université de BORDEAUX	ANNÉE UNIVERSITAIRE 2020 / 2021 Session 1 d'automne **PARCOURS / ÉTAPE : 4TMA903U** **Code UE : 4TTN901S, 4TTN901S** **Épreuve :** Structures algébriques 2 **Date :** 14/11/2020 **Heure :** 14h **Durée :** 1h30 Documents et équipements électroniques non autorisés Épreuve de Mr Brinon	**Collège Sciences et technologies**

Exercice 1

Déterminer les idéaux premiers de $A = \mathbf{Z}[X,Y]/\langle 6,(X-1)^2,Y^6\rangle$.

Solution : Soit $\mathfrak{p}$ un idéal premier de A. Notons $\mathfrak{P} \subset \mathbf{Z}[X,Y]$ son image inverse par le morphisme canonique $\mathbf{Z}[X,Y] \to A$: c'est un idéal premier de $\mathbf{Z}[X,Y]$ qui contient $I := \langle 6,(X-1)^2,Y^6\rangle$. Comme $\mathfrak{P}$ est premier, on a $(X-1)^2 \in \mathfrak{P} \Rightarrow X-1 \in \mathfrak{P}$ et $Y^6 \in \mathfrak{P} \Rightarrow Y \in \mathfrak{P}$. Par ailleurs, on a $6 \in \mathfrak{P} \Rightarrow (2 \in \mathfrak{P}$ ou $3 \in \mathfrak{P})$. Finalement, on a $\mathfrak{M}_2 \subset \mathfrak{P}$ ou $\mathfrak{M}_3 \subset \mathfrak{P}$, avec $\mathfrak{M}_2 = \langle 2, X-1, Y\rangle$ et $\mathfrak{M}_3 = \langle 3, X-1, Y\rangle$. Comme $\mathbf{Z}[X,Y]/\mathfrak{M}_2 \simeq \mathbf{Z}[X,Y]/\langle 2,X-1,Y\rangle \simeq \mathbf{Z}/2\mathbf{Z}$ et de même $\mathbf{Z}[X,Y]/\mathfrak{M}_3 \simeq \mathbf{Z}/3\mathbf{Z}$, les idéaux $\mathfrak{M}_2$ et $\mathfrak{M}_3$ sont maximaux : on a nécessairement $\mathfrak{P} \in \{\mathfrak{M}_2, \mathfrak{M}_3\}$. Il en résulte que A a deux idéaux premiers : $\mathfrak{m}_2 = \mathfrak{M}_2/I$ et $\mathfrak{m}_3 = \mathfrak{M}_3/I$. Ils sont maximaux tous les deux.

Exercice 2

Soient $n \in \mathbf{N}_{>0}$ et p premier impair.
(1) Montrer que le polynôme $X^n - p$ est irréductible dans $\mathbf{Q}[X]$.
(2) Montrer que p est soit irréductible, soit le produit de deux éléments irréductibles non associés dans $\mathbf{Z}[i]$ [indication : on pourra utiliser le stathme $N\colon \mathbf{Z}[i] \to \mathbf{N};\ z \mapsto |z|^2$ ou bien l'isomorphisme $\mathbf{Z}[X]/\langle X^2+1\rangle \xrightarrow{\sim} \mathbf{Z}[i]$]. En déduire que $X^n - p$ est irréductible dans $\mathbf{Q}(i)[X]$.

Solution : (1) On applique le critère d'Eisenstein, qui montre que $X^n - p$ est irréductible dans $\mathbf{Z}[X]$, donc dans $\mathbf{Q}[X]$.
(2) Comme $\mathbf{Z}[i]$ est factoriel, on peut écrire $p = \pi_1 \cdots \pi_r$ avec $\pi_1, \ldots, \pi_r$ premiers dans $\mathbf{Z}[i]$. En prenant la norme, il vient $p^2 = N(p) = N(\pi_1)\cdots N(\pi_r)$. Comme $N(\pi_i) > 1$ pour tout $i \in \{1,\ldots,r\}$, on a soit $r = 1$ (*i.e.* p est irréductible dans $\mathbf{Z}[i]$), soit $r = 2$ et $N(\pi_1) = N(\pi_2) = p$. Montrons que dans le deuxième cas, les éléments π_1 et π_2 ne sont pas associés : supposons qu'il existe $u \in \mathbf{Z}[i]^\times = \{\pm 1, \pm i\}$ tels que $\pi_1 = u^{-1}\pi_2$: on a $\pi_1^2 = up$. En écrivant $\pi_1 = a + ib$ avec $a, b \in \mathbf{Z}$, on a $a^2 - b^2 + 2abi \in \{\pm p, \pm pi\}$. Comme p est impair, on ne peut avoir $2ab = \pm p$: on a nécessairement $ab = 0$, et quitte à multiplier π_1 par i, on peut supposer que $b = 0$, de sorte que $a^2 = \pm p$, ce qui est impossible.

