Énoncés : V. Gritsenko
Corrections : J.-F. Barraud

Devoir à la maison et sujet de partiel

Exercice 1

Soit $\sqrt{d}$ non rationel. Dans l'anneau

$$\mathbb{Z}[\sqrt{d}] = \{n + m\sqrt{d} \,|\, n, m \in \mathbb{Z}\}$$

on definit la “conjugaison" $\bar{z}$:

$$\text{si } z = n + m\sqrt{d}, \text{ alors } \bar{z} = n - m\sqrt{d}.$$

On peut aussi définir la norme $N_d : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ par $N_d(z) = z\bar{z} = (n + m\sqrt{d})(n - m\sqrt{d})$.

0. Montrer que les aplications $\bar{z}$ et $N(z)$ sont multiplicatives :

$$\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2, \qquad N_d(z_1 \cdot z_2) = N_d(z_1) \cdot N_d(z_2).$$

Correction ▼ [002309]

Exercice 2

1. Montrer que $z \in \mathbb{Z}[\sqrt{d}]$ est inversible ssi $N_d(z) = \pm 1$. Déterminer les éléments inversibles de $\mathbb{Z}[\sqrt{-5}]$.
2. Montrer que si $N_d(z) = \pm p$, où p est un premier, alors z est irréductible dans $\mathbb{Z}[\sqrt{d}]$. Donner quelques exemples d'éléments irreductibles dans $\mathbb{Z}[\sqrt{d}]$ pour $d = -1$, 2, -6, p, où p un premier.
3. On note $A = \mathbb{Z}[\sqrt{-5}]$. Montrer que 3 et $2 + \sqrt{-5}$ sont irréductibles dans A.
4. Trouver tous les irréductibles de A de norme 9.
5. Trouver tous les diviseurs de 9 et de $3(2 + \sqrt{-5})$ dans l'anneau A à association près.
6. Trouver un *pgcd* $(3, 2 + \sqrt{-5})$, et montrer que 3 et $2 + \sqrt{-5}$ n'ont pas de *ppcm* dans l'anneau A.
7. Montrer que l'idéal $I = (3, 2 + \sqrt{-5}) \subset A$ n'est pas principal. Donc l'anneau A n'est pas principal. Est-il factoriel ?
8. Montrer que 9 et $3(2 + \sqrt{-5})$ n'ont pas de *pgcd* dans A. Possèdent-ils un *ppcm* ?

Correction ▼ [002310]

Exercice 3

Soit $\mathbb{Z}_{36} = \mathbb{Z}/36\mathbb{Z}$ l'anneau des entiers modulo 36.

1. Décrire tous les éléments inversibles, tous les diviseurs de zéro et tous les éléments nilpotents de l'anneau $\mathbb{Z}_{36}$. (*Un élément a d'un anneau A est dit nilpotent si il existe n tel que $a^n = 0$.*)
2. Trouver tous les idéaux de l'anneau $\mathbb{Z}_{36}$.
3. Soit A un anneau arbitraire. Montrer que

$$(a \in A^\times \text{ et } b \in A^\times) \iff (a \cdot b) \in A^\times.$$

4. Donner un exemple d'un polynôme inversible de degré 1 sur $\mathbb{Z}_{36}$.

5. Décrire tous les éléments inversibles de l'anneau $\mathbb{Z}_{36}[x]$.

Correction ▼ [002311]

Exercice 4

Montrer que les polynômes suivantes sont irréductibles dans $\mathbb{Z}[x]$:

1. $P = x^{2004} + 4x^{2002} + 2000x^4 + 2002$;
2. $Q = x^6 + 6x^5 + 12x^4 + 12x^3 + 3x^2 + 6x + 25$.

Correction ▼ [002312]

Exercice 5

Soit p un nombre premier impair. Montrer que la congruence
$x^2 \equiv -1 \mod p$ a une solution si et seulement si $p \equiv 1 \mod 4$.

Correction ▼ [002313]

Exercice 6

Soient $f = x^6 + x^5 + x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$, $g = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$ deux polynômes sur le corps $\mathbb{Z}_2$.

