Université Mohammed V-Rabat
Faculté des Sciences

`Filière SMA-Module: Algèbre 6`

Contrôles Finaux, Rattrapages et Solutions

D. Bennis, A. Cherrabi

Département de Mathématiques

Année Universitaire 2018/2019

Enoncés des Contrôles Continus, Contrôles Finaux et Rattrapages

Module : Algèbre 6
Contrôle Continu 2015-2016

Exercice 1. *On considère le groupe multiplicatif* $\mathcal{U}(17)$.

1) Calculer l'ordre de $\overline{3}$ *et en déduire que* $\mathcal{U}(17)$ *est cyclique.*

2) Déterminer les sous-groupes de $\mathcal{U}(17)$.

3) Déterminer les générateurs de $\mathcal{U}(17)$.

4) Déterminer les isomorphismes de groupes définis de $\mathbb{Z}_{16}$ *vers* $\mathcal{U}(17)$.

Exercice 2. *On considère le sous-groupe* $G = \{e, \sigma, \sigma^2, \sigma^3, \rho, \rho^3, \sigma\rho, \rho\sigma\}$ *de* S_8, *où* $\sigma = (1234)(5678), \rho = (1537)(2846) \in S_8$.

1) calculer σ^2, ρ^2, $\rho\sigma$ *et* $\rho\sigma^3$.

2) Déterminer les éléments de $H =< \sigma^2 >$.

3) Déterminer $(G/H)_g$ *et* $(G/H)_d$ *et en déduire que* G/H *est un groupe.*

4) G/H *est-il cyclique ? A quel groupe classique est-il isomorphe ?*

Contrôle Final 2015-2016

Exercice 3. *Soit* (A, δ) *un anneau euclidien qui n'est pas un corps. On pose* $\widetilde{A} = \mathcal{U}(A) \cup \{0\}$ *et* $N = \{\delta(a)/a \in A \setminus \widetilde{A}\}$.

1) Montrer que N *possède un plus petit élément. Le plus petit élément de* N *est noté* $\delta(u)$, *où* u *est un élément de* $A \setminus \widetilde{A}$.

2) Montrer que $\forall x \in A$, $\exists r \in \widetilde{A}$ *tel que* u *divise* $x - r$.

Exercice 4. *On considère l'anneau* $A = \mathbb{Z}[i\sqrt{11}] = \{a + ib\sqrt{11}/a, b \in \mathbb{Z}\}$.

1) Déterminer $\mathcal{U}(A)$.

2) Montrer que 2 *et* $1 + i\sqrt{11}$ *sont irréductibles dans* A.

3) Montrer que A *n'est pas principal.*

Exercice 5.

1) Montrer que $p(X) = X^3 + X + \overline{1}$ *est irréductible dans* $\mathbb{Z}_5[X]$.

2) On considère l'homomorphisme d'anneaux $g : \mathbb{Z}[X] \to \mathbb{Z}_5[X]$, $\sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} \overline{a_i} X^i$. *Montrer que* $\ker g = 5\mathbb{Z}[X]$.

3) *Soit* $I = (p(X))$ *l'idéal de* $\mathbb{Z}_5[X]$ *engendré par* $p(X)$ *et l'homomorphisme* $f = s \circ g$, *où* s *est la surjection canonique* $s : \mathbb{Z}_5[X] \to \mathbb{Z}_5[X]/I$.

   a) *Vèrifier que l'homomorphisme* f *est surjectif.*

   b) *Montrer que* $\ker f = J$, *où* $J = (q(X), 5) = q(X)\mathbb{Z}[X] + 5\mathbb{Z}[X]$ *est l'idéal de* $\mathbb{Z}[X]$ *engendré par* $q(X) = X^3 + X + 1$ *et* 5.

   c) *Montrer que* $\mathbb{Z}[X]/J$ *est un corps.*

Rattrapage 2015-2016

Exercice 6. *On considère l'anneau* $A = \{\frac{a+ib\sqrt{3}}{2}/a, b \in \mathbb{Z} \text{ et } a \equiv b\,(mod\,2)\}$.

1) *Montrer que* $\mathcal{U}(A) = \{1, -1, \frac{1+i\sqrt{3}}{2}, \frac{-1+i\sqrt{3}}{2}, \frac{1-i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\}$.

2) *Calculer l'ordre de* $\frac{1+i\sqrt{3}}{2}$ *considéré comme élément du groupe* $\mathcal{U}(A)$. $\mathcal{U}(A)$ *est-il cyclique ?*

3) *Déterminer tous les isomorphismes de* $\mathbb{Z}_6$ *vers* $\mathcal{U}(A)$.

Exercice 7.

1) *On considère le polynôme* $p(X) = X^5 + X^2 + 1 \in \mathbb{Z}_2[X]$.

   a) *Montrer que si* $p(X)$ *n'est pas irréductible dans* $\mathbb{Z}_2[X]$, *alors il existe un polynôme* $q(x) \in \mathbb{Z}_2[X]$ *de degré* 1 *ou* 2 *tel que* $q(X)$ *divise* $p(X)$.

   b) *Montrer que* $p(X)$ *n'a pas de diviseurs de degré* 1 *dans* $\mathbb{Z}_2[X]$.

   c) *Montrer que* $X^2 + X + 1$ *ne divise pas* $p(X)$ *dans* $\mathbb{Z}_2[X]$. *En déduire que* $p(X)$ *n'a pas de de diviseur de degré* 2 *dans* $\mathbb{Z}_2[X]$. *Conclure.*

2) *Montrer que* $\mathbb{Q}[X]/(X^5 + 8X^4 + 6X^3 + X^2 + 10X + 5)$ *est un corps.*

Exercice 8. *Soit* K *un corps (commutatif) et* $A = \{P(X) \in K[X]/P(X) = a_0 + a_2X^2 + \cdots + a_nX^n$, *avec* $n \in \mathbb{N}\}$, *i.e., A est l'ensemble des polynômes* $P(X)$ *élément* $K[X]$ *dont le coefficient de* X *est nul.*

1) *Montrer que* A *est un sous-anneau de* $K[X]$.

2) *Déterminer* $\mathcal{U}(A)$.

3) *Montrer que* X^2 *et* X^3 *sont irréductibles dans* A.

4) A *est-il principal ?*

Contrôle Continu 2016-2017

Exercice 9.

I) *Soit* $H =< a >$ *un sous-groupe d'un groupe* $(G, .)$. *Montrer que si* $\forall x \in G, xax^{-1}$, *alors* H *est distingué dans* G.

II) On considère le groupe multiplicatif $G = \{\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{0} & \overline{1} \end{pmatrix} / \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{0} & \overline{1} \end{pmatrix} \in GL_2(\mathbb{Z}_5)\}$.

1) Montrer que G n'est pas cyclique.

2) Soit $A = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}$. *Calculer l'ordre de A.*

3) Montrer que $H = \{\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{2} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{3} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{4} \\ \overline{0} & \overline{1} \end{pmatrix}\}$ *est un sous-groupe distingué de G.*

4) a) Déterminer G/H.

b) Montrer que $G/H \simeq \mathbb{Z}_4$.

Exercice 10. *On considère le groupe quotient $(G = \mathbb{Q}/\mathbb{Z}, +)$.*

1) Montrer que si $\overline{x} \in G$, alors $\circ(\overline{x})$ est fini.

2) a) Soit $n \in \mathbb{N}^\star$ et $H_n =< \frac{\overline{1}}{n} >$. Montrer que $|H_n| = n$.

b) Montrer que si K est un sous-groupe cyclique de G d'ordre n, alors $K = H_n$.

c) Déterminer tous les isomorphismes de $\mathbb{Z}_6$ dans H_6.

3) Soit $n \in \mathbb{N}^\star$. On considère la correspondance $f : G \to G$, $\overline{x} \mapsto n\overline{x}$.

a) Vérifier que f est un endomorphisme surjectif de G.

b) Montrer que $G/H_n \simeq G$.

c) En déduire que G est infini.

Contrôle Final/2016-2017

Exercice 11. *Soit $r \in \mathbb{R}^\star$ tel que $r + \frac{1}{r}$ est un entier impair.*

1) Montrer qu'il existe $p(X) = X^2 - nX + 1 \in \mathbb{Z}[X]$, où n est un entier impair, tel que r est une racine de $p(X)$ et $p(X)$ est irréductible sur $\mathbb{Q}$.

2) En déduire que r est irrationnel.

Exercice 12.

Soit p un nombre premier. On considère l'anneau commutatif unitaire $(\mathbb{Z}_p[i] = \{\overline{a} + i\overline{b}/\overline{a}, \overline{b} \in \mathbb{Z}_p\}, +, .)$, où l'addition et la multiplication sont définies respectivement par $(\overline{a} + i\overline{b}) + (\overline{c} + i\overline{d}) = (\overline{a+c}) + i(\overline{b+d})$ et $(\overline{a} + i\overline{b}).(\overline{c} + i\overline{d}) = (\overline{ac - bd}) + i(\overline{ad + bc})$. On admet que si $(\overline{a} + i\overline{b}) = \overline{0}$, alors $\overline{a} = \overline{b} = \overline{0}$.

On rappelle que :

— $\mathbb{Z}[i]$ *est un anneau* ***principal***,
— $\mathcal{U}(\mathbb{Z}[i]) = \{-1, 1, i, -i\}$.

1) a) *Montrer que s'il existe* $x, y \in \mathbb{Z}$ *tels que* $p = x^2 + y^2$, *alors* p *n'est pas irréductible dans* $\mathbb{Z}[i]$.

   b) *Montrer que* p *est irréductible dans* $\mathbb{Z}[i]$ *si, et seulement si,* $p \neq x^2+y^2$, $\forall x, y \in \mathbb{Z}$.

2) *On considère l'application* $f : \mathbb{Z}[i] \to \mathbb{Z}_p[i]$, $a + ib \mapsto \overline{a} + i\overline{b}$, *où* $a, b \in \mathbb{Z}$.

   a) *Vérifier que* f *est un homomorphisme d'anneaux surjectif.*

   b) *Montrer que* $\ker f = (p)$, *où* (p) *et l'idéal de* $\mathbb{Z}[i]$ *engendré par* p.

   c) *Montrer que* $\mathbb{Z}_p[i]$ *est un corps si, et seulement si,* $p \neq x^2 + y^2$, $\forall x, y \in \mathbb{Z}$.

   d) i) *Montrer que* $\mathbb{Z}_7[i]$ *est un corps.*

      ii) $\mathbb{Z}_5[i]$ *est-il un corps ? est-il intègre ?*

Exercice 13. *On considère le groupe multiplicatif* $((\mathbb{Z}_p)^\star, .)$, *où* p *est un nombre premier différent de* 2, *et l'application* $f : \mathbb{Z}_p^\star :\to \mathbb{Z}_p^\star$, $\overline{x} \mapsto \overline{x}^2$.

