Math I Algèbre. Corrigé du ccf du 22 janvier 2010.

Question 1. (5 pts)

(1) les solutions entières de l'équation $11\,u+13\,v=1$: par Euclide, on a $13=11+2$, $11=2\cdot 5+1$, d'où $1=11-5\cdot 2=11-5\cdot(13-11)=11\cdot 6-13\cdot 5$. Une solution particulière est donc $(u,v)=(6,-5)$.

Pour obtenir la solution générale, on observe que si (u',v') est solution, on a

$$11\,(u'-u)=13\,(v-v').$$

Par Gauss, 13 divise $(u'-u)$ i.e. il existe $l\in\mathbf{Z}$ tel que $u'-u=13l$, d'où

$$(u',v')=(u+13l,v-11l)=(6+13l,-5-11l).$$

On remarque enfin que quelquesoit $l\in\mathbf{Z}$, le couple (u',v') est solution.

(2) les restes de 3^{4444} par 11 et par 13: par Fermat, $3^{10}\equiv 1[11]$. On a $4444=444\cdot 10+4$, d'où

$$3^{4444}=(3^{10})^{444}\cdot 3^4\equiv 3^4[11]\equiv 4[11].$$

De même, par Fermat, $3^{12}\equiv 1[13]$. On a $4444=370\cdot 12+4$, d'où

$$3^{4444}=(3^{12})^{370}\cdot 3^4\equiv 3^4[13]\equiv 3[13].$$

(3) Par le (2), l'entier $N=3^{4444}$ est solution du système de congruences

$$x\equiv 4[11]\quad x\equiv 3[13]\qquad(\star)$$

Il s'agit donc de *restes chinois*.

Voici une méthode générale pour trouver le reste r de la division de N par $11\cdot 13=143$: puisque N satisfait $(\star)$, il existe des entiers U et V tels que $N=-11\,U+4$ et $N=13\,V+3$ ce qui implique

$$11\,U+13\,V=1.$$

Par le (1), $U=6+13l$ pour un certain $l\in\mathbf{Z}$ et

$$N=-11\cdot(6+13l)+4=-62-143l\equiv 81[143],$$

d'où $r=81$.

Voici une autre manière de faire qui utilise le fait que 3^4 apparait dans les deux congruences: par le (2), 11 et 13 divisent $N-3^4=N-81$. 11 et 13 étant premiers (donc étrangers), $11\cdot 13=143$ divise aussi $N-81$, d'où $r=81$.

Question 2. (4 pts)

(1) C'est *faux*. Les diviseurs positifs de $22^{22}=2^{22}\cdot 11^{22}$ sont les entiers $2^k\cdot 11^l, 0\le k,l\le 22$. L'entier 22^{22} admet donc 23^2 diviseurs positifs.

(2) C'est *vrai*. Le nombre de relations binaires sur E est égal au nombre de parties de $E\times E$ qui vaut $2^{|E\times E|}=2^4=16$.

(3) C'est *vrai*. C'est le binôme de Newton: $(1+x)^n = \sum_{l=0}^{n} \binom{n}{l} x^l$ pour $x = 2$.

(4) C'est *vrai*. Les multiples communs de 4 et 6 sont les multiples du ppcm $(4, 6) = 12$.

Question 3. (3 pts)

Les solutions de l'équation $z^6 - 2\,cos\,\alpha\, z^3 + 1 = 0$: $Z = z^3$ est solution de $Z^2 - 2\,cos\,\alpha Z + 1 = 0$ dont le discriminant vaut $4\,cos^2\,\alpha - 4 = -4\,sin^2\,\alpha \leq 0$. Les solutions pour Z sont donc

$$Z_{\pm} = cos\,\alpha \pm i sin\,\alpha = e^{\pm i\alpha}.$$

Ensuite (cf cours) $z^3 = e^{\pm i\alpha}$ équivaut à

$$z \in \{e^{\pm \frac{i\alpha}{3}}, e^{\frac{i(\pm\alpha+2\pi)}{3}}, e^{\frac{i(\pm\alpha+4\pi)}{3}}\}.$$

Question 4. (5 pts)

(1) Par Lagrange, l'ordre de tout sous-groupe de U_{17} est un diviseur de $\mid U_{17} \mid = 17$. Il y a donc deux sous-groupes, $\{1\}$ et U_{17}.

