Université Claude Bernard Lyon 1
Licence Sciences et Technologie

Unité d' enseignement: Math I Algèbre
Contrôle continu final
?? janvier 2010 - durée 2 heures

- Les documents et les calculettes ne sont pas autorisés.
- Les questions sont indépendantes et peuvent être traitées dans l'ordre de votre choix.

Question : 1.

(1) Déterminer tous les couples $(u,v)\in\mathbb{Z}^2$ tels que $11u+13v=1$.

(2) Déterminer les restes des divisions euclidienne de 3^{4444} par 11 et 13.

(3) En déduire le reste de la division euclidienne de 3^{4444} par 143.

Allez à : Correction question : 1

Question : 2.

Répondre par vrai ou faux aux énoncés qui suivent en justifiant votre réponse par un bref argument.

(1) 22^{22} admet 23 diviseurs.

(2) Il y a 16 relations binaires sur l'ensemble $E=\{1,2\}$.

(3) Pour tout entier $n\in\mathbb{N}$, $\sum_{i=0}^{n}\binom{n}{i}2^i=3^n$.

(4) Dans $\mathbb{Z}$ on a $4\mathbb{Z}\cap 6\mathbb{Z}=12\mathbb{Z}$. (Pour tout entier $n\in\mathbb{N}$, $n\mathbb{Z}=\{nl, l\in\mathbb{Z}\}$).

Allez à : Correction question : 2

Question : 3.

Soit $\alpha\in\mathbb{R}$. Résoudre l'équation :

$$z^6-2\cos(\alpha)\,z^3+1=0$$

Allez à : Correction question : 3

Question : 4.

Pour la suite, on désigne par $\mathcal{U}_n$ le groupe (pour la multiplication) des racines n-ième de l'unité dans $\mathbb{C}$.

(1) Faire la liste des sous-groupes de $\mathcal{U}_{17}$.

(2) Soit $\omega=e^{\frac{2i\pi}{n}}\in\mathcal{U}_n$. Montrer que pour tout entier $n\in\mathbb{N}$ on a :

$$\omega^m=1\Leftrightarrow n \text{ divise } m$$

(Indication : pour l'implication $\Rightarrow$ utiliser la division euclidienne)

(3) Déduire du point (2) que si $l\in\mathbb{N}\setminus\{0\}$ est premier avec n alors l'élément ω^l est d'ordre n dans $\mathcal{U}_n$.

(4) Faire la liste des éléments du sous-groupe $<\omega^{12}>$ de $\mathcal{U}_{15}$ engendré par ω^{12}.

Allez à : Correction question : 4

Question : 5.

(1) Montrer que l'application

$$f:\mathcal{U}_8\to\mathcal{U}_2$$
$$z\mapsto z^4$$

Est bien définie et que c'est un morphisme surjectif de groupe.

(2) Déterminer le noyau $\ker(f)$ du morphisme f et dresser sa table de multiplication.

(3) Expliciter un isomorphisme du groupe $\mathbb{Z}/4\mathbb{Z}$ pour l'addition sur le groupe $\ker(f)$.

(Rappel, pour l'addition sur l'ensemble des classes de restes $\mathbb{Z}/4\mathbb{Z}$ est définies par $\overline{a}+\overline{b}=\overline{a+b}$.)

Allez à : Correction question : 5

CORRECTION

Correction question : 1.

(1) Soit on voit directement que $11 \times 6 + 13 \times (-5) = 1$, soit on effectue la division euclidienne de 13 par 11.

$$13 = 1 \times 11 + 2$$
$$11 = 5 \times 2 + 1$$

Donc

$$1 = 11 - 5 \times 2 = 11 - 5(13 - 1 \times 11) = 6 \times 11 - 5 \times 13$$

On cherche alors toutes les solutions :

$$\begin{matrix} L_1 \\ L_2 \end{matrix}\begin{cases} 11u + 13v = 1 \\ 11 \times 6 + 13 \times (-5) = 1 \end{cases}$$

