Université Lyon 1 — Automne 2009/2010
Math I Algèbre — Seq 2 (J. Melleray)

Corrigé de l'examen final de janvier 2009

Question 1.
(1) Soit x, y deux éléments de E tels que $f(x) = f(y)$. On doit alors avoir $r(f(x)) = r(f(y))$; puisque $r \circ f = id_E$, on a $r(f(x)) = x$ et $r(f(y)) = y$, par conséquent on vient de démontrer que $x = y$. Ceci étant vrai pour toute paire (x, y) d'éléments de E tels que $f(x) = f(y)$, on vient de démontrer que f est injective.
(2) Supposons f injective, et posons $A = f(E)$. C'est une partie de E ; par définition de A, il existe pour tout $y \in A$ un élément x de E tel que $f(x) = y$, et comme f est injective il n'existe qu'un seul tel x. Pour $y \in A$, on définit $r(y)$ comme létant égal à cet élément : autrement dit, pour tout $y \in f(E)$ on trouve l'unique $x \in E$ tel que $f(x) = y$ et on pose $r(y) = x$. Cette fonction r n'est pas encore définie sur F tout entier, sauf si f est surjective ; si f n'est pas surjective alors on choisit $e \in E$ et on pose, pour tout $y \in F \setminus f(E)$, $r(y) = e$. Vérifions que cette fonction r est telle que $r \circ f = id_E$.
Pour cela, fixons $x \in E$ et notons $x' = r(f(x))$; puisque $f(x) \in f(E)$, on a par définition de r que x' est l'unique élément de E tel que $f(x') = f(x)$; autrement dit, $x' = x$ et on vient de démontrer que $r \circ f = id_E$.

Question 2
Avant de commencer cette question, rappelons simplement que $\mathbb{Z}/n\mathbb{Z}$ désigne l'ensembles formé par les classes de congruence des entiers modulo n. On peut munir cet ensemble de deux opérations : l'addition modulo n (qui munit cet ensemble d'une structure de groupe) et la multiplication modulo n . Rappelons que pour $k \in \mathbb{Z}$ la classe modulo n de k est l'ensemble des entiers qui sont congrus à k modulo n.
Cet exercice ne porte que sur la multiplication modulo n, qui est associative et a toujours un élément neutre (la classe de 1), mais ne munit pas $\mathbb{Z}/n\mathbb{Z}$ d'une structure de groupe puisque la classe de 0 n'a pas d'inverse.
(1) La classe $\overline{k}$ admet un inverse si, et seulement si, il existe un entier l tel que $k.l \equiv 1[n]$, autrement dit si, et seulement si, il existe un entier l et un entier m tel que $k.l - n.m = 1$. Grâce au théorème de Bezout, on voit donc que $\overline{k}$ admet un inverse si, et seulement si, k est premier avec n.
(2) Puisque 13 est premier avec 24, on sait que $\overline{13}$ doit avoir un inverse ; ce sera la classe d'un entier l tel que $13.m \equiv 1[24]$. On doit donc résoudre cette équation, d'inconnue m, et pour cela on applique la méthode habituelle consistant à trouver une relation de Bezout entre 13 et 24 en utilisant l'algorithme d'Euclide. Allons-y :

$$24 = 13 + 11; \qquad 13 = 11 + 2; \qquad 11 = 5 \times 2 + 1 \ .$$

On en déduit que

$$1 = 11 - 5 \times 2; \qquad 1 = 11 - 5 \times (13 - 11) = 6 \times 11 - 5 \times 13; \qquad 1 = 6 \times (24 - 13) - 5 \times 13 = 6 \times 24 - 11 \times 13 \ .$$

En réduisant modulo 13, on voit en particulier que $-11 \times 13 \equiv 1$ [24], par conséquent l'inverse de $\overline{13}$ est $\overline{-11}$, ou encore $\overline{13}$ (Et effectivement on a bien $13 \times 13 = 169 = 7 \times 24 + 1$; bien sûr, si on avait remarqué ça dès le début, on aurait pu s'épargner tous ces calculs).

Question 3
(1) On met 11 et 7 en relation de Bezout :

$$11 = 7 + 4; \qquad 7 = 4 + 3; \qquad 4 = 3 + 1 \ .$$

On en tire

$$1 = 4 - 3; \qquad 1 = 4 - (7 - 4) = 2 \times 4 - 7; \qquad 1 = 2 \times (11 - 7) - 7 = 2 \times 11 - 3 \times 7.$$

On a donc une solution particulière de l'équation $11u + 7v = 1$, d'inconnue (u, v) : c'est la paire $(2, -3)$. Comme 11 et 7 sont premiers entre eux, on peut appliquer un théorème du cours et en déduire que l'ensemble des solutions de cette équation est l'ensemble

$$\{(u, v) \in \mathbb{Z}^2 : u \equiv 2\ [7] \text{ et } v \equiv -3\ [11]\}\ .$$

