## QCM 3

1. La préimage d'un idéal par un morphisme d'anneaux est un idéal.
   (a) Vrai
   (b) Faux

2. L'image d'un idéal par un morphisme d'anneaux est un idéal.
   (a) Vrai
   (b) Faux

3. L'élément 3 est irréductible dans $\mathbb{Z}[i]$.
   (a) Vrai
   (b) Faux

4. L'idéal (3) est maximal dans $\mathbb{Z}[i]$.
   (a) Vrai
   (b) Faux

5. On considère le morphisme d'anneaux $f : \mathbb{Z}[X] \to \mathbb{C}, P \mapsto P(i)$. Le noyau de $f$
   (a) est l'idéal engendré par $X - i$
   (b) est égal au noyau de l'application $g : \mathbb{Z}[X] \to \mathbb{C}, P \mapsto P(-i)$
   (c) est égal à $\{0\}$
   (d) est égal à l'idéal engendré par $X^2 + 1$

6. On considère le morphisme d'anneaux $f : \mathbb{Z}[X] \to \mathbb{C}, P \mapsto P(2)$. Le noyau de $f$
   (a) est l'idéal engendré par $X - 2$
   (b) est égal au noyau de l'application $g : \mathbb{Z}[X] \to \mathbb{C}, P \mapsto P(-2)$
   (c) est égal à $\{0\}$
   (d) est égal à l'idéal engendré par $X^2 - 4$

7. Soit $A \subset M_2(\mathbb{R})$ l'ensemble des matrices de la forme $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Cochez l'unique affirmation fausse
   (a) L'ensemble $A$ est un espace vectoriel réel de dimension 4
   (b) L'ensemble $A$ est un corps isomorphe à $\mathbb{C}$
   (c) L'ensemble $A$ est un anneau isomorphe à $\mathbb{R}[X]/(X^2 + 1)$

8. Cochez les affirmations vraies. L'anneau quotient $\mathbb{R}[X]/(X^2 + X + 1)$ est
   (a) un $\mathbb{R}$-espace vectoriel de dimension 2
   (b) un corps
   (c) un anneau principal isomorphe à $\mathbb{R}[X]/(X^2 - 1)$
   (d) isomorphe à $\mathbb{R}[X]/(X^2 + 1)$

9. Le polynôme $X^4 + 1$ est :
   (a) irréductible sur $\mathbb{Q}$ et réductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$.
   (b) irréductible sur $\mathbb{Q}$ et irréductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$.
   (c) réductible sur $\mathbb{Q}$ et réductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$.
   (d) irréductible sur $\mathbb{Q}$ et irréductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$.

10. Le polynôme $X^4 - X - 1$ est :
   (a) irréductible sur $\mathbb{Q}$ et réductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$.
   (b) irréductible sur $\mathbb{Q}$ et irréductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$.
   (c) réductible sur $\mathbb{Q}$ et réductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$.
   (d) irréductible sur $\mathbb{Q}$ et irréductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$.

11. Le groupe $\mathbb{Z}[\sqrt{3}]^*$ est (indication : considérer $\frac{1}{2+\sqrt{3}}$).
   (a) cyclique infini
   (b) cyclique fini
   (c) infini non cyclique
   (d) fini non cyclique

12. L'idéal $(2, X)$ de $\mathbb{Z}[X]$ est :
   (a) principal et maximal
   (b) principal non maximal
   (c) non principal et maximal
   (d) ni principal ni maximal

13. Soit $j = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$. Le groupe des inversibles de l'anneau $\mathbb{Z}[j]$ est :
   (a) infini
   (b) $\{\pm 1, \pm j\}$
   (c) $\{\pm 1\}$
   (d) $\{\pm 1, \pm i\}$
   (e) $\{\pm 1, \pm j, \pm(1+j)\}$

14. Combien y a-t-il d'éléments inversibles dans l'anneau $\mathbb{Z}/36\mathbb{Z}$ ?
   (a) 6
   (b) 12
   (c) 24
   (d) 35

**CORRECTION**

1. Vrai

   Soit $f : A \longrightarrow B$ et $I$ un idéal de $B$. Par exemple si $a \in f^{-1}(I)$ et $b \in A$. On a $f(ab) = f(a)f(b)$ appartient à $I$ car $f(a) \in I$. Donc $ab \in f^{-1}(I)$.
2. Faux

   Soit $f : \mathbb{Z} \longrightarrow \mathbb{R}$ l'inclusion. L'image de l'ennsemble des nombres pairs n'est pas un idéal de $\mathbb{R}$.
3. Vrai

   Ecrivons $3 = z_1 z_2$ avec $z_1$ et $z_2$ dans $\mathbb{Z}[i]$. En prenant les modules au carré il vient $9 = |z_1|^2 |z_2^2|$. Comme $|z_1|^2$ et $|z_2^2|$ sont dans $\mathbb{N}$, quitte à échanger $z_1$ et $z_2$ on est dans l'un des deux cas suivants :
   Cas 1. $|z_1|^2 = 1$ et $|z_2|^2 = 9$.
   Cas 2. $|z_1|^2 = |z_2|^2 = 3$.