1) *Vérifier que* f *est un homomorphisme de groupes.*

2) *Montrer que* $\ker f = \{\overline{-1}, \overline{1}\}$.

3) *En déduire que* $[\mathbb{Z}_p^\star : \operatorname{Im} f] = 2$. f *est-il surjectif ?.*

4) *Soit* $\overline{r} \in \mathbb{Z}_p^\star$. *On suppose que* $\overline{-1}, \overline{r} \notin \operatorname{Im} f$.

   a) *Dire pourquoi* $\overline{-1} \operatorname{Im} f = \overline{r} \operatorname{Im} f$.

   b) *Montrer qu'il existe* $\overline{a} \in \mathbb{Z}_p^\star : \overline{a}^2 = \overline{-r}$.

Rattrapage/2016-2017

Exercice 14. *Soit* G *un groupe monogène tel que* G *possède exactement* 3 *sous-groupes distincts :* $\{e\}, G$ *et un sous-groupe* H *d'ordre* p, *où* e *est l'élément neutre de* G *et* p *est un nombre premier.*

1) *Montrer que* G *est cyclique.*

2) *Montrer que* $|G| \neq p$.

3) *Montrer que* $G \simeq \mathbb{Z}_{p^2}$.

Exercice 15. *Soit* $p(X) = X^3 + 9X + 6 \in \mathbb{Q}[X]$.

1) *Montrer que* $p(X)$ *est irréductible dans* $\mathbb{Q}[X]$.

2) *En déduire que* $\mathbb{Q}[X]/ < p(X) >$ *est un corps.*

3) *Montrer que* $1 + X$ *et* $p(X)$ *sont premiers entre eux dans* $\mathbb{Q}[X]$.

4) En déduire que $\overline{1+X}$ *est inversible dans* $\mathbb{Q}[X]/ < p(X) >$.

5) Déterminer l'inverse de $\overline{1+X}$ *dans* $\mathbb{Q}[X]/ < p(X) >$.

Exercice 16. *On considère l'anneau* $A = \mathbb{Z}[i\sqrt{3}] = \{a + ib\sqrt{3}/a, b \in \mathbb{Z}\}$ *et l'application* $f : A = \mathbb{Z}[i\sqrt{3}] \to \mathbb{Z}_4$, $a + ib\sqrt{3} \mapsto \overline{a+3b}$.

1) Montrer que f *est un homomorphisme d'anneaux surjectif.*

2) a) Déterminer $\mathcal{U}(A)$.

b) Montrer que $1 + i\sqrt{3}$ *est irréductible dans* A.

c) Montrer que $4 \in < 1 + i\sqrt{3} >$ *et en déduire que* $\ker f =< 1 + i\sqrt{3} >$.

d) Montrer que l'idéal $< 1 + i\sqrt{3} >$ *de* A *n'est pas maximal.*

e) L'anneau A *est-il principal ?*

Contrôle Continu 2017-2018

Exercice 17. *Soit* $(G, .)$ *un groupe,* $a \in G$ *d'ordre fini* n *et* H *un sous-groupe distingué de* G *d'indice* m. *Montrer que si* m *et* n *sont premiers entre eux, alors* $a \in H$.

Exercice 18. *On considère* $G = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} /(a, c) \in (\mathbb{R}^\star)^2, b \in \mathbb{R}\}$.

1) Montrer que G *est un sous-groupe de* $GL_2(\mathbb{R})$.

2) On considère l'application $f : G \to (\mathbb{R}^\star)^2$, $\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$.

a) Montrer que f *est un morphisme de groupes.*

b) Montrer que $H = \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} /b \in \mathbb{R}\}$ *est un sous-groupe distingué de* G *et que* G/H *et* $(\mathbb{R}^\star)^2$ *sont isomorphes.*

Exercice 19. *On considère le sous-groupe* $G = \{e, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3, \tau\sigma^4, \tau\sigma^5\}$ *de* S_6, *où* $\sigma = (123456)$ *et* $\tau = (15)(24)$.

1) G est-il cyclique ?

2) Calculer les ordres de σ *et* τ *et calculer* $\sigma\tau\sigma$ *en fonction de* τ.

3) En déduire que $\tau\sigma^2 = \sigma^4\tau$ *et* $\tau\sigma^4 = \sigma^2\tau$.

4) On considère le sous-groupe $H =< \sigma^2 >$ *de* G. *Déterminer l'ordre de* H *et donner tous les générateurs de* H.

5) Déterminer $(G/H)_g$ *et* $(G/H)_d$ *et en déduire que* G/H *est un groupe.*

6) G/H *est-il cyclique ? A quel groupe classique est-il isomorphe ?*

Contrôle Final 2017-2018

Exercice 20. *Montrer que* $P(X) = 21x^3 - 3x^2 + 2x + 9$ *est irréductible dans* $\mathbb{Q}[X]$.

Exercice 21. *On considère l'application* $f : \mathbb{Z}[i] \to \mathbb{Z}_2$, $a + ib \mapsto \overline{a - b}$, *où* $a, b \in \mathbb{Z}_2$.

1) Montrer que f *est un morphisme d'anneaux.*

2) En déduire que $I = \{a+ib / a, b \in \mathbb{Z} \text{ et } a \equiv b \pmod 2\}$ *est un idéal maximal de* $\mathbb{Z}[i]$.

Exercice 22. *Soit* $(G, .)$ *un groupe et* H *un sous-groupe distingué de* G *tel que pour tout sous-groupe* $K \neq \{e\}$, $H \cap K \neq \{e\}$.

1) Montrer que tout élément du groupe G/H *est d'ordre fini.*

2) Soit x *un élément de* G *d'ordre un nombre premier* p.

a) Déterminer tous les générateurs de $< x >$.

b) Montrer que $x \in H$.

Exercice 23. *On considère le sous-anneau* $A = \{P(X) \in \mathbb{Q}[X] / \widetilde{P}(0) \in \mathbb{Z}\}$ *de* $\mathbb{Q}[X]$, *où* $\widetilde{P}$ *est la fonction polynômiale associée à* $P(X)$.

1) Vérifier que $\mathcal{U}(A) = \{-1, 1\}$.

2) Soit $P(X) = p$, *où* p *est un nombre premier dans* $\mathbb{Z}$.

a) Montrer que $P(X)$ *est irréductible dans* A.

b) $P(X)$ *est-il irréductible dans* $\mathbb{Q}[X]$ *?*

3) Soit un entier $n \geq 1$ *et* $P(X) = X^n - 2$.

a) Montrer que $P(X)$ *est irréductible dans* $\mathbb{Q}[X]$ *?*

b) $P(X)$ *est-il irréductible dans* A *?*

4) Pour tout $n \in \mathbb{N}^\star$, *on note* $I_n = (\frac{1}{2^n}X)$ *l'idéal de* A *engendré per* $\frac{1}{2^n}X$.

a) Montrer que $\forall n \in \mathbb{N}$, $I_n \subsetneq I_{n+1}$.

b) A *est-il euclidien ?*

Rattrapage 2017-2018

Exercice 24. *Montrer que* $P(X) = X^4 + 2X - 1$ *est irréductible dans* $\mathbb{Q}[X]$ *(Ind : calculer* $P(X + 1)$*).*

Exercice 25. *On considère L'anneau quotient* $A = \mathbb{Z}[i] / < 1 + 2i >$.

1) Montrer que $\overline{-3} = \overline{i}$.

2) Montrer que $A = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

3) L'idéal $< 1 + 2i >$ *est-il maximal ?*

Exercice 26. *Soit* $(G =< x >, .)$ *un groupe monogène et* $H \neq \{e\}$ *un sous-groupe de* G *tel que* $[G : H] = n$. *On rappelle que* $H =< x^m >$, *où* m *est le plus petit entier strictement positif tel que* $x^m \in H$.

1) Soit $k, l \in \mathbb{Z}$. *Montrer que* $x^k H = x^l H$ *si, et seulement si,* m *divise* $k - l$.

2) En déduire que $H, \overline{x}, \ldots, \overline{x}^{m-1}$ *sont deux à deux distincts.*

3) En déduire que $m = n$.

Exercice 27. *On considère l'ensemble* A *des polynômes* $P(X) \in \mathbb{Z}[X]$ *tels que le coefficient de* X *dans* $P(X)$ *est divisible par* 2., *i.e.,* $A = \{P(X) = a + 2bX + X^2T(X)/a, b \in \mathbb{Z}, T(X) \in \mathbb{Z}[X]\}$.

1) a) Vérifier que A *est un sous-anneau (commutatif et unitaire) de* $\mathbb{Z}[X]$.

b) Dire pourquoi A *est intègre et vérifier que* $\mathcal{U}(A) = \{-1, 1\}$.

2) Montrer que $2X$ *est irréductible dans* A.

3) En déduire que 2 *et* $2X$ *sont premiers entre eux dans* A.

4) Existe-t-il $(P(X), Q(X)) \in A^2$ *tel que* $2P(X) + 2XQ(X) = 1$ *? A est-il principal ?*

Corrigés des Contrôles Continus, Contrôles Finaux et Rattrapages

Corrigé du contrôle Continu 2015-2016

Solution de l'exercice 1.

1) *Puisque* $|\mathcal{U}(17)| = 16$, $o(\overline{3})/16$ *d'où* $o(\overline{3}) \in \{1, 2, 4, 8, 16\}$. *On a* $\overline{3}^1 \not\equiv 1 \pmod{17}$, $\overline{3}^2 \equiv 9 \not\equiv 1 \pmod{17}$, $\overline{3}^4 \equiv -4 \not\equiv 1 \pmod{17}$ *et* $\overline{3}^8 \equiv -1 \not\equiv 1 \pmod{17}$, *alors* $o(\overline{3}) = 16$ *et ainsi* $\mathcal{U}(17) =< \overline{3} >$ *est cyclique.*

2) *Les sous-groupes de* $\mathcal{U}(17)$ *sont : le sous-groupe d'ordre 1 :* $< \overline{1} >= \{\overline{1}\}$ *; le sous-groupe d'ordre 2 :* $< \overline{3}^{\frac{16}{2}} >=< \overline{3}^8 >= \{\overline{1}, \overline{16}\}$ *; le sous-groupe d'ordre 4 :* $< \overline{3}^{\frac{16}{4}} >= \{1, \overline{13}, \overline{16}, \overline{4}\}$ *; le sous-groupe d'ordre 8 :* $< \overline{3}^{\frac{16}{8}} >= \{\overline{1}, \overline{9}, \overline{13}, \overline{15}, \overline{16}, \overline{8}, \overline{4}, \overline{2}\}$ *et le sous-groupe d'ordre 16 :* $\mathcal{U}(17)$.