(2) On applique la méthode habituelle pour calculer une puissance modulo un entier n ; autrement dit, on cheche la plus petite puissance congrue à 1 modulo n, puis on utilise les congruences. Pour les puissances de 2 modulo 7, on remarque simplement que $2^3 = 8$ donc $2^3 \equiv 1\ [7]$. Par compatibilité de la congruence et de la multiplication, on en déduit que pour tout $k \in \mathbb{N}$ on a $2^{3k} \equiv 1\ [7]$. Il nous reste simplement à écrire que $1000 = 3 \times 333 + 1$ pour en déduire que

$$2^{1000} \equiv 2^{333\times 3+1} \equiv (2^3)^{333} \times 2 \equiv 2\ [7]\ .$$

Le cas de 11 est un peu plus compliqué ; on calcule les puissances successives de 2 modulo 11, toujours en utilisant la compatibilité de la congruence et de la multiplication :

$$2^2 \equiv 4\ [11]; \qquad 2^3 \equiv 4 \times 2 \equiv -3\ [11]; \qquad 2^4 \equiv (-3) \times 2 \equiv -6\ [11]; \qquad 2^5 \equiv (-6) \times 2 \equiv -12 \equiv -1\ [11]\ .$$

Pas la peine de pousser nos calculs plus avant : de $2^5 \equiv -1\ [11]$ on déduit que $2^{10} \equiv (-1)^2 \equiv 1\ [11]$, par conséquent $2^{10k} \equiv 1\ [11]$ pour tout $k \in \mathbb{N}$. En particulier, $2^{1000} \equiv 1\ [11]$.
On a donc obtenu que $2^{1000} \equiv 2\ [7]$ et $2^{1000} \equiv 1\ [11]$. Puisque le reste de la division euclidienne de a par $b \geq 1$ est l'unique entier $r \in \{0, \dots, b-1\}$ tel que $r \equiv a\ [b]$, on a prouvé que le reste de la division euclidienne de 2^{1000} par 7 est 2, tandis que le reste de la division euclidienne de 2^{1000} par 11 est 1.
(3) Appelons r le reste de la division euclidienne de 2^{1000} par 77 ; c'est l'unique élément de $\{0, \dots, 76\}$ qui soit congru à 2^{1000} modulo 77, en particulier on doit avoir $r \equiv 2^{1000}\ [7]$ et $r \equiv 2^{1000}\ [11]$. Par conséquent, r est solution de l'équation

$$\begin{cases} r & \equiv 2\ [7] \\ r & \equiv 1\ [11] \end{cases}\ .$$

Comme 7 et 11 sont premiers entre eux, cette équation n'a qu'une solution modulo 77 et tout ce qu'il nous reste à faire est de résoudre cette équation, ce pour quoi on a simplement besoin de trouver une solution particulière r_0. A partir de la relation $2 \times 11 - 7 \times 3 = 1$ obtenue à la question (1), on voit que

$$\begin{cases} 22 & \equiv 0\ [11] \\ 22 & \equiv 1\ [7] \end{cases} \text{ et } \begin{cases} -21 & \equiv 1\ [11] \\ -21 & \equiv 0\ [7] \end{cases}$$

En utilisant la compatibilité de la congruence et de l'addition, on en déduit alors que $2 \times 22 + (-21) = 23$ est congru à $2 \times 1 + 0 = 2$ modulo 7, et à $2 \times 0 + 1$ [11]. Autrement dit, $r_0 = 23$ est une solution de notre équation ; puisque deux solutions sont égales modulo 77, et que $r \in \{0, \dots, 76\}$, on en déduit que $r = 23$. Finalement, le reste de la division euclidienne de 2^{1000} par 77 est 23.

Question 4.
(1) On cherche les racines carrées de $-2+2i$ en coordonnées cartésiennes, sous la forme $x+iy$. En utilisant le fait que $(x+iy)^2 = x^2 - y^2 + 2ixy$ et que $|x+iy|^2 = x^2 + y^2$, on obtient en identifiant parties réelles, parties imaginaires et modules que

$$\begin{cases} x^2 - y^2 & = -2 \\ 2xy & = 2 \\ x^2 + y^2 & = |-2+2i| = \sqrt{4+4} = 2\sqrt{2} \end{cases}$$

En sommant les deux premières lignes on obtient $2x^2 = -2 + 2\sqrt{2}$, doù $x^2 = \sqrt{2} - 1$; on en déduit immédiatement que $y^2 = \sqrt{2} + 1$. Puisque $2xy = 2$ on sait que x et y sont de même signe, par conséquent les racines de $-2 + 2i$ sont

$$\sqrt{\sqrt{2}-1} + i\sqrt{\sqrt{2}+1} \text{ et } -\sqrt{\sqrt{2}-1} - i\sqrt{\sqrt{2}+1}\ .$$

(2) Pour la forme polaire, on utilise le fait que $|-2+2i| = 2\sqrt{2}$ pour mettre $2\sqrt{2}$ en facteur et obtenir

$$-2+2i = 2\sqrt{2}\,\big(\frac{-\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\big) = 2\sqrt{2}\,e^{3i\pi/4}\ .$$

