Feuille TD 3 – Exercices Algèbre – Anneaux

► *Cette feuille de TD nous occupera deux semaines.*

Exercices fondamentaux de la semaine 1

Exercice 1. Montrer que tout anneau intègre fini est un corps.

Solution. Soit A un anneau intègre fini. On doit montrer que tout élément non nul de A est inversible. Pour $a \in A$, $a \neq 0$, on considère l'application[1] $\varphi_a : x \in A \mapsto ax \in A$ qui est un morphisme de groupes $(A,+)$ dans $(A,+)$. Comme A est intègre on voit facilement que φ_a est injectif[2], donc surjectif car A est fini. Il existe donc en particulier $a' \in A$ tel que $aa' = 1$. Comme A est supposé commutatif, on a bien montré que a était inversible.
On pouvait aussi considérer pour $x \in A \setminus \{0\}$ les éléments x^n pour $n \in \mathbf{N}$. Cela est motivé par le fait que dans un groupe fini de cardinal m, $x^m = e$ et l'inverse de x est alors une puissance de x. Comme A est fini, par principe des tiroirs, il existe $n' > n$ tels que $x^{n'} = x^n$ soit $x^n(1 - x^{n'-n}) = 0$ et par intégrité, puisque $x \neq 0$, il vient $1 = x \times x^{n'-n-1}$ et on a bien que x est inversible d'inverse $x^{n'-n-1}$. Noter qu'on a bien $n' - n - 1 \geqslant 0$.
Plus généralement, montrer que si l'on suppose que A est intègre et possède un nombre fini d'idéaux, alors c'est un corps. En effet, pour $x \in A \setminus \{0\}$, on a en considérant les (x^n) pour $n \in \mathbf{N}$ qu'il existe $p > q$ tels que $(x^p) = (x^q)$. En particulier, il existe $a \in A$ tel que $x^q = x^p a$ soit par intégrité $1 = x^{p-q}a$.

Exercice 2. Soit A un anneau commutatif, et soit S une partie multiplicative de A, c'est-à-dire que S contient 1, et si $s,t \in S$, alors $st \in S$. On veut définir la *localisation* $S^{-1}A$ de A par rapport à S.

1. Montrer qu'on peut définir une relation d'équivalence sur $A \times S$ comme suit : (a,s) est équivalent à (b,t) s'il existe un $u \in S$ tel que $u(at - bs) = 0$. Soit $S^{-1}A$ l'ensemble des classes d'équivalences. On écrira $\frac{a}{s}$ pour désigner la classe d'équivalence de (a,s).
2. Montrer que $S^{-1}A$, muni des opérations $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$ et $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$, est un anneau commutatif.
3. Montrer que si S contient 0, alors $S^{-1}A$ est un anneau trivial.
4. Montrer que l'application $f : A \to S^{-1}A$ définie par $a \mapsto \frac{a}{1}$ est un morphisme d'anneaux. Montrer que f est injectif si S ne contient pas de diviseurs de zéro.
5. Cas particulier : corps des fractions. Supposons que A est intègre, et que $S = A \setminus \{0\}$. Montrer que $S^{-1}A$ est un corps, appelé le *corps des fractions* de A.
6. Cas particulier : localisation en un idéal premier. Soit P un idéal premier de A. Montrer que $S = A \setminus P$ est une partie multiplicative de A. On écrit A_P pour désigner $S^{-1}A$ dans ce cas.
7. Cas particulier (suite) : Montrer que l'idéal engendré par l'image de P dans A_P est le seul idéal maximal de A_P.

Solution. La localisation d'un anneau, qui consiste à rendre inversible une partie multiplicative et dont on verra l'origine de la terminologie dans l'exercice 8 (qui correspond à l'étude de comportement local de fonctions), est un outil indispensable en géométrie algébrique et théorie des nombres notamment.

1. Montrons que la relation $\sim$ sur $A \times S$ est réflexive, symétrique et transitive. Soient $a,b,c \in A$ et $s,t,k \in S$:
   - $(a,s) \sim (a,s)$ car $1 \times (as - as) = 0$ et $1 \in S$;
   - Supposons $(a,s) \sim (b,t)$ alors il existe $u \in S$ tel que $u(at - bs) = 0$. Ainsi $(-u) \cdot (bs - at) = 0$ et donc $u(bs - at) = 0$ ce qui implique que $(b,t) \sim (a,s)$;
   - Si $(a,s) \sim (b,t)$ et $(b,t) \sim (c,k)$ alors $\exists u,v \in S$ tels que $u(at - bs) = 0$ et $v(bk - ct) = 0$. Donc

     $$uvtak = (uat)vk = ubsvk = (vbk)us = vctus \quad \text{soit} \quad uvt(ak - cs) = 0$$

     et on a que $(a,s) \sim (c,k)$ car $uvt \in S$ car S est multiplicative.

   ► **Remarque. –** Noter que la présence du u dans la définition de la relation d'équivalence (qui peut paraître étrange à première vue dans l'optique de définir la fraction $\frac{a}{s}$) est en réalité essentielle pour obtenir la transitivité ! La relation $(a,s) \sim (b,t)$ si, et seulement si, $at - bs = 0$ n'est pas transitive en général !
2. Montrons que la somme est bien définie : si $\frac{a}{s} = \frac{a'}{s'}$ et $\frac{b}{t} = \frac{b'}{t'}$ alors il existe $u,v \in S$ tels que $u(as' - a's) = 0$ et $v(bt' - b't) = 0$. On a donc que

   $$uv\big((at + bs)s't' - (a't' + b's')st\big) = uvtt'(as' - a's) + uvss'(bt' - b't) = 0 \quad \text{et} \quad \frac{at + bs}{st} = \frac{a't' + b's'}{s't'}.$$

1. Attention à bien voir qu'il ne s'agit pas d'un morphisme d'anneaux si $a \neq 1$ car par exemple $\varphi_a(1) = a \neq 1$.
2. En effet, si l'on se donne $x \in A$ tel que $\varphi_a(x) = 0$ (on peut établir l'injectivité en considérant le noyau car même si l'on n'a pas un morphisme d'anneaux, on a bien un morphisme de groupes !), on a $ax = 0$ et comme A est intègre et $a \neq 0$, on obtient bien $x = 0$.

De même $\frac{ab}{st} = \frac{a'b'}{s't'}$, car

$$\begin{aligned} uv(abs't' - a'b'st) &= uv(abs't' - a'bst' + a'bst' - a'b'st) \\ &= uv\big((as' - a's)bt' + (bt' - b't)a's\big) = 0. \end{aligned}$$

Les deux opérations sont donc bien définies. Montrons maintenant que $(S^{-1}A, +, .)$ est un anneau commutatif. Soient $\frac{a}{s}$, $\frac{b}{t}$, $\frac{c}{u} \in S^{-1}A$,

- $+$ est associative : $(\frac{a}{s} + \frac{b}{t}) + \frac{c}{u} = \frac{(at+bs)u+cst}{stu} = \frac{a}{s} + (\frac{b}{t} + \frac{c}{u})$;
- $\frac{0}{1}$ est l'élément neutre pour $+$;
- $\frac{-a}{s}$ est l'inverse de $\frac{a}{s}$;
- $(A, +)$ est commutative $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st} = \frac{bs+at}{ts} = \frac{b}{t} + \frac{a}{s}$;
- La multiplication est associative : $(\frac{a}{s} \cdot \frac{b}{t}) \cdot \frac{c}{u} = \frac{abc}{stu} = \frac{a}{s} \cdot (\frac{b}{t} \cdot \frac{c}{u})$;
- La multiplication est distributive par rapport à l'addition : $\frac{a}{s} \cdot (\frac{b}{t} + \frac{c}{u}) = \frac{abu+act}{stu}$ et $(\frac{a}{s} \cdot \frac{b}{t}) + (\frac{a}{s} \cdot \frac{c}{u}) = \frac{absu+acst}{s^2tu}$. Il sont égaux car $1 \cdot \big((absu + acst)stu - (abu + act)s^2tu\big) = 0$;
- L'élément unité est $\frac{1}{1}$;
- Le produit est commutatif $\frac{a}{s} \cdot \frac{b}{t} = \frac{b}{t} \cdot \frac{a}{s}$.

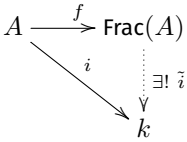
3. Supposons que $0 \in S$. Alors, pour tout $a, a' \in A$ et tout $s, s' \in S$, $\frac{a}{s} = \frac{a'}{s'}$ car $0 \cdot (as' - a's) = 0$. L'anneau $S^{-1}A$ est donc trivial.

4. Soit $f : a \in A \mapsto \frac{a}{1} \in S^{-1}A$. Il s'agit d'un morphisme d'anneaux :

- Pour tous $a, b \in A$, $f(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} = f(a)f(b)$;
- Pour tous $a, b \in A$, $f(a + b) = \frac{a+b}{1} = \frac{a\cdot 1+b\cdot 1}{1} = f(a) + f(b)$;
- $f(1) = \frac{1}{1}$.

Supposons que S ne contienne pas de diviseurs de zéro. Soit $a \in \mathrm{Ker}(f)$. Alors $f(a) = \frac{a}{1} = \frac{0}{1}$, donc il existe $u \in S$ tel que $u(a.1 - 1.0) = au = 0$. Comme S ne contient pas de diviseur de zéro, ceci implique que $a = 0$. Donc $\mathrm{Ker}(f) = \{0\}$ et f est bien injectif.

5. Supposons A est intègre. On donc que $S = A\backslash\{0\}$ et une partie multiplicative de A. Soit $\frac{a}{s}$ un élément non nul de $S^{-1}A$; on doit montrer qu'il est inversible. Comme $S = A\backslash\{0\}$ et $a \neq 0$, on a que $a \in S$ donc $\frac{s}{a}$ est un élément de $S^{-1}A$; il vérifie $\frac{a}{s} \cdot \frac{s}{a} = \frac{1}{1}$ car $1 \cdot (as - sa) = 0$. Le corps des fractions est le plus petit corps contenant A et il vérifie la propriété universelle suivante : si k est un corps et $i : A \to k$ est un morphisme injectif, alors il existe un unique morphisme de corps [3] $\tilde{i}$: Frac$(A) \to k$ injectif tel que $\tilde{i} \circ f = i$, autrement dit tel que le diagramme suivant commute.



6. Si $\mathfrak{P}$ est un idéal premier de A, alors pour tout $s, t \in A\backslash\mathfrak{P}$, $st \in A\backslash\mathfrak{P}$ et $1 \in A\backslash\mathfrak{P}$, donc $S = A\backslash\mathfrak{P}$ est bien multiplicative.