$L_1 - L_2$ donne $11(u-6) + 13(v+5) = 0 \Leftrightarrow 11(u-6) = -13(v+5)$

11 divise $-13(v+5)$ et $11 \wedge 13 = 1$, d'après le théorème de Gauss 11 divise $v+5$, il existe donc $k \in \mathbb{Z}$ tel que $v + 5 = 11k$, on remplace dans $11(u-6) = -13(v+5)$, ce qui donne

$$11(u-6) = -13 \times 11k \Leftrightarrow u - 6 = -13k$$

Finalement $\begin{cases} u = 6 - 13k \\ v = -5 + 11k \end{cases}$

(2) D'après le théorème de Fermat, comme 11 est premier et si $11 \wedge a = 1$ alors $a^{10} \equiv 1 \quad [11]$

On divise 4444 par 10, $4444 = 444 \times 10 + 4$:

$$3^{4444} = 3^{444 \times 10 + 4} = (3^{10})^{444} \times 3^4 \equiv 1^{444} \times 81 \quad [11] \equiv 81 \quad [11] \equiv 7 \times 11 + 4 \quad [11] \equiv 4 \quad [11]$$

le théorème de Fermat, comme 13 est premier et si $13 \wedge a = 1$ alors $a^{12} \equiv 1 \quad [13]$

On divise 4444 par 12, $4444 = 370 \times 12 + 4$:

$$3^{4444} = 3^{370 \times 12 + 4} = (3^{12})^{370} \times 3^4 \equiv 1^{370} \times 81 \quad [13] \equiv 81 \quad [13] \equiv 6 \times 13 + 3 \quad [13] \equiv 3 \quad [13]$$

(3) On remarque que $143 = 11 \times 13$, puis comme 11 et 13 sont premier entre eux, on peut appliquer le théorème des restes chinois.

$$\begin{cases} 3^{4444} \equiv 4 \quad [11] \\ 3^{4444} \equiv 3 \quad [13] \end{cases}$$

Or $11 \times 6 + 13 \times (-5) = 1$ entraine que $11 \times 6 \equiv 1 \quad [13]$ et que $13 \times (-5) \equiv 1 \quad [11]$

Donc $3^{4444} \equiv 4 \times 13 \times (-5) + 3 \times 11 \times 6 \quad [11 \times 13] \equiv -260 + 198 \quad [143] \equiv -62 \quad [143]$

Autre solution

$$\begin{cases} 3^{4444} \equiv 4 \quad [11] \\ 3^{4444} \equiv 3 \quad [13] \end{cases} \Leftrightarrow \begin{cases} 3^{4444} = 4 + 11l \\ 3^{4444} = 3 + 13l' \end{cases}$$

En faisant la différence de la première ligne par la seconde on trouve que :

$$0 = 1 + 11l - 13l' \Leftrightarrow -11l + 13l' = 1 \Leftrightarrow \begin{cases} l = -6 + 13k \\ l' = -5 + 11k \end{cases}$$

D'après la première question avec $u = -l$ et $v = l'$.

On remplace (par exemple) $l = -6 + 13k$ dans $3^{4444} = 4 + 11l$, ce qui donne

$$3^{4444} = 4 + 11(-6 + 13k) = -62 + 11 \times 13k \equiv -62 \quad [143]$$

-62 n'appartient pas à $[0,143[\cap \mathbb{N}$ donc -62 n'est pas le reste de la division euclidienne de 3^{4444} par 143,

$$3^{4444} \equiv -62 + 143 \quad [143] \equiv 81 \quad [143]$$

$0 \leq 81 < 143$, donc 81 est le reste de la division euclidienne de 3^{4444} par 143.

Allez à : Question : 1

Correction question : 2.

(1) $22^{22} = 2^{22} \times 11^{22}$ donc les diviseurs de 22^{22} sont de la forme $2^k \times 11^l$ avec $k \in \{0,1,\dots,22\}$ et $l \in \{0,1,\dots,22\}$, cela fait 23 possibilités pour k et 23 pour l, il y a donc 23×23 diviseur de 22^{22}, la réponse est : faux.

(2) Le nombre de relation binaire sur un ensemble à n éléments est 2^{n^2}, ici $n=2$, il y a donc $2^4=16$ relations binaires sur E, la réponse est : vrai

(3) $\sum_{i=0}^{n}\binom{n}{i}2^i=\sum_{i=0}^{n}\binom{n}{i}2^i\,1^{n-i}=(2+1)^n=3^n$ avec la formule du binôme de Newton. La réponse est : vrai.

