Correction TD5

Exercice 12.

1. On sait que les idéaux de $\mathbb{Z}$ sont les idéaux de la forme $n\mathbb{Z}$ pour $n \geqslant 0$. Plus généralement, si A est un anneau commutatif, et $a \in A$, l'ensemble $(a) = \{ax \mid x \in A\}$ des multiples de a est un idéal de A (il y a des idéaux qui ne sont pas de cette forme dans les anneaux non principaux, par exemple $(2, X)$ dans $\mathbb{Z}[X]$).

2. Dans $\mathbb{Z}$, prenons $n\mathbb{Z}$ et $m\mathbb{Z}$ deux idéaux. Par construction $n\mathbb{Z}\cup m\mathbb{Z}$ est l'ensemble des entiers qui sont multiples de n ou de m. Ce n'est en général pas un idéal. Par exemple $2\mathbb{Z} \cup 3\mathbb{Z}$ contient $2, 3$ mais pas $2 + 3 = 5$, donc ce n'est même pas un sous-groupe de $\mathbb{Z}$.
Plus généralement Soient A un anneau, I, J deux idéaux de A. On a

$$I \cup J \text{ idéal de } A \Rightarrow I \cup J \text{ sous-groupe de } (A, +).$$

On a vu dans le TD 1 que ceci implique $I \subset J$ ou bien $J \subset I$. Donc $I \cup J$ idéal de A entraîne $I \subset J$ ou $J \subset I$. Réciproquement, si $I \subset J$ (resp. $J \subset I$), alors $I \cup J = J$ (resp. $= I$) est un idéal de A. On a donc que $I \cup J$ est un idéal si et seulement si $I \subset J$ ou $J \subset I$.

3. On a vu que $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier. Si n n'est pas premier, alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre. Plus explicitement, si n n'est pas premier, on peut écrire $n = ab$ avec $1 < a, b < n$. On a alors $ab \equiv 0[n]$ sans avoir ni $a \equiv 0[n]$, ni $b \equiv 0[n]$.
Autre exemple : on a vu ensemble que $\mathcal{C}^0(\mathbb{R}, \mathbb{R})$ n'est pas intègre (il suffit de prendre deux fonctions dont les supports sont disjoints).
Autre autre exemple : dans un anneau de polynômes sur un corps k, on prend deux polynômes $P(X)$ et $Q(X)$ non constants. Le quotient $k[X]/(P(X)Q(X))$ n'est pas intègre (les classes de $P(X)$ et $Q(X)$ sont des diviseurs de 0).

4. L'anneau $\mathbb{Z}$ est intègre, et ses éléments inversibles sont ± 1 : ce n'est pas un corps.
Autre exemple : Tout sous-anneau d'un corps est intègre. Il suffit d'en prendre un qui n'est pas un corps (par exemple $\mathbb{Z}[i], \mathbb{Z}[i\sqrt{d}]$ pour d un entier,...).
Autre autre exemple : si A est un anneau intègre, alors $A[X]$ est intègre, donc plus généralement, tout anneau de la forme $A[X_1, \ldots, X_n]$ ou A est intègre est intègre.

5. Sur $A := \mathcal{C}^0(\mathbb{R}, \mathbb{R})$, soit f_1 une fonction continue telle que $f_0(x) = 0$ pour $x \notin [0, 1]$ (on construit facilement une telle fonction en recollant des droites). On définit $f_n(x) := f_1(x - n)$ pour tout $n \in \mathbb{Z}$, et on vérifie facilement que $f_n(x) = 0$ pour $x \notin [n, n + 1]$. En particulier, pour $n \neq m$, les supports de f_n et f_m sont disjoints, et $f_n(x)f_m(x) = 0$ pour tout $x \in \mathbb{R}$: on a $f_n f_m = 0$ dans A. Autrement dit, le polynôme $f_0T \in A[T]$ admet tout les f_n pour $n \neq 0$ comme racine.

6. L'anneau $\{0\}$ ne contient aucun élément non nul, ses éléments non nuls (qui n'existent pas) sont en particulier inversibles. Cependant, $\{0\}$ n'est pas un corps par définition.
Plus généralement l'anneau $\{0\}$ est le seul exemple : les anneaux non nuls dont les éléments non nuls sont inversibles sont exactement les corps (par définition).

7. Nous avons déjà vu des exemples : si $n \in \mathbb{Z}$ n'est pas premier, $\mathbb{Z}/n\mathbb{Z}$ est un quotient non intègre de l'anneau intègre $\mathbb{Z}$.
Plus généralement si A est intègre, et $I \subset A$ est un idéal qui n'est pas premier, le quotient A/I n'est pas intègre.

8. Par le théorème de d'Alembert-Gauss, tout polynôme non constant de $\mathbb{C}[X]$ admet une racine dans $\mathbb{C}$.
Plus généralement si A est un anneau satisfaisant la propriété voulue, alors pour tout $a \in A \setminus \{0_A\}$, le polynôme $aX - 1_A \in A[X]$ admet une racine : il existe $b \in A$ tel que $ab = 1_A$, autrement dit $a \in A^\times$. En

particulier, A est un corps, dans lequel tout polynôme non constant admet une racine, on dit que A est un corps *algébriquement clos*. Les corps $\mathbb{Q}$ et $\mathbb{R}$ ne sont pas algébriquement clos car X^2+1 n'admet de racine ni dans $\mathbb{Q}$ ni dans $\mathbb{R}$.

9. Dans $\mathbb{Z}$, les éléments non inversibles ne forment pas un idéal : ils ne forment même pas un sous-groupe : 2 et 3 sont non inversibles, et $3-2$ est inversible.