7. Pour montrer que l'idéal engendré par l'image de $\mathfrak{P}$ dans $A_{\mathfrak{P}}$ est le seul idéal maximal de $A_{\mathfrak{P}}$, démontrons d'abord qu'un élément $\frac{a}{s}$ est inversible dans $A_{\mathfrak{P}}$ si et seulement si $a \notin \mathfrak{P}$. En effet, si $a \notin \mathfrak{P}$ alors $a \in S$ par définition de S et donc, comme $\frac{a}{s} \cdot \frac{s}{a} = \frac{1}{1}$, $\frac{a}{s}$ est inversible dans $A_{\mathfrak{P}}$.
Réciproquement, si $\frac{b}{t}$ est l'inverse de $\frac{a}{s}$ dans $A_{\mathfrak{P}}$ alors il existe $u \in A\backslash\mathfrak{P}$ tel quel $u(ab - st) = 0$. Ceci est équivalent à dire qu'il existe $u \in A\backslash\mathfrak{P}$ tel que $uab = ust$, comme $ust \in A\backslash\mathfrak{P}$, on a que $uab \notin \mathfrak{P}$ et donc $a \notin \mathfrak{P}$ car $\mathfrak{P}$ est un idéal.
Remarquons alors que $f(\mathfrak{P}) = \left\{\frac{p}{1} \ : \ p \in \mathfrak{P}\right\}$ n'est pas un idéal [4] de $A_{\mathfrak{P}}$. On considère donc $S^{-1}\mathfrak{P}$ l'idéal engendré par $f(\mathfrak{P})$. Il est alors facile de voir que $\left\{\frac{p}{s} \ : \ p \in \mathfrak{P},\ s \notin \mathfrak{P}\right\}$ est un idéal de $A_{\mathfrak{P}}$ contenant $f(\mathfrak{P})$ et que c'est le plus petit. Il s'agit donc de $S^{-1}\mathfrak{P}$.
Soit maintenant I un idéal propre de $A_{\mathfrak{P}}$ et soit $\frac{a}{s} \in I$. Comme $I \neq A_{\mathfrak{P}}$, on sait que $\frac{a}{s}$ n'est pas inversible et donc $a \in \mathfrak{P}$ de sorte que $\frac{a}{s}$ appartient à l'idéal $S^{-1}\mathfrak{P}$. On a donc montré que $I \subset S^{-1}\mathfrak{P}$ et l'idéal engendré par $f(\mathfrak{P})$ est bien l'unique idéal maximal de $A_{\mathfrak{P}}$.
Noter qu'en composant la surjection canonique $\pi_{\mathfrak{P}} : A_{\mathfrak{P}} \to A_{\mathfrak{P}}/S^{-1}\mathfrak{P}$ avec le morphisme f de la question **4.**, il vient un morphisme de noyau $\mathfrak{P}$ si bien qu'on obtient un morphisme injectif [5] $A/\mathfrak{P} \to A_{\mathfrak{P}}/S^{-1}\mathfrak{P}$ défini par $\pi(a) \to \pi_{\mathfrak{P}}\left(\frac{a}{1}\right)$ avec $A_{\mathfrak{P}}/S^{-1}\mathfrak{P}$ un corps, appelé *corps résiduel*. Par propriété universelle du corps de fractions, on obtient un morphisme injectif Frac$(A/\mathfrak{P}) \to A_{\mathfrak{P}}/S^{-1}\mathfrak{P}$

3. Je vous laisse vérifier que $\tilde{i}\left(\frac{a}{s}\right) = \frac{i(a)}{i(b)}$ est cet unique morphisme.

4. Par exemple car $\frac{p}{1} \cdot \frac{1}{s} = \frac{p}{s} \notin f(\mathfrak{P})$ pour $s \in S \setminus \{1\}$.

5. En effet, un élément du noyau vérifie que $\frac{a}{1} = \frac{p}{s}$ avec $p \in \mathfrak{P}$ and $s \notin \mathfrak{P}$. Ainsi, il existe $u \notin \mathfrak{P}$ tel que $uas = up \in \mathfrak{P}$. Cela impose $a \in \mathfrak{P}$ par primalité de $\mathfrak{P}$ et car $u, s \notin \mathfrak{P}$.

donné par[6] $\frac{\pi(a)}{\pi(s)} \to \pi_{\mathfrak{P}}\left(\frac{a}{s}\right)$ dont on peut montrer qu'il est surjectif. En effet, si $\pi_{\mathfrak{P}}\left(\frac{a}{s}\right)$ avec $s \notin \mathfrak{P}$, alors si l'on dénote par $\pi : A \to A/\mathfrak{P}$ la surjection canonique, $\pi(s) \neq 0$ et alors $\frac{\pi(a)}{\pi(s)} \in \mathrm{Frac}(A/\mathfrak{P})$ et est un antécédent de $\pi_{\mathfrak{P}}\left(\frac{a}{s}\right)$ où tout est indépendant du choix d'un représentant. On a donc $\mathrm{Frac}(A/\mathfrak{P}) \cong A_{\mathfrak{P}}/S^{-1}\mathfrak{P}$. Dans le cas de $A = \mathbf{Z}$ et $\mathfrak{P} = p\mathbf{Z}$ pour p premier, il vient que $\mathbf{Z}_{(p)}/S^{-1}p\mathbf{Z} \cong \mathbf{F}_p$. Noter qu'on a

$$\mathbf{Z}_{(p)} = \left\{\frac{a}{b} \ : \ p \nmid b\right\} = \mathbf{Z}\left[\frac{1}{\ell} \ : \ \ell \neq p \text{ premier}\right].$$

On appelle un tel anneau un anneau *local* sur lesquels on reviendra plus en détails dans l'exercice 8. On peut également montrer que le résultat ne se généralise pas à la partie multiplicative formée d'une réunion d'idéaux premiers. Dans ce cas, on obtient un anneau *semi-local* qui contient autant d'idéaux maximaux que d'idéaux premiers dans la réunion (exercice !).

On donne les exemples suivants dont les détails sont laissés e exercice :

- $\mathrm{Frac}(\mathbf{Z}) \cong \mathbf{Q}$;
- $\mathrm{Frac}(k[X]) \cong k(X)$ pour un corps k;
- Si $A = \mathbf{Z}$ et $S = \left\{10^k \ : \ k \in \mathbf{N}\right\}$, alors $S^{-1}A = \mathbf{D}$ l'ensemble des décimaux;
- Un idéal de $\mathbf{Z}/n\mathbf{Z}$ est par le théorème de correspondance la projection d'un idéal de $\mathbf{Z}$ contenant $n\mathbf{Z}$ donc par principalité de $\mathbf{Z}$, de la forme $d\mathbf{Z}$ avec $d \mid n$. L'image réciproque par un morphisme d'anneaux d'un idéal premier étant premier, on voit qu'un idéal premier de $\mathbf{Z}/n\mathbf{Z}$ provient d'un $p\mathbf{Z}$ avec $p \mid n$ premier et il n'est pas difficile de voir que le quotient de $\mathbf{Z}/n\mathbf{Z}$ par $p\mathbf{Z}/n\mathbf{Z}$ est isomorphe au corps $\mathbf{F}_p$ si bien qu'on a là tous les idéaux premiers de $\mathbf{Z}/n\mathbf{Z}$ qui sont également maximaux[7]. On vérifie alors que

$$(\mathbf{Z}/n\mathbf{Z})_{(p)} \cong \mathbf{Z}/p^{\alpha}\mathbf{Z}$$

pour $p \mid n$ premier et si $n = p^{\alpha}m$ avec $p \nmid m$. En effet, le morphisme[8] $\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z} \to (\mathbf{Z}/n\mathbf{Z})_{(p)}$ est surjectif. Soit $\frac{\pi(y)}{s} \in (\mathbf{Z}/n\mathbf{Z})_{(p)}$ avec $y \in \mathbf{Z}$ et $s \notin (p)$. Alors s et p^{α} sont premiers entre eux et il existe deux entiers u et v tels que $us + p^{\alpha}v = 1$. On a donc $m(suy - y) = mvyp^{\alpha} = nvy$ de sorte que $m(s\pi(uy) - \pi(y)) = 0$ dans $\mathbf{Z}/n\mathbf{Z}$ et $m \notin (p)$ si bien que $\frac{\pi(uy)}{1} = \frac{y}{s}$ et uy est un antécédent de $\frac{y}{s}$. On montre alors que le noyau de ce morphisme est $p^{\alpha}\mathbf{Z}$. Il est clairement contenu dans le noyau car $\frac{\pi(p^{\alpha})}{1} = \frac{\pi(mp^{\alpha})}{m} = 0$. Réciproquement, soit x dans le noyau. Alors $\frac{\pi(x)}{1} = 0$ donc il existe $\pi(s) \notin (p)$ tel que $\pi(sx) = 0$ soit $n \mid sx$. On en déduit que $p^{\alpha} \mid sx$ mais s est premier à p donc $p^{\alpha} \mid x$ et on a le résultat et en fait on peut même en déduire par le théorème chinois que

$$\mathbf{Z}/n\mathbf{Z} \cong \bigoplus_{p \mid n} (\mathbf{Z}/n\mathbf{Z})_{(p)}.$$

On démontre aussi que tout idéal I de $S^{-1}A$ est de la forme

$$S^{-1}J = \left\{\frac{a}{s} \ : \ a \in J, \ s \in S\right\}$$

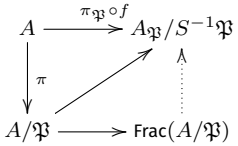
pour un idéal J de A. On a clairement que $s^{-1}J$ est un idéal (c'est celui engendré par $f(J)$)et pour tout idéal I de $S^{-1}A$, l'ensemble

$$J = \left\{a \in A \ : \ \exists s \in S, \text{ tel que } \frac{a}{s} \in I\right\}$$

est un idéal de A vérifiant $S^{-1}J = I$. En particulier, les idéaux premiers de $S^{-1}A$ s'identifient aux idéaux premiers de A ne rencontrant pas S. Les propriétés suivantes découlent facilement des définitions et de cette description des idéaux de $S^{-1}A$ pour S une partie multiplicative ne contenant pas 0 :

- Si A est intègre, alors $S^{-1}A$ est intègre[9];
- Si A est principal, alors $S^{-1}A$ est principal[10];

6. Je laisse à vos soins de vérifier que tout est bien défini et que tout cela correspond en réalité au diagramme commutatif suivant :



7. En effet, puisque $p \mid n$, la surjection canonique $\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ passe au quotient modulo $n\mathbf{Z}$ pour donner un morphisme d'anneaux $\mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ surjectif de noyau $p\mathbf{Z}/n\mathbf{Z}$.

8. Composé de la surjection canonique $\pi : \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ et du morphisme de **4.**

9. Si $\frac{a}{s} \cdot \frac{b}{t} = 0$ alors il existe $u \in S$ tel que $uab = 0$ soit $a = 0$ ou $b = 0$ (car $0 \notin S$ par hypothèse et par intégrité de A).

10. Un tel idéal I est de la forme $S^{-1}J$ pour $J = (a)$ par principalité de A et donc $I = \left(\frac{a}{1}\right)$.

— Si A est factoriel, alors $S^{-1}A$ est factoriel [11].

Enfin, si on considère A un anneau et $a \in A$, alors $S = \{a^n \ : \ n \in \mathbf{N}\}$. On voit facilement que $S^{-1}A \cong A[X]/(aX-1)$ et on peut en déduire par exemple que $\mathbf{C}[X,Y]/(XY-1)$ est principal.

Exercice 3. Soit $\mathbf{Z}[i]$ l'anneau des entiers de Gauß.

1. Soit p un nombre premier. Montrer que p est irréductible dans $\mathbf{Z}[i]$ si, et seulement si, p ne s'écrit pas comme somme de deux carrés d'entiers.
2. Soit p un nombre premier congru à 3 modulo 4. Montrer que si pour deux entiers a et b, on a $a^2+b^2 \equiv 0 \pmod p$, alors p divise a et b. *Indication : on pourra calculer* $(p-1)!$ *modulo* p.
3. Montrer qu'une somme de deux carrés d'entiers est congrue à 0, 1 ou 2 modulo 4.
4. En déduire qu'un nombre premier p est irréductible dans $\mathbf{Z}[i]$ si, et seulement si, $p \equiv 3 \pmod 4$.

