2$ *et* $p \geq 3$ *un nombre premier. On a*

$$\left(\mathbb{Z}/p^n\mathbb{Z}\right)^* = \mathbb{Z}/p^{n-1}(p-1)\mathbb{Z}.$$

Comme p divise $p^{n-1}(p-1)$, il existe un morphisme non trivial de $\mathbb{Z}/p\mathbb{Z}$ dans $\left(\mathbb{Z}/p^n\mathbb{Z}\right)^*$, et donc un produit semi direct non trivial $\mathbb{Z}/p^n\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.

On a

$$\left(\mathbb{Z}/4\mathbb{Z}\right)^* = \mathbb{Z}/2\mathbb{Z}$$

donc il existe évidemment un morphisme non trivial de $\mathbb{Z}/2\mathbb{Z}$ dans $\left(\mathbb{Z}/2^2\mathbb{Z}\right)^*$, et donc un produit semi direct non trivial $\mathbb{Z}/2^2\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

Si $n \geq 3$, on a

$$\left(\mathbb{Z}/2^n\mathbb{Z}\right)^* = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$$

donc en envoyant 1 sur $(1,0)$, on construit un morphisme non trivial de $\mathbb{Z}/2\mathbb{Z}$ dans $\left(\mathbb{Z}/2^n\mathbb{Z}\right)^*$, et donc un produit semi direct non trivial $\mathbb{Z}/2^n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

3. *Si $p \neq 2$, alors $\left(\mathbb{Z}/p^n\mathbb{Z}\right)^*$ est cyclique, et a donc un unique sous groupe H d'ordre p. Tout morphisme non trivial de $\mathbb{Z}/p\mathbb{Z}$ dans $\left(\mathbb{Z}/p^n\mathbb{Z}\right)^*$ est donnée par l'image de 1 qui doit être un générateur de H. Or, tous ces morphismes diffèrent par un automorphisme de $\mathbb{Z}/p\mathbb{Z}$, donc produisent des produits semi-directs isomorphes.*

4. *Si $p = 2$ et $n = 2$, alors on a aussi unicité du produit semi-direct.*

   Si $p = 2$ et $n \geq 3$, alors $\left(\mathbb{Z}/2^n\mathbb{Z}\right)^* = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$ a 3 éléments d'ordre 2, $(1,0)$, $(0,2^{n-3})$ et $(1,2^{n-3})$. Donc on a au plus 3 produits semi-directs non isomorphes. On va montrer qu'il en existe au moins 2. On sait que le groupe diédral D_{2^n} est un tel produit semi direct. Le groupe D_{2^n} a un unique sous groupe cyclique H d'ordre 2^n, et l'action par conjugaison de tout élément de $G \setminus H$ sur H est donnée par $x \mapsto x^{-1}$. Or, l'automorphisme $x \mapsto x^{-1}$ de $H = \mathbb{Z}/2^n\mathbb{Z}$ est donné par l'élément $(1,0)$ de $\left(\mathbb{Z}/2^n\mathbb{Z}\right)^* = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$, donc les deux autres produits semi-directs ne peuvent donner D_{2^n}. On a donc au moins 2 produits semi-directs non isomorphes de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/2^n\mathbb{Z}$.