Feuille d'exercices numéro 7

☞ **Exercice 1.** Montrer que tout anneau intègre fini non réduit à zéro est un corps.

☞ **Exercice 2.** Montrer que tout homomorphisme de corps est injectif et que sa source et sa cible sont des corps de même caractéristique.

Un corps commutatif K est dit « algébriquement clos » si les irréductible de $K[X]$ sont les polynômes de degré 1.

☞ **Exercice 3.** *On va montrer que $\mathbb{C}$ est algébriquement clos en utilisant le fait que pour tout entier $n \geq 1$, tout nombre complexe z a une racine $n^{\text{ième}}$.*([1])

(a) Soit $P(X) \in \mathbb{C}[X]$ un polynôme non constant. Montrer que $|P(z)|$ tend vers $+\infty$ quand $|z|$ tend vers $+\infty$.

(b) On suppose que $P(X)$ n'a pas de racine complexe. Montrer qu'il existe $z_0 \in \mathbb{C}$ tel que $0 < |P(z_0)| = \inf_{z\in\mathbb{C}} |P(z)|$.

(c) On pose $Q(X) = \dfrac{P(z_0 + X)}{P(z_0)}$. Montrer que $Q(X) = 1 - aX^n(1 + XR(X))$ avec $a \neq 0$ et $n \geq 1$ et où $R(X) \in \mathbb{C}[X]$.

(d) En utilisant une racine $n^{\text{ième}}$ de a, montrer qu'il existe $z \in \mathbb{C}$ tel que $|Q(z)| < 1$.

(e) Montrer que le résultat de la question précédente produit une contradiction et en déduire que $\mathbb{C}$ est algébriquement clos (théorème de d'Alembert-Gauss).

☞ **Exercice 4.** *Soit K un corps commutatif ayant un sous-corps isomorphe à $\mathbb{R}$ (qu'on notera $\mathbb{R}$). On suppose K de dimension finie comme espace vectoriel sur $\mathbb{R}$. Soit $u \in K$ tel que $u \notin \mathbb{R}$.*

(a) Montrer qu'il existe un polynôme $P(X)$ du second degré à coefficients réels sans racine réelle tel que $P(u) = 0$.

(b) Montrer que le sous-espace vectoriel E de K engendré par 1 et u est un corps isomorphe à $\mathbb{C}$.

(c) Soit $v \in K$ tel que $v \notin E$. Montrer que le polynôme $X^2 + 1$ a au moins trois racines distinctes dans K. Conclure.

☞ **Exercice 5.** **(a)** Montrer que sur le corps $\mathbb{Z}/2\mathbb{Z}$ il existe un unique polynôme irréductible de degré 2.

(b) Construire un corps à 4 éléments.

On pose $K = \dfrac{(\mathbb{Z}/2\mathbb{Z})[X]}{X^3 + X + 1}$ *et* $L = \dfrac{(\mathbb{Z}/2\mathbb{Z})[X]}{X^3 + X^2 + 1}$.

(c) Montrer que K et L sont des corps à 8 éléments, et calculer le carré de $X^2 + 1$ dans chacun d'entre eux.

(d) Montrer que K et L sont isomorphes (on pourra considérer le morphisme qui envoie X sur $X + 1$).

☞ **Exercice 6.** *Soit K un corps fini qu'on ne suppose pas commutatif. Soit $Z = \{x \in K \mid \forall_{y\in K}\ xy = yx\}$ le centre de K. Pour tout ensemble fini X, on note $|X|$ le cardinal de X.*

(a) Montrer que Z est un corps commutatif et que K est un espace vectoriel de dimension finie sur Z.

On note q le cardinal de Z et d la dimension de K sur Z. Pour tout $x \in K$, on pose $Z_x = \{y \in K \mid xy = yx\}$.

(b) Montrer que pour tout $x \in K$, Z_x est un sous-corps de K contenant Z et que si $x \notin Z$, la dimension d_x de Z_x comme espace vectoriel sur Z est un diviseur strict de d (c'est-à-dire distinct de d).

On note K^* le groupe des éléments inversibles de K. K^* agissant sur lui-même par conjugaison (via $(g, x) \mapsto gxg^{-1}$), on note S_x le stabilisateur de x pour cette action. Pour tout orbite incluse dans $K - Z$, on choisit un élément dans cette orbite, et on note $\{x_1, \ldots, x_k\}$ l'ensemble des ces éléments.