Solution.
L'anneau $\mathbf{Z}[i]$ est un anneau euclidien de stathme $N : a+bi \in \mathbf{Z}[i] \mapsto a^2+b^2 \in \mathbf{N}$. Il est facile de voir que N est multiplicative, *i.e.* si $z, z' \in \mathbf{Z}[i]$ alors $N(zz') = N(z)N(z')$ car $N(z) = z\overline{z}$. On a aussi que $z \in \mathbf{Z}[i]$ est inversible si et seulement si $N(z) = 1$. On renvoie [12] d'ailleurs aux pages 56-58 du Perrin ainsi qu'à l'exercice page 64 pour de plus amples compléments sur cet anneau des entiers de Gauß et le fait notamment qu'il est euclidien et le lien avec le fait qu'un entier n est somme de deux carrés si, et seulement si, pour tout nombre premier $p \equiv 3 \pmod 4$, alors $\nu_p(n)$ est paire. C'est un sujet passionnant qui donne lieu à tout un tas de questions et de problèmes encore ouverts aujourd'hui tels que (entre autres) le nombre de telles représentations comme somme de deux carrés, le nombre de points entiers dans un cercle de rayon donné ou à des généralisations à des sommes de trois, quatre ou plus de carré qui font intervenir tout une palette d'outils passionnants allant de l'algèbre, la théorie analytique des nombres ou les formes modulaires !

1. Montrons le sens direct par contraposée. Supposons qu'il existe $a, b \in \mathbf{Z}$ tel que $p = a^2+b^2$. Alors $p = (a+ib)(a-ib)$ n'est pas irréductible car $ab \neq 0$ et donc $a \pm ib \notin \mathbf{Z}[i]^\times$.
   Réciproquement, supposons $p = uv$ avec $u, v \notin \mathbf{Z}[i]^\times$, alors $N(p) = N(u)N(v) = p^2$; donc $N(u)$ divise p^2 et comme u n'est pas inversible, $N(u) \neq 1$ et donc $N(u) = p$ (si $N(u) = p^2$ on aurait que $N(v) = 1$ mais v n'est pas inversible non plus). Donc $p = N(u) = u_1^2 + u_2^2$ où $u = u_1 + iu_2 \in \mathbf{Z}[i]$; c'est la somme de deux carrés.
2. Soit $p \equiv 3 \pmod 4$. Soient $a, b \in \mathbf{Z}$ tels que $a^2+b^2 \equiv 0 \pmod p$. Supposons $b \not\equiv 0 \pmod p$ alors b est inversible dans $\mathbf{Z}/p\mathbf{Z}$ et $(ab^{-1})^2 \equiv a^2(b^{-1})^2 \equiv -b^2(b^2)^{-1} \equiv -1 \pmod p$; on a aussi que $a^2 \not\equiv 0 \pmod p$ car $b^2 \not\equiv 0 \pmod p$ et $a^2 \equiv -b^2 \pmod p$. Si on pose $x = ab^{-1}$ on a alors que $x \not\equiv 0 \pmod p$ et $x^2 \equiv -1 \pmod p$; autrement dit -1 est un carré modulo p. Mais $(x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p$ car l'ordre de $(\mathbf{Z}/p\mathbf{Z})^\times$ est $p-1$. Donc, $\frac{p-1}{2}$ doit être pair et $p \equiv 1 \pmod 4$ ce qui est une contradiction car on supposé $p \equiv 3 \pmod 4$. On a donc montré que $b \equiv 0 \pmod p$. De même, si on suppose $a \not\equiv 0 \pmod p$ on arrive à une contradiction et $a \equiv 0 \pmod p$ aussi.
3. Pour tout entier $a \in \mathbf{Z}$ les classes possibles modulo 4 de a^2 sont : 0 ou 1 ; donc pour $a, b \in \mathbf{Z}$ les classes possibles pour a^2+b^2 modulo 4 sont $0, 1$ ou 2.
4. Montrons que les trois conditions suivantes sont équivalentes
   (a) p est irréductible,
   (b) $p \equiv 3 \pmod 4$,
   (c) p n'est pas la somme de deux carrés.

   On sait par **1.** que (a) et $c)$ sont équivalents. C'est facile de voir que (b) implique (c) : d'après la question **3.** si $p = a^2+b^2$ alors $p \not\equiv 3 \pmod 4$. Montrons que (a) implique (b). Supposons p irréductible dans $\mathbf{Z}[i]$, alors par **1.** il n'est pas somme de deux carrés et donc $p \neq 2 = 1^2+1^2$. Supposons alors que $p \equiv 1 \pmod 4$ et montrons à l'aide du théorème de Wilson [13] qu'il existe $x \in \mathbf{Z}$ tel que $x^2 \equiv -1 \pmod p$. Dans ce cas p divise $x^2+1 = (x+i)(x-i)$ or on a supposé que p était irréductible donc on a forcément que p divise $x+i$ ou $x-i$, ce qui est absurde car s'il existait $a, b \in \mathbf{Z}$ tels que $x+i = p(a+ib)$, on aurait $pb = 1$ ce qui n'est pas possible. Montrons alors que -1 est un carré modulo p. En effet, p s'écrit comme $p = 2k+1$ avec k un entier pair et on écrit $(p-1)! = 2k(2k-1)\cdots(k+1)k(k-1)\cdots 2\times 1$ Comme pour tout $i \in \{0, \dots, k-1\}$ on a que $2k-i \equiv -(i+1) \pmod p$, on

11. Commencer par établir que les inversibles de $S^{-1}A$ sont les $\frac{a}{s}$ avec a divisant un élément de S et que les irréductibles de $S^{-1}A$ sont (modulo les inversibles) les $\frac{p}{1}$ avec p irréductible de A ne divisant aucun élément de S.

12. Dont je recommande très fortement la lecture attentive, en particulier à celles et ceux qui ont l'intention de passer l'agrégation l'an prochain !

13. Je rappelle que pour démontrer le théorème de Wilson, on écrit

$$(p-1)! \equiv \prod_{x \in \mathbf{F}_p^\times} x \pmod p$$

et regroupant chaque $x \neq \pm 1$ avec son inverse x^{-1} qui vérifie $x \neq x^{-1}$, on obtient que $(p-1)! \equiv 1 \times (-1) \equiv -1 \pmod p$.

a que

$$\begin{aligned}(p-1)! &\equiv -1 \times -2^2 \times \cdots \times \left(-(i+1)^2\right) \times \cdots \times \left(-(k-1)^2\right) \times (-k^2) \\ &\equiv (-1)^k \times 2^2 \times 3^2 \times \cdots \times (k-1)^2 \times k^2 \\ &\equiv (-1)^2 (k!)^2 \\ &\equiv -1 \,(\mathrm{mod}\, p)\end{aligned}$$

d'après le théorème de Wilson. Comme k est pair on a alors que $(k!)^2 \equiv -1 \,(\mathrm{mod}\, p)$ et donc -1 est bien un carré modulo p.

► **Remarques et compléments.–** Noter qu'on a en réalité l'équivalence

$$-1 \text{ est un carré dans } \mathbf{F}_p \quad \Longleftrightarrow \quad p \not\equiv 3 \,(\mathrm{mod}\, 4)\,.$$

L'implication de gauche à droite est claire par **2.**. Il est également clair que si $p = 2$, $-1 \equiv 1 \equiv 1^2 \,(\mathrm{mod}\, 2)$. On peut donc supposer $p \equiv 1 \,(\mathrm{mod}\, 4)$ dans la suite et on veut montrer que -1 est un carré modulo p sans recourir au théorème de Wilson. On peut le démontrer en remarquant que le morphisme $\mathbf{F}_p^\times \to \mathbf{F}_p^\times$ donné par $x \mapsto x^2$ est de noyau $\{\pm 1\}$ de sorte que l'image de ce morphisme (autrement dit les carrés de $\mathbf{F}_p^\times$) sont au nombre de $\frac{\#\mathbf{F}_p^\times}{2} = \frac{p-1}{2}$. On sait alors par le petit théorème de Fermat que pour tout $a \in \mathbf{F}_p^\times$, $a^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$ de sorte que $a^{\frac{p-1}{2}}$ est racine de $X^2 - 1 =$ dans $\mathbf{F}_p^\times$ et donc vaut 1 ou -1. Il est clair que si $a \equiv b^2 \,(\mathrm{mod}\, p)$ est un carré, alors $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$. Or tout élément de $\mathbf{F}_p^\times$ est racine de $X^{p-1} - 1 = \left(X^{\frac{p-1}{2}} - 1\right)\left(X^{\frac{p-1}{2}} + 1\right)$. Comme on a $\frac{p-1}{2}$ carrés, on voit que ces carrés sont exactment les racines de[14] $X^{\frac{p-1}{2}} - 1$. Mais comme $\frac{p-1}{2}$ est paire, on voit que -1 est racine de $X^{\frac{p-1}{2}} - 1$ et est donc un carré modulo p.

Par ailleurs, pour déterminer si p est irréductible (et donc si (p) est premier puisque l'anneau est euclidien donc factoriel), on pouvait aussi raisonner comme suit. On a par définition $A = \mathbf{Z}[i] \cong \mathbf{Z}[X]/(X^2+1)$. On utilise alors le fait que pour deux idéaux I et J de A, alors

$$(A/I)/J = (A/I)/\pi(J)$$

avec $\pi = A \to A/I$ la surjection canonique et où $\pi(J)$ est un idéal car π est surjective. On sait alors par le cours que $\pi(J) = (I+J)/I$ et le troisième théorème d'isomorphisme fournit

$$(A/I)/J = (A/I)/\pi(J) = (A/I)/((I+J)/I) \cong A/(I+J).$$

Par symétrie, il vient

$$(A/I)/J \cong (A/J)/I \cong A/(I+J)$$

et on peut en fait faire "commuter les quotients"! Ainsi, dans notre cas,

$$A/(p) \cong \left(\mathbf{Z}[X]/(X^2+1)\right)/(p) \cong \mathbf{Z}[X]/(p, X^2+1) \cong \left(\mathbf{Z}[X]/(p)\right)/(X^2+1).$$

Or, à partir du fait que[15] $\mathbf{Z}[X]/(p) \cong \mathbf{F}_p[X]$, on a $\left(\mathbf{Z}[X]/(p)\right)/(X^2+1) \cong \mathbf{F}_p[X]/(X^2+1)$ si bien qu'on a

$$A/(p) \cong \mathbf{F}_p[X]/(X^2+1).$$

Il suffit alors de voir que si -1 est un carré, disons $\alpha^2 \equiv -1 \,(\mathrm{mod}\, p)$, modulo p (autrement dit d'après ce qui précède si $p = 2$ ou $p \equiv 1 \,(\mathrm{mod}\, 4)$), alors $X^2 + 1 = (X-\alpha)(X+\alpha)$ et l'anneau $\mathbf{F}_p[X]/(X^2+1)$ n'est pas intègre et p n'est pas premier tandis que si -1 n'est pas un carré modulo p (autrement dit si $p \equiv 3 \,(\mathrm{mod}\, p)$), alors X^2+1 n'a pas de racine dans le corps $\mathbf{F}_p$ et est de degré 2 donc irréductible et $\mathbf{F}_p[X]/(X^2+1) \cong \mathbf{F}_4$ est un corps et (p) est premier. On a en réalité que si k est un corps et que $P \in k[X]$ non nul, alors $k[X]/(P)$ est intègre si, et seulement si, $k[X]/(P)$ est un corps si, et seulement si, P est irréductible. On peut le voir en construisant un inverse à l'aide du théorème de Bézout comme dans le TD ou en disant que $k[X]$ est principal car k est un corps donc P irréductible équivaut à (P) premier non nul (qui équivaut donc à $k[X]/(P)$ intègre) qui équivaut à (P) maximal (qui équivaut à $k[X]/(P)$ corps). Enfin, si le degré de P est inférieur à 3, être irréductible sur k équivaut à ne pas avoir de racine sur k. Le résultat tombe en défaut pour des degrés supérieurs[16] mais on a un critère le généralisant que vous trouverez dans le chapitre 3 du Perrin! Je rappelle enfin que les irréductibles de $\mathbf{C}[X]$ sont les polynômes de degré 1 et ceux de $\mathbf{R}[X]$ les polynômes de degré 1 ou les polynômes de degré 2 sans racines réelles[17] comme on l'a établi en TD! En revanche, on verra que sur $\mathbf{Q}$ ou un corps fini, il existe des polynômes irréductibles de tout degré!