Autre preuve. On a $\mathbf{Z}[i]/p\,\mathbf{Z}[i] \simeq (\mathbf{Z}/p\,\mathbf{Z})[X]\langle X^2+1\rangle$. Le polynôme X^2+1 est soit irréductible dans $(\mathbf{Z}/p\,\mathbf{Z})[X]$, soit il se factorise sous la forme $X^2+1 = (X+a)(X-a)$ avec $a \in (\mathbf{Z}/p\,\mathbf{Z})^\times$. Dans le premier cas, $\mathbf{Z}[i]/p\,\mathbf{Z}[i]$ est un corps *i.e.* p est premier dans $\mathbf{Z}[i]$, et dans le deuxième cas, on a $\mathbf{Z}[i]/p\,\mathbf{Z}[i] \simeq \mathbb{Z}[X]/\langle (X-a)(X+a)\rangle \simeq \mathbf{F}_p \times \mathbf{F}_p$ (en vertu du théorème des restes chinois, vu que $\mathrm{pgcd}(X-a, X+a) = 1$ parce que p est impair). Cela implique alors que p est le produit de deux éléments irréductibles non associés dans $\mathbf{Z}[i]$.

Lorsque p est premier dans $\mathbf{Z}[i]$, le critère d'Eisenstein appliqué avec l'idéal premier $\langle p\rangle$ montre que $X^n - p$ est irréductible dans $\mathbf{Z}[i][X]$, donc dans $\mathbf{Q}(i)[X]$. Lorsque $p = \pi_1\pi_2$ avec π_1, π_2 irréductibles non associés dans $\mathbf{Z}[i]$, on applique le critère d'Eisenstein avec l'idéal premier $\langle \pi_1\rangle$.

Exercice 3

Posons $A = \mathbf{R}[X,Y]/\langle X^2+Y^2-1\rangle$. On note x et y les images de X et de Y dans A.
(1) Montrer que A est intègre.
(2) Montrer que l'unique morphisme $\mathbf{R}[Y] \to A$ qui envoie tout réel sur (la classe de) lui-même et Y sur y est injectif. Il induit donc un isomorphisme $\mathbf{R}[Y] \xrightarrow{\sim} \mathbf{R}[y] \subset A$.
(3) Montrer que $A = \mathbf{R}[y] \oplus \mathbf{R}[y]x$. Tout élément de A s'écrit donc de façon unique sous la forme $P(y) + Q(y)x$ avec $P(y), Q(y) \in \mathbf{R}[y]$.
(4) Si $\alpha = P(y) + Q(y)x$, on pose $\overline{\alpha} = P(y) - Q(y)x$. Montrer que $\alpha \mapsto \overline{\alpha}$ est un automorphisme de l'anneau A.
(5) Montrer que pour tout $\alpha \in A$, on a $N(\alpha) := \alpha\overline{\alpha} \in \mathbf{R}[y]$, puis que $N\colon A \to \mathbf{R}[y]$ est multiplicative (*i.e.* que $N(\alpha_1\alpha_2) = N(\alpha_1)N(\alpha_2)$).
(6) Montrer que $\alpha \in A^\times \Leftrightarrow N(\alpha) \in \mathbf{R}^\times$.
(7) Montrer que si $\alpha = P(y) + Q(y)x$ avec $P(y), Q(y) \in \mathbf{R}[y]$, on a

$$\deg(N(\alpha)) = 2\max\{\deg(P), \deg(Q)+1\}$$

(on rappelle que $\deg(0) = -\infty$). En déduire que x est irréductible dans A.
(8) Décrire $A/\langle x\rangle$ et en déduire que A n'est pas factoriel.