1. En utilisant l'algorithme d'Euclide trouver le p.g.c.d. de f et g et sa représentation linéaire.
2. Les polynômes f et g sont-ils irréductibles ?
3. Soit (g) l'idéal principal engendré par g. Combien d'éléments contient l'anneau quotient $A = \mathbb{Z}_2[x]/(g)$?
4. Soit $\pi : \mathbb{Z}_2[x] \to A$ la projection canonique. On pose $\pi(x) = \bar{x} \in A$. Trouver l'inverse de l'élément $\pi(f)$ dans l'anneau quotient A.
5. L'anneau quotient $B = \mathbb{Z}_2[x]/(f)$ est-il un corps ? Justifier la réponse, i.e. donner une démonstration si B est un corps ou trouver un élément non-inversible dans B dans le cas contraire.

Correction ▼ [002314]

Correction de l'exercice 1 ▲

Soit $z = n + m\sqrt{d}, z' = n' + m'\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Alors

$$\begin{aligned}\overline{zz'} &= \overline{(n+m\sqrt{d})(n'+m'\sqrt{d})} \\ &= \overline{(nn'+mm'd)+(nm'+n'm)\sqrt{d}} \\ &= (nn'+mm'd)-(nm'+n'm)\sqrt{d} \\ &= (n-m\sqrt{d})(n'-m'\sqrt{d}) \\ &= \bar{z}\bar{z}'\end{aligned}$$

Donc $\forall z, z' \in \mathbb{Z}[\sqrt{d}], \overline{zz'} = \bar{z}\bar{z}'$.
On a alors $\forall z, z' \in \mathbb{Z}[\sqrt{d}],\ N(zz') = zz'\overline{zz'} = z\bar{z}z'\bar{z}' = N(z)N(z')$.

Correction de l'exercice 2 ▲

1. – Si $z \in \mathbb{Z}[\sqrt{d}]$ est inversible :
   Alors $zz^{-1} = 1$, donc $N(z)N(z^{-1}) = 1$. Comme $N(z) \in \mathbb{Z}$ et $N(z^{-1}) \in \mathbb{Z}$, on a donc $N(z) \in \{1, -1\}$.
   – Si $N(z = \pm 1)$:
   Alors $z\bar{z} = \pm 1$, donc $z(\pm\bar{z}) = 1$. Comme $\pm\bar{z} \in \mathbb{Z}[\sqrt{d}]$, z est inversible.
2. Soient $z_1, z_2 \in \mathbb{Z}[\sqrt{d}]$ tels que $z = z_1 z_2$. Alors $N(z_1)N(z_2) = \pm p$. Comme $\pm p$ est irréductible sur $\mathbb{Z}$, on en déduit que $N(z_1) = \pm 1$ ou $N(z_2) = \pm 1$. D'après la question précédente, on a $z_1 \in \mathbb{Z}[\sqrt{d}]^\times$ ou $z_2 \in \mathbb{Z}[\sqrt{d}]^\times$: on en déduit que z est irréductible dans $\mathbb{Z}[\sqrt{d}]$.
   (Attention : p est premier donc irréductible dans $\mathbb{Z}$, mais peut être réductible dans $\mathbb{Z}[\sqrt{d}]$! cf. 2 dans $\mathbb{Z}[i]$.)
3. On a $N(3) = N(2+\sqrt{-5}) = 9$. On peut montrer en fait que tout élément z de norme 9 est irréductible : si $z = z_1 z_2$, alors $N(z_1)N(z_2) = 9$. Donc $\{N(z_1), N(z_2)\} = \{1, 9\}$ ou $\{3, 3\}$ (dans $\mathbb{Z}[\sqrt{-5}]$, la norme est toujours positive). Or pour tout $(n, m) \in \mathbb{Z}^2, n^2 + 5m^2 \neq 3$. En effet, si $|m| \geq 1, n^2 + 5m^2 \geq 5$ et pour $m = 0$, l'équation revient à $n^2 = 3$, qui n'a pas de solution entière. Ainsi, $N(z_1) = 1$ ou $N(z_2) = 1$, donc z_1 ou z_2 est inversible. z n'a donc pas de factorisation non triviale : z est irréductible dans $\mathbb{Z}[\sqrt{-5}]$. En particulier, 3 et $2+\sqrt{-5}$ le sont.
4. Tout élément de A de norme 9 est irréductible. Il suffit donc de trouver tous les éléments de norme 9. Soit $z = n + m\sqrt{-5} \in A$. Si $|m| \geq 2$ ou $|n| \geq 4$, alors $N(z) > 9$. On cherche donc les éléments de norme 9 parmi les éléments $z = n + m\sqrt{-5}$ avec $|n| \leq 3$ et $|m| \leq 1$. Pour $m = 0$, les seules solutions sont $n = \pm 3$, pour $|m| = 1$, les solutions sont obtenues pour $|n| = 2$. Ainsi :
   $$\forall z \in A : \quad N(z) = 9 \Leftrightarrow z \in \{\pm 3, \pm(2 \pm \sqrt{5})\}$$
5. On a $N(9) = 81$. Donc si $9 = z_1 z_2$ est une factorisation de 9 dans A, $N(z_1)N(z_2)$ est une factorisation de 81 (dans $\mathbb{Z}$), et plus précisément on a $\{N(z_1), N(z_2)\} \in \Big\{\{1, 81\}, \{3, 27\}, \{9, 9\}\Big\}$.
   Si $N(z_1) = 1$ ou $N(z_2) = 1$, la factorisation est triviale.
   A n'a pas d'élément de norme 3 donc la paire $\{3, 27\}$ n'est pas réalisable.
   Si enfin $N(z_1) = N(z_2) = 9$, alors $z_1, z_2 \in \{\pm 3, \pm(2 \pm \sqrt{5})\}$. Comme $9 = 3 \cdot 3 = (2+\sqrt{-5})(2-\sqrt{-5})$, tous ces éléments sont diviseurs de 9.
   Les diviseurs de 9 sont donc $\{\pm 1, \pm 3, \pm(2 \pm \sqrt{-5}), \pm 9\}$.