1. Ceci se prouve facilement en utilsant le fait que l'application $z \mapsto e^z$ de $\mathbb{C}$ vers $\mathbb{C}^*$ est surjective. Cette surjectivité se prouve elle-même élémentairement avec un peu de calcul intégral.

(c) Montrer que :

$$q^d - 1 = q - 1 + \sum_{i=1}^{k} \frac{q^d - 1}{q^{d_{x_i}} - 1}$$

On pose $F(X) = X^d - 1 + \sum_{i=1}^{k} \frac{X^d - 1}{X^{d_{x_i}} - 1}$.

(d) Montrer que $F(X)$ est un polynôme à coefficients entiers et que le polynôme cyclotomique([2]) $\Phi_d(X)$ divise le polynôme $F(X)$ dans $\mathbb{Z}[X]$.

(e) Montrer que $|\Phi_d(q)| \leq q - 1$.

(f) Montrer que pour tout $n > 1$, $|\Phi_n(q)| > q - 1$.

(g) Montrer que K est commutatif (théorème de Wedderburn).

(h) Énoncer un perfectionnement du résultat de l'exercice 1.

2. Voir l'exercice 10 de la feuille 6.

Solutions des exercices de la feuille 7

☞ **Exercice 1.** Comme l'anneau $\mathscr{A}$ n'est pas réduit à 0, on a $1 \neq 0$ (car $1 = 0$ entraîne $x = 1x = 0x = 0$). Il y a juste à montrer que tout $x \neq 0$ est inversible. Soit $x \neq 0$. L'application $y \mapsto xy$ de $\mathscr{A}$ vers $\mathscr{A}$ est injective, car comme $\mathscr{A}$ est intègre, $xy = xy'$ (c'est-à-dire $x(y - y') = 0$) et $x \neq 0$ entraînent $y - y' = 0$. Comme $\mathscr{A}$ est fini, elle est aussi surjective, et 1 appartient à son image. Il existe donc y tel que $xy = 1$. Il existe de même z tel que $zx = 1$, et on a $z = zxy = y$. Ainsi, x est inversible.

☞ **Exercice 2.** Soit $f : K \to L$ un morphisme de corps. Comme $f^{-1}(0)$ est un idéal de K, et comme f n'est pas nul (car $f(1) = 1$), cet idéal ne peut être que 0, et f est donc injectif. Si K est de caractéristique 0, tout entier n est non nul dans K donc non nul dans L par injectivité de f, et donc L est de caractéristique 0. Si la caractéristique de K est un nombre premier p, p est nul dans K, donc dans L et la caractéristique de L divise p. Ce ne peut donc être que p.

☞ **Exercice 3.** **(a)** Un polynôme de degré strictement positif définit une fonction qui tend vers l'infini quand son argument tend vers l'infini. Il suffit de mettre le terme du plus haut degré en facteur et de constater que l'autre facteur est la somme d'une constante non nulle et d'une espression qui tend vers zéro.

(b) Notons f la fonction $z \mapsto |P(z)|$. Soit D un disque de centre 0 dans $\mathbb{C}$ assez grand pour que $f(z) > 2f(0)$ pour tout $z \in \mathbb{C} - D$, ce qui est possible d'après la question **(a)**. L'image de f est la réunion de $f(D)$ et de $f(\mathbb{C} - D)$, tous deux inclus dans $]0, +\infty[$ puisque f ne prend que des valeurs strictement positives. Comme D est compact, $f(D)$ est compact et contient sa borne inférieure qui est donc de la forme $f(z_0)$ et est strictement positive. Pour tout $z \in \mathbb{C} - D$, on a $f(z) > 2f(0) > 2f(z_0)$. Ainsi $f(z_0) > 0$ est la borne inférieure de $f(\mathbb{C})$, ce qui donne le résultat demandé.

(c) On a $Q(0) = 1$, et $Q(X)$ est un polynôme non constant. Il existe donc un plus petit exposant $n \geq 1$ tel que le terme de degré n de $Q(X)$ soit non nul, donc de la forme $-aX^n$ avec $a \neq 0$. En mettant ce monôme en facteur sur les termes autres que le terme constant, on a la forme annoncée.