Solution : (1) Il s'agit de montrer que X^2+Y^2-1 est premier dans $\mathbf{R}[X,Y]$. Comme ce dernier est factoriel, il suffit de montrer qu'il est irréductible. Cela résulte du critère d'Eisenstein, appliqué avec l'idéal premier $\langle Y-1\rangle$ de l'anneau $\mathbf{R}[Y][X]$.
(2) Soit $P(Y)$ un élément du noyau : il existe $f(X,Y) \in \mathbf{R}[X,Y]$ tel que $P(Y) = (X^2 + Y^2-1)f(X,Y)$. Pour des raisons de degré en l'indéterminée X (l'anneau $\mathbf{R}[Y]$ est intègre), cela implique $P(Y) = 0$.
(3) Un élément $\alpha \in A$ est l'image d'un polynôme $f(X,Y) \in \mathbf{R}[X,Y]$. Comme le polynôme X^2+Y^2-1 est unitaire vu comme polynôme en l'indéterminée X, on dispode de la division euclidienne de $f(X,Y)$ par X^2+Y^2-1 dans $(\mathbf{R}[Y])[X]$: il existe $g(X,Y) \in \mathbf{R}[X,Y]$ et $P(Y), Q(Y) \in \mathbf{R}[Y]$ uniques tels que $f(X,Y) = (X^2+Y^2-1)g(X,Y) + Q(Y)X + P(Y)$. On a alors $\alpha = P(y) + Q(y)x$ avec $P(Y), Q(Y) \in \mathbf{R}[Y]$ uniques. Cela montre que $A = \mathbf{R}[y] \oplus \mathbf{R}[y]x$.
(4) La propriété universelle de l'anneau de polynômes $\mathbf{R}[X,Y]$ implique qu'il existe un unique morphisme d'anneaux $\mathbf{R}[X,Y] \to A$ qui envoie X sur $-x$ et Y sur y. Il envoie alors X^2+Y^2-1 sur $(-x)^2 + y^2 - 1 = 0$: il se factorise en un morphisme d'anneaux $A \to A$ qui est précisément $\alpha \mapsto \overline{\alpha}$. Il est involutif : c'est un automorphisme.
(5) Écrivons $\alpha = P(y) + Q(y)x$ avec $P(y), Q(y) \in \mathbf{R}[Y]$. On a

$$N(\alpha) = (P(y)+Q(y)x)(P(y)-Q(y)x) = P(y)^2 - x^2Q(y)^2 = P(y)^2 + (y^2-1)Q(y)^2 \in \mathbf{R}[y].$$

La multiplicativité de N résulte de celle de $\alpha \mapsto \overline{\alpha}$ (c'est un morphisme d'anneaux).
(6) Si $N(\alpha) \in \mathbf{R}^\times$, alors α est inversible dans A, d'inverse $N(\alpha)^{-1}\overline{\alpha}$. Réciproquement, supposons $\alpha \in A^\times$: il existe $\beta \in A$ tel que $\alpha\beta = 1$. Comme N est multiplicative, on a $N(\alpha)N(\beta) = 1$, ce qui implique que $N(\alpha) \in \mathbf{R}[y]^\times = \mathbf{R}^\times$ (rappelons que $\mathbf{R}[y] \simeq \mathbf{R}[Y]$).
(7) On a vu que $N(\alpha) = P(y)^2 + (y^2-1)Q(y)^2$ donc $\deg(N(\alpha)) \leqslant 2\max\{\deg(P), \deg(Q)+1\}$, avec égalité lorsque $\deg(P) \neq \deg(Q)+1$. Lorsque $\deg(P) = \deg(Q)+1$, le coefficient de $y^{2\deg(P)}$ dans $N(\alpha)$ est $a^2+b^2 > 0$, où a (resp. b) est le coefficient dominant de P (resp. de Q) : on a $\deg(N(\alpha)) = 2\max\{\deg(P), \deg(Q)+1\}$ dans tous les cas.
Si $x = \alpha\beta$, on a $y^2 - 1 = N(x) = N(\alpha)N(\beta)$ dans $\mathbf{R}[y]$, donc $\deg(N(\alpha)) + \deg(N(\beta)) = 2$: comme $N(\alpha)$ et $N(\beta)$ sont pairs, on a nécessairement $N(\alpha) \in \mathbf{R}^\times$ ou $N(\beta) \in \mathbf{R}^\times$, ce qui montre que x est irréductible.
(8) On a $A/\langle x\rangle \simeq \mathbf{R}[X.Y]/\langle X^2+Y^2-1, X\rangle \simeq \mathbf{R}[Y]/\langle Y^2-1\rangle \simeq \mathbf{R}^2$ (en vertu du théorème des restes chinois). En particulier, l'anneau $A/\langle x\rangle$ n'est pas intègre : l'élément x n'est pas premier. Contenant un élément irréductible mais pas premier, l'anneau A n'est pas factoriel.