   Comme $N(3(2+\sqrt{-5})) = 81$, le même raisonnement montre que si $d \in A$ divise $3(2+\sqrt{-5})$, alors $d \in \{\pm 1, \pm 3, \pm(2 \pm \sqrt{-5}), \pm 3(2 \pm \sqrt{-5})\}$.
   Si $(2-\sqrt{-5})a = 3(2+\sqrt{-5})$, alors $N(a) = 9$, donc $a = \pm 3$ ou $\pm(2 \pm \sqrt{-5})$. Comme A est intègre, si $a = \pm 3$, on obtient $2 - \sqrt{-5} = \pm(2+\sqrt{-5})$, ce qui est faux. Si $a = \pm(2+\sqrt{-5})$, on obtient $2 - \sqrt{-5} = \pm 3$, ce qui est faux. Si enfin $a = \pm(2-\sqrt{-5})$, on obtient $\pm(-1-4\sqrt{-5}) = 6 + 3\sqrt{-5})$, ce qui est encore faux. Donc $2 - \sqrt{-5}$ ne divise pas $3(2+\sqrt{-5})$ dans A. Tous les autres éléments de norme 9 divisent $3(2+\sqrt{-5})$, donc, finalement :

Les diviseurs de $3(2+\sqrt{-5})$ sont $\{\pm1,\pm3,\pm(2+\sqrt{-5}),\pm3(2+\sqrt{-5})\}$.

(Attention : Le seul fait que 3 et $2+\sqrt{-5}$ soient irréductibles ne permet pas de conclure ! Si l'anneau n'est pas factoriel, un produit d'irréductibles p_1p_2 peut avoir d'autres diviseurs (à association près) que p_1 et p_2... cf $3\cdot3=(2+\sqrt{-5})(2-\sqrt{-5})$!)

6. On connaît la liste des diviseurs de 3 et de $2+\sqrt{-5}$. Les seuls qui soient communs sont 1 et -1. On en déduit que 1 est un pgcd de 3 et $2+\sqrt{-5}$.