(2) Pour $\Leftarrow$: s' il existe $d \in \mathbf{N}$ tel que $m = nd$ on a $\omega^m = (\omega^n)^d = 1$.

Pour $\Rightarrow$: par division $m = nq + r, 0 \leq r \leq n-1$. Doù

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

ω étant d'ordre n, on a $(\omega^r = 1$ et $r < n) \Rightarrow r = 0$.

(3) Notons $d = \text{ord}\ (\omega^l)$. Par Lagrange, d divise n. Par (2) on a

$$1 = (\omega^l)^d = \omega^{ld} \Leftrightarrow n \text{ divise } ld.$$

Puisque pgcd $(n, l) = 1$, par Gauss, n divise d. Conclusion: $n = d$.

(Remarque: pour (2) et (3), on a utilisé uniquement le fait que ω est un élément d'ordre n dans un groupe fini d'ordre n. Ce qui précède s'applique dès lors, mutatis mutandis, à tout groupe fini d'ordre n.)

(4) On utilise $\omega^{15} = 1$ pour calculer les puissances successives de ω^{12} ce qui donne $(\omega^{12})^2 = \omega^{24} = \omega^9$, $(\omega^{12})^3 = \omega^{36} = \omega^6$, $(\omega^{12})^4 = (\omega^9)^2 = \omega^3$, $(\omega^{12})^5 = \omega^3 \cdot \omega^{12} = 1$. Conclusion:

$$\langle \omega^{12} \rangle = \{1, \omega^3, \omega^6, \omega^9, \omega^{12}\}.$$

Remarque: par Lagrange on savait *a priori* que $\mid \langle \omega^{12} \rangle \mid \in \{3, 5\}$.

Question 5 (5 pts)

(1) $z \in U_8$ signifie $1 = z^8 = (z^4)^2$. En clair: $z \in U_8 \Leftrightarrow z^4 \in U_2$ et l'application $f : U_8 \to U_2 : z \mapsto z^4$ est bien définie.

f est un morphisme car $f(zz') = (zz')^4 = z^4 z'^4 = f(z) \cdot f(z')$.

f est surjective car $U_2 = \{1, -1\}$ et $f(1) = 1$ et $f(\omega) = -1$.

(2) Par définition du noyau, $z \in Ker\,f \Leftrightarrow z^4 = 1$, i.e.

$$Ker\,f = U_4 = \{e^{\frac{i\pi l}{2}}, 0 \leq l \leq 3\} = \{1, i, -1, -i\}.$$

Voici la table de U_4:

$$\begin{array}{r|rrrr} \times & 1 & i & -1 & -i \\ 1 & 1 & i & -1 & -i \\ i & i & -1 & -i & 1 \\ -1 & -1 & -i & 1 & i \\ -i & -i & 1 & i & -1 \end{array}$$

(3) Pour commencer, un rappel: soient $(K, \star)$ et $(K', \star')$ deux groupes finis de même ordre (i.e. de même cardinal) n et

$$f : K \to K' : k_i \mapsto f(k_i) = k'_i,\ 1 \leq i \leq n,$$

une bijection. Par définition, f est un morphisme ssi

$$f(k_i \star k_j) = k'_i \star' k'_j,\ 1 \leq i, j \leq n.$$

En d'autres termes, f est un isomorphisme si et seulement si en remplaçant dans la table de K chaque k_i par k'_i on obtient la table de K'.

Voici la table de $\mathbf{Z}/4\mathbf{Z}$ pour l'addition:

$$\begin{array}{r|rrrr} + & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \overline{0} & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \overline{1} & \overline{1} & \overline{2} & \overline{3} & \overline{0} \\ \overline{2} & \overline{2} & \overline{3} & \overline{0} & \overline{1} \\ \overline{3} & \overline{3} & \overline{0} & \overline{1} & \overline{2} \end{array}$$

En comparant les tables de $\mathbf{Z}/4\mathbf{Z}$ et U_4 on voit que l'application

$$\overline{0} \mapsto 1, \quad \overline{1} \mapsto i, \quad \overline{2} \mapsto -1, \quad \overline{3} \mapsto -i$$

convient.

Remarquez que cet isomorphisme est un cas particulier du fait suivant: quelquesoit $n \in \mathbf{N} \setminus \{0\}$, l'application

$$\mathbf{Z}/n\mathbf{Z} \to U_n : \overline{l} \mapsto e^{\frac{2i\pi l}{n}}$$

est un isomorphisme de groupes.