Université Claude Bernard Lyon 1

MASTER M1-G

Algèbre

CORRECTION DE L'EXAMEN-2015

Exercice clef

On sait que $(\mathbb{Z}/8\mathbb{Z})^*$ est un groupe multiplicatif, il possède 4 éléments, 1, 3, 5 et 7. Comme 3 et 7 et 5 sont d'ordre 2, c'est le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Du coup tout nombre impair a, qui est donc premier avec 8, a sa classe dans $\mathbb{Z}/8\mathbb{Z}^*$. On a donc $\bar{a}^2 = 1$, d'où l'assertion.

Problème 1. Une équation de Mordell

A. *Etude de l'anneau A*

1. La première formule vient d'un calcul direct. Toutefois, on peut remarquer que α possède pour représentation complexe la matrice $\begin{pmatrix} 1/2 & \sqrt{11}/2 \\ -\sqrt{11}/2 & 1/2 \end{pmatrix}$ et utiliser Cayley-Hamilton.

   Pour montrer l'égalité, $\mathbb{Z}[\alpha] = \{a + b\alpha,\ a,\ b \in \mathbb{Z}\}$, on note que l'inclusion inverse est évidente. Maintenant, tout élément de $\mathbb{Z}[\alpha]$ s'écrit, par définition comme $P(\alpha)$, avec $P \in \mathbb{Z}[X]$. On peut effectuer la division euclidienne de P par le polynôme *unitaire* $X^2 - X + 3 = 0$. On obtient $P = Q(X^2 - X + 3) + a + bX$, et donc $P(\alpha) = a + b\alpha$ comme souhaité.
2. On a $N(a + b\alpha) = (a + b\alpha)(a + b\bar{\alpha}) = a^2 + ab(\alpha + \bar{\alpha}) + N(\alpha)b^2 = a^2 + ab + 3b^2$.

   Toute unité u de A vérifie $uu' = 1$ pour un u' de A. Si on remarque que $N(z) \in \mathbb{N}$ pour tout élément z de A, alors l'égalité $N(u)N(u') = N(uu') = 1$ prouve bien que $N(u) = 1$.

   Pour la réciproque, si $N(u) = 1$, alors $\bar{u}$ est un inverse de u et il est bien dans A car A est stable par conjugaison.

   Il reste à résoudre $a^2 + ab + 3b^2 = 1$. Cette égalité donne $(a + b/2)^2 + (11/4)b^2 = 1$, ce qui force $b = 0$ car $11/4 > 1$. Donc, $a^2 = 1$, ce qui donne le résultat.
3. On veut montrer que A est un anneau euclidien. On fixe $z = x + iy \in \mathbb{C}$.
   (a) Pour tout réel t, il existe un entier n tel que $|t - n| \leq 1/2$. On applique cela successivement à $\frac{2y}{\sqrt{11}}$ et ensuite à $x - \frac{n}{2}$.

   (b) On a $|z - m - n\alpha|^2 = \left|x - m - \frac{n}{2} + i(y - n\sqrt{11}/2\right|^2 = (x - m - \frac{n}{2})^2 + \frac{11}{4}(\frac{2y}{\sqrt{11}} - n)^2$.

   (c) C'est du cours : D'après ce qui précède, $N(z - m - n\alpha) \leq (1/2)^2 + 11/4(1/2)^2 = 1/4 + 11/16 = 15/16 < 1$ (ouf!). Soit donc w et w' dans A, avec w' non nul, alors, on pose $z = w/w'$, et $q = m + n\alpha$, avec m et n définis comme ci-dessus. Il vient $w = zw' = (q + z - q)w' = qw' + (z - q)w'$ et $N((z - q)w')N(z - q)N(w') < N(w')$. L'anneau A est bien euclidien.
4. $N(2) = 4$. Or, 2 ne peut pas s'écrire sous la forme $N(z)$ avec $z \in A$, car l'équation $(a + b/2)^2 + (11/4)b^2 = 2$ n'a pas de solution entière (on le voit facilement). On conclut

que 2 est irréductible dans A, car si 2 se réduit, forcément un des facteurs est de norme 1 donc inversible. Comme A est euclidien, donc *factoriel*, 2 est premier. Idem pour $-1+2\alpha$ qui vérifie $N(-1+2\alpha)=11$.

B. *Etude préliminaire de l'équation*

1. On réduit l'équation $y^2+11=x^3$ modulo 2. Si y est impair, alors $\bar{x}^3=\bar{0}$ et donc $\bar{x}=0$ dans le *corps* $\mathbb{Z}/2\mathbb{Z}$.