Exercice 4. Soit A le sous-anneau de $\mathbf{C}$ engendré par $\alpha = \frac{1+i\sqrt{19}}{2}$. Le but de cet exercice est de montrer que A est principal, mais pas euclidien.

14. Dans un corps commutatif, un polynôme ne peut avoir plus de racines que son degré.
15. En effet, la réduction modulo p des coefficients fournit un morphisme surjectif $\mathbf{Z}[X] \to \mathbf{F}_p[X]$ de noyau (p).
16. Comme par exemple, $(X^2+1)^2$ sur $\mathbf{R}[X]$.
17. Car si P est de degré au moins 3, il possède une racine complexe z. Si $z \in \mathbf{R}$, P n'est pas irréductible et si $z \in \mathbf{C} \setminus \mathbf{R}$, alors $\overline{z}$ est aussi racine de P et P est divisible par $(X-z)(X-\overline{z}) \in \mathbf{R}[X]$ n'est pas irréductible non plus!

1. Montrer d'abord que, si B est un anneau euclidien, alors il existe un élément non inversible $x \in B$ tel que la restriction à $B^* \cup \{0\}$ de la projection de B sur $B/(x)$ soit surjective.
   Ceci nous servira de critère pour montrer que l'anneau A n'est pas euclidien.
2. Donner un polynôme du second degré à coefficients entiers P s'annulant en α. En déduire que A est isomorphe à $\mathbf{Z}[X]/P$ et que le groupe abélien sous-jacent à A est engendré par 1 et α. Vérifier que l'application norme, qui à $z \in A$ associe $N(z) = z\overline{z}$, prend ses valeurs dans $\mathbf{N}$.
3. Montrer que 1 et -1 sont les seuls éléments inversibles de A.
4. Montrer qu'il n'existe pas de morphisme d'anneaux de A dans $\mathbf{Z}/2\mathbf{Z}$ ou $\mathbf{Z}/3\mathbf{Z}$.
   Indication : pour chacun des deux cas, supposer que f soit un tel morphisme, et étudier l'image par f du polynôme trouvé en ***2.***
5. En déduire que A n'est pas euclidien.
   Indication : utiliser le critère de ***1.***
6. On va montrer que A est principal.
   (a) Montrer que pour tout a, b éléments non nuls de A, il existe $q, r \in A$ tels que $r = 0$ ou $N(r) < N(b)$ et qui vérifient, soit $a = bq + r$, soit $2a = bq + r$.
   (b) Montrer que l'idéal engendré par 2 est maximal dans A (on pourra utiliser le fait que A est isomorphe à un quotient de $\mathbf{Z}[X]$).
   (c) Montrer que A est principal.

SOLUTION.

1. Supposons B euclidien et notons ν son stathme. On doit montrer qu'il existe $x \in B$ non inversible tel que, si on note (x) l'idéal de B engendré par x, pour tout $a \in B$ il existe $b \in B^\times \cup \{0\}$ tel que $b - a \in (x)$, *i.e.* tel que $a = qx + b$ pour $q \in B$ et b inversible. Si B est un corps, alors $x = 0$ convient. Sinon soit[18] $x \in B\backslash(B^\times \cup \{0\})$ tel que $\nu(x)$ soit minimal dans $B\backslash(B^\times \cup \{0\})$. Comme B est euclidien, pour tout $a \in B$ il existe $q, b \in B$ tels que $a = qx + b$ avec $b = 0$ ou $\nu(b) < \nu(x)$. Si $b = 0$ on a que $a \in (x)$ et donc $\pi(0) = \pi(a)$. Sinon, $\nu(b) < \nu(x)$ implique que b est nul ou inversible et $\pi(b) = \pi(a)$ avec $\pi : B \to B/(x)$ la surjection canonique.
2. Puisque clairement $\alpha + \overline{\alpha} = 1$ et $\alpha\overline{\alpha} = 5$, on voit que[19] $\alpha = \frac{1+i\sqrt{19}}{2}$ est racine de $P(X) = X^2 - X + 5$. Montrons que A est isomorphe à $\mathbf{Z}[X]/(P)$. Pour tout $F \in \mathbf{Z}[X]$ il existe $Q, R \in \mathbf{Z}[X]$ tels que $F = QP + R$ où $R = 0$ ou $\deg(R) < \deg P = 2$ car le coefficient dominant de P est inversible dans[20] $\mathbf{Z}$. On peut donc définir un morphisme π de $\mathbf{Z}[X]$ dans $\mathbf{Z}[X]/(P)$ qui a F associe R, le reste de la division euclidienne de F par P. Comme $P(\alpha) = 0$ le morphisme

$$\begin{aligned} \varphi : \mathbf{Z}[X] &\to \mathbf{Z}[\alpha] \\ X &\mapsto \alpha \end{aligned}$$

   se factorise par (P) et on obtient un morphisme $\tilde{\varphi} : \mathbf{Z}[X]/(P) \to \mathbf{Z}[\alpha]$ tel que $\varphi = \tilde{\varphi} \circ \pi$. Le morphisme $\tilde{\varphi}$ est en fait surjectif : comme $\alpha^2 = \alpha - 5$ on sait que 1 et α engendrent $\mathbf{Z}[\alpha]$. Si $R(X) \in \mathbf{Z}[X]/(P)$ alors R est de la forme $R(X) = aX + b$ car $\deg(R) < 2$ et donc $\tilde{\varphi}(aX + b) = a\alpha + b$. On a en plus que $\tilde{\varphi}$ est injectif : si $\tilde{\varphi}(aX + b) = \tilde{\varphi}(a'X + b')$ alors α est racine de $(a - a')X + b - b' = 0$ donc $\alpha = \frac{b'-b}{a-a'} \in \mathbf{Q}$; or $\alpha = \frac{1+i\sqrt{19}}{2}$ donc $a = a'$ et $b = b'$. On en déduit que $\mathbf{Z}[X]/(P) \simeq \mathbf{Z}[\alpha]$.
   On vérifie facilement que pour $z = a\alpha + b \in \mathbf{Z}[\alpha]$, $N(z) = z\overline{z} = (a\alpha + b)(\overline{a\alpha + b}) = 5a^2 + ab + b^2 \in \mathbf{N}$.
3. Supposons z inversible et z' tel que $zz' = 1$. Alors $N(zz') = N(z)N(z') = 1$, donc $N(z) = 1$. Si $z = a\alpha + b$ on a que $5a^2 + ab + b^2 = 1$ donc $a = 0$ et $b = \pm 1$ donc $z = \pm 1$. On vérifie ensuite que 1 et -1 sont effectivement inversibles et donc $\mathbf{Z}[\alpha]^* = \{-1, 1\}$.
4. Supposons $f : A \to \mathbf{Z}/2\mathbf{Z}$ un morphisme d'anneaux. Puisque $f(1) = 1$ et qu'on a un morphisme d'anneaux, pour tout $n \in \mathbf{Z}$, $f(n)$ n'est autre que la réduction de n modulo 2. Par ailleurs, on a dans A que $\alpha^2 - \alpha + 5 = 0$ donc donc il existe $\beta = f(\alpha) \in \mathbf{Z}/2\mathbf{Z}$ tel que $\beta^2 - \beta + 1 = 0$, or $\beta^2 - \beta + 1 = 1 \neq 0$ dans $\mathbf{Z}/2\mathbf{Z}$ car $x^2 = x$ pour tout $x \in \mathbf{Z}/2\mathbf{Z}$. Ainsi on a une contradiction. De même si $f : A \to \mathbf{Z}/3\mathbf{Z}$ on aurait $\beta = f(\alpha) \in \mathbf{Z}/3\mathbf{Z}$ tel que $\beta^2 - \beta - 1 = 0$ mais $X^2 - X - 1$ n'a pas de racines dans $\mathbf{Z}/3\mathbf{Z}$.
5. Supposons A euclidien ; d'après **1.** il existe x non inversible et non nul tel que la restriction de $\pi : A \to A/(x)$ à $A^\times \cup \{0\}$ soit surjective. Comme $A \simeq \mathbf{Z}[\alpha]$, on a $A^\times : \{-1, 1\}$ et $\pi|_{A^\times \cup \{0\}} : \{-1, 1, 0\} \to A/(x)$ est surjective. On montre que $A/(x)$ est un corps[21] : pour tout $a + (x) \in A/(x)$ il existe b inversible ou $b = 0$ tel que $a + (x) = b + (x)$. Si $b = 0$ alors $a + (x)$ est l'élément neutre de $A/(x)$; si b est inversible alors $\pi(b) = a + (x)$ est inversible d'inverse $\pi(b^{-1})$. Ainsi $A/(x)$ est donc un corps. Comme $p|_{A^\times \cup \{0\}}$ est surjective le cardinal de $A/(x)$ est inférieur ou égal à 3, $A/(x)$ est donc isomorphe soit à $\mathbf{Z}/2\mathbf{Z}$ soit à $\mathbf{Z}/3\mathbf{Z}$. On aurait donc un morphisme de A dans $\mathbf{Z}/2\mathbf{Z}$ ou dans $\mathbf{Z}/3\mathbf{Z}$, ce qui est impossible. Donc A n'est pas euclidien.

18. Bien noter que puisque B n'est pas un corps, $B\backslash(B^\times \cup \{0\}) \neq \varnothing$.
19. Ou on utilise que l'on sait que si α est racine d'un polynôme à coefficients entiers (et donc réels), alors $\overline{\alpha}$ aussi et on calcule alors $(X - \alpha)(X - \overline{\alpha})$.
20. C'est un résultat très important. Voir par exemple le lemme 3.31 du Perrin.
21. Ou alors on raisonne en termes de groupes sous-jacents.

▶ **Remarque.–** Cela découle qu'un corps de cardinal p est de caractéristique p et contient $\mathbf{F}_p$ comme sous-corps premier donc lui est égal. On peut le redémontrer en considérant le morphisme si k est un corps de cardinal p

$$f : \left\{ \begin{array}{ccc} \mathbf{Z} & \longrightarrow & k \\ n & \longmapsto & n \cdot 1_k. \end{array} \right.$$

Ce morphisme a pour noyau un idéal de $\mathbf{Z}$ de la forme $c\mathbf{Z}$ tel que $\mathbf{Z}/c\mathbf{Z}$ soit un sous-anneau de k intègre. Cela impose c premier et par cardinalité, $c = p$ de sorte que le théorème de factorisation fournit $k \cong \mathbf{Z}/p\mathbf{Z}$. On pouvait aussi raisonner en termes de groupe sous-jacent et voir qu'un isomorphisme de groupes avec $\mathbf{Z}/2\mathbf{Z}$ ou $\mathbf{Z}/2\mathbf{Z}$ s'étendait naturellement en un isomorphisme d'anneaux (et même de corps).