   Dans ce cas 1, $z_1.\bar{z}_1 = 1$ dans $z_1$ est inversible dans $\mathbb{Z}[i]$.
   Dans le cas 2. Ecrivons $z_1 = a + ib$ avec $a$ et $b$ dans $\mathbb{Z}$. Alors $a^2 + b^2 = 3$ : contradiction. 3 n'est pas la somme de deux carrés.
4. Vrai

   3 est irréducible et $\mathbb{Z}[i]$ est principal car euclidien.

   Attention : Dans $\mathbb{Z}[X]$, l'déal (3) n'est pas maximal car :
   $X$ n'est pas inversible modulo 3. En effet, il n'existe pas de polynômes $P$ et $Q$ dans $\mathbb{Z}[X]$ tel que $XP = 3Q + 1$.
5. Deux bonnes réponses.
   (a) Faux car $X - i \notin \mathbb{Z}[X]$ ;
   (b) Vrai. Pour $P \in \mathbb{R}[X]$ (et donc $\mathbb{Z}[X]$) $P(i) = 0$ si et seulement si $0 = \overline{P(i)} = P(-i)$.
   (c) Faux. $X^2 + 1$ est dans le noyau.
   (d) Vrai.
   Il est clair que cet idéal est dans le noyau.
   Réciproquement, soit $P$ dans le noyau. Comme $X^2 + 1$ est unitaire, il existe $Q$ et $R$ dans $\mathbb{Z}[X]$ tels que $P = (X^2 + 1)Q + R$ et $R$ nul ou de degré 1. Mais alors $P(i) = 0$ implique que $R(i) = R(-i) = 0$. Donc $R = 0$ et $P$ est dans l'idéal.
6. (a) Vrai. Même preuve que 5.d.
   (b) Faux. Pensez à $X + 2$.
   (c) Faux. Pensez à $X - 2$.
   (d) Faux. Pensez à $X + 2$.
7. (a) Faux. Sa dimension est 2.
   (b) Vrai. L'isomorphisme est l'aaplication qui à $z = a + ib$ associe la matrice de l'application $\mathbb{R}$-linnéaire de $\mathbb{C}$ dans $\mathbb{C}$ qui a $z'$ associe $zz'$ dans la base $(1, i)$.
   (c) Vrai car $\mathbb{C}$ l'est.
8. Tout est vrai sauf la troisième. La dimension de $\mathbb{K}[X]/(P)$ est le degré de $P$. De plus $X^2+X+1 = (X + \frac{1}{2})^2 + \frac{3}{4}$ n'a pas de racines. Donc $X^2 + X + 1$ est irréductible. Donc le quotient est un corps. Après changement affine de variable $X^2 + X + 1$ est égal à $X^2 + 1$. D'où le dernier isomorphisme. L'anneau $\mathbb{R}[X]/(X^2 - 1)$ n'est pas un corps car $(X - 1)(X + 1) = 0$ alors que $X + 1$ et $X - 1$ sont non nuls.

9. Dans $\mathbb{Z}/2\mathbb{Z}$, on a $(X^2+1)^2 = X^4 + 2X^2 + 1 = X^4 + 1$. Donc le polynôme est réductible.
Dans $\mathbb{Q}[X]$. D'après le théorème de Gauss (contenu 1), il suffit de vérifier l'irréductiblité dans $\mathbb{Z}[X]$. A cause du signe $X^4+1$ n'a pas de racines. Donc $X^4+1$ n'a pas de facteur de degré 1. Supposons que
$$X^4 + 1 = (aX^2 + bX + c)(a'X^2 + b'X + c')$$
avec $a, b, c, a', b'$ et $c'$ dans $\mathbb{Z}$. Alors $aa' = 1$. Quitte à multiplier par $-1$, on peut supposer que $a = a' = 1$. Donc
$$X^4 + 1 = (X^2 + bX + c)(X^2 + b'X + c')$$
Donc $cc' = 1$. Donc $c = c' = \pm 1$. Le terme en $X$ est $c(b + b')$ donc $b' = -b$. Le terme en $X^2$ est $2c + bb' = 2c - b^2$. Donc $b^2 = 2$. Contradiction.
Donc le polynôme est irréductible dans $\mathbb{Q}[X]$.

