

**Exercice 1.** On pose :

$$A = \mathbb{Z}[j] := \{a + bj \mid a, b \in \mathbb{Z}\}$$

**1. Structure d'anneau.** (a) On vérifie que  $\mathbb{Z}[j] \subseteq \mathbb{C}$  est stable par addition et multiplication, qu'il contient 1 et 0 ainsi  $\mathbb{Z}[j]$  est un anneau, on voit facilement qu'il est stable par conjugaison complexe. Comme  $j$  est algébrique sur  $\mathbb{Q}$  ( avec  $\text{Irr}(j, \mathbb{Q}, X) = X^2 + X + 1$  ) on sait que  $\mathbb{Q}[j] = \mathbb{Q}(j)$ . On peut aussi le vérifier à la main : soit  $z := a + bj \in \mathbb{Q}[j] - \{0\}$  alors

$$\frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{a + b\bar{j}}{a^2 + ab(j + \bar{j}) + b^2},$$

on conclut en disant que  $j + \bar{j} + 1 = 0$  et  $\bar{j} = j^2$ .

(b) Clair.

**2. Inversibles.** (a) Si  $u \in A^\times$  alors  $\exists v \in A, uv = 1$ . De l'écriture  $N(uv) = N(u)N(v) = N(1) = 1$  on obtient  $N(u) \in \mathbb{Z}^\times = \{\pm 1\}$ , or  $\forall z \in \mathbb{C}, N(z) \geq 0$  donc  $N(u) = 1$ . Inversement si  $N(u) = u\bar{u} = 1$  alors  $\bar{u}$  est l'inverse de  $u$  dans  $A$ .

(b) On a  $N(u) = a^2 + b^2 - ab = 1$  c'est à dire  $a^2 + b^2 = 1 + ab$ . Si  $ab < 0$  on aurait  $a^2 + b^2 \leq 0$  et donc  $a = b = 0$  or  $u = 0 \notin A^\times$ . Ainsi  $ab \geq 0$ . De plus l'écriture  $N(u) = (a-b)^2 + ab = 1$  implique que  $(a-b)^2 = 1$  et  $ab = 0$  ou bien  $(a-b)^2 = 0$  et  $ab = 1$ , on termine en distinguant tous les cas.

(c) On combine les deux questions précédentes.

**3. L'anneau est principal.** (a) On a  $N(\alpha + \beta j) = \alpha^2 + \beta^2 - \alpha\beta \leq \alpha^2 + \beta^2 + |\alpha\beta|$  pour tous  $\alpha, \beta \in \mathbb{Q}$ .

(b) On a  $z_1/z_2 \in \mathbb{Q}(j) = \mathbb{Q}[j]$  et le degré de  $\mathbb{Q}[j]$  sur  $\mathbb{Q}$  est 2 donc  $\{1, j\}$  est une  $\mathbb{Q}$ -base de  $\mathbb{Q}[j]$ .

(c) On a  $N(R) = N(z_2)N(a + bj - \frac{z_1}{z_2}) = N(z_2)N((a-r) + (b-s)j) \leq N(z_2)((a-r)^2 + (b-s)^2 + |(r-a)(b-s)|) \leq 3/4N(z_2) < N(z_2)$  d'après les deux questions précédentes.

(d) C'est une application de la définition.

**4. Eléments irréductibles.** (a) Soit  $f \in \mathbb{Z}[j]$  un élément irréductible.

(i) On a  $N(f) = f\bar{f} \in \mathbb{Z} \cap f\mathbb{Z}[j]$  et  $N(f) \neq 0$  car  $f \neq 0$ .

- (ii) On vérifie que le morphisme  $\mathbb{Z} \rightarrow \mathbb{Z}[j] \rightarrow \mathbb{Z}[j]/f\mathbb{Z}[j]$  a pour noyau  $\mathbb{Z} \cap f\mathbb{Z}[j]$ , le théorème de factorisation montre alors que  $\mathbb{Z}/(\mathbb{Z} \cap f\mathbb{Z}[j])$  s'injecte dans  $\mathbb{Z}[j]/f\mathbb{Z}[j]$  qui est intègre (car  $\mathbb{Z}[j]$  est principal et  $f$  irréductible), donc  $\mathbb{Z} \cap f\mathbb{Z}[j]$  est un idéal premier de  $\mathbb{Z}$  non nul.
- (iii) On a  $N(f) \in \mathbb{Z} \cap f\mathbb{Z}[j] = p\mathbb{Z}$ , donc  $f\bar{f} = N(f) = ps$  avec  $s \in \mathbb{N}$ . On remarque que  $f$  et  $\bar{f}$  sont irréductibles dans  $A$ , donc  $f\bar{f} = ps$  est la décomposition en irréductibles de  $ps$  dans l'anneau factoriel  $A$ . Si  $s \neq 1$  alors  $s \notin A^\times$  donc  $s$  a un facteur irréductible dans  $A$  et par unicité de l'écriture en irréductibles on a :