6. (a) Soient $a, b \in A$ non nuls. Soit $x = \frac{a}{b} \in \mathbf{C}$; il s'écrit $x = u + v\alpha$ avec $u, v \in \mathbf{Q}$. ($x = \frac{a\bar{b}}{b\bar{b}} = \frac{1}{N(b)}(a\bar{b}) \in \mathbf{Q}[\alpha]$). Soit n la partie entière de v. Alors $v \in [n, n+1[$. Supposons[22] $v \notin \left]n + \frac{1}{3}, n + \frac{2}{3}\right[$ et soient s, t les entiers les plus proches de u et de v respectivement. Alors $|s - u| \leqslant \frac{1}{2}$, $|t - v| \leqslant \frac{1}{3}$. On pose $q = s + t\alpha$ et donc $q \in A = \mathbf{Z}[\alpha]$. On a alors que $N(x-q) = N((u-s)+(v-t)\alpha) = (s-u)^2+(s-u)(t-v)+5(t-v)^2 \leq \frac{1}{4}+\frac{1}{6}+\frac{5}{9} = \frac{35}{36} < 1$. On pose $r = a - bq \in A$. On a alors que $a = bq + r$ et $N(r) < N(b)$.
Supposons maintenant $v \in \left]n + \frac{1}{3}, n + \frac{2}{3}\right[$. On prend $2x = 2u + 2v\alpha$ et $2v \in \left]2n + \frac{2}{3}, 2n + 1 + \frac{1}{3}\right[$, si m est la partie entière de $2v$ alors $2v \notin \left]m + \frac{1}{3}, m + \frac{2}{3}\right[$. On se ramène donc au cas précédent et $2a = bq + r$ avec $N(r) < N(b)$.

(b) On a que $A \simeq \mathbf{Z}[X]/(X^2 - X + 5)$ donc

$$A/(2) \simeq \mathbf{Z}[X]/(2, X^2 - X + 5) \simeq (\mathbf{Z}/2\mathbf{Z})[X]/(X^2 - X + 5) \simeq \mathbf{F}_2[X]/(X^2 + X + 1)$$

et $X^2 + X + 1$ est irréductible dans $\mathbf{F}_2[X]$ (car de degré 2 sans racine), on a que $A/(2)$ est un corps (isomorphe à $\mathbf{F}_4$).

(c) Soit I un idéal non nul de A et $a \in I$, $a \neq 0$ tel que $N(a)$ soit minimal parmi les éléments non nuls de I. Montrons que $I = (a)$. Soit $x \in I \backslash (a)$. Si $x = aq + r$ avec $N(r) < N(a)$ ou $r = 0$, comme $x, a \in I$ on a que $r \in I$ et donc $r = 0$ car $N(a)$ est minimal dans I. Dans ce cas $x \in (a)$, donc $I \subseteq (a)$ et $I = (a)$.
Sinon $2x = aq + r$, $N(r) < N(a)$ ou $r = 0$, on a aussi $r = 0$ et $2x = aq$ donc $aq \in (2)$. Comme (2) est maximal, il est premier donc soit $a \in (2)$ soit $q \in (2)$. Si $q \in (2)$, alors q est de la forme $q = 2q'$, donc $2x = a2q'$ donc $2(x - aq) = 0$ ce qui implique que $x = qa$ car A est intègre. Donc $x \in (a)$ et à nouveau $I = (a)$. On peut donc supposer que $a \in (2)$ et on peut même supposer que $q \notin (2)$. Donc a est de la forme $a = 2a'$ et $x = a'q \in (a')$; comme $N(a) = N(2)N(a')$ on a $N(a') < N(a)$. Montrons que $a' \in I$. Comme (2) est maximal et $q \notin (2)$ on a que l'idéal engendré par 2 et q, $(2) + (q)$ est égal à A. Il existe alors $\lambda, \mu \in A$ tels que $2\lambda + q\mu = 1$, ce qui implique que $a' = 2\lambda a' + q\mu a' = a\lambda + \mu x \in I$. Mais $N(a)$ est minimal dans I, donc on arrive à une contradiction. On a finalement bien que $I = (a)$ et A est principal.

Un autre exemple (utilisant le même critère que celui en **1.**) est donné en exercice dans le Perrin (corrigé dans *Exercices de mathématiques pour l'agrégation : Algèbre 1* de Francinou et Gianella). Il s'agit de l'anneau $\mathbf{R}[X, Y]/(X^2 + Y^2 + 1)$ qui est principal non euclidien et constitue un bon exercice pour s'entraîner sur les anneaux de polynômes.

Exercices complémentaires de la semaine 1

Exercice 5. Soit A un anneau factoriel. On suppose qu'il vérifie le théorème de Bezout, i.e. pour tous $a, b \in A$ premiers entre eux, il existe $u, v \in A$ avec $ua + vb = 1$.

1. Montrer que si $a, b \in A$ ont pour pgcd d, alors il existe $u, v \in A$ avec $ua + bv = d$.

2. Montrer que si une famille finie $a_1, ..., a_n$ d'éléments de A a pour pgcd 1, alors il existe des éléments $u_1, ..., u_n$ de A avec $\sum_{i=1}^{n} u_i a_i = 1$.

3. Montrer que si I est un idéal de A, alors il existe une famille finie d'éléments de I dont le pgcd est le pgcd de tous les éléments de I.

4. En déduire que A est principal.

Solution.

1. C'est immédiat en notant que a/d et b/d sont premiers entre eux[23].

2. Par récurrence sur n. C'est clair pour $n \leqslant 2$ avec l'hypothèse. Supposons le résultat vrai jusqu'à $n - 1$. Soit $d = \text{pgcd}(a_1, \ldots, a_{n-1})$. Alors il existe u, v dans A avec $ud + va_n = 1$ car $\text{pgcd}(d, a_n) = 1$ par définition du pgcd. Ensuite, l'hypothèse de récurrence appliquée à $a_1/d, \ldots, a_{n-1}/d$ donne une décomposition

$$d = u_1 a_1 + \cdots + u_{n-1} a_{n-1}, \quad u_1, \ldots, u_{n-1} \in A,$$

d'où on déduit le résultat.

22. Il est conseillé ici de s'aider d'un dessin !

23. Noter que comme A est intègre et a, b sont divisibles par d, a/d et b/d ont bien un sens

3. Si I est nul ou $I = A$, c'est clair (si $I = A$ le pgcd de tous ses éléments est évidemment 1). Sinon I contient un élément non nul et non inversible a, qu'on peut écrire

$$a = u.\prod_{i=1}^{r} p_i^{v_i(a)},$$

avec $u \in A^\times$, $v_i(a) \in \mathbf{N}$, et les p_i irréductibles non associés deux à deux. Soit alors, pour chaque $i \in \{1, \dots, r\}$, a_i un élément de I tel que $w_i := v_i(a_i)$ soit minimum parmi les $v_i(x)$ avec $x \in I$ non nuls. Posons alors

$$d = \prod_{i=1}^{r} p_i^{w_i}.$$

Notons également μ le pgcd de $a_1, a_2, \dots, a_r, a$. Par **2.**, $\mu \in I$ et par définition des a_i, $p_i^{w_i}$ divise μ et donc $d \mid \mu$. Réciproquement, μ divise a et n'a donc pas d'autres facteurs irréductibles que $p_1, \dots, p_r$ et comme μ divise a_i pour tout i, sa valuation p_i-adique est inférieure à w_i de sorte que $\mu \mid d$ et enfin d est le pgcd de de $a_1, a_2, \dots, a_r, a$ et appartient par conséquent à I par **2**. On vérifie alors que par définition, d divise tous les éléments de I. C'est alors le plus grand car si on a un autre élément d' qui divise tous les éléments de I, alors puisque d est dans [24] I, on aurait que d' divise d et donc d' est plus petit que d (au sens de la divisibilité), ce qui prouve que d est le plus grand diviseur commun à tous les éléments de I.

4. Soient I un idéal de A et d le pgcd de tous les éléments de I. D'après **3.**, c'est aussi le pgcd d'une famille finie $a_1, \dots, a_r$ d'éléments de I. En appliquant **2.** à $a_1/d, \dots, a_r/d$, on obtient que $d \in I$, d'où $(d) \subseteq I$. Par ailleurs $I \subseteq (d)$ par définition du pgcd de tous les éléments de I. Finalement I est bien principal.

Noter qu'on pouvait conclure directement sans passer par **3.** En effet, si $I \neq (0)$, on prend $x \in I$ l'élément dont le nombre de facteurs irréductibles (avec multiplicité) est minimal [25] parmi les éléments non nuls de I. On a alors que pour tout $a \in I$, $\text{pgcd}(a, x) \mid x$ donc a moins de facteurs irréductibles que x et est dans I d'après **1.** mais donc par minimalité, $\text{pgcd}(a, x) = ux$ avec $u \in A^\times$, autrement dit $x \mid a$ et $I \subseteq (x)$ tandis que l'inclusion $(x) \subseteq I$ est triviale donc $I = (x)$ et il n'est pas difficile de voir que x est le pgcd de tous les éléments de I.

► **Remarques.–** On peut en revanche construire des anneaux de Bézout non principaux comme l'anneau des fonctions holomorphes étudiés ici ou dans le TD d'il y a deux ans. Enfin, le TD d'il y a deux ans que vous trouverez sur la page web de David Harari utilise cet exercice pour établir qu'un anneau factoriel dans lequel tout idéal premier non nul est maximal est principal.

Exercice 6. Le *radical de Jacobson* d'un anneau commutatif A est l'intersection de tous les idéaux maximaux de A. On le note $\operatorname{rad} A$.

1. Soit A un anneau. Montrer qu'un élément a est dans le radical de A si, et seulement si, pour tout $x \in A$, $1 - ax$ est inversible.
2. Toujours en supposant que A est commutatif, montrer que si $x \in A$ est nilpotent, alors $1 - ax$ est inversible, pour tout élément $a \in A$.
3. Toujours dans le cas commutatif, montrer que le radical de A est le plus grand idéal de A tel que $1 - x$ est inversible pour tout $x \in \operatorname{rad} A$.
4. Toujours dans le cas où A est commutatif, soit I un idéal dont tous les éléments sont nilpotents. Montrer que $I \subseteq \operatorname{rad} A$.
5. Calculer le radical de $\mathbf{Z}$, $\mathbf{R}[X]$, $\mathbf{Z}/n\mathbf{Z}$ (pour un entier $n > 1$).

Solution.

1. Supposons que $a \in \operatorname{rad}(A)$ et soit $x \in A$. Si $1 - ax$ est non inversible, $1 - ax$ appartient à un idéal maximal $\mathfrak{M}$ de A. Mais par définition, $a \in \mathfrak{M}$ donc $1 = 1 - ax + ax \in \mathfrak{M}$, ce qui est absurde.
   Réciproquement, soit $a \in A$ tel que pour tout $x \in A$, $1 - ax \in A^\times$. Supposons qu'il existe un idéal maximal $\mathfrak{M}$ ne contenant pas a. Alors si $\pi : A \to A/\mathfrak{M}$ est la surjection canonique, on a que $\pi(a) \neq 0$ et $A/\mathfrak{M}$ étant un corps et par surjectivité de π, il existe $x \in A$ tel que $\pi(a)\pi(x) = \pi(ax) = 1$ soit $1 - ax \in \mathfrak{M}$, ce qui contredit l'inversibilité de $1 - ax$. Finalement, $a \in \operatorname{rad}(A)$.
   On pouvait aussi raisonner en disant que dans ce cas $\mathfrak{M} + (a) = A$ de sorte que $1 = m + ax$ et $1 - ax = m \in \mathfrak{M}$ ne peut être inversible.
2. Supposons que $x^k = 0$ pour $k \in \mathbf{N}^\times$. On pose alors [26]

$$u = \sum_{n=0}^{+\infty} (ax)^n = \sum_{n=0}^{+\infty} a^n x^n = \sum_{n=0}^{k-1} a^n x^n$$

qui est bien défini car x est nilpotent et A est commutatif. On a alors

$$(1 - ax)u = \sum_{n=0}^{k-1} a^n x^n - \sum_{n=1}^{k-1} a^n x^n = 1$$

si bien que u est l'inverse de $1 - ax$ qui est donc inversible.

24. Voir un argument ci-dessous pour le fait que $d \in I$.
25. Ce qui est bien défini puisque le nombre de facteurs irréductibles des éléments non nul est une partie non vide de $\mathbf{N}$.
26. Reconnaître la série $\frac{1}{1-ax}$.