10. Maintenant $X^4 - X + 1$.
Dans $\mathbb{Z}/2\mathbb{Z}[X]$. Le polynôme n'a pas de racines (ni 0 ni 1). Donc seule possiblité 2 polynômes de degré 2. Donc unitaires et de termes constants non nuls. D'où l'équation
$$X^4 + X + 1 = (X^2 + bX + 1)(X^2 + b'X + 1)$$
Le coef en $X$ est $b + b'$. Donc quitte à échanger $b' = 0$ et $b = 1$. Or $(X^2 + X + 1)(X^2 + 1) = X^4 + X^3 + X + 1 \neq X^4 + X + 1$.
Ainsi $X^4 - X + 1$ est irréductible dans $\mathbb{Z}/2\mathbb{Z}[X]$.

Dans $\mathbb{Q}[X]$. Comme le contenu vaut 1, d'après Gauss, il suffit de regarder les factorisations dans $\mathbb{Z}[X]$. Quitte à multiplier par $-1$, avec des polynômes unitaires.
Donc si $X^4 - X + 1$ a un tel facteur de degré 1, il a une racine dans $\mathbb{Z}$. Ce qui est impossible.
Reste le cas de deux polynômes de degré 2. On arrive alors à
$$X^4 + X + 1 = (X^2 + bX + \varepsilon)(X^2 + b'X + \varepsilon)$$
avec $b$ et $b'$ dans $\mathbb{Z}$ et $\varepsilon = \pm 1$. Le terme en $X^3$ montre que $b' = -b$. Alors le terme en $X^2$ donne $b^2 = \pm 2$ ce qui est impossible.
Ainsi $X^4 - X + 1$ est irréductible dans $\mathbb{Q}[X]$.

11. On a
$$\frac{1}{2+\sqrt{3}} = \frac{2-\sqrt{3}}{4-3} = 2 - \sqrt{3}.$$
Donc $\frac{1}{2+\sqrt{3}}$ est innversible ainsi que ces puissances. Donc, $\mathbb{Z}[\sqrt{3}]^*$ est infini.
Comme de plus $-1 \in \mathbb{Z}[\sqrt{3}]^*$, il n'est pas cyclique. ERn effet, un sous-groupe d'un groupe cyclique est cyclique.

12. Pas principal (voir cours). Mais maximal car le quotient est $\mathbb{Z}/2\mathbb{Z}$ qui est unn corps.

13. $\mathbb{Z}[j]^* = \{\pm 1, \pm j, \pm(1 + j)\}$.

Un calcul direct montre que $j^2 = -j - 1 = \bar{j}$. Soit $a$ et $b$ des entiers et $z = a + bj$. On calcule
$$z\bar{z} = a^2 - ab + b^2 = (a - \frac{b}{2})^2 + \frac{3}{4}b^2 \in \mathbb{Z}.$$
Donc si $z$ est inversible, $z\bar{z}$ est inversible dans $\mathbb{Z}$. On tombe sur l'équation
$$(a - \frac{b}{2})^2 + \frac{3}{4}b^2 = \pm 1$$
Bienn sûr $-1$ est impossible. Pour $+1$ on a $-1 \leq a - \frac{b}{2} \leq 1$. On obtient $(a - \frac{b}{2}) = -1, -\frac{1}{2}, 0, \frac{1}{2}$ ou 1.
Or 0 est impossible car $b^2 = \frac{4}{3}$ n'a pas de solution dans $\mathbb{Z}$. Mais alors $b = 0$ et $a = \pm 1$. Pour $a - \frac{b}{2} = \frac{1}{2}$ on trouve $-j$ et $1 + j\ldots$

14. Un élément $\bar{k}$ est inversible s'il existe $l \in \mathbb{Z}$ tel que 36 divise $kl - 1$. D'après Bezout cela équivaut à $k$ et 36 premiers entre eux.

    Aux 36 entiers, $0, 1, \ldots, 35$ on enlève les pairs il en reste 18. On enlève aussi $3, 9, 15, \ldots, 33$ les 6 multiples de 3 impairs. Donc $36 - 24 = 12$ éléments inversibles.