3) *Les générateurs de* $\mathcal{U}(17)$ *sont les éléments de* $\mathcal{U}(17)$ *de la forme* $\overline{3}^k$, *où* k *est un entier tel que* $0 \leq k < 16$ *et* $k \wedge 16 = 1$, *ainsi les générateurs de* $\mathcal{U}(17)$ *sont :* $\overline{3} = \overline{3}^1$, $\overline{10} = \overline{3}^3$, $\overline{5} = \overline{3}^5$, $\overline{11} = \overline{3}^7$, $\overline{14} = \overline{3}^9$, $\overline{7} = \overline{3}^{11}$, $\overline{12} = \overline{3}^{13}$ *et* $\overline{6} = \overline{3}^{15}$.

4) *Soit* f *un morphisme de groupes de* $\mathbb{Z}_6$ *vers* $\mathcal{U}(17)$. *D'après le cours,* f *est déterminé par* $f(\overline{1})$ *car* $\mathbb{Z}_{16} =< \overline{1} >$ *et comme* $|\mathbb{Z}_{16}| = |\mathcal{U}(17)| = 16$, f *est un isomorphisme si, et seulement si,* f *est surjectif. Aussi, on a* f *est surjectif si, et seulement si,* $f(\overline{1})$ *est un générateur de* $\mathcal{U}(17)$ *; ainsi les isomorphismes de groupes de* $\mathbb{Z}_{16}$ *vers* $\mathcal{U}(17)$ *sont les les morphismes de groupes* $f_1, f_2, f_3, f_4, f_5, f_6, f_7$ *et* f_8 *définis par :* $f_1(\overline{1}) = \overline{3}$, $f_2(\overline{1}) = \overline{5}$, $f_3(\overline{1}) = \overline{6}$, $f_4(\overline{1}) = \overline{7}$, $f_5(\overline{1}) = \overline{10}$, $f_6(\overline{1}) = \overline{11}$, $f_7(\overline{1}) = \overline{12}$ *et* $f_8(\overline{1}) = \overline{14}$.

Solution de l'exercice 2.

1) *On a* $\sigma^2 = \rho^2 = (13)(24)(57)(68)$, $\rho\sigma = (1836)(2745)$, $\sigma^3 = (1432)(5876)$ *et* $\rho\sigma^3 = (1638)(2547)$.

2) *Puisque* $\sigma^2 \neq e$ *et* $(\sigma^2)^2 = \sigma^4 = e$, *alors* $\circ(\sigma^2) = 2$ *et par suite* $H = \{e, \sigma^2\}$.

3) — *Les éléments de* $(G/H)_g$ *sont* $eH = H$, $\sigma H = \{\sigma, \sigma^3\}$, $\rho H = \{\rho, \rho^3\}$ *(car* $\rho\sigma^2 = \rho^3$*) et* $\rho\sigma H = \{\rho\sigma, \rho\sigma^3\}$.
   — *Les éléments de* $(G/H)_d$ *sont* $He = H$, $H\sigma = \{\sigma, \sigma^3\}$, $H\rho = \{\rho, \rho^3\}$ *(car* $\sigma^2\rho = \rho^3$*) et* $H\rho\sigma = \{\rho\sigma, \rho\sigma^3\}$ *(car* $\sigma^2\rho\sigma = \rho^3\sigma = \rho\sigma^3$*).*
   — *On remarque que* $\forall g \in G$, $gH = Hg$, *alors* H *est un sous-groupe distingué de* G *et ainsi* G/H *est un groupe.*

4) *On a* $G/H = \{H, \sigma H, \rho H, \rho\sigma H\}$ *d'où* $|G/H| = 4$. *Aussi, on a* $(\sigma H)^2 = \sigma^2 H = H$, $(\rho H)^2 = \rho^2 H = H$ *et* $(\rho\sigma H)^2 = (\rho\sigma)^2 H = H$ *(car* $(\rho\sigma)^2 = \sigma^2$*),*

ainsi aucun élément de G/H n'est d'ordre 4 et par suite G/H n'est pas cyclique.
Puisque G/H est un groupe d'ordre 4 non cyclique, alors $G/H \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Corrigé du contrôle Final 2015-2016

Solution de l'exercice 3.

1) On a $A \setminus \widetilde{A} \neq \emptyset$ car A n'est pas un corps, d'où $N \neq \emptyset$ et puisque N est une partie de $\mathbb{N}$ non vide, alors N possède un plus petit élément.

2) Soit x un élément de A. Comme $u \neq 0$ et A est euclidien, alors il existe $(q, r) \in A^2$ tels que $x = qu + r$, avec $r = 0$ ou $\delta(r) < \delta(u)$. Comme $\delta(u)$ est le plus petit élément de N, si $\delta(r) < \delta(u)$, alors $r \in \widetilde{A}$ et ainsi il existe $r \in \widetilde{A}$ tel que u divise $x - r$ (on remarque que si $r = 0$, alors $r \in \widetilde{A}$).

Solution de l'exercice 4.

1) Soit $x = a + ib\sqrt{11} \in \mathcal{U}(A)$, avec $a, b \in \mathbb{Z}$. Alors, il existe $y = c + id\sqrt{11}$, avec $c, d \in \mathbb{Z}$, tel que $xy = 1$, d'où $|xy|^2 = |x|^2|y|^2 = 1$, i.e., $(a^2+11b^2)(c^2+11d^2) = 1$ ainsi $a = \pm 1$ et $b = 0$ d'où $x = \pm 1$ alors $\mathcal{U}(A) \subset \{-1, 1\}$. D'autre part, on a $\{-1, 1\} \subset \mathcal{U}(A)$ et par suite $\mathcal{U}(A) = \{-1, 1\}$.

2) On a $2 \notin \mathcal{U}(A)$. Soit $x = a + ib\sqrt{11} \in A$, avec $a, b \in \mathbb{Z}$, tel que $x/2$, alors il existe $y = c + id\sqrt{11}$,avec $c, d \in \mathbb{Z}$, tel que $xy = 2$, ainsi $a^2 + 11b^2 = |x|^2$ divise 4, d'où $a^2 + 11b^2 \in \{1, 2, 4\}$ et comme $a^2 + 11b^2 \neq 2$, alors $a^2 + 11b^2 \in \{1, 4\}$. On remarque que si $a^2 + 11b^2 = 1$, alors $a = \pm 1$ et $b = 0$ et ainsi $x \in \mathcal{U}(A)$ et que si $a^2 + 11b^2 = 4$, alors $c^2 + 11d^2 = 1$ ainsi $y = \pm 1$ d'où x et 2 sont associés. Ainsi 2 est irréductible dans A.
On a $1 + i\sqrt{11} \notin \mathcal{U}(A)$. Soit $x = a + ib\sqrt{11} \in A$, avec $a, b \in \mathbb{Z}$, tel que $x/1 + i\sqrt{11}$, alors il existe $y = c + id\sqrt{11}$,avec $c, d \in \mathbb{Z}$, tel que $xy = 1+i\sqrt{11}$, ainsi $a^2+11b^2 = |x|^2$ divise 12, d'où $a^2+11b^2 \in \{1, 2, 3, 4, 6, 12\}$ et comme $a^2 + 11b^2 \notin \{2, 3, 6\}$, alors $a^2 + 11b^2 \in \{1, 4, 12\}$. Aussi, on a $a^2 + 11b^2 \neq 4$ (sinon, $x = \pm 2$ et ainsi $\pm 2c = 1$), d'où $a^2 + 11b^2 \in \{1, 12\}$ et on vérifie facilement que si $a^2 + 11b^2 = 1$, alors x est inversible et que si $x = 12$, alors x et $1 + i\sqrt{11}$ sont associés et par suite $1 + i\sqrt{11}$ est irréductible dans A.

3) On a 2 divise $12 = (1 + i\sqrt{11})(1 - i\sqrt{11})$ mais 2 ne divise ni $1 + i\sqrt{11}$ ni $1 - i\sqrt{11}$ (si 2 divise $1 \pm i\sqrt{11}$, alors il existe $c \in \mathbb{Z}$ tel que $2c = 1$) ainsi 2 n'est pas premier dans A et par suite A n'est pas principal car il contient un élément qui est irréductible mais non premier.

Solution de l'exercice 5.

1) *On a* $\widetilde{p}(0)=1$, $\widetilde{p}(1)=3$, $\widetilde{p}(2)=1$, $\widetilde{p}(3)=1$, $\widetilde{p}(4)=4$ *et comme* $\mathbb{Z}_5$ *est un corps et* $p(X)\in\mathbb{Z}_5[X]$ *est de degré* 3 *et n'a pas de racines dans* $\mathbb{Z}_5$, *alors* $p(X)$ *est irréductible dans* $\mathbb{Z}_5[X]$.

2) *Soit* $t(X)=\sum_{i=0}^{n}a_iX^i\in\mathbb{Z}[X]$. *Supposons que* $t(X)\in\ker g$, *alors* $\sum_{i=0}^{n}\overline{a_i}X^i=\overline{0}$ *d'où* $\forall i=0,\dots,n$, $\overline{a_i}=\overline{0}$, *i.e.,* $\forall i=0,\dots,n$, $a_i=5b_i$, *où* $b_i\in\mathbb{Z}$, *alors* $t(X)=5.\sum_{i=0}^{n}b_iX^i\in 5\mathbb{Z}[X]$. *Aussi, on vérifie facilement que si* $t(X)\in 5\mathbb{Z}[X]$, *alors* $t(X)\in\ker g$ *et ainsi* $\ker g=5\mathbb{Z}[X]$.

3) a) *Il suffit de remarquer que* s *et* g *sont surjectifs et ainsi* $f=s\circ g$ *est surjectif.*

b) *Soit* $t(X)\in\mathbb{Z}[X]$. *Supposons que* $t(X)\in\ker f$, *alors* $g(t(X))\in\ker s=I$ *d'où il existe* $v(X)\in\mathbb{Z}_5[X]$ *:* $g(t(X))=p(X)v(X)$, *alors* $g(t(X))=g(q(X)).g(u(X))$ *(puisque* g *est surjectif, il existe* $u(X)\in\mathbb{Z}[X]$ *tel que* $v(X)=g(u(X))$*), i.e.,* $g(t(X))=g(q(X)u(X))$ *ainsi* $t(X)-q(X)u(X)\in\ker g$ *alors* $t(X)=q(X)u(X)+5h(X)$, *avec* $h(X)\in\mathbb{Z}[X]$, *et par suite* $t(X)\in J$. *On vérifie facilement que* $J\subset\ker f$, *ainsi* $\ker f=J$.

c) *Comme* f *est un morphisme surjectif, alors, d'après le premier théorème d'isomorphisme,* $\mathbb{Z}[X]/J\simeq\mathbb{Z}_5[X]/I$. *D'autre part, on a* $p(X)$ *est irréductible dans* $\mathbb{Z}_5[X]$ *et* $\mathbb{Z}_5[X]$ *est principal (car* $\mathbb{Z}_5$ *est un corps), alors* $I=(p(X))$ *est maximal ainsi* $\mathbb{Z}_5[X]/I$ *est un corps et par suite* $\mathbb{Z}[X]/J$ *est un corps.*

Corrigé du Rattrapage 2015-2016

Solution de l'exercice 6.