(4) $a\mathbb{Z}\cap b\mathbb{Z}=PPCM(a,b)\mathbb{Z}$ or $PPCM(4,6)=12$ d'où le résultat.

La réponse est : vrai.

Allez à : Question : 2

Correction question : 3.

On pose $X=z^3$

$$z^6-2\cos(\alpha)\,z^3+1=0\Leftrightarrow X^2-2\cos(\alpha)\,X+1=0$$

Il s'agit d'une équation du second degré dont le déterminant est :

$$\Delta=(-2\cos(\alpha))^2-4=4(\cos^2(\alpha)-1)=-4\sin^2(\alpha)=(2i\sin(\alpha))^2$$

Les deux solutions sont :

$$X_1=\frac{2\cos(\alpha)-2i\sin(\alpha)}{2}=\cos(\alpha)-i\sin(\alpha)=e^{-i\alpha}$$

Et

$$X_2=\frac{2\cos(\alpha)+2i\sin(\alpha)}{2}=\cos(\alpha)+i\sin(\alpha)=e^{i\alpha}$$

Il reste à résoudre $z^3=e^{-i\alpha}$ et $z^3=e^{i\alpha}$

$$z^3=e^{-i\alpha}\Leftrightarrow\begin{cases}|z^3|=|e^{-i\alpha}|\\ \arg(z^3)=-\alpha+2k\pi\quad k\in\mathbb{Z}\end{cases}\Leftrightarrow\begin{cases}|z|^3=1\\ 3\arg(z)=-\alpha+2k\pi\quad k\in\mathbb{Z}\end{cases}$$

$$\Leftrightarrow\begin{cases}|z|=1\\ \arg(z)=-\dfrac{\alpha}{3}+\dfrac{2k\pi}{3}\quad k\in\{0,1,2\}\end{cases}\Leftrightarrow z_k=e^{i\left(-\frac{\alpha}{3}+\frac{2k\pi}{3}\right)}\quad k\in\{0,1,2\}$$

$$z^3=e^{i\alpha}\Leftrightarrow\begin{cases}|z^3|=|e^{i\alpha}|\\ \arg(z^3)=\alpha+2k\pi\quad k\in\mathbb{Z}\end{cases}\Leftrightarrow\begin{cases}|z|^3=1\\ 3\arg(z)=\alpha+2k\pi\quad k\in\mathbb{Z}\end{cases}$$

$$\Leftrightarrow\begin{cases}|z|=1\\ \arg(z)=\dfrac{\alpha}{3}+\dfrac{2k\pi}{3}\quad k\in\{0,1,2\}\end{cases}\Leftrightarrow z_k=e^{i\left(\frac{\alpha}{3}+\frac{2k\pi}{3}\right)}\quad k\in\{0,1,2\}$$

Les solutions sont $\left\{e^{-i\frac{\alpha}{3}},e^{i\frac{-\alpha+2\pi}{3}},e^{i\frac{-\alpha+4\pi}{3}},e^{i\frac{\alpha}{3}},e^{i\frac{\alpha+2\pi}{3}},e^{i\frac{\alpha+4\pi}{3}}\right\}$

Allez à : Question : 3

Correction question : 4.

(1) Le cardinal de $\mathcal{U}_{17}$ est de 17, le cardinal d'un sous-groupe de $\mathcal{U}_{17}$ divise 17 (d'après le théorème de Lagrange), les seuls diviseurs positifs de 17 sont 1 et 17 (car 17 est premier), $\mathcal{U}_{17}$ a donc deux sous-groupes $\{1\}$ et $\mathcal{U}_{17}$.

(2) Si $\omega^m=1$, la division euclidienne de m par n dit qu'il existe $(q,r)\in\mathbb{N}\times\{0,1,\dots,n-1\}$ tels que :

$$m=nq+r$$

Donc

$$\omega^m=1\Leftrightarrow\omega^{nq+r}=1\Leftrightarrow(\omega^n)^q\omega^r=1\Leftrightarrow1^q\omega^r=1\Leftrightarrow\omega^r=1$$

$\omega^n=1$ parce que n est l'ordre (=cardinal) du groupe $\mathcal{U}_n$.

$$\omega^r=1\Leftrightarrow e^{\frac{2ir\pi}{n}}=1\Leftrightarrow\text{il existe }k\in\mathbb{Z},\frac{2r\pi}{n}=2k\pi\Leftrightarrow\text{il existe }k\in\mathbb{Z},\frac{r}{n}=k\Leftrightarrow\text{il existe }k\in\mathbb{Z},r=kn$$

Comme $0\le r<n$, on a $k=0$ et donc $r=0$, par conséquent $m=nq$ ce qui signifie bien que n divise m.