$$f|s \text{ ou } \bar{f}|s.$$

Faisons le cas  $f|s$  (l'autre est similaire). On a donc  $fu = s$  avec  $u \in A$ , donc  $\bar{f}\bar{u} = \bar{s} = s$  ainsi  $up = \bar{f}$ , on en déduit que  $p^2u\bar{u} = ps$ . Or  $u \in A^\times$  sinon  $u$  aurait un facteur irréductible dans  $A$  qui ne peut être que  $\bar{f}$  et donc  $s = f\bar{f}$ , or  $ps = f\bar{f}$  ce qui est une contradiction. Ainsi  $N(u) = u\bar{u} = 1$  et  $ps = p^2$ . Dans cette situation, si  $p \in N(\mathbb{Z}[j])$ , il existe  $z \in A$  tel que  $N(f) = p^2 = N(z^2)$  ce qui s'écrit

$$f\bar{f} = z^2\bar{z}^2,$$

ce qui implique (par exemple) que  $f|z$ , donc  $\bar{f}|\bar{z}$  et donc  $f\bar{f}|z\bar{z}$  ce qui donne une contradiction.

- (b) Soit  $z \in \mathbb{Z}[j]$ .
- (i) Si  $z$  avait deux facteurs irréductibles, en appliquant la norme on trouverait deux facteurs différents de 1 à l'élément  $p \in \mathbb{Z}$ .
- (ii) Si  $z = ab$  avec  $a, b \notin A^\times$  alors  $N(z) = p^2 = N(a)N(b)$ . Si  $p|N(a)$  et  $p|N(b)$  alors on a en fait  $N(a) = p$  et  $N(b) = p$ , ce qui contredit les hypothèses. Ainsi on a  $p^2 = N(a)$  et  $1 = N(b)$  ou le contraire, dans tous les cas on a bien  $a$  ou  $b$  dans  $A^\times$ .
- (c) Les éléments  $2 + j$  et  $2 + 3j$  sont de norme 3 et 7 donc sont irréductibles. L'élément  $3 + 8j$  est de norme  $49 = 7^2$ . Or on vient de voir que  $2 + 3j$  est de norme 7, donc  $7 \in N(\mathbb{Z}[j])$ , donc  $3 + 8j$  n'est pas irréductible.

**Exercice 2.** 1. L'anneau  $\mathbb{Z}[X, Y]/(2XY - 3)$  est intègre si et seulement si  $(2XY - 3)$  est un idéal premier de  $\mathbb{Z}[X, Y]$  si et seulement si  $(2XY - 3)$  est un élément irréductible de  $\mathbb{Z}[X, Y]$  (car  $\mathbb{Z}[X, Y]$  est factoriel). On pose  $A := \mathbb{Z}[X]$ , c'est un anneau factoriel de corps de fractions  $K = \mathbb{Q}(X)$ , or le polynôme  $2XY - 3 \in K[Y]$  est de degré 1 donc

irréductible. Finalement  $2XY - 3 \in A[Y]$  est de degré  $\geq 1$ , de contenu 1 (attention, on calcule le contenu dans  $A$ , pas dans  $\mathbb{Z}$ ) et irréductible sur le corps de fractions de  $A$ , donc c'est un irréductible de  $A[Y]$ .

Le polynôme  $2XY - 6 = 2(XY - 3)$  n'est pas irréductible dans  $\mathbb{Z}[X, Y]$  car  $XY - 3, 2 \notin \mathbb{Z}[X, Y]^\times = \mathbb{Z}^\times$ , donc  $\mathbb{Z}[X, Y]/(2XY - 6)$  n'est pas intègre.

L'anneau  $\mathbb{Q}[X, Y]/(2XY - 6)$  est intègre car  $2XY - 6$  est un polynôme irréductible de  $A[Y]$  avec  $A = \mathbb{Q}[X]$ . En effet,  $A$  est factoriel de corps de fractions  $K = \mathbb{Q}(X)$  et  $2XY - 6 \in K[Y]$  est de degré 1 donc irréductible. Le polynôme  $2XY - 6 \in A[Y]$  est donc de degré  $\geq 1$ , de contenu 1 (contenu calculé dans  $A$ ) et irréductible de  $K[Y]$ , c'est donc un irréductible de  $A[Y]$ .

2. L'équation  $X^2 = 1$  est une équation polynomiale de degré 2. Sur l'anneau  $\mathbb{Z}/8\mathbb{Z}$ , on vérifie qu'elle a 4 racines:  $1, -1, 3, -3$ . Sur le corps  $\mathbb{Z}/53\mathbb{Z}$ , (53 est premier), elle a au plus deux racines. 1 et  $-1$  sont racines donc elle a exactement 2 racines.