Par conséquent, les racines de $-2+2i$ sont les nombres complexes $re^{i\theta}$ tels que

$$\begin{cases} r^2 &= 2\sqrt{2} \\ 2\theta &\equiv \frac{3\pi}{4}\ [2\pi] \end{cases},\ \text{ou encore }\ \begin{cases} r &= \sqrt{2\sqrt{2}} \\ \theta &\equiv \frac{3\pi}{8}\ [\pi] \end{cases}\ .$$

Sous forme polaire, les deux racines carrées de $-2+2i$ sont donc

$$\sqrt{2\sqrt{2}}\,e^{3i\pi/8} \text{ et } \sqrt{2\sqrt{2}}\,e^{11i\pi/8}\ .$$

(3) Puisque $3\pi/8 \in [0, \pi/2]$, la racine carrée de $-2+2i$ d'argument $3\pi/8$ est celle dont la partie réelle et la partie imaginaire sont positives ; à partir des questions (1) et (2) on obtient donc

$$\sqrt{2\sqrt{2}}\,e^{3i\pi/8} = \sqrt{\sqrt{2}-1} + i\sqrt{\sqrt{2}+1}\ .$$

En identifiant les parties réelles de ces deux nombres complexes, on a enfin

$$\sqrt{2\sqrt{2}}\cos(\frac{3\pi}{8}) = \sqrt{\sqrt{2}-1},\ \text{ou encore}\ \cos(\frac{3\pi}{8}) = \frac{\sqrt{\sqrt{2}-1}}{\sqrt{2\sqrt{2}}}\ .$$

Finalement, on a donc $\cos(\frac{3\pi}{8}) = \sqrt{\frac{\sqrt{2}-1}{2\sqrt{2}}} = \sqrt{\frac{2-\sqrt{2}}{4}} = \frac{\sqrt{2-\sqrt{2}}}{2}$.

Question 5.
(1) Notons que 2 divise 6 ; par conséquent, si deux entiers sont congrus modulo 6 ils sont aussi congrus modulo 2. En utilisant les notations de l'énoncé, cela signifie que $\overline{l} = \overline{m}$ alors on a aussi $\hat{l} = \hat{m}$. Ceci montre que la fonction f est bien définie.
Pour voir que f est un morphisme de groupes, on doit vérifier que si $l \equiv a\ [6]$ et $m \equiv b\ [6]$ alors $l+m \equiv a+b\ [6]$. Or, on sait par compatibilité de la congruence et de l'addition que $l+m \equiv a+b\ [6]$, et ceci entraîne (puisque 2 est un diviseur de 6) que $l+m \equiv a+b\ [2]$.
On vient de démontrer que $f(\overline{l}+\overline{m}) = f(\overline{l}) + f(\overline{m})$, autrement dit que f est un morphisme de groupes. Pour voir que f est surjective, il nous suffit de voir que tout élément de $\mathbb{Z}/2\mathbb{Z} = \{\hat{0}, \hat{1}\}$ a un antécédent par f ; c'est bien le cas, puisque $\hat{0} = f(\overline{0})$ et $\hat{1} = f(\overline{1})$.
(2) Le noyau $Ker\,f$ de f est, par définition, l'ensemble des classes modulo 6 qui sont envoyées sur $\hat{0}$ par f. Autrement dit, le noyau de f est constitué des classes modulo 6 des entiers congrus à 0 modulo 2, c'est-à-dire des classes modulo 6 des entiers pairs. On a donc

$$Ker\,f = \{\overline{0}, \overline{2}, \overline{4}\}$$

C'est un groupe à 3 éléments, dont la table de composition se trouve au début de la page suivante.

$+$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{0}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{2}$

TABLE 1 – La table de composition de $Ker\, f$

(3) Considérons l'application $\varphi\colon Ker\, f \to \mathbb{Z}/3\mathbb{Z}$ telle que $\varphi(\overline{0})$ soit la classe de 0 modulo 3, $\varphi(\overline{2})$ soit la classe de 1 modulo 3, et $\varphi(\overline{4})$ soit la classe de 2 modulo 3.
Alors φ est une surjection d'un ensemble fini de cardinal 3 sur un ensemble fini de cardinal 3, donc φ est une bijection. La vérification du fait que φ est un morphisme est immédiate : notons $\tilde{l}$ la classe modulo 3 de l'entier l. Alors on a

$$\varphi(\overline{0}+\overline{2}) = \tilde{1} = \tilde{0}+\tilde{1} = \varphi(\overline{0})+\varphi(\overline{2})\ ;$$
$$\varphi(\overline{0}+\overline{4}) = \tilde{2} = \tilde{0}+\tilde{2} = \varphi(\overline{0})+\varphi(\overline{4})\ ;$$
$$\varphi(\overline{2}+\overline{4}) = \tilde{0} = \tilde{1}+\tilde{2} = \varphi(\overline{0})+\varphi(\overline{2})\ .$$

Ceci démontre que φ est un morphisme ; comme on a déjà justifié le fait que φ est bijective, on a bien construit un isomorphisme de $Ker\, f$ sur $\mathbb{Z}/3\mathbb{Z}$.