Si n divise m, il existe $q\in\mathbb{N}$ tel que $m=qn$ donc $\omega^{qn}=(\omega^n)^q=1^q=1$, car comme précédemment $\omega^n=1$.

(3) Soit d l'ordre de ω^l, $(\omega^l)^d = 1$ donc $\omega^{ld} = 1$, d'après la question précédente n divise ld, il existe $k \in \mathbb{Z}$ tel que $ld = kn$, on en déduit que l divise kn or $l \wedge n = 1$, d'après le théorème de Gauss l divise k, il existe donc $k' \in \mathbb{Z}$ tel que $k'l = k$, on remplace dans $ld = kn$, cela donne $ld = k'ln \Leftrightarrow d = k'n$ car $l \neq 0$.
D'autre part l'ordre d d'un élément d'un groupe divise l'ordre du groupe, il existe $k'' \in \mathbb{Z}$ tel que $n = k''d$
On a $d = k'n$ et $n = k''d$, d'où l'on déduit que $n = kk'n$, n est non nul donc $kk' = 1$ par conséquent $k = k' = \pm 1$ comme n et d sont positif $k = k' = 1$ et enfin $d = n$.
(4) 12 n'est pas premier avec 15, on ne peut pas appliquer le résultat ci-dessus. D'après (2) $\omega^m = 1 \Leftrightarrow$ 15 divise m. Donc l'ordre, d, de ω^{12} est un multiple de 15 et un multiple de 12, par définition de l'ordre d'un élément (c'est-à-dire le plus petit entier d tel que $g^d = e$ où e est l'élément neutre du groupe) on en déduit que $d = PPCM(12,15) = 60$ par conséquent $< \omega^{12} > = < 1, \omega^{12}, \omega^{24}, \omega^{36}, \omega^{48} >$ (en effet $\omega^{60} = 1$).
Allez à : Question : 4

Correction question : 5.

(1) Le problème est de savoir si $f(z) \in \mathcal{U}_2$, or $(z^4)^2 = z^8 = 1$ car $z \in \mathcal{U}_8$ donc $z^4 \in \mathcal{U}_2$. f est bien définie. $f(z_1 z_2) = (z_1 z_2)^4 = z_1^4 z_2^4 = f(z_1)f(z_2)$ donc f est bien un morphisme de groupe.
$\mathcal{U}_2 = \{-1,1\}$ or $1^4 = 1 \Leftrightarrow f(1) = 1$ donc 1 admet un antécédent.
$e^{\frac{i\pi}{4}} = e^{\frac{2i\pi}{8}} \in \mathcal{U}_8$ et $f\left(e^{\frac{i\pi}{4}}\right) = \left(e^{\frac{i\pi}{4}}\right)^4 = e^{i\pi} = -1$ donc -1 admet un antécédent.
Tous les éléments de $\mathcal{U}_2$ admettent un antécédent, f est surjective.
(2) Soit $z \in \mathcal{U}_8$, $z \in Ker(f) \Leftrightarrow f(z) = 1 \Leftrightarrow z^4 = 1 \Leftrightarrow z \in \{1, i, -1, -i\}$
Donc $Ker(f) = \{1, i, -1, -i\} = \mathcal{U}_4$