3. Le radical est clairement un idéal vérifiant la condition. Soit alors un idéal I tel que pour tout $y \in I$, $1-y$ est inversible. Soit $a \in I$ et utilisons le critère de **1.** pour montrer que $a \in \mathrm{rad}(A)$. Soit $x \in A$, alors $y = ax \in I$ et donc $1 - ax = 1 - y$ est inversible, ce qui démontre le résultat.

4. C'est évident en combinant **2.** et **1.**.

5. On sait que les idéaux maximaux de $\mathbf{Z}$ sont les $p\mathbf{Z}$ avec p premier si bien que

$$\mathrm{rad}(\mathbf{Z}) = \bigcap_{p \text{ premier}} p\mathbf{Z} = \{0\}.$$

De même, les idéaux de $\mathbf{R}[X]$ sont les idéaux engendrés par un polynôme irréductible de $\mathbf{R}[X]$ et $\mathrm{rad}(\mathbf{R}[X]) = \{0\}$. La discussion page 3 fournit que

$$\mathrm{rad}\left(\mathbf{Z}/n\mathbf{Z}\right) = \bigcap_{\substack{p|n \\ p \text{ premier}}} p\mathbf{Z}/n\mathbf{Z} = r(n)\mathbf{Z}/n\mathbf{Z}$$

avec $r(n) = \prod_{p|n} p$ le *radical*[27] de n.

Le radical et le radical de Jacobson d'un idéal jouent un rôle important en géométrie algébrique notamment.

Exercices fondamentaux de la semaine 2

Exercice 7. Montrer qu'un polynôme $P(X,Y) \in \mathbf{Z}[X,Y]$ est tel que $P\left(t^2,t^3\right) = 0$ pour tout $t \in \mathbf{Z}$ si, et seulement si, il existe un polynôme $Q(X,Y) \in \mathbf{Z}[X,Y]$ tel que $P(X,Y) = (X^3 - Y^2) \cdot Q(X,Y)$. En déduire un isomorphisme de $\mathbf{Z}$-algèbres

$$\mathbf{Z}[X,Y]/\left(X^3 - Y^2\right) \cong \{P \in \mathbf{Z}[T] \ : \ P'(0) = 0\} \cong \mathbf{Z}[T^2,T^3].$$

Solution. Commençons par préciser que l'on peut toujours effectuer une division euclidienne dans $k[X]$ pour k corps avec unicité du quotient et du reste. On a vu dans l'exercice 10 du TD III que l'on peut toujours effectuer une division euclidienne (en perdant l'unicité cependant) de P par Q dans $A[X]$ à condition que le coefficient dominant de Q soit inversible[28] dans A. Si jamais le coefficient dominant de Q n'est pas inversible, alors on peut parfois s'en sortir en voyant $A[X] \subseteq \mathrm{Frac}(A)[X]$ et effectuer le division euclidienne dans $\mathrm{Frac}(A)[X]$. Par exemple, soient $P, Q \in A[X,Y] = A[X][Y]$. Si le coefficient dominant de Q vu dans $A[X][Y]$ n'est pas dans $A[X]^\times = A^\times$, alors on effectue la division dans $A(X)[Y]$, ce qui fournit $B, R \in A[X,Y]$ avec $\deg_Y(R) < \deg_Y(Q)$ et $A \in A[X]$ non nul tel que $A(X)P(X,Y) = Q(X,Y)B(X,Y) + R(X,Y)$.

Venons-en alors à l'exercice à proprement parler. Il est immédiat que si $P \in (X^3 - Y^2)$, alors pour tout entier relatif t, $P(t^2,t^3) = 0$. Réciproquement, supposons que pour tout entier relatif t, $P(t^2,t^3) = 0$. le coefficient dominant de[29] $X^3 - Y^2 \in \mathbf{Z}[X][Y]$ est égal à $-1 \in \mathbf{Z}^\times = \mathbf{Z}[X]^\times$. On peut donc effectuer une division euclidienne de P par $X^3 - Y^2$ si bien qu'il existe $Q, R \in \mathbf{Z}[X,Y]$ avec $\deg_Y(R) < 2$ tels que $P(X,Y) = (X^3 - Y^2)Q(X,Y) + R(X,Y)$. Puisque $\deg_Y(R) < 2$, il existe $A, B \in \mathbf{Z}[X]$ tels que $R(X,Y) = A(X)Y + B(X)$ de sorte que $P(X,Y) = (X^3 - Y^2)Q(X,Y) + A(X)Y + B(X)$. On peut alors évaluer cela en $t \in \mathbf{Z}$ pour obtenir que

$$0 = P(t^2,t^3) = (t^6 - t^6)Q(t^2,t^3) + A(t^2)t^3 + B(t^2) = A(t^2)t^3 + B(t^2).$$

On en déduit (puisque $\mathbf{Z}$ est infini) que $A(X^2)X^3 + B(X^2) = 0$. On voit que $A(X^2)X^3$ ne fait intervenir que des monômes impairs distincts et que $B(X^2)$ ne fait intervenir que des monômes pairs distincts. On en déduit que $A = B = 0$ et donc $R = 0$ et $P \in (X^3 - Y^2)$ et on a bin démontré l'équivalence.
On pose alors $\mathbf{Z}[T^2,T^3] = \{P(T^2,T^3) \ : \ P \in \mathbf{Z}[X,Y]\}$ et on considère le morphisme surjectif de $\mathbf{Z}$-algèbre $f : \mathbf{Z}[X,Y] \to \mathbf{Z}[T^2,T^3]$ définie par $P \mapsto P(T^2,T^3)$. Ce qui précède garantit que le noyau est égal à l'idéal $(X^3 - Y^2)$ si bien qu'au quotient on a bien

$$\mathbf{Z}[X,Y]/\left(X^3 - Y^2\right) \cong \mathbf{Z}[T^2,T^3].$$

Reste donc à voir que $\{P \in \mathbf{Z}[T] \ : \ P'(0) = 0\} \cong \mathbf{Z}[T^2,T^3]$. On a évidemment $\mathbf{Z}[T^2,T^3] \subseteq \{P \in \mathbf{Z}[T] \ : \ P'(0) = 0\}$ puisqu'un tel polynôme n'a pas de terme en T. Réciproquement, si $P \in \{P \in \mathbf{Z}[T] \ : \ P'(0) = 0\}$, alors il existe un $d \in \mathbf{N}$ tel que

$$P = \sum_{\substack{i=0 \\ i \neq 1}}^{d} a_i T^i.$$

Mais pour tout $i \neq 1$, on peut effectuer la division euclidienne de i par 3 pour obtenir l'existence de $q \in \mathbf{Z}$ et $r \in \{0,1,2\}$ tel que $i = 3q + r$. Si $r = 0$, alors $T^i = (T^3)^q$ tandis que si $r = 2$, alors $T^i = (T^3)^q T^2$. Enfin, si $r = 1$, on a $i = 3(q-1) + 4$ et $T^i = (T^3)^{q-1}(T^2)^2$ qui a bien un sens car $q - 1 \geqslant 0$ puisque sinon $q = 0$ et $r = 1$ donc $i = 1$ ce qui est exclu. On a donc bien que $P \in \mathbf{Z}[T^2,T^3]$, ce qui conclut la démonstration. On pouvait aussi traiter les cas i pairs d'un côté et les $i \geqslant 3$ impairs en remarquant que $i - 3$ est positif et pair.

27. Qui intervient notamment dans la célèbre conjecture abc qui explore le lien entre les structures additive et multiplicative des entiers.
28. Voir le lemme 3.31 du Perrin pour une démonstration.
29. Noter que ce choix est plus judicieux que $A[Y][X]$ car le degré en Y de $X^3 - Y^2$ est strictement inférieur à son degré en X.

Exercice 8. Soit k un corps. On note $F = k(X)$ le corps des fractions rationnelles.

1. Soient $R_1 = P_1/Q_1, \ldots, R_s = P_s/Q_s$ des éléments de F, avec $P_i \in k[X]$ et Q_i non nul dans $k[X]$ pour tout i de $\{1, \ldots, s\}$. Soit B la sous-k-algèbre de F engendrée par $R_1, \ldots, R_s$. Montrer qu'il existe un polynôme non nul $G \in k[X]$ tel que $B \subseteq (k[X])[G^{-1}]$.
2. En déduire que F n'est pas de type fini en tant que k-algèbre.

Solution.

1. Par définition, tout élèment f de B est un polynôme en les R_i, et en particulier $f = P/Q$ avec $P \in k(X)$ et Q de la forme $Q_1^{\alpha_1} \cdots Q_r^{\alpha_r}$, où les α_i sont dans $\mathbf{N}$. Il suffit alors de prendre $G = Q_1 \cdots Q_r$.
2. Il suffit de montrer qu'une algèbre B comme ci-dessus ne peut pas être égale à $k(X)$. Or, la fraction rationnelle $1/(G+1)$ n'est clairement pas dans $(k[X])[G^{-1}]$, sinon on pourrait écrire $1/(G+1) = H/G^m$ avec $H \in k[X]$ premier à G, ce qui contredit $(G+1)H = G^m$ vu que $(G+1)$ est premier à G.

Exercice 9. Soient B un anneau, L un sous-anneau de B et A un sous-anneau de L. On suppose que L est un corps, que B est un L-espace vectoriel de dimension finie, et que B est aussi une A-algèbre de type fini. On se propose de montrer que L est une A-algèbre de type fini. Soient $\alpha_1, \ldots, \alpha_n$ dans B tels que $B = A[\alpha_1, \ldots, \alpha_n]$.

1. Soit $\beta_1, \ldots, \beta_m$ une base de B sur L, avec $\beta_1 = 1$. On écrit

$$\beta_i\beta_j = \sum_{k=1}^{m} a_{ijk}\beta_k; \quad \alpha_i = \sum_{j=1}^{m} b_{ij}\beta_j,$$

avec $a_{ijk}, b_{ij} \in L$. Soit C la sous A-algèbre de L engendrée par les a_{ijk} et les b_{ij}. Montrer que tout élément x de B s'écrit :

$$x = \sum_{i=1}^{m} \lambda_i\beta_i,$$

où les λ_i sont dans C.

2. En déduire que $L = C$, et conclure.

Solution.

1. Soit B' l'ensemble des éléments de B de la forme $\sum_{i=1}^{m} \lambda_i\beta_i$ avec les λ_i dans C (c'est le C-module engendré par les β_i). Si x est dans B, c'est un polynôme en les α_i à coefficients dans A. Il suffit donc de montrer que tous les monômes

$$\alpha_1^{r_1} \cdots \alpha_n^{r_n}$$

en les α_i sont dans B'. Comme chaque α_i est une combinaison linéaire des β_j à coefficients dans C, il suffit de montrer que tout monôme

$$\beta_1^{s_1} \cdots \beta_m^{s_m}$$

en les β_j est dans B'. Or, d'après la définition des a_{ijk}, chaque β_i (rappelons que $\beta_1 = 1$) et chaque produit $\beta_i\beta_j$ sont dans B'. Ainsi B' est stable par multiplication par chaque β_i, ce qui montre que tous les monômes $\beta_1^{s_1} \cdots \beta_m^{s_m}$ comme ci-dessus sont bien dans B'. Finalement $B' = B$.

2. Soit $y \in L$, alors $y = y\beta_1 \in B$, et d'aprés a) on peut écrire $y = \sum_{i=1}^{m} \lambda_i\beta_i$ avec les λ_i dans $C \subset L$. Mais par unicité de la décomposition d'un élément de B sur la base $(\beta_1, \ldots, \beta_m)$ du L-ev B, on obtient $y \in C$. Finalement $L = C$, et L est bien de type fini comme A-algèbre.