   On réduit donc modulo 8 et on obtient, par l'exercice clef que $1+11=0 \bmod 8$. Absurde. Donc, y ne peut être impair.
2. Si 11 divise y, alors 11 divise x^3, et par le *lemme d'Euclide*, 11 étant *premier*, 11 divise x. Mais du coup, 11^2 divise à la fois x^3 et y^2 et donc $y^2-x^3=11$. Absurde. Donc, 11 ne divise pas y.
3. Si δ divise $y+i\sqrt{11}$ et $y-i\sqrt{11}$ dans A, alors δ divise la différence $2i\sqrt{11}$ qui est dans A. Donc, $N(\delta)$ divise $N(2i\sqrt{11})=44$ dans $\mathbb{N}$.
4. On sait par l'indication de SAGE que si $N(a+b\alpha)$ divise 44, et distinct de 1, alors $a+b\alpha=\pm2, \pm(-1+2\alpha)$, ou $\pm2(-1+2\alpha)$. Comme δ, 2 et $(-1+2\alpha)$ sont premiers, le *lemme d'Euclide* dit que δ divise 2 ou $(-1+2\alpha)$ et donc δ est associé à 2 ou $(-1+2\alpha)$.

   Si 2 divise $y+i\sqrt{11}=y-1+2\alpha$ dans A, alors $y-1$ est pair et donc y est impair. Ce qui est absurde. De même, si $(-1+2\alpha)$ divise $y+i\sqrt{11}$ dans A, alors en prenant la norme, on voit que 11 divise y^2+11 et donc 11 divise y car 11 est premier dans $\mathbb{Z}$ *factoriel.* C'est encore une fois absurde d'après ce qui précède.
5. On vient de voir qu'il n'y a pas de premier qui divise simultanément $y+i\sqrt{11}$ et $y-i\sqrt{11}$. Ils sont donc premiers entre eux dans A.

C. *Résolution de l'équation*

1. Comme A est factoriel, le fait que $y+i\sqrt{11}$ et $y-i\sqrt{11}$ sont premiers entre eux et que leur produit est un cube implique que $y+i\sqrt{11}$ est un cube modulo unité, *i.e.* il existe z dans A tel que $y+i\sqrt{11}=uz^3$, avec u unité. Or, $-1=(-1)^3$, et comme les unités de A sont 1 ou -1, $y+i\sqrt{11}$ est un cube.
2. On identifie la partie imaginaire dans $y+i\sqrt{11}=(a+b\alpha)^3$. Cela donne après calcul $2=b(3a^2+3ab-2b^2)$. Cela implique que $b=\pm1$ ou ±2 car 2 est premier dans $\mathbb{Z}$ *factoriel.*
3. C'est juste du calcul en identifiant les parties réelles.
4. Idem.

Problème 2. Un cas particulier de la réciprocité quadratique

A. *Etude du polynôme* X^4+1 *sur* $\mathbb{F}_q$

1. Soit α une racine multiple de X^4+1 dans une extension de $\mathbb{F}_q$. Alors, $\alpha^4=-1$ et, en prenant la dérivée, $4\alpha^3=0$. Or, 4 est non nul dans le corps $\mathbb{F}_q$ car *q est impair.* Donc la dernière égalité implique $\alpha=0$, et donc $0=-1$, absurde.
2. Les éléments $\alpha, -\alpha$ sont clairement racines de X^4+1 et $\alpha^{-1}, -\alpha^{-1}$ également car -1 est son propre inverse.

   Reste à montrer qu'elles sont distinctes. On a clairement $\alpha\neq-\alpha$, sinon $2\alpha=0$ et comme *q impair*, $\alpha=0$ absurde. De même, $\alpha^{-1}\neq-\alpha^{-1}$. Montrons $\alpha\neq\alpha^{-1}$, ce qui prouvera également $-\alpha\neq-\alpha^{-1}$. Si, par l'absurde, $\alpha=\alpha^{-1}$, alors $\alpha^2=1$ et donc $\alpha=\pm1$. Or, $(\pm1)^4+1\neq0$ car *q est impair.*