   9 et $3(2+\sqrt{-5})$ sont des multiples communs de 3 et $2+\sqrt{-5}$, donc si ces deux éléments admettent un ppcm m, on a $m|9$ et $m|3(2+\sqrt{-5})$. On connaît la liste des diviseurs de 9 et $3(2+\sqrt{-5})$: à association près, on en déduit que $m\in\{1,3,2+\sqrt{-5}\}$. Comme $3|m$, la seule possibilité est $m=3$, et comme $(2+\sqrt{-5})|m$, la seule possibilité est $m=2+\sqrt{-5}$. Il y a donc contradiction :

   3 et $2+\sqrt{-5}$ n'ont pas de ppcm dans A.

7. Supposons I principal : soit $a\in A$ un générateur : $I=(a)$. Alors a est un diviseur commun à 3 et $2+\sqrt{-5}$, donc $a=\pm1$. (En particulier, $I=A$). Soient $u=u_1+u_2\sqrt{-5}$ et $v=v_1+v_2\sqrt{-5}$ deux éléments de A. On a :

$$\begin{aligned}3u+(2+\sqrt{-5})v=1 &\Leftrightarrow (3u_1+2v_1-5v_2)+(3u_2+v_1+2v_2)\sqrt{-5}=1\\ &\Leftrightarrow \begin{cases}3u_1+2v_1-5v_2 &=1\\ 3u_2+v_1+2v_2 &=0\end{cases}\\ &\Rightarrow \begin{cases}-v_1+v_2 &\equiv 1[3]\\ v_1-v_2 &\equiv 0[3]\end{cases}\end{aligned}$$

   Donc $\forall u,v\in A,\ 3u+(2+\sqrt{-5})v\neq1$. Donc $1\notin I$, ce qui est une contradiction : I n'est pas principal.

   L'anneau A n'est pas principal puisqu'il a au moins un idéal non principal. Il n'est pas non plus factoriel, puisque $9=3\,3=(2+\sqrt{-5})(2-\sqrt{-5})$ admet deux factorisation en irréductibles non équivalentes à association près.

8. – Les diviseurs communs de 9 et $3(2+\sqrt{-5})$ sont $\{\pm1,\pm3,\pm(2+\sqrt{-5})\}$. Si 9 et $3(2+\sqrt{-5})$ admettent un pgcd d, alors d est dans cette liste, et divisible par tous les membre de cette liste. Mais 3 n'est pas divisible par $2+\sqrt{-5}$ et $2+\sqrt{-5}$ ne divise pas 3 : 9 et $2+\sqrt{-5}$ n'ont pas de pgcd.
   – Supposons que 9 et $3(2+\sqrt{-5})$ admettent un ppcm M. Alors il existe des éléments $a,b\in A$ tels que $M=9a=3(2+\sqrt{-5})b$. Notons $m=3a=(2+\sqrt{-5})b$ (A est intègre).
     m est un multiple commun de 3 et $2+\sqrt{-5}$.
     Soit k un multiple commun de 3 et $2+\sqrt{-5}$. Alors $3k$ est un multiple commun de 9 et $3(2+\sqrt{-5})$, donc $M|3k$: $\exists c\in A, 3k=Mc=3mc$. On en déduit que $k=mc$ (A est intègre), donc $m|k$. On en déduit que m est un ppcm de 3 et $2+\sqrt{-5}$, ce qui est impossible.

Correction de l'exercice 3 ▲

1. $\bar n$ est inversible ssi $\mathrm{pgcd}(n,36)=1$ (Bezout !), i.e. $\bar n\in\{\pm1,\pm5,\pm7,\pm11,\pm13,\pm17\}$. Les autres éléments sont tous des diviseurs de 0 puisque $\bar n$ divise 0 ssi $\mathrm{pgcd}(n,36)\neq1$. Enfin, $\bar n$ est nilpotent ssi $2|n$ et $3|n$, donc ssi $6|n$, soit $\bar n\in\{0,\pm6,\pm12,18\}$.

2. Montrons que l'ensemble $\mathscr{I}$ des idéaux de $\mathbb{Z}/36\mathbb{Z}$ est en bijection avec l'ensemble $\mathscr{D}=\{1,2,3,4,6,9,12,18,36\}$ des diviseurs (positifs) de 36.

   Considérons l'application $\phi:\mathscr{D}\to\mathscr{I}$ définie par $\phi(d)=(\bar d)$.

