Du cours aux exercices (Aide à la révision du cours)

Chapitre IV — Arithmétique des entiers et des polynômes

1 Autre point de vue sur l'arithmétique

1.1 Compléments sur les anneaux, algèbres

Motivation de cette partie

On étudiera plus loin, de plus près, les propriétés de $\mathbb{Z}/n\mathbb{Z}$ comme anneau, et pour parler de systèmes de congruences (trouver x tel que $x \equiv a \bmod m$ et $x \equiv b \bmod n$) nous avons besoin de mettre une structure d'anneau sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Les compléments de cette section sont à cette fin. La structure d'algèbre sera pour étudier les propriétés à la fois arithmétiques et algébriques de $K[X]$.

Proposition 1 (Le groupe $A^\times$)**.**

✓	— La démontrer. C'est facile mais il y a tout de même une subtilité rédactionnelle concernant la stabilité par inverse. — Est-ce que $A^\times$ est un sous-anneau de A ?
★	Donner une condition nécessaire pour que $A^\times = \{1\}$. Ce groupe est rarement trivial. Se demander ensuite si cette condition nécessaire est suffisante (ne pas produire une démonstration : chercher des exemples ou contre-exemples).

Définition 2 (Produit fini d'anneaux)**.**

✓	— La démontrer. Il n'y a pas de subtilité majeure. Quels sont les éléments neutres pour $+$ et $\times$? — A-t-on $(A_1 \times A_2)^\times = A_1^\times \times A_2^\times$? — Si A_1 et A_2 sont commutatifs, est-ce que $A_1 \times A_2$ l'est ? Question analogue pour l'intégrité, la structure de corps, l'existence d'éléments nilpotents, etc. Attention à ne pas conclure trop vite.

Définition 3 (Algèbre, sous-algèbre, morphisme d'algèbres)**.**

✓	Se demander pourquoi on a choisi cette terminologie.

Proposition 4 (Exemples usuels)**.**

✓	Chercher d'autres exemples de K-algèbres parmi les anneaux et espaces vectoriels usuels. En fait, ils sont presque tous des K-algèbres : mettre en valeur ceux qui n'en sont pas.
★	Si X est vide, que dire de $\mathcal{F}(X, K)$? Est-ce une K-algèbre ?

Définition 5 (Polynôme en un élément d'une algèbre)**.**

✓	Vérifier *vraiment* que l'application d'évaluation est un morphisme de K-algèbres.
★	Soit $\mathbb{H}$ l'ensemble des quaternions, dont on retiendra seulement que c'est une $\mathbb{R}$-algèbre non commutative, dont tout élément non nul est inversible (en particulier elle est intègre), et qu'elle admet une $\mathbb{R}$-base $(1, i, j, k)$ telle que : $i^2 = j^2 = k^2 = ijk = -1$ (cela suffit à entièrement déterminer $\mathbb{H}$). Trouver ce qui est faux dans le raisonnement suivant, et qui met en évidence une subtilité qui passe quasiment inaperçue dans la définition de $K[u]$ et du morphisme d'évaluation : « on a : $X^2 + 1 = (X + i)(X - i)$. En évaluant en j cette égalité, on obtient : $0 = j^2 + 1 = (j + i)(j - i)$, et comme $\mathbb{H}$ est intègre on en déduit : $i = \pm j$. ». C'est impossible puisque (i, j) est libre, donc j'ai fait une erreur : où ? Après avoir compris d'où vient l'erreur, reprendre avec soin la vérification que l'application d'évaluation est un morphisme de K-algèbres, et voir ce qui fait que tout marche dans ce contexte.

1.2 Arithmétique des idéaux

Motivation de cette partie

Euler montra qu'il était possible de faire de l'arithmétique dans d'autres anneaux que $\mathbb{Z}$ et $K[X]$, puisqu'il établit l'existence de solutions entières non nulles à l'équation de Fermat $x^3 + y^3 = z^3$ en factorisant le membre de gauche dans $\mathbb{Z}[j] = \left\{a + bj \mid (a,b) \in \mathbb{Z}^2\right\}$ et en étudiant les relations de divisibilité que cela implique. L'objectif de cette partie est de comprendre à quelle condition il est effectivement possible de faire de l'arithmétique dans un anneau A. Nous allons voir que pour correctement définir la relation de divisibilité (pour en faire une relation d'ordre), et pour permettre les raisonnements sur le « plus petit » élément à vérifier une propriété donnée, le bon cadre est celui des idéaux.