1) *Soit* $x=\frac{a+ib\sqrt{3}}{2}\in A$, *avec* $a,b\in\mathbb{Z}$ *et* $a\equiv b\pmod 2$. *Si* $x\in\mathcal{U}(A)$, *alors il existe* $y=\frac{c+id\sqrt{3}}{2}\in A$, *avec* $c,d\in\mathbb{Z}$ *et* $c\equiv d\pmod 2$, *tel que* $xy=1$ *d'où* $|x|^2|y|^2=1$, *i.e.,* $\frac{1}{16}(a^2+3b^2)(c^2+3d^2)=1$ *ainsi* a^2+3b^2 *divise* 16 *et par suite* $a^2+3b^2\in\{1,2,4,8,16\}$. *On* $a^2+3b^2\neq 1$ *(sinon* $a=\pm1,b=0$ *qui ne sont pas de même parité),* $a^2+3b^2\neq 16$ *(sinon* $c=\pm1,d=0$ *qui ne sont pas de même parité) et* $a^2+3b^2\notin\{2,8\}$ *(sinon* $a^2\equiv 2\pmod 3$*) et ainsi* $a^2+3b^2=4$ *d'où (*$a=\pm1$ *et* $b=\pm1$*) ou (*$a=\pm2$ *et* $b=0$*) et il vient que* $x\in\{1,-1,\frac{1+i\sqrt{3}}{2},\frac{-1+i\sqrt{3}}{2},\frac{1-i\sqrt{3}}{2},\frac{-1-i\sqrt{3}}{2}\}$.
Pour conclure, il suffit de vérifier que tous les éléments de $\{1,-1,\frac{1+i\sqrt{3}}{2},\frac{-1+i\sqrt{3}}{2},\frac{1-i\sqrt{3}}{2},\frac{-1-i\sqrt{3}}{2}\}$ *sont inversibles.*

2) *On a* $\frac{1+i\sqrt{3}}{2}\neq 1$, $(\frac{1+i\sqrt{3}}{2})^2=\frac{-1+i\sqrt{3}}{2}\neq 1$ *et* $(\frac{1+i\sqrt{3}}{2})^3=-1\neq 1$ *et puisque l'ordre de* $\frac{1+i\sqrt{3}}{2}$ *divise* $|\mathcal{U}(A)|=6$, *alors l'ordre de* $\frac{1+i\sqrt{3}}{2}$ *est égal à 6.*

Comme $|\mathcal{U}(A)| = 6$ *et* $\circ(\frac{1+i\sqrt{3}}{2}) = 6$, *alors* $\mathcal{U}(A)$ *est cyclique et est engendré par* $\frac{1+i\sqrt{3}}{2}$.

3) Supposons que f *est un isomorphisme de* $\mathbb{Z}_6$ *vers* $\mathcal{U}(A)$, *alors* f *est déterminé par* $f(1)$. *Aussi, puisque* f *est un isomorphisme,* $\circ(f(1)) = \circ(1) = 6$ *ainsi* $f(1)$ *est nécessairement un générateur de* $\mathcal{U}(A)$ *et par suite* $f(1) = \frac{1+i\sqrt{3}}{2}$ *ou* $f(1) = (\frac{1+i\sqrt{3}}{2})^5 = \frac{1-i\sqrt{3}}{2}$.

Solution de l'exercice 7.

1) a) Supposons que $p(X)$ *n'est pas irréductible dans* $\mathbb{Z}_2[X]$ *; puisque* $p(X)$ *n'est pas nul et n'est pas inversible dans* $\mathbb{Z}_2[X]$ *(*$\mathbb{Z}_2$ *est intègre donc* $\mathcal{U}(\mathbb{Z}_2[X]) = \mathbb{Z}_2^\star$*), alors il existe un polynôme* $t(x) \in \mathbb{Z}_2[X]$ *non inversible dans* $\mathbb{Z}_2[X]$ *et non associé à* $p(X)$ *tel que* $p(X) = t(X)s(X)$, *avec* $s(X) \in \mathbb{Z}_2[X]$. *Puisque* $\deg(t(X)) \neq 0$ *car* $t(X) \notin \mathcal{U}(\mathbb{Z}_2[X]) = \mathbb{Z}_2^\star$ *et* $\deg(t(X)) \neq 5$ *car* $t(X)$ *et* $p(X)$ *ne sont pas associés, alors* $\deg(t(X)) \in \{1, 2, 3, 4\}$. *Si* $\deg(t(X)) = 3$ *(resp.* $\deg(t(X)) = 4$*), alors* $\deg(s(X)) = 2$ *((resp.* $\deg(s(X)) = 1$*) et ainsi il existe un polynôme* $q(X) = s(X)$ *de degré* 2 *(resp. de degré* 1*) qui divise* $p(X)$. *Si* $\deg(t(X)) \in \{1, 2, \}$, *il suffit de prendre* $q(X) = t(X)$.

b) Pour montrer que $p(X)$ *n'a pas de diviseurs de degré* 1 *dans* $\mathbb{Z}_2[X]$, *il suffit de vérifier que* $p(X)$ *n'a pas de racines dans* $\mathbb{Z}_2$ *ce qui est évident car* $\widetilde{p}(\overline{0}) = \overline{1}$ *et* $\widetilde{p}(\overline{1}) = \overline{1}$.

c) Supposons que $X^2 + X + 1$ *divise* $p(X)$ *dans* $\mathbb{Z}_2[X]$, *alors il existe* $q(X) \in \mathbb{Z}_2[X]$ *tel que* $p(X) = (X^2 + X + 1)q(X)$ *ainsi, par passage au degré, on obtient* $\deg(q(X)) = 3$. *Puisque* $X^2 + X + 1$ *et* $p(X)$ *sont unitaires et leurs coefficients constants sont égaux à 1 ,* $q(X)$ *est unitaire et son coefficient constant est 1 ainsi on pose* $q(X) = X^3 + aX^2 + bX + 1$, *avec* $a, b \in \mathbb{Z}_2$. *A partir de l'égalité* $p(X) = (X^2 + X + 1)q(X)$ *et par identification, on obtient le système* $\begin{cases} 1 + a = 0 \\ b + a = 0 \\ 1 + b + a = 0 \end{cases}$ *qui n'a pas de solutions dans* $\mathbb{Z}_2$, *ce qui contredit l'hypothèse et par suite* $X^2 + X + 1$ *ne divise pas* $p(X)$ *dans* $\mathbb{Z}_2[X]$.
Ainsi, $p(X)$ *est irréductible dans* $\mathbb{Z}_2[X]$, *en effet : supposons que* $p(X)$ *n'est pas irréductible, alors, d'après 1)a) il existe un diviseur* $q(X)$ *de* $p(X)$ *dans* $\mathbb{Z}_2[X]$ *tel que* $\deg(q(X)) = 1$ *ou* 2. *Aussi, d'après 1)b),* $\deg q(X) \neq 1$ *ainsi* $\deg q(X) = 2$ *et par suite* $q(X) = X^2 + ax + b$, *avec* $a, b \in \mathbb{Z}_2$. *On a aussi* $b = \overline{1}$ *(sinon* $\overline{0}$ *est une racine de* $p(X)$*) ainsi* $q(X) = X^2 + aX + 1$. *De même,* $a = \overline{1}$ *(sinon* $\overline{1}$ *est une racine de* $p(X)$*) donc* $q(X) = X^2 + X + 1$, *ce qui contredit le fait que* $X^2 + X + 1$ *ne divise pas* $p(X)$ *ainsi* $p(X)$ *est irréductible dans* $\mathbb{Z}_2[X]$.

2) En prenant $p = 2$ et en appliquant le réduction modulo p au polynôme $X^5 + 8X^4 + 6X^3 + X^2 + 10X + 5$, on obtient le polynôme $X^5 + X^2 + 1 = p(X) \in \mathbb{Z}_2[X]$ donc $X^5 + 8X^4 + 6X^3 + X^2 + 10X + 5$ est irréductible dans $\mathbb{Q}[X]$ (car $p(X)$ est irréductible dans $\mathbb{Z}_2[X]$). Alors l'idéal de $\mathbb{Q}[X]$ engendré par $X^5 + 8X^4 + 6X^3 + X^2 + 10X + 5$ est un idéal maximal et par suite $\mathbb{Q}[X]/(X^5 + 8X^4 + 6X^3 + X^2 + 10X + 5)$ est un corps.

Solution de l'exercice 8.

1) Il est évident que $A \subset K[X]$ et que $1 \in A$. Soit $P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n, Q(X) = b_0 + b_1X + a_2X^2 + \cdots + a_mX^m \in A$, alors le coefficient du monôme X dans $P - Q$ est $a_1 - b_1 = 0$ car $a_1 = b_1 = 0$ ainsi $P - Q \in A$. Aussi, le coefficient de X dans PQ est $a_0b_1 + a_1b_0 = 0$ donc $PQ \in A$ et ainsi A est un sous-anneau de $K[X]$.

2) Soit $P(X) \in \mathcal{U}(A)$, alors il existe $Q(X) \in A$ tel que $P(X)Q(X) = 1$ donc $P(X) \in \mathcal{U}(K[X]) = K^\star$. Aussi, il est évident que tout élément de $K^\star$ est un élément de A et est inversible dans A ainsi $\mathcal{U}(A) = K^\star$.

3) On a X^2 est non nul et $X^2 \notin K^\star = \mathcal{U}(A)$. Soit $P(X) \in A$ tel que $P(X)$ divise X^2, alors il existe $Q(X) \in A$ tel que $X^2 = P(X)Q(X)$ d'où, par passage au degré, $\deg P(X) \in \{0, 1, 2\}$ et comme $P(X) \in A$, $\deg P(X) \in \{0, 2\}$. Si $\deg P(X) = 0$, alors $P(X) \in K^\star$ d'où $P(X)$ est inversible et si $\deg P(X) = 2$, alors $Q(X) \in K^\star$ d'où $Q(X)$ est inversible donc X^2 et $P(X)$ sont associé ainsi X^2 est irréductible dans A.
De la même façon, on montre que X^3 est irréductible dans A : il suffit de remarquer que si $P(X) \in A$ est un diviseur de X^3, alors $\deg P(X) \neq 2$ (sinon $\deg Q(X) = 1$, ce qui est faux car $Q(X) \in A$).