   Injectivité : Si $\phi(d)=\phi(d')$, alors $\exists a,b\in\mathbb{Z}, d=d'a+36b$. Comme $d|36$, on en déduit que $d|d'$. De même, on a $d'|d$, et donc $d=d'$.

   *Surjectivité :*Soit $I\in\mathscr{I}$. $\mathbb{Z}/36\mathbb{Z}$ est principal, donc $\exists a\in\mathbb{Z}, I=(\bar a)$. Soit $d=\mathrm{pgcd}(a,36)$. Notons $a=da'$: $\mathrm{pgcd}(a',36)=1$. On en déduit que $\bar a'$ est inversible dans $\mathbb{Z}/36\mathbb{Z}$. Alors $\bar d\sim\bar a$ dans $\mathbb{Z}/36\mathbb{Z}$. On en déduit que $I=(\bar d)=\phi(d)$.

   Finalement, il y a donc 9 idéaux dans $\mathbb{Z}_{36}$:
   – $(\bar 1)=\mathbb{Z}_{36}$,
   – $(\bar 2)=\{0,\pm2,\pm4,\pm6,\pm8,\pm10,\pm12,\pm14,\pm16,18\}$,

– $(\bar{3}) = \{0, \pm 3, \pm 6, \pm 9, \pm 12, \pm 15, 18\}$,
– $(\bar{4}) = \{0, \pm 4, \pm 8, \pm 12, \pm 16\}$,
– $(\bar{6}) = \{0, \pm 6, \pm 12\}$
– $(\bar{9}) = \{0, \pm 9, 18\}$
– $(\overline{12}) = \{0, \pm 12\}$
– $(\overline{18}) = \{0, 18\}$
– $(\overline{36}) = \{0\}$,

3. Si $a, b \in A^\times$, alors $(ab)(b^{-1}a^{-1}) = 1$ donc $ab \in A^\times$.
   Si $ab \in A^\times$, soit $c = (ab)^{-1}$. Alors $a(bc) = 1$ donc $a \in A^\times$ et $b(ac) = 1$ donc $b \in A^\times$.
4. On a $(6x+1)(-6x+1) = 1$ dans $\mathbb{Z}_{36}[x]$, donc $18x+1$ y est inversible.
5. Soit f un inversible de $\mathbb{Z}_{36}[x]$. Choisissons $P \in \mathbb{Z}[x]$ tel que $\bar{P} = f$ et $Q \in \mathbb{Z}[x]$ tel que $\bar{Q} = f^{-1}$.
   La projection $\mathbb{Z} \to \mathbb{Z}_2$ se factorise par $\mathbb{Z} \to \mathbb{Z}_{36} \to \mathbb{Z}_2$. Ces projections sont bien définies, et sont des morphismes d'anneaux. Notons $P_{[2]}$ la réduction de P modulo 2 : on a alors $P_{[2]}Q_{[2]} = (PQ)_{[2]} = 1$, et comme $\mathbb{Z}_2$ est un corps, $P_{[2]} = 1$, $Q_{[2]} = 1$. On en déduit que 2 divise tous les coefficients de P, sauf celui de degré 0. De même, en considérant la réduction modulo 3, on obtient que 3 divise tous les coefficients de P, sauf celui de degré 0. Finalement, 6 divise tous les coefficients de P sauf celui de degré 0, qui est inversible modulo 36 : à association (dans $\mathbb{Z}_{36}$) près, f est donc de la forme :

$$f = \sum_{i=1}^{d} 6a_i x^i + 1, \qquad (a_i) \in \mathbb{Z}_{36}.$$

   Réciproquement, si f est de cette forme, c'est à dire $f = 1 + 6xf_1$, avec $f_1 \in \mathbb{Z}_{36}[x]$, alors :

$$(1+6xf_1)(1-6xf_1) = 1$$

   donc f est inversible.