**Exercice 3.** 1. Le critère d'Eisenstein appliqué à l'irréductible  $Y - 1$  de  $\mathbb{Q}[Y]$  donne que  $X^2 + Y^2 - 1$  est irréductible dans  $\mathbb{Q}(Y)[X]$ . De plus le contenu de  $X^2 + Y^2 - 1$  est égal à  $\text{pgcd}(1, 0, Y^2 - 1)$  dans  $\mathbb{Q}[Y]$  et vaut donc 1. Donc  $X^2 + Y^2 - 1$  est irréductible dans  $\mathbb{Q}[X, Y]$ .

$\mathbb{Q}[X, Y]$  étant factoriel,  $X^2 + Y^2 - 1$  est donc premier donc  $A = \mathbb{Q}[X, Y]/\langle X^2 + Y^2 - 1 \rangle$  est intègre.

2. Soit  $C \in \mathbb{Q}[X, Y]$ , le coefficient dominant de  $X^2 + Y^2 - 1$  vu comme polynôme à coefficient dans  $\mathbb{Q}[Y]$  est 1 donc inversible, par division euclidienne il existe un unique couple  $(Q, R) \in (\mathbb{Q}[X, Y])^2$  tel que

$$C(X, Y) = (X^2 + Y^2 - 1)Q(X, Y) + R(X, Y) \text{ et } \deg_X R \leq 1.$$

Donc  $R(X, Y) = A_1(Y)X + A_2(Y)$  et  $s(C) = s(R) = A_1(y)x + A_2(y)$ . L'unicité de cette écriture provient de l'unicité du reste dans la division euclidienne.

3. Considérons le morphisme  $\phi = s \circ t$  où  $s$  et  $t$  sont les morphismes canoniques surjectifs

$$s : \mathbb{Q}[X, Y] \rightarrow A \text{ et } t : A \rightarrow A/\langle x \rangle.$$

$\phi$  est clairement surjectif.

On montre facilement que le noyau de  $\phi$  est  $\langle X^2 + Y^2 - 1, X \rangle$ . Or  $\langle X^2 + Y^2 - 1, X \rangle = \langle Y^2 - 1, X \rangle$ . Donc, par théorème de factorisation:

$$\mathbb{Q}[X, Y]/\langle Y^2 - 1, X \rangle \simeq A/\langle x \rangle.$$

Or  $\mathbb{Q}[X, Y]/\langle Y^2 - 1, X \rangle \simeq \mathbb{Q}[Y]/\langle Y^2 - 1 \rangle$  d'où le résultat.

4.  $\mathbb{Q}[Y]/\langle Y^2 - 1 \rangle$  n'est pas intègre car  $(\bar{Y} - 1)(\bar{Y} + 1) = 0$ , donc  $A/\langle x \rangle$  ne l'est pas donc  $x$  n'est pas premier dans  $A$ .
5.  $x$  est non nul.  $x$  n'est pas inversible dans  $A$ . En effet, il existerait  $b \in A$  tel que  $xb = 1$  c'est-à-dire, il existerait  $B$  et  $C$  dans  $\mathbb{Q}[X, Y]$  tels que  $XB(X, Y) = 1 + C(X, Y)(X^2 + Y^2 - 1)$ . En prenant  $Y = 1$ , on obtient

$$X^2C(X, 1) + XB(X, 1) = 1.$$

Le coefficient constant du polynôme du membre de droite est 0, donc ne peut être égal à 1, donc  $x$  n'est pas inversible.

Supposons maintenant que  $x = bc$  et montrons que  $b$  ou  $c$  est inversible dans  $A$ . D'après la question 2),  $b = P(y) + xQ(y)$  et  $c = R(y) + xS(y)$ , donc comme  $x^2 = 1 - y^2$  dans  $A$ ,

$$x = bc = P(y)R(y) + (1 - y^2)Q(y)S(y) + x(P(y)S(y) + Q(y)R(y)).$$

D'après l'unicité d'une telle écriture, on a

$$\begin{cases} P(y)R(y) + (1 - y^2)Q(y)S(y) = 0 \\ P(y)S(y) + Q(y)R(y) = 1 \end{cases}$$

Donc  $P = P^2S + QPR = P^2S + Q^2(Y^2 - 1)S = (P^2 + Q^2(Y^2 - 1))S$ .

Si  $S = 0$  alors  $P = 0$  et  $Q(y)R(y) = 1$  donc  $c = R(y)$  est inversible.

Si  $S \neq 0$ , alors du fait de la positivité des coefficients dominants de  $P^2$  et  $Q^2(Y^2 - 1)$ ,

$$\deg P = \deg (P^2 + Q^2(Y^2 - 1))S \geq \max(2 \deg P, 2 \deg Q + 2).$$

donc  $\deg(P) \leq 0$  et  $Q \equiv 0$ . On en déduit  $P(y)S(y) = 1$  donc  $b = P(y)$  est inversible dans  $A$ .

Donc  $x$  est bien irréductible dans  $A$ .

6.  $x$  est un élément irréductible dans  $A$  mais qui n'est pas premier dans  $A$ . Donc  $A$  n'est pas factoriel.