4) A n'est pas principal, en effet, on a $X^6 \in A$ et $X^6 = (X^2)^3 = (X^3)^2$ sont deux décomposions de X^6 en produit d'éléments irréductibles dans A ; cependant, il est évident que X^2 et X^3 ne sont pas associés.

Corrigé du contrôle Continu 2016-2017

Solution de l'exercice 9.

I) Soit $x \in G$ et $h \in H$. On a $H =< a >$ d'où $h = a^n$, avec $n \in \mathbb{Z}$. Alors, $xhx^{-1} = xa^nx^{-1}$. D'autre part, on vérifie facilement que $xa^nx^{-1} = (xax^{-1})^n$ ainsi $xhx^{-1} = (xax^{-1})^n$ d'où $xhx^{-1} \in H$ car $xax^{-1} \in H$ et par suite H est distingué dans G.

II) 1) Soit $A = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}, B = \begin{pmatrix} \overline{2} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}$. On a $A, B \in G$, $AB = \begin{pmatrix} \overline{2} & \overline{2} \\ \overline{0} & \overline{1} \end{pmatrix}$, $BA = \begin{pmatrix} \overline{2} & \overline{3} \\ \overline{0} & \overline{1} \end{pmatrix}$ d'où G n'est pas commutatif et ainsi G n'est pas cyclique.

2) On a $A^2 = \begin{pmatrix} \overline{1} & \overline{2} \\ \overline{0} & \overline{1} \end{pmatrix}, A^3 = \begin{pmatrix} \overline{1} & \overline{3} \\ \overline{0} & \overline{1} \end{pmatrix}, A^4 = \begin{pmatrix} \overline{1} & \overline{4} \\ \overline{0} & \overline{1} \end{pmatrix}$ *et* $A^5 = I_2$ *d'où* $\circ(A) = 5$ *et* $< A >= \{\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{2} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{3} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{4} \\ \overline{0} & \overline{1} \end{pmatrix}\} = H$ *et par suite* H *est un sous-groupe de* G.

Soit $X = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{0} & \overline{1} \end{pmatrix} \in G$, *on a* $XAX^{-1} = \begin{pmatrix} \overline{1} & \overline{a} \\ \overline{0} & \overline{1} \end{pmatrix} \in H$ *ainsi, d'après I),* H *est distingué dans* G.

3) a) On a $\begin{pmatrix} \overline{2} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} \notin H$ *d'où* $H \neq \begin{pmatrix} \overline{2} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} H$. *Aussi, on a* $\begin{pmatrix} \overline{3} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} \notin H$ *d'où* $H \neq \begin{pmatrix} \overline{3} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} H$ *et comme* $\begin{pmatrix} \overline{2} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}^{-1} \begin{pmatrix} \overline{3} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{4} & . \\ . & . \end{pmatrix} \notin H$, *alors* $\begin{pmatrix} \overline{3} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} H \neq \begin{pmatrix} \overline{2} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} H$. *De la même façon, on a* $\begin{pmatrix} \overline{4} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} H \neq H$, $\begin{pmatrix} \overline{4} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} H \neq \begin{pmatrix} \overline{2} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} H$ *et* $\begin{pmatrix} \overline{4} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} H \neq \begin{pmatrix} \overline{3} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} H$. *D'autre part,* $|G| = 4.5 = 20$ *d'où* $|G/H| = 4$ *et ainsi* $G/H = \{H, \begin{pmatrix} \overline{2} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}.H, \begin{pmatrix} \overline{3} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}.H, \begin{pmatrix} \overline{4} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}.H\}$.

b) On a $\begin{pmatrix} \overline{2} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} H \in G/H$, $(\begin{pmatrix} \overline{2} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} H)^2 = \begin{pmatrix} \overline{4} & . \\ . & . \end{pmatrix} H \neq H$, *d'où* $\circ(\begin{pmatrix} \overline{2} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} H) = 4$ *car* $|G/H| = 4$ *et* $\circ(\begin{pmatrix} \overline{2} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} H) \notin \{1, 2\}$. *Alors,* $G/H =< (\begin{pmatrix} \overline{2} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} H) >$ *est cyclique et par suite* $G/H \simeq \mathbb{Z}_4$.

Solution de l'exercice 10.

1) Soit $\overline{x} \in G$, *avec* $x = \frac{a}{b}, a \in \mathbb{Z}, b \in \mathbb{N}^\star$. *On a* $b\overline{x} = \overline{a} = \overline{0}$ *car* $a \in \mathbb{Z}$ *ainsi l'ordre de* $\overline{x}$ *est fini.*

2) a) On a $n\overline{(\frac{1}{n})} = \overline{0}$, *alors* $\circ(\overline{(\frac{1}{n})})$ *divise* n. *D'autre part, si* k *est un entier* > 0 *tel que* $k\overline{(\frac{1}{n})} = \overline{0}$, *alors* $\frac{k}{n} \in \mathbb{Z}$ *ainsi* n *divise* k *et par suite l'ordre de* $\overline{(\frac{1}{n})} = n$ *et puisque* $\circ(\overline{(\frac{1}{n})}) = |H_n|$, *alors* $|H_n| = n$.

b) Comme K *est cyclique, alors il existe* $a \in \mathbb{Z}, b \in \mathbb{N}^\star$ *tels que* $a \wedge b = 1$ *et* $K =< \overline{(\frac{a}{b})} >$. *On a* $n\overline{(\frac{a}{b})} = \overline{0}$ *(car l'ordre de* $\overline{(\frac{a}{b})} = n$*) ainsi* b *divise*

na d'où b divise n (car $a \wedge b = 1$) alors il existe $k \in \mathbb{Z} : n = bk$ et par suite $\overline{(\frac{a}{b})} = \overline{(\frac{ka}{n})} = ka(\overline{(\frac{1}{n})}) \in H_n$ donc $K \subset H_n$, alors $K = H_n$ car K et H_n ont le même ordre.

c) On a $H_6 = (\overline{(\frac{1}{6})}$ est cyclique d'ordre 6 dont les générateurs sont $\overline{(\frac{1}{6})}$ et $\overline{(\frac{5}{6})}$ ainsi les isomorphismes de $\mathbb{Z}_6$ vers H_6 sont $f_1 : \overline{1} \mapsto \overline{(\frac{1}{6})}$ et $f_2 : \overline{1} \mapsto \overline{(\frac{5}{6})}$.

3) a) Il est évident que f est une application bien définie. Aussi, on vérifie facilement que f est un morphisme de groupes.
Soit $\overline{x} \in G$, avec $x \in \mathbb{Q}$, d'où $\frac{x}{n} \in \mathbb{Q}$ ainsi il existe $\overline{\frac{x}{n}} \in G$: $f(\overline{\frac{x}{n}}) = n\overline{\frac{x}{n}} = \overline{\frac{nx}{n}} = \overline{x}$ d'où f est surjectif.

b) On a $\ker f = H_n$, en effet : on a $f(\overline{\frac{1}{n}}) = \overline{0}$ d'où $\ker f$ est un sous-groupe de G contenant $\overline{\frac{1}{n}}$ et comme $H_n =< \overline{\frac{1}{n}} >$, alors $H_n \subset \ker f$.
Inversement, soit $\overline{(\frac{a}{b})} \in \ker f$, avec $a \in \mathbb{Z}, b \in \mathbb{N}^\star$ et $a \wedge b = 1$. On a $f(\overline{(\frac{a}{b})}) = \overline{0}$, alors b divise na d'où b divise n ainsi il existe $k \in \mathbb{Z} : n = bk$ et par suite $\overline{(\frac{a}{b})} = ka(\overline{(\frac{1}{n})}) \in H_n$.
Comme $\ker f = H_n$ et f est surjectif, alors, d'après le premier théorème d'isomorphisme, $G/H_n \simeq G$.

c) Si G est fini, alors $\frac{|G|}{|H_n|} = |G|$ d'où $\frac{|G|}{n} = |G|$, ceci $\forall n \in \mathbb{N}^\star$, ce qui est faux. Alors, G est infini.

Corrigé du contrôle Final 2016-2017

Solution de l'exercice 11.

1) Soit $r \in \mathbb{R}^\star$ tel que $r + \frac{1}{r}$ est un entier impair, alors il existe $k \in \mathbb{Z}$: $r + \frac{1}{r} = 2k + 1$ d'où $r^2 - (2k + 1)r + 1 = 0$ ainsi r est une racine de $p(X) = X^2 - nX + 1$, où $n = 2k + 1$. D'autre part, $p(X) = X^2 - nX + 1 \in \mathbb{Z}[X]$ et en appliquant la réduction modulo p avec $p = 2$, on obtient $\overline{p}(X) = X^2 + X + 1 \in \mathbb{Z}_2[X]$ qui est irréductible dans $\mathbb{Z}_2[X]$ ($\overline{p}(X)$ est de degré 2 et à coefficients dans le corps $\mathbb{Z}_2$ et n'a pas de racines dans $\mathbb{Z}_2$) ainsi $p(X) = X^2 - nX + 1$ est irréductible dans $\mathbb{Q}[X]$.

2) r est irrationnel, en effet, si $r \in \mathbb{Q}$, alors $X - r$ divise $X^2 - nX + 1$ dans $\mathbb{Q}[X]$, ce qui contredit le fait que $X^2 - nX + 1$ est irréductible dans $\mathbb{Q}[X]$.

Solution de l'exercice 12.

1) a) Supposons qu'il existe $x, y \in \mathbb{Z}$ tels que $p = x^2 + y^2$, alors $p = (x + iy)(x - iy)$ d'où $x + iy$ divise p dans $\mathbb{Z}[i]$. Or, $x + iy \notin \mathcal{U}(\mathbb{Z}[i])$ et $x + iy$ et p ne sont pas associés, en effet, si $x + iy \in \mathcal{U}(\mathbb{Z}[i])$, alors $x = \pm 1$ et $y = 0$ ou $x = 0$ et $y \pm 1$ d'où $p = 1$, ce qui est faux ; aussi, si $x + iy$

et p sont associés, alors $(x-iy) \in \mathcal{U}(\mathbb{Z}[i])$ ainsi $x = \pm 1$ et $y = 0$ ou $x = 0$ et $y \pm 1$ d'où $p = 1$, ce qui est faux. Puisque $x+iy$ divise p et $x+iy \notin \mathcal{U}(\mathbb{Z}[i])$ et $x+iy$ et p ne sont pas associés, alors p n'est pas irréductible dans $\mathbb{Z}[i]$.

b) D'après 1)a), si p est irréductible dans $\mathbb{Z}[i]$, alors $p \neq x^2+y^2$, $\forall x, y \in \mathbb{Z}$.