Correction de l'exercice 4 ▲

1. Le critère d'Eisenstein avec 2 pour module donne directement le résultat.
2. La réduction modulo 2 de Q est $Q_{[2]} = x^6 + x^2 + 1$, qui n'a pas de racine, et n'est pas divisible par x^2+x+1, le seul irréductible de degré 2 de $\mathbb{Z}_2[x]$. Ainsi, $Q_{[2]}$ est soit irréductible, auquel cas Q l'est aussi sur $\mathbb{Z}$, soit le produit de deux irréductibles de degré 3.
   Si $Q_{[2]}$ n'est pas irréductible, on considère la réduction modulo 3 de Q : $Q_{[3]} = x^6 + 1 = (x^2+1)^3$. x^2+1 est irréductible sur $\mathbb{Z}_3$, car il est de degré 2 et n'a pas de racine. Soit $Q = RS$ une factorisation non triviale de Q sur $\mathbb{Z}$. On peut supposer R et S unitaires. Alors, en considérant la réduction modulo 2, on obtient que $R_{[2]}$ et $S_{[2]}$ sont deux irréductibles de degré 3 de $\mathbb{Z}_2[x]$. En particulier $\deg(R) = \deg(R_{[2]}) = 3$ (car R est unitaire) et $\deg(S) = \deg(S_{[2]}) = 3$. Cependant, la réduction modulo 3 de Q n'admet pas de factorisation suivant deux polynômes de degré 3. C'est une contradiction : on en déduit que Q n'a pas de factorisation non triviale.

Correction de l'exercice 5 ▲

Soit p un nombre premier impair. Notons $p = 2m+1$. On a

$$(m!)^2 \equiv (-1)^{m+1} [p]$$

en effet, (modulo p) :

$$\begin{aligned}(p-1)! &= \prod_{k=1}^{2m} k = m! \prod_{k=1}^{m} (m+k) \\ &= m! \prod_{k=1}^{m} (m+k-p) = m! \prod_{k=1}^{m} (-k) \\ &= (-1)^m (m!)^2\end{aligned}$$

Or, dans $\mathbb{Z}_p[x]$, $1^{-1}=1$ et $(p-1)^{-1}=p-1$, donc $\forall k\in\{2,\dots,p-2\}$, $k^{-1}\in\{2,\dots,p-2\}$. Ainsi, $\prod_{k=2}^{p-1}k\equiv 1[p]$, et donc $(p-1)!\equiv -1[p]$. D'où le résultat.

– Si $p\equiv 1[4]$, $(-1)^{m+1}=-1$, et donc $m!$ est une solution de $x^2\equiv -1[p]$.
– Si cette équation a une solution, alors $x^{2m}\equiv 1[p]$, et comme $x^{p-1}\equiv 1[p]$, $1\equiv(-1)^m[p]$. On en déduit que m est pair, donc $p\equiv 1[4]$.

Correction de l'exercice 6 ▲

1.
$$f=g(x^3+x+1)+(x^2+x)$$
$$g=(x^2+x)x+1$$

donc $\mathrm{pgcd}(f,g)=1$ et

$$1=g-(x^2+x)x=g-(f-g(x^3+x+1))x=(x^4+x^2+x+1)g-xf$$

2. $f=(x^4+x+1)(x^2+x+1)$ donc f n'est pas irréductible.
   g est de degré 3 et n'a pas de racine, donc g est irréductible.
3. Les éléments de A sont en bijection avec les polynômes de $\mathbb{Z}_2[x]$ de degré $<\deg(g)=3$. Il y a 8 polynômes de degré au plus 2 sur $\mathbb{Z}_2$, donc A a 8 éléments.
4. On utilise la représentation linéaire $uf+vg=1$ de $\mathrm{pgcd}(f,g)$ obtenue plus haut. $uf=1+vg$, donc $\bar{u}\bar{f}=\bar{1}+\bar{0}=\bar{1}$. Donc $(\bar{f})^{-1}=\bar{u}=\bar{x}$.
5. Soit $f_1=x^2+x+1$ et $f_2=x^4+x+1$. Alors $f_1f_2=f$ donc $\bar{f_1}\bar{f_2}=\bar{0}$. Pourtant, f ne divise ni f_1 ni f_2, donc $\bar{f_1}\neq\bar{0}$ et $\bar{f_2}\neq\bar{0}$: B n'est pas intègre, donc B n'est pas un corps.
