ENS Lyon
Algèbre 2 **1er mars 2022**
Examen partiel

Notes de cours autorisées, pas d'autre document.

Exercice 1.— Pour quelles valeurs de n l'anneau $\mathbb{F}_2[X]/(X^n-1)$ est-il intègre?

Solution de l'exercice 1.— L'anneau est intègre s'il n'a pas de diviseur de 0. Or on a $X^n-1=(X-1)(X^{n-1}+X^{n-2}+\cdots+X+1)$. Donc pour $n>1$, $X-1$ est un diviseur de 0, et donc l'anneau n'est pas intègre. Pour $n=1$, on a $\mathbb{F}_2[X]/(X-1)\simeq\mathbb{F}_2$, qui est intègre.

Exercice 2.— Un anneau est *artinien* si toute suite décroissante d'idéaux $I_1\supseteq I_2\supseteq\dots$ est stationnaire : il existe un entier m tel que $I_m=I_{m+1}=\dots$.

1. Donner un exemple d'anneau artinien.
2. Donner un exemple d'anneau noethérien non artinien.
3. Montrer qu'un anneau artinien et intègre est un corps.
4. Montrer que si A est artinien et I un idéal de A, alors A/I est artinien.
5. Montrer que si A est un anneau artinien, alors tout idéal premier de A est maximal.

Solution de l'exercice 2.—

1. Un anneau fini n'a qu'un nombre fini d'idéaux, donc il est artinien. N'importe quel $\mathbb{Z}/n\mathbb{Z}$ marche donc.
2. L'anneau $\mathbb{Z}$ est noethérien, puisque principal (puisqu'euclidien). En revanche il n'est pas artinien puisque la suite $(2)\supseteq(2^2)\supseteq(2^3)\supseteq\dots$ est décroissante non stationnaire.
3. Soit A un anneau artinien intègre et soit x un élément non nul de A. On considère la suite $(x)\supseteq(x^2)\supseteq(x^3)\supseteq\dots$. Comme A est artinien, elle est stationnaire, donc il existe n tel que $(x^n)=(x^{n+1})$. En particulier $x^n\in(x^{n+1})$, donc il existe $y\in A$ tel que $x^n=yx^{n+1}$. Par intégrité on a alors $1=yx$, donc x est inversible.
4. Notons $\pi:A\to A/I$ la projection canonique. Soit $J_1\supseteq J_2\supseteq\dots$ une suite d'idéaux de A/I. Alors $\pi^{-1}(J_1)\supseteq\pi^{-1}(J_2)\supseteq\dots$ est une suite décroissante d'idéaux de A. Par artinianité, elle est stationnaire, donc il existe m tel que $\pi^{-1}(J_m)=\pi^{-1}(J_{m+1})=\dots$. On a alors $J_m=J_{m+1}=\dots$.
5. Soit I un idéal premier de A. Alors A/I est intègre (par le cours) et artinien (par la question précédente). Par la question 3, c'est un corps. Donc I est maximal (par le cours).

Exercice 3.— Soit d un nombre entier positif qui n'est pas un carré. On travaille dans l'anneau $\mathbb{Z}[\sqrt{d}]$.

1. Montrer que $\mathbb{Z}[\sqrt{d}]$ est noethérien.

   On considère l'application $\tau:\mathbb{Z}[\sqrt{d}]\to\mathbb{Z}[\sqrt{d}]$ définie pour $a,b\in\mathbb{Z}$ par $\tau(a+b\sqrt{d})=a-b\sqrt{d}$. On admet que c'est un automorphisme d'anneau. On définit l'application $N_d:\mathbb{Z}[\sqrt{d}]\to\mathbb{N}$ par $N_d(x)=x\cdot\tau(x)$.

2. Montrer que N_d vérifie d'une part $N_d(xy) = N_d(x)N_d(y)$, et d'autre part $N_d(x) = 0 \iff x = 0$.

3. Montrer qu'un élément $x \in \mathbb{Z}[\sqrt{d}]$ est une unité si et seulement si on a $N_d(x) = \pm 1$.

   Désormais on se place dans le cas $d = 2$.