Réciproquement, supposons que $p \neq x^2+y^2$, $\forall x, y \in \mathbb{Z}$. On a p est non nul et $p \notin \mathcal{U}(\mathbb{Z}[i])$. Soit $a+ib \in \mathbb{Z}[i]$ un diviseur de p dans $\mathbb{Z}[i]$ ($a, b \in \mathbb{Z}$, alors il existe $c, d \in \mathbb{Z}$: $p = (a+ib)(c+id)$ d'où $p^2 = (a^2+b^2)(c^2+d^2)$ et puisque $a^2+b^2 \neq p$ alors $a^2+b^2 \in \{1, p^2\}$. Si $a^2+b^2 = 1$, alors $a+ib$ est inversible dans $\mathbb{Z}[i]$ et si $a^2+b^2 = p^2$, alors $c^2+d^2 = 1$ d'où $c+id \in \mathcal{U}(\mathbb{Z}[i])$ donc $a+ib$ et p sont associés. Alors, p est irréductible dans $\mathbb{Z}[i]$.

2) On considère l'application $f : \mathbb{Z}[i] \to \mathbb{Z}_p[i]$, $a+ib \mapsto \overline{a}+i\overline{b}$, où $a, b \in \mathbb{Z}$.

a) On vérifie facilement que f est un homomorphisme d'anneaux surjectif.

b) Soit $x+iy \in \mathbb{Z}[i]$, avec $x, y \in \mathbb{Z}$. On $ax+iy \in \ker f$ si, et seulement si, $f(x+iy) = \overline{0}$ si, et seulement si, $\overline{x}+i\overline{y} = \overline{0}$ si, et seulement si, $\overline{x} = \overline{y} = \overline{0}$ si, et seulement si, p/x et p/y si, et seulement si, il existe $h, k \in \mathbb{Z}$ tels que $x+iy = p(h+ik)$ si, et seulement si, $x+iy \in (p)$, où (p) et l'idéal de $\mathbb{Z}[i]$ engendré par p.

c) D'après le premier théorème d'isomorphisme, $\mathbb{Z}[i]/(p) \simeq \mathbb{Z}_p[i]$, alors $\mathbb{Z}_p[i]$ est un corps si, et seulement si, $\mathbb{Z}[i]/(p)$ est un corps si, et seulement si, (p) est un idéal maximal de $\mathbb{Z}[i]$ si, et seulement si, p est irréductible dans $\mathbb{Z}[i]$ (car $\mathbb{Z}[i]$ est principal (il est aussi euclidien)) si, et seulement si, $p \neq x^2+y^2$, $\forall x, y \in \mathbb{Z}$ (voir 1)b)).

d) i) Il est évident que $\forall x, y \in \mathbb{Z}$, $x^2+y^2 \neq 7$ d'où, d'après la question précédente, $\mathbb{Z}_7[i]$ est un corps.

ii) On a $5 = 1^2+2^2$, alors, d'après la question précédente, $\mathbb{Z}_5[i]$ n'est pas un corps. $\mathbb{Z}_5[i]$ n'est pas un intègre car $(\overline{1}+\overline{2}i)(\overline{1}+\overline{3}i) = \overline{0}$ mais $\overline{1}+\overline{2}i \neq \overline{0}$ et $\overline{1}+\overline{3}i \neq \overline{0}$.

Solution de l'exercice 13.

1) On a $\forall \overline{x}, \overline{y} \in \mathbb{Z}_p^\star$, $f(\overline{xy}) = ((\overline{xy})^2 = \overline{x}^2\overline{y}^2 = f(\overline{x})f(\overline{y})$, alors f est un homomorphisme de groupes.

2) Soit $\overline{x} \in \mathbb{Z}_p^\star$. On a $\overline{x} \in \ker f$ si, et seulement si, $f(\overline{x}) = \overline{1}$ si, et seulement si, p/x^2-1 si, et seulement si, $p/x-1$ ou $p/x+1$ si, et seulement si, $\overline{x} = \overline{1}$ ou $\overline{x} = \overline{-1}$ ainsi $\ker f = \{\overline{-1}, \overline{1}\}$.

3) D'après le premier théorème d'isomorphisme, $\mathbb{Z}_p^\star/\ker f \simeq \operatorname{Im} f$ d'où $\frac{|\mathbb{Z}_p^\star|}{|\ker f|} = |\operatorname{Im} f|$ ainsi $[\mathbb{Z}_p^\star : \operatorname{Im} f] = \frac{|\mathbb{Z}_p^\star|}{|\operatorname{Im} f|} = |\ker f| = 2$ et par suite $\operatorname{Im} f \neq \mathbb{Z}_p^\star$ donc f n'est pas surjective.

4) a) Puisque $|\mathbb{Z}_p^\star/\operatorname{Im} f| = [\mathbb{Z}_p^\star : \operatorname{Im} f] = 2$, *alors* $\mathbb{Z}_p^\star/\operatorname{Im} f = \{\operatorname{Im} f, \overline{-1}\operatorname{Im} f\}$ *car* $\overline{-1} \notin \operatorname{Im} f$ *et comme* $\overline{r} \notin \operatorname{Im} f$, $\overline{r}\operatorname{Im} f \neq \operatorname{Im} f$ *donc* $\overline{r}\operatorname{Im} f = \overline{-1}\operatorname{Im} f$.

b) Puisque $\overline{r}\operatorname{Im} f = \overline{-1}\operatorname{Im} f$, *alors* $(\overline{-1})^{-1}\overline{r} \in \operatorname{Im} f$ *d'où* $\overline{-r} \in \operatorname{Im} f$ *ainsi il existe* $\overline{a} \in \mathbb{Z}_p^\star : \overline{a}^2 = \overline{-r}$.

Corrigé du Rattrapage 2016-2017

Solution de l'exercice 14.

1) Puisque G est monogène, il suffit de vérifier qu'il est fini. Supposons que G est infini, alors $G \simeq \mathbb{Z}$ et par suite G possède des sous-groupes autre que $\{e\}$, G et H, ce qui contredit l'hypothèse.

2) Supposons que $|G| = p$, alors $H = G$ et ainsi G a seulement deux sous-groupes $\{e\}$ et G, contradiction.

3) Comme G est fini et H est un sous-groupe de G d'ordre p, alors p divise n, où n est l'ordre de G, ainsi $n = pk$, où $k \in \mathbb{N}$. On a, d'après 2), $k \neq 1$. Puisque k divise n et G est cyclique, alors il existe un sous-groupe K de G d'ordre k et comme $k \notin \{1, n\}$ et les sous-groupes de G sont $\{e\}$, H et G, alors $K = H$ ainsi $k = p$ et par suite $|G| = p^2$.

Solution de l'exercice 15.

1) Il suffit d'appliquer le critère d'Eisenstein en prenant $p = 3$.

2) Puisque $p(X)$ est irréductible dans $\mathbb{Q}[X]$, alors l'idéal $< p(X) >$ est un idéal maximal de $\mathbb{Q}[X]$ et par suite $\mathbb{Q}[X]/ < p(X) >$ est un corps.

3) Soit $d(X)$ un pgcd de $1+X$ et $p(X)$ d'où $d(X)$ est un diviseur de $p(X)$ et comme $p(X)$ est irréductible dans $\mathbb{Q}[X]$, alors $d(X) \in \mathcal{U}(\mathbb{Q}[X]) = \mathbb{Q}^\star$ ou $d(X) \sim p(X)$ donc $d(X) \in \mathbb{Q}^\star$ (sinon, p(X)/1+X, ce qui est faux) ainsi $1 + X$ et $p(X)$ sont premiers entre eux dans $\mathbb{Q}[X]$.

4) Comme $\mathbb{Q}[X]$ est principal et $1 + X$ et $p(X)$ sont premiers entre eux dans $\mathbb{Q}[X]$, alors, d'après le théorème de Bezout, il existe $u(X), v(X) \in \mathbb{Q}[X]$ tels que $u(X)(1 + X) + v(X)p(X) = 1$ donc $\overline{u(X)}(1 + X) = \overline{1}$ dans $\mathbb{Q}[X]/ < p(X) >$ (car $\overline{p(X)} = \overline{0}$) et ainsi $\overline{(1 + X)}$ est inversible dans $\mathbb{Q}[X]/ < p(X) >$.

5) En utilisant l'algorithme d'Euclide étendu, on obtient $(X + 1)(\frac{1}{4}(X^2 - X + 10)) - \frac{1}{4}P(X) = 1$, ainsi $\overline{(X + 1)}\overline{\frac{1}{4}(X^2 - X + 10)} = \overline{1}$ $\overline{(X + 1)}^{-1} = \overline{\frac{1}{4}(X^2 - X + 10)}$.

Solution de l'exercice 16.