Nous allons donc reformuler les propriétés de base de l'arithmétique en termes d'idéaux. Dans le cas où les idéaux sont tous principaux, nous retrouverons tous les théorèmes d'arithmétique connus dans $\mathbb{Z}$ et $K[X]$.

Définition 6 (Divisibilité dans un anneau intègre, éléments associés)**.**

✓	On note que l'intégrité intervient déjà dans la caractérisation des éléments associés. Et la commutativité ?

Remarque.

✓	Vérifier ces affirmations sans mystère. Et si A n'est pas supposé intègre, que dire des éléments qui divisent 0_A ?
★	Dans un anneau non intègre, proposer des éléments qui sont associés sans être égaux à un élément inversible près.

Remarque.

✓	— Vérifier que c'est effectivement une relation d'équivalence. — Vérifier que la relation de divisibilité est effectivement correctement définie sur $A/A^\times$: si a divise b et si : $a \sim a'$, alors a' divise b. De même si $b \sim b'$. Ainsi, toutes les notions fondamentales de l'arithmétique sont « aux inversibles près ». — On voit que faire de l'arithmétique dans A nécessite de connaître $A^\times$. Déterminer $A^\times$ pour les anneaux usuels.
★	— Est-ce que la notation $A/A^\times$ désigne un groupe quotient ? Un anneau quotient ? — Montrer que l'application $A^\times \to S_A$ définie par $u \mapsto (\varphi_u : a \mapsto ua)$ est un morphisme de groupes. Cela équivaut à la donnée d'une action de groupe : la notation $A/A^\times$ provient de là (c'est l'ensemble des orbites de cette action, c'est-à-dire les ensembles de la forme $\left\{\varphi_u(a) \mid u \in A^\times\right\}$).

Remarque.

✓	Pourquoi tient-on absolument à avoir une relation d'ordre ? Où cela nous est-il utile, lorsqu'on fait de l'arithmétique dans $\mathbb{Z}$ ou $K[X]$ (pour prendre des exemples connus) ?

Proposition 7 (Divisibilité en termes d'idéaux)**.**

✓	— Déduire de cette proposition que multiplier un élément par un inversible ne change pas l'idéal qu'il engendre. — Vérifier la cohérence de cet énoncé avec ce que je dis plus haut : la relation de divisibilité est correctement définie sur $A/A^\times$. — Plus généralement, dans l'intégralité de cette section : vérifier que les affirmations sur les idéaux valent aussi sur les éléments de $A/A^\times$. — En quoi cette traduction de la divisibilité en termes d'idéaux permet de résoudre le problème formulé plus haut, à savoir que la relation de divisibilité n'est pas une relation d'ordre ?
★	Reformuler les commentaires ci-dessus par la donnée d'une bijection entre $A/A^\times$ et l'ensemble des idéaux principaux, vérifiant une certaine propriété de « monotonie » qui reflète les équivalences de cette proposition. Si vous avez trouvé cette bijection, vous avez trouvé une formulation succincte et savante du fait que « raisonner avec $A/A^\times$ ou des idéaux, cela revient au même en arithmétique ».

Remarque. ♡

★	— Proposer une autre démonstration. — En particulier, qu'est-ce que cela nous dit des idéaux d'un corps ? Et de l'intérêt arithmétique des corps ?

Définition 8 (Éléments irréductibles)**.**

✓	Est-ce que la notion d'irréductibilité peut être définie sur $A/A^\times$? C'est-à-dire : si a est irréductible, et si $a \sim a'$, est-ce que a' est irréductible ?
★	— Pourquoi exclure les inversibles ? Se poser éventuellement la question plus tard, après avoir vu plusieurs énoncés faisant intervenir des éléments irréductibles. — Reformuler cette définition en termes d'idéaux. — Si a est irréductible, que dire de l'anneau quotient A/aA ?