(d) Soit b un racine $n^{\text{ième}}$ de a. On a donc $a = b^n$ et donc $Q(X) = 1 - (bX)^n - aX^{n+1}R(X)$. Soit $\varepsilon > 0$ et posons $z = \varepsilon/b$. On a $Q(z) = 1 - \varepsilon^n + o(\varepsilon^n)$ (où $o(\varepsilon^n)$ est négligeable devant ε^n). On voit donc qu'en prenant ε assez petit, on a $|Q(z)| < 1$.

(e) La fonction $z \mapsto |Q(z)|$ atteint son minimum en 0 et ce minimum est 1, ce qui contredit le résultat de la question précédente. On en déduit que $P(X)$ a nécessairement une racine dans $\mathbb{C}$, et qu'il n'est donc pas irréductible si son degré est au moins 2.

☞ **Exercice 4.** **(a)** Notons k la dimension de K sur $\mathbb{R}$. Les vecteurs $1, u, u^2, \ldots, u^k$ sont au nombre de $k + 1$ et ne peuvent donc pas être linéairement indépendants sur $\mathbb{R}$. Il existe donc des réels $a_k, \ldots, a_0$ tels que $a_k u^k + \cdots + a_0 = 0$, autrement-dit, un polynôme à coefficients réels $P(X)$ tel que $P(u) = 0$.

D'après le théorème de d'Alembert-Gauss $P(X)$ se décompose en facteurs du premier degré sur $\mathbb{C}$, donc en facteurs de degrés 1 et 2 sur $\mathbb{R}$, puisque s'il a une racine non réelle il a aussi sa conjuguée comme racine. Comme $\mathbb{R}[X]$ est intègre, u est racine de l'un de ces facteurs irréductibles sur $\mathbb{R}$, qui ne peut pas être de degré 1 car $u \notin \mathbb{R}$. Il est donc de degré 2 et sans racine réelle.

(b) Voir l'exercice **2** de la feuille 5bis.

(c) Noter que v n'existe que si la dimension de K sur $\mathbb{R}$ est au moins 3. Pour la même raison que pour u, le sous-espace F engendré par 1 et v est un corps isomorphe à $\mathbb{C}$. Il existe donc $u_1 \in E$ et $v_1 \in F$ tel que $u_1^2 = v_1^2 = -1$. Comme $v \notin E$, les vecteurs 1, u et v sont linéairement indépendants, ce qui implique que $E \cap F = \mathbb{R}$. On en déduit que $v_1 \notin E$. Il en résulte que u_1, $-u_1$ et v_1 sont trois éléments distincts (de K !) tous racines de $X^2 + 1$. Mais K étant un corps commutatif, ceci est impossible. Il en résulte que la dimension de K sur $\mathbb{R}$ est au plus 2, et donc que K est isomorphe à $\mathbb{R}$ ou à $\mathbb{C}$.

☞ **Exercice 5.** **(a)** Il n'y a que quatre polynômes de degré 2 sur $\mathbb{Z}/2\mathbb{Z}$, qui sont X^2, $X^2 + X$, $X^2 + 1$ et $X^2 + X + 1$. Les trois premiers ne sont pas irréductibles car égaux à XX, $X(X + 1)$ et $(X + 1)(X + 1)$. Le dernier est irréductible, car étant de degré 2, il aurait une racine s'il était réductible, or ni 0 ni 1 n'est racine de ce polynôme.

(b) Il résulte immédiatement de la question précédente que $\dfrac{(\mathbb{Z}/2\mathbb{Z})[X]}{X^2 + X + 1}$ est un corps. Il a quatre éléments

qui sont (les classes de) 0, 1, X et $X+1$.

(c) Les deux polynômes X^3+X^2+1 et X^3+X+1 sont irréductibles pour la même raison que pour X^2+X+1. K et L sont donc des corps. Ils ont 8 éléments qui sont toutes les combinaisons linéaires de 1, X et X^2, mais leurs multiplications sont différentes. En effet, dans K, $(X^2+1)^2 = X^4+1 = XX^3+1 = X(X+1)+1 = X^2+X+1$, alors que dans L, $(X^2+1)^2 = XX^3+1 = X(X^2+1)+1 = X^3+X+1 = X^2+1+X+1 = X^2+X$.