4. Montrer que tous les nombres de la forme $(1+\sqrt{2})^n$, avec n entier, sont des unités de $\mathbb{Z}[\sqrt{2}]$.

5. Montrer qu'il n'y a aucune unité de $\mathbb{Z}[\sqrt{2}]$ dans l'intervalle réel $]1, 1 + \sqrt{2}[$.

6. En déduire l'ensemble des unités de $\mathbb{Z}[\sqrt{2}]$.

Solution de l'exercice 3.—

1. Comme $\mathbb{Z}$ est noethérien, par le théorème de transfert de Hilbert, $\mathbb{Z}[X]$ l'est. Donc $\mathbb{Z}[X]/(X^2 - d)$ aussi. Or $\mathbb{Z}[\sqrt{d}] \simeq \mathbb{Z}[X]/(X^2 - d)$.

2. L'application N_d est multiplicative puisque τ est un morphisme multiplicatif.

   D'autre part si $x = a + b\sqrt{d}$, on a $N_d(x) = 0 \iff a^2 - b^2 d = 0$. Comme d est n'est pas un carré, cette condition est équivalente à $a = 0$ et $b = 0$.

3. Si x est inversible, on a $1 = N_d(1) = N_d(x)N_d(x^{-1})$, donc $N_d(x)$ est un inversible de $\mathbb{Z}$, donc $N_d(x) = \pm 1$.

   Réciproquement si on a $N_d(x) = \pm 1$, alors on a $x \cdot \pm\tau(x) = \pm \pm 1 = 1$ pour un bon choix de signe, donc x admet $\pm\tau(x)$ pour inverse.

4. On a $N_2(1 + \sqrt{2}) = 1$, donc $1 + \sqrt{2}$ est une unité. Or les unités forment un groupe pour la multiplication, donc tous les $(1 + \sqrt{2})^n$ sont des unités.

5. Si $\mathbb{Z}[\sqrt{2}]$ compte une unité $a+b\sqrt{2}$ entre 1 et $1+\sqrt{2}$, alors son inverse est entre $(1+\sqrt{2})^{-1} = -1 + \sqrt{2}$ et 1. Or cet inverse est $a - b\sqrt{2}$ ou $-a + b\sqrt{2}$.

   Dans le premier cas, on trouve $1+(-1+\sqrt{2}) < (a+b\sqrt{2})+(a-b\sqrt{2}) = 2a < (1+\sqrt{2})+1$, d'où $0 < 2a < 4$, et donc $a = 1$, puis $b = 0$ ou 1, ce qui redonne 1 ou $1 + \sqrt{2}$.

   Dans le second cas, on trouve $1+(-1+\sqrt{2}) < (a+b\sqrt{2})+(-a+b\sqrt{2}) = 2b\sqrt{2} < (1+\sqrt{2})+1$, d'où $0 < 2b\sqrt{2} < 4\sqrt{2}$, donc $b = 1$, puis $a = 1$.

   On ne trouve aucune nouvelle unité entre 1 et $1 + \sqrt{2}$.

6. Montrons que l'ensemble des unités strictement supérieures à 1 est l'ensemble $\{(1+\sqrt{2})^n; n \in \mathbb{N}\}$.

   Supposons l'existence d'une unité $a + b\sqrt{2}$ supérieure à 1 pas dans cet ensemble. Alors il existe n tel que $(1 + \sqrt{2})^n < a + b\sqrt{2} < (1 + \sqrt{2})^{n+1}$. Alors le quotient $\frac{a+b\sqrt{2}}{(1+\sqrt{2})^n}$ est une unité, et elle est entre 1 et $1 + \sqrt{2}$, ce qui contredit la question précédente.

   Alors l'ensemble des unités entre 0 et 1 est l'ensemble des inverses des unités précédentes, c'est-à-dire l'ensemble $\{(-1 + \sqrt{2})^n; n \in \mathbb{N}\}$.