1) Soit $x = a + ib\sqrt{3}, y = c + id\sqrt{3} \in \mathbb{Z}[i\sqrt{3}]$, *où* $a, b, c, d \in \mathbb{Z}$.
On a $f(x+y) = \overline{(a+b)+3(c+d)} = \overline{(a+3b)} + \overline{(c+3d)} = f(x) + f(y)$.
Aussi, $f(xy) = \overline{(ac-3bd)+3(ad+bc)} = (ac+bd)+3(ad+bc)$ *(car* $\overline{-3} = \overline{1} \pmod 4$*) d'où* $f(xy) = f(x)f(y)$ *et comme* $f(1) = \overline{1}$, *alors* f *est un morphisme d'anneaux. Aussi, il est évident que* f *est surjectif.*

2) a) Soit $x = a + ib\sqrt{3} \in \mathcal{U}(\mathbb{Z}[i\sqrt{3}])$, *avec* $a, b \in \mathbb{Z}$, *alors il existe* $y = c + id\sqrt{3} \in \mathbb{Z}[i\sqrt{3}]$, *avec* $a, b \in \mathbb{Z}$, *tel que* $xy = 1$ *d'où* $|xy|^2 = 1$ *alors* $(a^2+3b^2)(c^2+3d^2) = 1$ *ainsi* $a^2+3b^2 = 1$ *et par suite* $a = \pm 1$ *et* $b = 0$ *donc* $x = \pm 1$ *et comme* $\{-1, 1\} \subset \mathcal{U}(\mathbb{Z}[i\sqrt{3}])$, *alors* $\mathcal{U}(\mathbb{Z}[i\sqrt{3}]) = \{-1, 1\}$.

b) D'après 2)a), $1 + i\sqrt{3}$ *n'est pas inversible dans* $\mathbb{Z}[i\sqrt{3}]$. *Soit* $x = a + ib\sqrt{3}$, *avec* $a, b \in \mathbb{Z}$, *un diviseur de* $1 + i\sqrt{3}$ *dans* $\mathbb{Z}[i\sqrt{3}]$, *alors il existe* $y = c + id\sqrt{3} \in \mathbb{Z}[i\sqrt{3}]$, *avec* $c, d \in \mathbb{Z}$ *tel que* $xy = 1 + i\sqrt{3}$ *d'où* $(a^2+3b^2)(c^2+3d^2) = 4$ *et comme* $a^2+3b^2 \neq 2, \forall a, b \in \mathbb{Z}$, *alors* $a^2+3b^2 \in \{1, 4\}$ *ainsi si* $a^2+3b^2 = 1$, *alors* $x = \pm 1 \in \mathcal{U}(\mathbb{Z}[i\sqrt{3}])$ *et si* $a^2+3b^2 = 4$, *alors* $c^2+3d^2 = 1$ *d'où* $y = \pm 1 \in \mathcal{U}(\mathbb{Z}[i\sqrt{3}])$ *et par suite* $x \sim 1 + i\sqrt{3}$ *ainsi* $1 + i\sqrt{3}$ *est irréductible dans* $\mathbb{Z}[i\sqrt{3}]$.

c) Il est évident que $4 = (1 - i\sqrt{3})(1 + i\sqrt{3})$ *d'où* $4 \in < 1 + i\sqrt{3} >$.
Comme $f(1+i\sqrt{3}) = \overline{1+3.1} = \overline{0}$, *alors* $1+i\sqrt{3} \in \ker f$ *et puisque* $\ker f$ *est un idéal,* $< 1 + i\sqrt{3} > \subset \ker f$. *Inversement, soit* $x = a + ib\sqrt{3} \in \ker f$, *avec* $a, b \in \mathbb{Z}$, *alors* $f(x) = \overline{a+3b} = \overline{0}$ *d'où il existe* $k \in \mathbb{Z}$ *tel que* $a + 3b = 4k$ *ainsi* $x = 4k - 3b + ib\sqrt{3} = 4k + ib\sqrt{3}(1 + i\sqrt{3})$ *et il vent que* $x \in < 1 + i\sqrt{3} >$ *car* $4 \in < 1 + i\sqrt{3} >$.

d) D'après le premier théorème d'isomorphisme, $\mathbb{Z}[i\sqrt{3}]/\ker f \simeq \operatorname{Im} f = \mathbb{Z}/4\mathbb{Z}$, *d'où* $\mathbb{Z}[i\sqrt{3}]/\ker f$ *n'est pas un corps et il vient que* $\ker f = < 1 + i\sqrt{3} >$ *n'est pas maximal.*

e) D'après 2)b), $1 + i\sqrt{3}$ *est irréductible et comme* $< 1 + i\sqrt{3} >$ *n'est pas maximal donc* A *n'est pas principal.*

Corrigé du contrôle Continu 2017-2018

Solution de l'exercice 17. *On a* $\overline{a^n} = \overline{e}$ *d'où* $a^n \in H$. *Aussi,* $\overline{a^m} = \overline{a}^m = \overline{e}$ *car l'ordre de* G/H *est* m *d'où* $a^m \in H$. *Comme* $m \wedge n = 1$, *il existe* $u, v \in \mathbb{Z}$ *:* $um + vn = 1$ *ainsi* $a = a^{um+vn} = (a^m)^u.(a^n)^v \in H$.

Solution de l'exercice 18.

1) On a $G \subset GL_2(\mathbb{R})$ *car* $\forall A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G$, $\det A \neq 0$. *Aussi,* $G \neq \emptyset$ *car* $I_2 \in G$. *Soit* $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, B = \begin{pmatrix} r & s \\ 0 & t \end{pmatrix} \in G$, *alors* $AB^{-1} =$

$\frac{1}{rt}\begin{pmatrix} at & -as+br \\ 0 & cr \end{pmatrix}$ *ainsi* $AB^{-1} \in G$ *car* $at \neq 0$ *et* $cr \neq 0$ *et par suite* G *est un sous-groupe de* $GL_2(\mathbb{R})$.

2) *a) On vérifie facilement que* $\forall A, B \in G,\ f(AB) = f(A).f(B)$.

b) Soit $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G$. *On a* $A \in \ker f$ *si, et seulement si,* $f(A) = (1,1)$ *si, et seulement si,* $(a,c) = (1,1)$ *si, et seulement si,* $A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in H$ *ainsi* $\ker f = H$ *et par suite* H *est un sous-groupe distingué de* G.

D'autre part, soit $(a,c) \in (\mathbb{R}^\star)^2$, *alors il existe* $A = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \in G$: $f(A) = (a,c)$ *ainsi* f *est surjectif et par suite, d'après le premier théorème d'isomorphisme,* $G/H \simeq (\mathbb{R}^\star)^2$.

Solution de l'exercice 19.

1) *On a* $\tau\sigma = (14)(23)(56) \neq (16)(25)(34) = \sigma\tau$ *d'où* G *est non abélien et par suite* G *est non cyclique.*

2) $\circ(\sigma) = 6$ *et* $\circ(\tau) = 2$. *On a aussi* $\sigma\tau\sigma = (15)(24) = \tau$.

3) *On a* $\tau\sigma^2 = (\tau\sigma)\sigma = (\sigma^5\tau)\sigma = \sigma^4(\sigma\tau\sigma) = \sigma^4\tau$. *De la même façon, on a* $\tau\sigma^4 = \sigma^2\tau$.

4) *On a* $\circ(\sigma^2) = \frac{\circ(\sigma)}{2\wedge\circ(\sigma)} = 3$ *ainsi* $|H| = 3$ *et* $H = \{e, \sigma^2, \sigma^4\}$.

5) *On a* $(G/H)_g = \{H, \sigma H, \tau H, \tau\sigma H\}$ *avec* $\sigma H = \{\sigma, \sigma^3, \sigma^5\}$, $\tau H = \{\tau, \tau\sigma^2, \tau\sigma^4\}$ *et* $\tau\sigma H = \{\tau\sigma, \tau\sigma^3, \tau\sigma^5\}$. *Aussi,* $(G/H)_d = \{H, H\sigma, H\tau, H\tau\sigma\}$ *avec* $H\sigma = \{\sigma, \sigma^3, \sigma^5\}$, $H\tau = \{\tau, \sigma^2\tau, \sigma^4\tau\}$ *et* $H\tau\sigma = \{\tau\sigma, \sigma^2\tau\sigma, \sigma^4\tau\sigma\}$.
Il est évident que $\sigma H = H\sigma$. *On a* $\tau H = H\tau$ *car* $\tau\sigma^2 = \sigma^4\tau$ *et* $\tau\sigma^4 = \sigma^4\tau$ *(question 3). Aussi, on a* $\tau\sigma H = H\tau\sigma$ *car* $\sigma^2\tau\sigma = (\sigma^2\tau)\sigma = (\tau\sigma^4)\sigma = \tau\sigma^5$ *et* $\sigma^4\tau\sigma = (\sigma^4\tau)\sigma = (\tau\sigma^2)\sigma = \tau\sigma^3$ *ainsi* H *est un sous-groupe distingué de* G *et par suite* G/H *est un groupe.*

6) *On a* $(\sigma H)^2 = \sigma^2 H = \overline{e}$ *car* $\sigma^2 \in H$, $(\tau H)^2 = \tau^2 H = eH = H = \overline{e}$, $(\tau\sigma H)^2 = (\tau\sigma)^2 H = \tau(\sigma\tau\sigma)H = \tau^2 H = H = \overline{e}$ *ainsi* G/H *est un groupe d'ordre 4 non cyclique et par suite* $G/H \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ *(groupe de Klein).*

Corrigé du contrôle Final 2017-2018

Solution de l'exercice 20. *En utilisant une réduction modulo* $p = 2$, *on obtient* $\overline{P}(X) = x^3 + x^2 + 1 \in \mathbb{Z}_2[X]$. *Comme* $\overline{P}(X)$ *n'a pas de racines dans* $\mathbb{Z}_2$ *et* $\deg \overline{P}(X) = 3$, *alors* $\overline{P}(X)$ *est irréductible dans* $\mathbb{Z}_2[X]$ *et par suite* $P(X)$ *est irréductible dans* $\mathbb{Q}[X]$.

Solution de l'exercice 21.

1) *On vérifie facilement que* $\forall x, y \in \mathbb{Z}[i], f(x+y) = f(x) + f(y), f(xy) = f(x)f(y)$ *et* $f(1) = \overline{1}$.

2) *On an* $I = \ker f$, *en effet, soit* $x = a + ib \in \ker f$, *où* $a, b \in \mathbb{Z}$, *d'où* $f(x) = \overline{0}$, *alors* $\overline{a} = \overline{b}$ *ainsi* $a \equiv b \pmod 2$ *donc* $x \in I$. *Inversement, si* $x \in I$, *alors* $\overline{a} = \overline{b}$ *ainsi* $\overline{a-b} = \overline{0}$ *et par suite* $x \in \ker f$. *Alors* $\ker f = I$ *et par suite* I *est un idéal de* $\mathbb{Z}[i]$. *Aussi,* f *est surjective car* $\forall \overline{a} \in \mathbb{Z}_2$, *il existe* $x = a \in \mathbb{Z}[i]$ *tel que* $f(x) = \overline{a}$. *Ainsi, d'après le premier théorème d'isomorphisme,* $\mathbb{Z}[i]/\ker f = \mathbb{Z}[i]/I \simeq \operatorname{Im} f = \mathbb{Z}_2$ *donc* I *est un idéal maximal de* $\mathbb{Z}[i]$ *car* $\mathbb{Z}_2$ *est un corps.*

Solution de l'exercice 22.

1) *Soit* $\overline{x} \in G/H$, *où* $x \in G$. *Si* $x = e$, *alors* $\circ(\overline{x}) = 1$. *Supposons que* $x \neq e$. *Alors* $< x > \neq \{e\}$ *d'où* $< x > \cap H \neq \{e\}$ *alors* $\exists n \in \mathbb{N}^\star : x^n \in H$ *donc* $\overline{x}^n = \overline{e}$ *et ainsi l'ordre de* $\overline{x}$ *est fini.*

2) *Soit* x *un élément de* G *d'ordre un nombre premier* p.

   a) *Les générateurs de* $< x >$ *sont* $x, x^2, \ldots, x^{p-1}$.

   b) *On a* $< x > \neq \{e\}$ *d'où* $< x > \cap H \neq \{e\}$ *ainsi il existe* $k \in \{1, \ldots, p-1\} : x^k \in H$ *alors* $< x^k > \subset H$ *et comme* $< x > = < x^k >$, *alors* $x \in H$.