Exercice 10 — Lemme de Zariski. Cet exercice utilise les exercices 8 et 9. Soient $k \subset K$ deux corps, tels que K soit une k-algèbre de type fini. Le but de l'exercice est de montrer que K est un k-espace vectoriel de dimension finie. Pour cela on écrit $K = k[\alpha_1, \ldots, \alpha_n]$, et on raisonne par récurrence en supposant le résultat vrai jusqu'à $n-1$, le cas $n = 0$ étant trivial.

1. On pose[30] $L = k(\alpha_1)$. Comparer K et $L[\alpha_2, \ldots, \alpha_n]$, et en déduire que K est de dimension finie sur L.
2. En utilisant l'exercice 9, montrer que L est une k-algèbre de type fini.
3. En utilisant l'exercice 8, montrer que α_1 est racine d'un polynôme unitaire de $k[X]$, puis que L est de dimension finie sur k.
4. En déduire le résultat annoncé.

Solution.

30. C'est le corps des fractions de $k[\alpha_1]$.

1. Comme K est un corps, il contient $k(\alpha_1)$, et donc aussi $L[\alpha_2, \dots, \alpha_n]$. Comme par hypothèse $K = k[\alpha_1, \dots, \alpha_n]$, on a finalement $K = L[\alpha_2, \dots, \alpha_n]$, et l'hypothèse de récurrence donne alors que K (qui est donc une L-algèbre de type fini) est un L-ev de dimension finie.
2. Il suffit d'appliquer le résultat de l'exercice 8 avec $A = k$, $L = L$ et $B = K$.
3. Si α_1 n'est pas racine d'un polynôme non nul de $k[X]$, alors le morphisme de k-algèbre de $k[X]$ dans $k[\alpha_1]$ qui envoie X sur α_1 est injectif, donc $k[\alpha_1]$ est isomorphe à $k[X]$ et son corps des fractions L à $k(X)$. Ceci est impossible d'après l'exercice 3 puisque d'après **2.**, L est une k-algèbre de type fini. Si P est un polynôme unitaire de degré d qui annule α_1, on a alors que $k[\alpha_1] = k(\alpha_1) = \mathrm{Vect}_k(1, \alpha_1, \dots, \alpha_1^{d-1})$ est de dimension finie sur k.
4. D'après **3.**, L est de dimension finie sur k et d'après **1.**, K est de dimension finie sur L. Donc, K est de dimension finie sur k.

Exercice 11 — Théorème des zéros de Hilbert. Cet exercice utilise le résultat de l'exercice 10. Soit k un corps.

1. Soient $a_1, \dots, a_n$ dans k. Montrer que le morphisme $u : P \mapsto P(a_1, \dots, a_n)$ de $k[X_1, \dots, X_n]$ dans k est surjectif de noyau l'idéal $J = \langle X_1 - a_1, \dots, X_n - a_n \rangle$.

   On suppose dans la suite que k est algébriquement clos et on se donne I un idéal maximal de $k[X_1, \dots, X_n]$.
2. Montrer que le corps $L = k[X_1, \dots, X_n]/I$ est isomorphe (en tant que k-algèbre) à k.
   Indication : On appliquera le résultat principal de l'exercice 12.
3. En déduire qu'il existe $a_1, \dots, a_n$ dans k tel que I soit l'idéal J du **1.**, c'est-à-dire que I est l'ensemble des polynômes $P \in k[X_1, \dots, X_n]$ tels que $P(a_1, \dots, a_n) = 0$.

Solution.

1. Le morphisme u est surjectif (prendre P constant). Si maintenant $P \in k[X_1, \dots, X_n]$, on peut faire la division euclidienne de P par $(X_1 - a_1)$ dans l'anneau $(k[X_2, \dots, X_n])[X_1]$, ce qui permet d'écrire $P = Q_1(X_1 - a_1) + R$ avec $R \in k[X_2, \dots, X_n]$. Par récurrence, on peut écrire $P = Q_1(X_1 - a_1) + \cdots + Q_n(X_n - a_n) + b$ avec $b \in k$, après quoi le résultat est évident.
2. Par définition L est une k-algèbre de type fini, donc d'après l'exercice 10 il est de dimension finie sur k. Mais k est algébriquement clos, donc comme tout élément x de L annule un polynôme unitaire à coefficients dans k (vu que $(x^n)_{n \in \mathbf{N}}$ est liée dans le k-ev L), on obtient $x \in k$. Finalement L est isomorphe à k.
3. On vient de voir que le morphisme canonique $k \to k[X_1, \dots, X_n]/I$ est un isomorphisme. Soient $a_1, \dots, a_n$ les antécédents de $X_1, \dots, X_n$, alors par définition les polynômes $(X_i - a_i)$ sont dans I, donc I contient l'idéal J engendré par les $(X_i - a_i)$. Or J est aussi un idéal maximal car d'après a), $k[X_1, \dots, X_n]/J$ est un corps (isomorphe à k). Finalement $I = J$.

Exercice 12. Montrer que les polynômes suivants sont irréductibles.

1. Pour $n > 0$ et p premier, $X^n - p$ sur $\mathbf{Q}$;
2. $X^4 + X + 1$ sur $\mathbf{Q}$;
3. $X^6 + X^2 + 1$ sur $\mathbf{Q}$;
4. Pour $n > 0$, $X^n - T$ sur $K(T)$ (K un corps);
5. $1 + X + \cdots + X^{p-1}$ sur $\mathbf{Q}$, pour p premier.

Solution.

1. On applique le critère d'Eisenstein avec p.
2. On commence par montrer que l'on n'a pas de racine dans $\mathbf{Q}$ car une telle racine $\frac{p}{q}$ vérifierait $q = \pm 1$ et $p = \pm 1$ mais ni 1 ni -1 n'est racine. On raisonne alors par l'absurde et on voit qu'on n'a aucune factorisation du type $(X^2 + aX + b)(X^2 + cX + d)$.
   Une autre preuve est fournie dans le Perrin page 78. On pouvait aussi réduire modulo 2 et vérifier qu'il n'y a pas de racine et que le seul polynôme irréductible de degré 2 unitaire sur $\mathbf{F}_2$ est $X^2 + X + 1$. Ainsi, si $X^4 + X + 1$ n'est pas irréductible, il est égal à
   $$(X^2 + X + 1)^2 = X^4 + X^2 + 1$$
   ce qui est absurde !
3. Plusieurs méthodes sont possibles. Attention que le fait que $X^3 + X + 1$ soit irréductible sur $\mathbf{Q}$ (car sans racine et de degré $\leqslant 3$) implique que $X^6 + X^2 + 1$ est sans racine rationnelle mais pas qu'il est irréductible [31]. On peut alors raisonner par l'absurde et montrer qu'on n'a aucune factorisation du type $(X^2 + aX + b)(X^4 + cX^3 + dX^2 + eX + f)$ (ce qui implique en particulier l'abscence de factorisation comme un produit de trois polynômes de degré 2) ni de la forme $(X^3 + aX^2 + bX + d)(X^3 + eX^2 + fX + g)$ mais c'est un peu fastidieux.
   On pouvait sinon raisonner modulo certains nombres premiers. On voit tout de suite que $X^6 + X^2 + 1 = (X^3 + X + 1)^2$ dans $\mathbf{F}_2$ et

31. Par exemple, $X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$ est réductible mais $X^2 + 4$ est irréductible.

on vérifie que X^3+X+1 y est irréductible (car de degré 3 sans racine). Ceci nous fournit[32] que X^6+X^2+1 est soit irréductible sur $\mathbf{Q}$ soit est un produit de deux polynômes de degré 3. Mais, on vérifie que dans $\mathbf{F}_3$ on a deux racines (à savoir ± 1) si bien que $X^6+X^2+1=(X-1)(X+1)Q$ avec Q de degré 4 sans racine[33] dans $\mathbf{F}_3$. Cela implique que X^6+X^2+1 est irréductible. En effet, on a vu modulo 2 que soit P est irréductible soit il est produit de deux irréductibles de degré 3. Mais la réduction modulo 3 de P s'écrirait alors comme un produit de deux polynômes de degré 3. La seule possibilité pour obtenir une décomposition de la forme $(X-1)(X+1)Q$ avec Q de degré 4 sans racine est que chaque polynôme de degré 3 se scinde en un polynôme de degré 1 fois un polynôme irréductible de degré 2 et cela impliquerait en particulier que $Q=X^4+X^2+2$ est produit de deux polynômes irréductibles unitaires de degré 2 sur $\mathbf{F}_3[X]$. Mais un polynôme unitaire de degré 2 irréductible sur $\mathbf{F}_3[X]$ est de la forme X^2+aX+b sans racine. Notamment cela impose $b\neq 0$. Testant alors toutes les combinaisons possibles de $a,b\in\mathbf{F}_3$, on constate que les seuls polynômes irréductibles unitaires de degré 2 sur $\mathbf{F}_3[X]$ sont X^2+1, X^2+X-1 et X^2-X-1. On vérifie alors qu'aucun produit de deux de ces polynômes de fournit Q. On en conclut que P n'est pas produit de deux irréductibles de degré 3 et que par conséquent P est irréductible[34].

►**Remarque.–** On a notamment que s'il existe p premier tel que $\overline{P}$ soit irréductible modulo p, alors P est irréductible sur $\mathbf{Q}$. Attention en revanche qu'un tel p n'existe pas toujours (on verra notamment que X^4+1 est irréductible sur $\mathbf{Z}$ mais réductible modulo tout premier p. cela a à voir encore une fois avec le groupe de Galois de P (voir par exemple le Théorème 4.13 ici). Vous pourrez trouver des compléments dans le chapitre 4 du cours ou en section III.3 du Perrin.
Terminons par mentionner que factoriser un polynôme sur un corps fini se fait très bien algorithmiquement via l'algorithme de Berlekamp et que cet algorithme et des réductions modulo des nombres premiers bien choisis (grâce aux bornes de Mignotte) permet d'obtenir un algorithme de factorisation sur $\mathbf{Z}$. Rendez-vous lors du cours de calcul formel du semestre prochain si ces thématiques vous intéressent!

4. L'élément T est irréductible dans l'anneau factoriel $K[T]$ et on peut lui appliquer le critère d'Eisenstein (comme en **1.**) qui fournit l'irréductibilité dans $K[T][X]$ et comme le polynôme est primitif, dans $K(T)[X]$.

5. On remarque qu'il s'agit du polynôme cyclotomique[35] Φ_p. On constate que $(X-1)\Phi_p=X^p-1$ et en évaluant en $X+1$, il vient que $X\Phi_p(X+1)=(X+1)^p-1$, autrement dit

$$\Phi_p(X+1)=X^{p-1}+\sum_{k=1}^{p-2}C_{k+1}^p X^k+p.$$

On remarque alors que[36] $p\mid C_{k+1}^p$ pour tout $k\in\{1,\dots,p-2\}$ et on peut alors déduire d'Eisenstein appliqué à p que le polynôme $\Phi_p(X+1)$ est irréductible, ce qui implique que Φ_p est irréductible lui-même[37].

Exercices complémentaires de la semaine 2

Exercice 13 — Anneau local. Un anneau est dit *local* s'il n'admet qu'un seul idéal maximal.