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

(3) première méthode compliquée mais qui se généralise aux isomorphismes de $\mathbb{Z}/n\mathbb{Z}$ sur $\mathcal{U}_n$.
On pose $\varphi(\overline{a}) = e^{\frac{2ia\pi}{4}} = e^{\frac{ia\pi}{2}}$, où $\overline{k} \in \mathbb{Z}/4\mathbb{Z}$.
Il faut d'abord vérifier que φ est bien définie, c'est-à-dire que si on change de représentant dans $\overline{a}$ alors l'image est bien la même. Soit $b \in \overline{a}$, $b = a + 4k$, $k \in \mathbb{Z}$.
$$e^{\frac{2ib\pi}{4}} = e^{\frac{2i(a+4k)\pi}{4}} = e^{\frac{2ia\pi+2i\times 4k\pi}{4}} = e^{\frac{2ia\pi}{4}} e^{\frac{2ik\times 4\pi}{4}} = e^{\frac{2ia\pi}{4}} \times e^{2ik\pi} = e^{\frac{2ia\pi}{4}} \times 1 = e^{\frac{2ia\pi}{4}}$$
Donc tout va bien.
$$\varphi(\overline{a} + \overline{b}) = \varphi(\overline{a+b}) = e^{\frac{i(a+b)\pi}{2}} = e^{\frac{ia\pi}{2}} e^{\frac{ib\pi}{2}} = \varphi(\overline{a})\varphi(\overline{b})$$
φ est bien un morphisme de $\mathbb{Z}/4\mathbb{Z}$ sur $\mathcal{U}_4$.
Montrons que le noyau de φ est bien réduit à $\overline{0}$ (l'élément neutre de $\mathbb{Z}/4\mathbb{Z}$), ce qui montrera que φ est injective.
$$\overline{a} \in Ker(\varphi) \Leftrightarrow \varphi(\overline{a}) = 1 \Leftrightarrow e^{\frac{ia\pi}{2}} = 1 \Leftrightarrow \text{il existe } k \in \mathbb{Z}, \frac{a\pi}{2} = 2k\pi \Leftrightarrow \text{il existe } k \in \mathbb{Z}, a = 4k \Leftrightarrow \overline{a} = \overline{0}$$
Donc φ est injective.
Comme le cardinal de $\mathbb{Z}/4\mathbb{Z}$ est le même que le cardinal de $\mathcal{U}_4$, on en déduit que φ est bijective, finalement φ est un isomorphisme de groupe.
Deuxième méthode.
On pose $\varphi(\overline{0}) = 1$, $\varphi(\overline{1}) = i$, $\varphi(\overline{2}) = -1$ et $\varphi(\overline{3}) = -i$
Chaque élément de $\mathcal{U}_4$ admet un unique antécédent donc φ est une bijection.
Il reste à montrer que c'est un morphisme.
$$\varphi(\overline{0} + \overline{0}) = \varphi(\overline{0}) = 1 = 1 \times 1 = \varphi(\overline{0})\varphi(\overline{0})$$
$$\varphi(\overline{0} + \overline{1}) = \varphi(\overline{1}) = i = 1 \times i = \varphi(\overline{0})\varphi(\overline{1})$$

$$\varphi(\overline{0}+\overline{2})=\varphi(\overline{2})=-1=1\times(-1)=\varphi(\overline{0})\varphi(\overline{2})$$
$$\varphi(\overline{0}+\overline{3})=\varphi(\overline{3})=-i=1\times(-i)=\varphi(\overline{0})\varphi(\overline{3})$$

$$\varphi(\overline{1}+\overline{1})=\varphi(\overline{2})=-1=i\times i=\varphi(\overline{1})\varphi(\overline{1})$$
$$\varphi(\overline{1}+\overline{2})=\varphi(\overline{3})=-i=i\times(-1)=\varphi(\overline{1})\varphi(\overline{2})$$
$$\varphi(\overline{1}+\overline{3})=\varphi(\overline{0})=1=i\times(-i)=\varphi(\overline{1})\varphi(\overline{3})$$

$$\varphi(\overline{2}+\overline{2})=\varphi(\overline{0})=1=(-1)\times(-1)=\varphi(\overline{2})\varphi(\overline{2})$$
$$\varphi(\overline{2}+\overline{3})=\varphi(\overline{1})=i=(-1)\times(-i)=\varphi(\overline{2})\varphi(\overline{3})$$

$$\varphi(\overline{3}+\overline{3})=\varphi(\overline{2})=-1=(-i)\times(-i)=\varphi(\overline{3})\varphi(\overline{3})$$

Par commutativité on obtient ceux qui manquent.

φ est bien un morphisme de groupe. Comme il est bijectif, c'est un isomorphisme.

Allez à : Question : 5