Solution de l'exercice 23.

1) *Soit* $P(X) \in \mathcal{U}(A)$, *alors* $\exists Q(X) \in A : P(X)Q(X) = 1$ *d'où* $\deg P + \deg Q = 0$ *ainsi* $P, Q \in \mathbb{Z}$ *et comme* $PQ = 1$, *alors* $P = \pm 1$. *D'autre part,* $-1, 1 \in \mathcal{U}(A)$ *donc* $\mathcal{U}(A) = \{-1, 1\}$.

2) a) *On a* $P(X) = p \notin \mathcal{U}(A)$. *Soit* $Q(X) \in A$ *tel que* $Q(X)/p$ *alors il existe* $T(X) \in A : p = QT$ *d'où* $\deg(Q) = \deg(T) = 0$ *donc* $Q, T \in \mathbb{Z}$ *ainsi* $Q = \pm 1$ *ou* $Q = \pm p$.

   b) p *n'est pas irréductible dans* $\mathbb{Q}[X]$ *car* p *est inversible dans* $\mathbb{Q}[X]$.

3) a) *En utilisant le critère d'Eisenstein avec* $p = 2$, *on a* $P(X) = X^n - 2$ *est irréductible dans* $\mathbb{Q}[X]$.

   b) *On a* $P(X) = X^n - 2 = 2(\frac{1}{2}X^n - 1)$, *alors* 2 *divise* $P(X)$ *dans* A *et comme* $2 \notin \mathcal{U}(A)$ *et aussi* 2 *et* $P(X)$ *ne sont pas associés dans* A, *alors* $P(X)$ *n'est pas irréductible dans* A.

4) a) *Soit* $n \in \mathbb{N}^\star$. *On a* $\frac{1}{2^n}X = 2\frac{1}{2^{n+1}}X \in I_{n+1}$, *alors* $I_n \subset I_{n+1}$. *Supposons qu'il existe* $n \in \mathbb{N}^\star$ *tel que* $I_n = I_{n+1}$, *alors* $\frac{1}{2^{n+1}}X \in I_n$ *d'où* $\exists P(X) \in A : \frac{1}{2^{n+1}}X = P(X)\frac{1}{2^n}X$ *ainsi* $P(X) = \frac{1}{2}$ *ce qui est faux car* $\frac{1}{2} \notin A$, *ainsi,* $I_n \subsetneq I_{n+1}$.

   b) *D'après la question précédente,* A *ne vérifie pas la condition de chaîne ascendante d'où* A *n'est pas principal et par suite* A *n'est pas euclidien.*

Corrigé du Rattrapage 2017-2018

Solution de l'exercice 24. *On a* $Q(X) = P(X+1) = X^4 + 4X^3 + 6X^2 + 6X + 2$, *alors, en prenant* $p = 2$ *et en utilisant le critère d'Eisenstein,* $Q(X) = P(X+1)$ *est irréductible dans* $\mathbb{Q}[X]$ *ainsi* $P(X)$ *est irréductible dans* $\mathbb{Q}[X]$.

Solution de l'exercice 25.

1) *Puisque* $i + 3 = (1-i)(1+2i)$, *alors* $i + 3 \in < 1 + 2i >$ *ainsi* $\overline{i+3} = \overline{0}$ *dans* A *et par suite* $\overline{i} = \overline{-3}$.

2) *Soit* $\overline{x+iy} \in A$, *avec* $x, y \in \mathbb{Z}$, *alors* $\overline{x+iy} = \overline{x} + \overline{i}\overline{y} = \overline{x-3y}$. *En effectuant la division euclidienne de* $x - 3y$ *par* 5 *dans* $\mathbb{Z}$, *on obtient* $x - 3y = 5q + r$, *avec* $(q, r) \in \mathbb{Z} \times \mathbb{N}$ *et* $r < 5$ *ainsi* $\overline{x+iy} = \overline{5q+r} = \overline{5}\overline{q} + \overline{r}$ *et en remarquant que* $\overline{5} = \overline{0}$ *dans* A *(car* $5 = (1-2i)(1+2i)$*), on obtient* $\overline{x+iy} = \overline{r}$, *avec* $r \in \{0, 1, 2, 3, 4\}$, *donc* $A \subset \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ *et comme* $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\} \subset A$, *alors* $A = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

3) *On considère l'application* $f : \mathbb{Z} \to A$, $m \mapsto m.\overline{1}$. *D'après le cours,* f *est un morphisme d'anneaux et* $\ker f = n\mathbb{Z}$, *avec* $n = car(A)$ *ainsi* $\ker f = 5\mathbb{Z}$ *(car* $car(A) = 5$*) donc, d'après le premier théorème d'isomorphisme,* $\operatorname{Im} f \simeq \mathbb{Z}_5$ *et par suite* A *possède un sous-anneau* B *isomorphe à* $\mathbb{Z}_5$ *ainsi il vient que* $A = B \simeq \mathbb{Z}_5$ *(car* $|A| = 5$*) alors* A *est un corps donc* $< 1+2i >$ *est un idéal maximal.*

Solution de l'exercice 26. *1) On a* G *est commutatif car* G *est monogène et par suite tous les sous-groupes de* G *sont distingués dans* G *ainsi* G/H *est un groupe. On a aussi* $|G/H| = [G : H] = n$. *Soit* $x \in G$ *et* $k, l \in \mathbb{Z}$. *On a* $x^k H = x^l H$ *si, et seulement si,* $(x^l)^{-1} x^k \in H$ *si, et seulement si,* $x^{k-l} \in H$ *si, et seulement si,* $\overline{x}^{k-l} = \overline{e}$ *(1). D'autre part, puisque* m *est le plus petit entier* > 0 *tel que* $x^m \in H$, *alors* $\circ(\overline{x}) = m$ *dans* G/H. *Ainsi, on a (1) si, et seulement si,* $m/k - l$.

2) *Supposons que* $\overline{x}^k = \overline{x}^l$ *avec* $k, l \in \{0, \ldots, m-1\}$ *d'où* $x^k H = x^l H$ *ainsi, d'après 1),* m *divise* $k - l$ *alors* m *divise* $|k - l|$ *et comme* $0 \leq |k - l| < m$, $|k - l| = 0$ *ainsi* $k = l$ *donc* $H, \overline{x}, \ldots, \overline{x}^{m-1}$ *sont deux à deux distincts.*

3) *D'après 2), on a* $\{H, \overline{x}, \ldots, \overline{x}^{m-1}\} \subset G/H$. *D'autre part, Soit* $\overline{a} \in G/H$, *alors* $a = x^k$, *avec* $k \in \mathbb{Z}$. *En effectuant la division euclidienne de* k *par* m, *on obtient* $k = qm + r$, *avec* $q, r \in \mathbb{Z}$ *et* $0 \leq r < m$ *ainsi* $\overline{a} = (\overline{x}^m)^q \overline{x}^r = \overline{x}^r \in \{H, \overline{x}, \ldots, \overline{x}^{m-1}\}$ *donc* $\{H, \overline{x}, \ldots, \overline{x}^{m-1}\} = G/H$ *ainsi* $|G/H| = m$ *et par suite* $m = n$.

Solution de l'exercice 27.

1) a) Il est évident que $A \neq \emptyset$ *(car le polynôme nul est un élément de A). Soit* $P(X) = a + 2bX + X^2T(X), Q(X) = c + 2dX + X^2S(X) \in A$, *avec* $a, b, c, d \in \mathbb{Z}$ *et* $T(X), S(X) \in \mathbb{Z}[X]$, *alors* $P(X) - Q(X) = (a-c) + 2(b-d)X + X^2(T(X) - S(X)) \in A$. *Aussi,* $P(X)Q(X) = ac + 2(ad+bc)X + X^2(4bd + 2bXS(X) + 2dXT(X) + aS(X) + cT(X) + x^2T(X)S(X)) \in A$ *et le polynôme* $1 \in A$ *donc A est un sous-anneau de* $\mathbb{Z}[X]$.

b) A est intègre car A est un sous-anneau de l'anneau intègre $\mathbb{Z}[X]$. *Soit* $P(X) \in \mathcal{U}(A)$, *alors* $P(X) \in \mathcal{U}(\mathbb{Z}[X]) = \mathcal{U}(\mathbb{Z}) = \{-1, 1\}$ *(*$\mathbb{Z}$ *est intègre). Inversement, on vérifie facilement que* $\{-1, 1\} \subset \mathcal{U}(A)$ *ainsi* $\mathcal{U}(A) = \{-1, 1\}$.

2) Il est évident que $2X \notin \mathcal{U}(A)$. *Soit* $P(X) \in A$ *un diviseur de* $2X$ *dans A, alors il existe* $Q(X) \in A$ *tel que* $2X = P(X)Q(X)$ *d'où* $1 = \deg P + \deg Q$ *d'où* $\deg P \in \{0, 1\}$. *Si* $\deg P = 0$, *alors* $\deg Q = 1$ *ainsi* $2X = a(b + 2cX)$, *avec* $P = a, c \in \mathbb{Z}^\star$ *et* $b \in \mathbb{Z}$ *alors* $2ca = 2$ *d'où* $ac = 1$ *donc* $P(X) \in \mathcal{U}(A)$. *De la même façon, on montre que si* $\deg P = 1$, $Q(X) \in \mathcal{U}(A)$ *donc* $2X$ *est irréductible dans A.*

3) Il est évident que les inversibles de A divisent 2 *et* $2X$. *Soit* $D(X) \in A$ *un diviseur commun de* 2 *et de* $2X$ *alors* $D(X) \in \mathcal{U}(A)$ *ou* $D(X) \sim 2X$ *dans A (car* $2X$ *est irréductible dans A). Cependant,* $D(X)$ *et* $2X$ *ne sont pas associés dans A (sinon* $\deg D(X) = \deg 2X = 1$ *et par suite* $D(X)$ *ne divise pas 2) donc* $D(x)$ *est inversible dans A et ainsi* 2 *et* $2X$ *sont premiers entre eux.*

4) Supposons qu'il existe $P(X), Q(X) \in A$ *tels que* $2P(X) + 2XQ(X) = 1$, *alors* $2\widetilde{P}(0) = 1$, *ce qui contredit le fait que* $P(X) \in A \subset \mathbb{Z}[X]$.
A n'est pas principal car dans un anneau principal, si deux éléments sont premiers entre eux, alors ils vérifient l'identité de Bezout.