   Enfin, pour les négatifs, un raisonnement analogue à la question 6 montre que s'il existe une unité qui est un réel négatif, il en existe une qui satisfait $(a + b\sqrt{2})^2 = (1 + \sqrt{2})$ ou $(1 + \sqrt{2})^2$. Or $1 + \sqrt{2}$ n'a pas de racine dans $\mathbb{Z}[\sqrt{2}]$, donc la plus petite (en module) unité inférieure à -1 est $-1 - \sqrt{2}$.

   En regroupant, on trouve que $\mathbb{Z}[\sqrt{2}]^\times = \{(\pm 1 \pm \sqrt{2})^n; n \in \mathbb{N}\}$.

Exercice 4.— Soit p un nombre premier différent de 2. On considère le corps $\mathbb{F}_p$ à p éléments.

1. Combien d'éléments de $\mathbb{F}_p$ sont le carré d'un élément de $\mathbb{F}_p$? Combien d'éléments de $\mathbb{F}_p$ ne sont pas des carrés?

2. Montrer que si x et y ne sont pas des carrés dans $\mathbb{F}_p$, alors xy est un carré dans $\mathbb{F}_p$. (On pourra considérer l'ensemble des carrés non nuls et en faire un groupe.)

   On fixe désormais un élément d de $\mathbb{F}_p$ qui n'est pas un carré.

3. Montrer que le quotient $\mathbb{F}_p[X]/(X^2-d)$ est un corps. Combien a-t-il d'éléments?

   Pour $P(X)$ un élément dans $\mathbb{F}_p[X]$, on note $\bar{P}(X)$ sa classe dans $\mathbb{F}_p[X]/(X^2-d)$.

4. L'élément $\bar{X}$ engendre-t-il le groupe multiplicatif $(\mathbb{F}_p[X]/(X^2-d))^\times$?

5. Soit a, b, c trois éléments de $\mathbb{F}_p$ avec $a \neq 0$. Donner (en distinguant 3 cas) la solution générale dans $\mathbb{F}_p[X]/(X^2-d)$ de l'équation $ax^2+bx+c=0$ d'inconnue x.

Solution de l'exercice 4.—

1. Notons c le nombre de carrés non nuls dans $\mathbb{F}_p$.

   Soit d un élément de $\mathbb{F}_p$. Alors l'équation x^2-d a au plus deux solutions dans $\mathbb{F}_p$. De plus si α est solution, alors $-\alpha$ aussi. Et comme p est impair, seul 0 est égal à son opposé. Donc pour tout d non nul, l'équation x^2-d a 0 ou 2 solutions. Comme tout élément non nul a un carré non nul, on a alors $2c = p-1$, donc $c = \frac{p-1}{2}$. En rajoutant 0, il y a $\frac{p+1}{2}$ carrés dans $\mathbb{F}_p$.

   Par différence, il y a donc $\frac{p-1}{2}$ éléments qui ne sont pas des carrés.

2. L'ensemble $(\mathbb{F}_p^*)^2$ des éléments qui sont des carrés non nuls forme un groupe (abélien) pour la structure multiplicative, qui est donc distingué dans $\mathbb{F}_p^*$. Le quotient $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$ est un groupe de cardinal 2. En particulier, si x et y ne sont pas des carrés, leurs classes dans $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$ sont l'élément non nul, et donc leur produit dans $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$ est nul, ce qui signifie que xy est un carré dans $\mathbb{F}_p$.

3. Si d n'est pas un carré, le polynôme X^2-d n'a pas de racine dans $\mathbb{F}_p$, donc il est irréductible. Par conséquent l'idéal de $\mathbb{F}_p[X]$ qu'il engendre est maximal, et donc $\mathbb{F}_p[X]/(X^2-d)$ est un corps. Tout élément de ce corps admet un unique représentant qui est un polynôme de degré au plus 1. Il y a p^2 tels polynômes, donc c'est un corps à p^2 éléments.