(d) On a un unique morphisme d'anneaux $(\mathbb{Z}/2\mathbb{Z})[X] \to L$ envoyant X sur (la classe de) $X+1$, et envoyant donc X^3+X+1 sur $(X+1)^3+(X+1)+1 = X^3+X^2+1$. Il en résulte que l'idéal de K engendré par X^3+X+1 est inclus dans le noyau de ce morphisme, et qu'on a donc un morphisme d'anneaux (donc de corps) $K \to L$. Ce dernier est injectif d'après l'exercice **2**, et est donc un isomorphisme (dont l'inverse n'est autre que le morphisme $L \to K$ qui envoie X sur $X+1$!).

☞ **Exercice 6.** **(a)** On a clairement $0 \in Z$. Si $x, x' \in Z$ alors $(x+x')y = xy+x'y = yx+yx' = y(x+x')$ pour tout $y \in K$, donc $x+x' \in Z$. De même, si $x \in Z$ alors $-x \in Z$. Par ailleurs, pour $x, x' \in Z$, $xx'y = xyx' = yxx'$ pour tout $y \in K$, donc $xx' \in Z$. On a $1 \in Z$, et enfin, si $0 \neq x \in Z$, de $xy = yx$ on déduit $yx^{-1} = x^{-1}y$ en multipliant de chaque coté par x^{-1}. Z est donc un corps, bien sûr commutatif. La dimension de K sur Z est finie parce que K est fini.

(b) Il est immédiat que $Z \subset Z_x$. La vérification du fait que Z_x est un sous-corps de K est triviale. Ainsi, K est un espace vectoriel sur Z_x. Soit $x_1, \ldots, x_p$ une base de K comme Z_x-espace vectoriel. Alors tout élément de $u \in K$ s'écrit de manière unique $u = a_1x_1 + \cdots + a_px_p$, et chaque $a_i \in Z_x$ s'écrit de manière unique comme $a_i = b_1^i y_1^i + \cdots + b_{d_x}^i y_{d_x}^i \in Z$ où les b_j^i dont dans Z. Ainsi u s'écrit de manière unique sous la forme d'une combinaison linéaire des vecteurs $y_j^i x_i$ qui sont au nombre de pd_x. Comme la dimension de K sur Z est d, on a $d = pd_x$. Par ailleurs, comme $x \notin Z$, on a $p > 1$ (sinon $Z_x = K$ et x est dans le centre de K), d_x est un diviseur strict de d.

(c) L'orbite d'un élément de Z est évidemment réduite à cet élément. Par ailleurs, le nombre d'éléments dans l'orbite d'un x_i $(1 \leq i \leq k)$ est le quotient $\dfrac{|K^*|}{|S_{x_i}|}$, c'est-à-dire $\dfrac{q^d-1}{q^{d_{x_i}}-1}$, puisque S_x n'est autre que $Z_x - \{0\}$. La formule des classes donne donc le résultat.

(d) Le polynôme X^d-1 est le produit des $\Phi_s(X)$ où s parcourt les diviseurs de d (Feuille 6, exercice 10 **(b)**). Comme d_{x_i} divise d, $X^{d_{x_i}}-1$ divise X^d-1 (feuille 6, exercice 8 **(a)**), et donc que $F(X)$ est un polynôme à coefficients entiers. De plus, le quotient $\dfrac{X^d-1}{X^{d_{x_i}}-1}$ est divisible par $\Phi_d(X)$, car d_x est un diviseur strict de d.

(e) L'entier q (cardinal de Z) est au moins 2, car tout corps a au moins deux éléments (0 et 1). On a donc $0 < q-1$. Par ailleurs, $F(q) = q-1$ d'après la question **(c)**, et comme on vient de le voir $F(q) = \Phi(q)Q(q)$, où $Q(X)$ est un polynôme à coefficients entiers. Comme $1 \leq q-1 = |F(q)| = |\Phi_d(q)||Q(q)|$, on a $|Q(q)| \geq 1$. Il en résulte que $|\Phi_d(q)| \leq q-1$.

(f) Si ζ est une racine de l'unité distincte de 1, on a $|q-\zeta| > q-1$, puisque 1 est l'unique point du cercle des complexes de module 1 le plus proche de l'entier naturel $q \geq 2$. Comme $|\Phi_n(q)|$ est, pour $n > 1$, un produit de telles expressions $|q-\zeta|$ $(\zeta \neq 1)$, et comme $q-1 \geq 1$, on voit que $|\phi_n(q)| > q-1$.

(g) Des deux questions précédentes il résulte que d ne peut être que 1, donc que $K = Z$, donc que K est commutatif.

(h) Tout anneau fini intègre non réduit à zéro est un corps commutatif.