3. (a) Comme q *est impair*, 8 divise $q^2 - 1$ qui est l'ordre du groupe multiplicatif $\mathbb{F}_{q^2}^*$.
   (b) Comme le groupe multiplicatif $\mathbb{F}_{q^2}^*$ est *cyclique*, on sait (réciproque de Lagrange dans le cas cyclique) que $\mathbb{F}_{q^2}^*$ possède un sous-groupe (forcément cyclique, c'est utile, et unique, mais c'est inutile) d'ordre 8. D'où l'existence de α'.
   (c) Comme α' est d'ordre 8 on a $(\alpha')^8 = 1$ et donc $((\alpha')^4 - 1)((\alpha')^4 + 1) = 0$. Comme on travalle dans un *corps*, il vient $(\alpha')^4 = 1$ ou $(\alpha')^4 = -1$. Mais la première égalité est impossible car α est d'ordre 8. D'où l'assertion.
4. D'après ce qui précède, comme α et α' sont racines, α s'écrit α', $-\alpha'$, α'^{-1} ou $-\alpha'^{-1}$, et donc α est dans $\mathbb{F}_{q^2}$ puisque α' est dans $\mathbb{F}_{q^2}$.
5. Si, par l'absurde, $X^4 + 1$ était irréductible sur $\mathbb{F}_q$, alors on aurait $\mathbb{F}_q(\alpha)$ de degré 4 sur $\mathbb{F}_q$. Or, manifestement, $\mathbb{F}_q(\alpha)$ est inclus dans $\mathbb{F}_{q^2}$ qui est de degré 2.

B. *Implication « 2 est un carré de* $\mathbb{F}_q \Longrightarrow q \equiv \pm 1$ *modulo* 8 »

1. On a $\alpha^5 = \alpha^4\alpha = -\alpha$. De plus, $\alpha^{-1} = \alpha^8\alpha^{-1} = \alpha^7$, et, du coup, $-\alpha^{-1} = -\alpha^7 = (-1)^{-1}\alpha^7 = \alpha^{-4}\alpha^7 = \alpha^3$. Voici pour la première assertion.

   L'élément α^q est l'image de α par le morphisme de *Frobenius*, qui laisse invariant $\mathbb{F}_q$ et donc le polynôme $X^4 + 1 \in \mathbb{F}_q[X]$. Conclusion, α^q est encore une racine de $X^4 + 1$.
2. L'égalité $\alpha^q = \alpha^n$ implique $\alpha^{q-n} = 1$ et donc 8 divise $q - n$, puisque α est d'ordre 8.
3. On a $\beta^2 = (\alpha + \alpha^{-1})^2 = \alpha^2 + 2 + \alpha^{-2} = \alpha^{4-2} + \alpha^{-2} + 2 = -\alpha^{-2} + \alpha^{-2} + 2 = 2$.

   L'autre racine est bien sûr son opposée $-\alpha - \alpha^{-1}$.
4. Si 2 est un carré de $\mathbb{F}_q$, alors β ou $-\beta$ est dans $\mathbb{F}_q$ et donc, dans les deux cas, β est dans $\mathbb{F}_q$. Ceci implique $\beta^q = \beta$.
5. On a $\beta^q = \beta$ et donc, par le Frobenius, $\alpha^q + \alpha^{-q} = \alpha + \alpha^{-1}$. Or, on sait que α^q est dans $\{\alpha, \alpha^3, \alpha^5, \alpha^{-1}\}$. Si on avait α^q égal à α^3 ou α^5, alors on aurait $\alpha^3 + \alpha^5 = \alpha + \alpha^{-1}$. Mézalors, $-\beta = \beta$, et donc $\beta = 0$, ce qui est absurde.

   Donc $\alpha^q = \alpha^{\pm 1}$. ce qui implique, par ce qui précède que q est congru à ± 1 modulo 8.

C. *Implication «* $q \equiv \pm 1$ *modulo* 8 $\Longrightarrow$ 2 *est un carré de* $\mathbb{F}_q$ »

1. Tout s'inverse très bien. Si q est congru à ± 1 modulo 8, alors, $\alpha^q + \alpha^{-q} = \alpha + \alpha^{-1}$ et donc $\beta^q = \beta$, ce qui prouve que β est dans $\mathbb{F}_q$ et 2 est un carré.
2. On sait que $p^2 - 1$ est toujours multiple de 8 puisque p est impair. De deux chose l'une, soit p est congru à ± 1 modulo 8, soit p est congru à ± 3 modulo 8. Dans le premier cas, on a d'une part (facilement) que $(p^2 - 1)/8$ pair, et d'autre part que 2 est un carré par ce qui précède. Dans le second cas, on a d'une part (facilement) que $(p^2 - 1)/8$ impair, et d'autre part que 2 n'est un carré par ce qui précède. Voilà ce que la formule de Gauss (et oui, c'est bien lui !) raconte.