32. En effet, $P=X^6+X^2+1$ est primitif et si on écrit sa factorisation en produit d'irréductibles dans l'anneau factoriel $\mathbf{Z}[X]$, alors on obtient des polynômes irréductibles de $\mathbf{Z}[X]$ de degré $\geqslant 1$ donc primitifs et irréductibles sur $\mathbf{Q}[X]$. Par unicité (aux unités près) d'une telle décomposition, on peut donc supposer que la décomposition de P en produit d'irréductibles est de la forme

$$P=\prod_{i=1}^{r}P_i^{n_i}$$

avec les P_i des polynômes irréductibles de $\mathbf{Z}[X]$ unitaires non constants et 2 à deux non associés. Soit alors p un nombre premier et $\overline{P}$ le polynôme obtenu en réduisant modulo p les coefficients de P. On a (c'est un morphisme d'algèbres) que

$$\overline{P}=\prod_{i=1}^{r}\overline{P_i}^{n_i}=(X^3+X+1)^2.$$

Puisque les P_i sont unitaires, $\overline{P_i}$ a même degré que P_i. Si on avait un P_i irréductible de degré 2 dans la décomposition de P, alors on obtiendrait un facteur $\overline{P}_i$ de degré 2 qui est soit irréductible soit produit de deux polynômes irréductibles de degré 1, ce qui est exclu car on a un seul facteur irréductible de degré 3 de multiplicité 2. De même, si on avait un P_i de degré 1, alors on aurait une racine modulo p, ce qui n'est pas le cas. Les seuls types de factorisation possibles sont donc P irréductible ou P produit de deux polynômes irréductibles de degré 3.

33. Ici, on obtient le sans racine soit en utilisant que $Q=X^4+X^2+2$ soit en utilisant le fait que sur un corps, x est racine multiple si, et seulement si, $P(x)=P'(x)=0$ (même en caractéristique >0). En effet, si $P=(X-x)^2Q$, il est clair que $P(x)=P'(x)=0$. Réciproquement (noter qu'en revanche la démonstration habituelle à base de formule de Taylor ne fonctionne plus), mais le fait que $P(x)=0$ implique que $P=(X-x)Q$ et donc $P'=(X-x)Q'+Q$ et on voit que $P'(x)=0$ équivaut à $Q(x)=0$ et donc au fait que x soit racine multiple. Attention en revanche que du fait que la dérivée de X^p est nulle en caractéristique p que l'équivalence x est de multiplicité m si, et seulement si, $P(x)=P'(x)=\cdots=P^{(m-1)}(x)=0$ et $P^{(m)}(x)\neq 0$ tombe en défaut! En revanche, on peut établir que cela reste toutefois vrai si $m\leqslant p-1$.

34. On verra que les types de factorisation qui apparaissent modulo p et que l'on a utilisés ici sont liés aux groupes de Galois des polynômes!

35. On reviendra en détails sur ces polynômes importants dans le chapitre sur les corps. Ils sont par exemple à la base d'une démonstration d'une version faible du théorème de la progression arithmétique de Dirichlet stipulant qu'il existe une infinité de nombres premiers $p\equiv 1\pmod n$ pour tout entier naturel n ou du théorème de Wedderburn stipulant que tout corps fini est commutatif.

36. Car pour $k\in\{1,\dots,p-2\}$, $p\mid (k+1)!C_{k+1}^p=p(p-1)\cdots(p-k)$ et $(k+1)!$ est premier à p.

37. Sinon, on a $\Phi_p=Q_1Q_2$ avec Q_1 et Q_2 non constants si bien que $\Phi_p(X+1)=Q_1(X+1)Q_2(X+1)$ avec $Q_1(X+1)$ et $Q_2(X+1)$ non constants, ce qui est absurde.

1. Montrer que A est local si, et seulement si, l'ensemble de ses éléments non inversibles est un idéal et que, dans ce cas, cet idéal est l'unique idéal maximal.
2. Montrer que A est local si, et seulement si, pour tout élément $x \in A$, $1-x$ ou x est inversible.
3. Un élément $x \in A$ est dit *idempotent* si $x^2 = x$. Montrer que si A est un anneau local, alors ses seuls idempotents sont 0 et 1. Donner un exemple d'anneau pour lequel la réciproque est fausse.
4. Soit k un corps et $n > 0$ un entier. Montrer que $k[X]/(X^n)$ est un anneau local et donner son idéal maximal.
5. Soit p un nombre premier, montrer que la localisation $\mathbf{Z}_{(p)}$ par rapport à l'idéal premier (p) est un anneau local et donner son idéal maximal.

Solution.
On rappelle qu'on a établi en TD que

$$A \smallsetminus A^\times = \bigcup_{\substack{\mathfrak{M} \subsetneq A \\ \text{maximal}}} \mathfrak{M}.$$

L'inclusion de droite à gauche est clair car tout idéal maximal est propre et l'autre inclusion découle du théorème de Krull.

1. Notons $I = \{x \in A \,|\, x \notin A^\times\}$. Supposons que c'est un idéal. Soit $\mathfrak{M}$ un idéal maximal de A. Alors pour tout $y \in \mathfrak{M}$, $y \notin A^\times$ car sinon $\mathfrak{M} = A$, donc $\mathfrak{M} \subset I$ et $I = \mathfrak{M}$ par maximalité. Ainsi A est bien local.
   Réciproquement, supposons A local et montrons que I est un idéal. Soit $\mathfrak{M}$ l'unique idéal maximal de A, on a alors

   $$A \smallsetminus A^\times = \bigcup_{\substack{\mathfrak{M} \subsetneq A \\ \text{maximal}}} \mathfrak{M} = \mathfrak{M}$$

   puisqu'on a un unique idéal maximal et on a le résultat !
2. Supposons A local et supposons $x \notin A^\times$; alors $x \in I = A \backslash A^\times$ qui est un idéal. Si $1-x \in I$, alors $1 = 1-x+x \in I$ mais $1 \in A^\times$; donc $1-x \notin I$ et donc $1-x \in A^\times$. De même, si $1-x \notin A^\times$ alors $1-x \in I$ et si $x \in I$ alors $1 \in I$, donc $x \notin I$ et $x \in A^\times$.
   Réciproquement, supposons pour tout $x \in A$, $x \in A^\times$ ou $1-x \in A^\times$. Soit $\mathfrak{M}$ un idéal maximal de A et soit $y \in A \backslash \mathfrak{M}$ alors $(y, \mathfrak{M}) = A$ et il existe $a \in A$, $m \in \mathfrak{M}$ tels que $1 = ay + m$ donc $ay = 1 - m \in A^\times$ car $m \in \mathfrak{M} \neq A$ donc $m \in A^\times$. On a donc montré que (y) contenait un élément inversible, donc $(y) = A$. On a alors que $y \in A^\times$. On a montré que $A \backslash \mathfrak{M} \subseteq A^\times$ donc[38] $A \backslash A^\times = \mathfrak{M}$ est un idéal et donc A est local.
3. Soit $x \in A$ tel que $x^2 = x$, alors $x^2 - x = x(x-1) = 0$ et x et $x-1$ sont des diviseurs de zéro. Comme A est local on a que : soit $x \in A^\times$ et dans ce cas $x = 1$, soit $x - 1 \in A^\times$ et dans ce cas $x = 0$.
   Si $A = \mathbf{Z}$ alors il est intègre donc si $x^2 = x$ on a que $x = 1$ ou $x = 0$, donc les seuls idempotents sont 1 et 0 mais $\mathbf{Z}$ n'est pas local car pour tout nombre premier p, l'idéal $p\mathbf{Z}$ est maximal.
4. Les idéaux de $k[x]/(x^n)$ sont en bijection avec les idéaux de $k[x]$ qui contiennent (x^n) ; comme $k[x]$ est principal, ils sont engendrés par un $P \in k[x]$ tel que $(x^n) \subseteq (P)$, c'est-à-dire tels que P divise (x^n), ce qui implique que $P = x^k$ avec $k \leqslant n$. Le seul idéal maximal est alors (x) car pour tout $k \leqslant n-1$, on a

   $$(x^n) \subseteq (x^{n-1}) \subseteq \cdots \subseteq (x^k) \subseteq \cdots \subseteq (x)$$

   .

   On pose $A = k[x]/(x^n)$. On pouvait aussi montrer que

   $$A^\times = \{\pi(P) \ : P(0) \neq 0 \ \} = A \smallsetminus (x)$$

   pour $\pi : K[X] \to A$ la surjection canonique. En effet, un tel polynôme est premier avec x^n et par Bézout dans $k[X]$ (qui est principal !), on dispose de $u, v \in A$ tels que $1 = uP + x^n v$ donc en prenant l'image par π, il vient $1 = \pi(P)\pi(u)$ et $\pi(P)$ est inversible ! Réciproquement, si $\pi(P)$ est inversible, on dispose de $\pi(u)$ tel que $1 = \pi(P)\pi(u)$ soit $\pi(1 - Pu) = 0$ donc $x^n \mid 1 - Pu$ et donc il existe $v \in A$ tel que $1 = Pu + x^n v$ et en évaluant en 0, $1 = P(0)u(0)$ et $P(0) \neq 0$.
5. Pour rappel, $\mathbf{Z}_{(p)} = S^{-1}\mathbf{Z}$ où $S = A \backslash (p)$ qui est une partie multiplicative de $\mathbf{Z}$. On a déjà montré que l'idéal engendré par l'image de (p) était le seul idéal maximal de $\mathbf{Z}_{(p)}$ dans l'exercice 2 !

► **Complément.–** L'ensemble des *germes de fonctions continues en* 0 est l'ensemble des classes d'équivalences de couples (f, U) avec U un intervalle ouvert de $\mathbf{R}$ contenant 0 et $f : U \to \mathbf{R}$ continue, pour la relation d'équivalence définie par $(f, U) \sim (g, V)$ si, et seulement si, il existe un ouvert $W \subseteq U \cap V$ contenant 0 tel que $f_{|W} = g_{|W}$. On vérifie facilement que $G = \{(f, U)\}/\sim$ l'ensemble des germes de fonctions continues en zéro est un anneau pour $(f, U) + (g, V) = (f + g, U \cap V)$, $(f, U).(g, V) = (f.g, U \cap V)$ (l'élément neutre pour + est la fonction nulle définie sur n'importe quel ouvert U, elles sont toutes équivalentes, l'identité est la fonction identité sur $\mathbb{R}$ définie partout. Si $f(0) \neq 0$ alors f est inversible au voisinage de 0 donc sa classe est inversible dans G. Si $f(0) = 0$ alors $(1 - f)(0) \neq 0$ et donc est inversible au voisinage de 0, sa classe est donc inversible dans G. l s'agit donc d'un anneau local et c'est cet anneau qui rend compte du comportement local d'une fonction en un point qui a donné lieu à cette terminologie d'*anneau local*.

38. Car l'inclusion réciproque est immédiate car $\mathfrak{M} \neq A$.

Exercice 14. Soit $Q \in \mathbf{Z}[X]$ unitaire. On note $z_1, \ldots, z_n$ ses racines (pas forcément distinctes) dans $\mathbf{C}$. Montrer que

$$\prod_{i \neq j} (z_i - z_j) \in \mathbf{Z}.$$

Solution. On observe que le polynôme en n indéterminées

$$P = \prod_{i \neq j} (X_i - X_j)$$

est un polynôme symétrique de $\mathbf{Z}[X_1, \ldots, X_n]$; en effet, il est clairement invariant pour l'action de toute transposition, et les transpositions engendrent $\mathfrak{S}_n$. D'après le théorème de structure, il existe $R \in \mathbf{Z}[X_1, \ldots, X_n]$ tel que

$$P = R(\sigma_1, \ldots, \sigma_n),$$

où les σ_i sont les polynômes symétriques élèmentaires. D'autre part, on a

$$Q = \prod_{i=1}^{n} (z - z_i) = z^n - \sigma_1(z_1, \ldots, z_n) z^{n-1} + \cdots + (-1)^n \sigma_n(z_1, \ldots, z_n),$$

ce qui montre que chaque $\sigma_i(z_1, \ldots, z_n)$ est entier. Du coup,

$$P(z_1, \ldots, z_n) = R(\sigma_1(z_1, \ldots, z_n), \ldots, \sigma_n(z_1, \ldots, z_n))$$

est bien entier comme on voulait.