4. L'élément $\bar{X}$ engendre $(\mathbb{F}_p[X]/(X^2-d))^\times$ si et seulement si il est d'ordre $|(\mathbb{F}_p[X]/(X^2-d))^\times| = p^2-1$. Dans $\mathbb{F}_p[X]/(X^2-d)$, on a $(\bar{X})^2 = \bar{d}$. Or $\bar{d}$ est un élément de $\mathbb{F}_p$, donc son ordre (multiplicatif) divise $p-1$. Par conséquent l'ordre multiplicatif de $\bar{X}$ divise $2(p-1)$. Et comme on a $2(p-1) < p^2-1$, l'élément $\bar{X}$ n'engendre pas $(\mathbb{F}_p[X]/(X^2-d))^\times$.

5. Notons $\Delta = b^2-4ac$.

   Si Δ est nul, alors on a $a(x+\frac{b}{2a})^2 = ax^2+bx+a\frac{b^2}{4a^2} = ax^2+bx+c$, donc $-\dfrac{b}{2a} \in \mathbb{F}_p$ est racine double.

   Si Δ est un carré dans $\mathbb{F}_p$, notons δ un élément de $\mathbb{F}_p$ tel que $\delta^2 = \Delta$. Alors on a $a(x-\frac{-b+\delta}{2a})(x-\frac{-b-\delta}{2a}) = a(x+\frac{b}{2a})^2 - a(\frac{\delta}{2a})^2 = ax^2+bx+\frac{b^2}{4a} - a\frac{b^2-4ac}{4a^2} = ax^2+bx+c$, donc les racines sont $\dfrac{-b+\delta}{2a} \in \mathbb{F}_p$ et $\dfrac{-b-\delta}{2a} \in \mathbb{F}_p$.

Enfin si Δ n'est pas un carré dans $\mathbb{F}_p$, c'en est un dans $\mathbb{F}_p[X]/(X^2-d)$. En effet, $d\Delta$ est le produit de deux éléments non carrés de $\mathbb{F}_p$, donc c'est un carré dans $\mathbb{F}_p$. Donc il existe $\delta \in \mathbb{F}_p$ tel que $\delta^2 = d\Delta$, et comme $d = \bar{X}^2$, on a $\Delta = (\delta\bar{X}/d)^2$.

Alors on a

$$\begin{aligned} a(x+\frac{b}{2a}+\frac{\delta\bar{X}}{2ad})(x+\frac{b}{2a}-\frac{\delta\bar{X}}{2ad}) &= a(x+\frac{b}{2a})^2 - a(\frac{\delta\bar{X}}{2ad})^2 \\ &= ax^2+bx+\frac{b^2}{4a}-a\frac{b^2-4ac}{4a^2} \\ &= ax^2+bx+c, \end{aligned}$$

donc les racines sont $\dfrac{bd+\delta\bar{X}}{2ad}$ et $\dfrac{bd-\delta\bar{X}}{2ad}$.

Exercice 5.— Soient m et n deux entiers naturels non nuls premiers entre eux, soit K un corps et a un élément de K. Montrer que les polynômes $X^m - a$ et $X^n - a$ sont tous deux irréductibles dans $K[X]$ si et seulement si le polynôme $X^{mn} - a$ est irréductible dans $K[X]$. (On pourra travailler dans un corps de rupture de $X^{mn} - a$.)

Solution de l'exercice 5.— Si $X^m - a$ ou $X^n - a$ est réductible, alors $X^{mn} - a$ l'est aussi. L'implication difficile est donc : "Si $X^m - a$ et $X^n - a$ sont irréductibles, alors $X^{mn} - a$ l'est aussi."
Soit L un corps de rupture pour $X^{mn} - a$ et x une racine de $X^{mn} - a$ dans L. Alors x^m est une racine de $X^n - a$ et x^n est une racine de $X^m - a$.
Si $X^n - a$ est irréductible sur K, alors x^m est de degré n sur K. On a donc $[K(x^m) : K] = n$. De même on a $[K(x^n) : K] = m$. Ainsi, $[K(x) : K]$ est divisible par m et par n, donc par mn. Le degré de $P_{min,x}$ est donc supérieur ou égal à mn. Puisque x annule $X^{mn} - a$, on a $P_{min,x}(X) = X^{mn} - a$ et donc $X^{mn} - a$ est irréductible sur K.