10. Dans un corps, l'ensemble des éléments non inversibles est $\{0\}$, qui forme un idéal (c'est vrai dans tout anneau).

11. Sur $\mathbb{R}$, on peut considérer la famille de polynômes $P_n := X^{2n}+1$. Comme un carré est toujours positif sur $\mathbb{R}$, on trouve que P_n n'a aucune racine dans $\mathbb{R}$.
Plus généralement : Si A est un anneau, et si $P(X)$ est un polynôme non constant qui n'a aucune racine sur A (ce qui existe si A n'est pas un corps algébriquement clos), alors pour tout n, le polynôme $P_n := P(X^n)$ n'a pas de racines. En effet si α est une racine de P_n, alors α^n est une racine de P, ce qui est impossible. Comme P est non constant, on a que $(P_n)_{n\in\mathbb{N}}$ est une suite de polynômes de degrés arbitrairement grand.

12. C'est du cours : on sait que $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ si et seulement si n et m sont premiers entre eux. Toutes les paires d'entiers non premiers entre eux répondent à la question 12, toutes les paires d'entiers premiers entre eux répondent à la question 13.

14. Dans $\mathbb{Z}[X]$, considérons les idéaux

$$(2,X) = \{2P(X) + XQ(X) \mid P,Q \in \mathbb{Z}[X]\}$$
$$(3,Y) = \{3R(X) + XS(X) \mid R,S \in \mathbb{Z}[X]\}$$

Le produit de ces deux idéaux est l'ensemble des polynômes s'écrivant sous la forme

$$(2P+XQ)(3R+XS) = 6PR + 3XQR + 2XPS + X^2QS$$

On a $2 \in (2,X)$ et $X \in (3,X)$, donc $2X$ appartient au produit. De même $X \in (2,X)$ et $3 \in (3,X)$ et donc $3X$ appartient au produit. Si le produit est un idéal, il contient $3X - 2X = X$. Or X ne peut pas s'écrire comme un produit d'un élément de $(2,X)$ et de $(3,X)$: on aurait

$$\begin{cases} PR = 0, \\ 3QR + 2PS = 1, \\ QS = 0. \end{cases}$$

On a alors soit $P = 0$ et $3QR = 1$, ce qui est impossible dans $\mathbb{Z}[X]$, soit $R = 0$ et $2PS = 1$, ce qui est impossible dans $\mathbb{Z}[X]$.

15. Dans $\mathbb{Z}[X]$, le polynôme X^2+1 est irréductible. Comme $\mathbb{Z}[X]$ est factoriel, l'idéal (X^2+1) est donc premier, et le quotient $\mathbb{Z}[X]/(X^2+1)$ est donc intègre. On a vu en cours que ce quotient est isomorphe à $\mathbb{Z}[i]$, qui n'est pas un corps. L'idéal (X^2+1) n'est donc pas maximal (le quotient n'est pas un corps).
Plus généralement : Dans un anneau A, un idéal I est premier si et seulement si A/I est intègre. Il est maximal si et seulement si A/I est un corps (comme corps$\Rightarrow$ intègre, un idéal maximal est toujours premier). Dans un anneau intègre A, (0) est un idéal, et on a $A/(0) \simeq A$. Si A n'est pas un corps, on a donc que (0) est un idéal premier non maximal.

16. Si k est un corps, $(0_k) = \{0_k\}$ est un idéal de k tel que $k/(0_k) \simeq k$ est un corps, donc (0_k) est un idéal maximal de k.
Autre exemple : dans un anneau principal A, un idéal (a) est premier si et seulement si il est maximal si et seulement si a est un élément irréductible. On peut donc citer $p\mathbb{Z} \subset \mathbb{Z}$ avec p premier, ou encore $(P(X)) \subset k[X]$ où k est un corps, et $P(X)$ est irréductible.

17. On a déjà vu que $n\mathbb{Z} \subset \mathbb{Z}$ où n n'est pas premier donne une réponse.

18. On sait que, par définition $\mathbb{Q}[X]$ admet $\mathbb{Q}(X)$ comme corps des fractions. On a également $\mathrm{Frac}(\mathbb{Z}[X]) = \mathbb{Q}(X)$ étant donné que, en général $\mathrm{Frac}(A[X]) = (\mathrm{Frac}\,A)(X)$. On peut aussi ajouter que, comme $\mathbb{Q}(X)$ est un corps,

on a trivialement $\mathrm{Frac}(\mathbb{Q}(X)) = \mathbb{Q}(X)$.

19. Comme $\mathrm{Frac}(A)$ est un corps, ses seuls idéaux sont $\{0_{\mathrm{Frac}(A)}\}$ et $\mathrm{Frac}(A)$. Les quotients associés sont donc $\mathrm{Frac}(A)$ et $\{0\}$ respectivement. Parmi ceux-ci, seul $\mathrm{Frac}(A)$ est un corps. Le corps des fractions $\mathrm{Frac}(A/I)$ de A/I est un corps. Si il est isomorphe à un quotient de $\mathrm{Frac}(A)$, ce dernier quotient est un corps, donc la seule possibilité est $\mathrm{Frac}(A/I) \simeq \mathrm{Frac}(A)$.
En prenant $A = \mathbb{Z}$, on prend $p\mathbb{Z}$ comme idéal premier (avec p premier donc), et on se pose la question $\mathrm{Frac}(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z} \simeq \mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$, ce qui n'arrive jamais ($\mathbb{Z}/p\mathbb{Z}$ est fini, $\mathbb{Q}$ ne l'est pas).