Exemple 1.

Définition 9 (Anneau principal)**.**

★	En introduisant les idéaux au chapitre III, je disais qu'ils étaient les « bons » analogues des sous-espaces vectoriels d'un espace vectoriel (quand on remplace les espaces vectoriels par des anneaux). Ayant ceci en tête, comprendre pourquoi un anneau principal est un candidat crédible à une généralisation de la théorie de la dimension : que serait la « dimension » de A sur A, si cela avait un sens ? Et par conséquent, à quoi devrait-on s'attendre, pour la « dimension » d'un idéal de A sur A ? À comparer avec cette définition.
☢	Trouver des exemples d'anneaux (non nécessairement intègres, mais on évitera tout de même le cas non commutatif) dont certains idéaux ne sont pas principaux. Penser à des anneaux de fonctions, de polynômes...

Définition-Proposition 10 (Définition des pgcd et des ppcm dans un anneau principal)**.**

✓	— Démontrer ce que j'ai omis. — Si $a \in A$ et p est irréductible, que dire d'un pgcd et d'un ppcm de p et a C'est souvent utile. — Si $a_1, \dots, a_n$ sont premiers entre eux, est-ce que pour tous $i \neq j$, les éléments a_i et a_j sont premiers entre eux ? Et réciproquement ?
★	— Après avoir démontré cette proposition : montrer que, réciproquement, si l'on définit un ppcm des a_i comme le plus petit élément (modulo $A^\times$) de l'ensemble des multiples communs des a_i (modulo $A^\times$), alors il doit nécessairement engendrer $\cap_i a_i A$? Cela permet de rendre naturelle cette définition qui semble sortir de nulle part. Même question avec les pgcd. — Pourquoi la réunion des $a_i A$ n'est pas intéressante à étudier ? — Si d et m sont un pgcd et un ppcm des $a_1, \dots, a_n$, a-t-on toujours la relation $dm = \prod_{i=1}^{n} a_i$?

☢ Si l'on n'est pas dans un anneau principal, on peut tout de même définir les pgcd et ppcm, s'ils existent, comme les grands ou plus petits éléments d'ensembles de diviseurs ou de multiples, etc. Le cas échéant :

- montrer que $a_1, \dots, a_m$ admettent un ppcm si et seulement si l'idéal $\bigcap_i a_i A$ est principal ;
- montrer qu'il est possible que $a_1, \dots, a_m$ admettent un pgcd sans pour autant qu'ils engendrent un idéal principal (chercher dans $\mathbb{R}[X, Y]$, ou $\mathbb{Z}[X]$) ;
- montrer qu'il est possible que $a_1, \dots, a_m$ admettent un pgcd si et seulement si l'ensemble des idéaux *principaux* admet un plus petit élément ;
- montrer pour tout a non nul, les a_i admettent un ppcm si et seulement si les $a \cdot a_i$ en admettent un (et donner un lien entre les deux ppcm), mais que c'est faux pour les pgcd ;
- montrer que pour tout a non nul, si les $a \cdot a_i$ admettent un pgcd, alors les a_i aussi (et donner un lien entre les deux pgcd) ;
- montrer que si x et y ont un ppcm, alors m divise xy, et que l'élément d tel que $xy = md$ est un pgcd (ainsi on a ppcm $\Rightarrow$ pgcd) ;
- montrer qu'on peut avoir un pgcd sans avoir un ppcm, mais que, s'il existe d tel que ad soit un pgcd de ax et ay pour tout $a \in A \setminus \{0\}$, alors x et y admettent un ppcm, qui est un élément m tel que $md = xy$;
- montrer que si $xA + yA$ est principal alors $xA \cap yA$ aussi ;
- montrer que toute intersection de deux idéaux principaux est principale si et seulement si tout couple d'éléments admet un ppcm, si et seulement si tout couple d'éléments admet un pgcd ; et que dans ce cas $xy = \text{pgcd}(x, y)\text{ppcm}(x, y)$ modulo $A^\times$;
- montrer que dans $\mathbb{Z}[i\sqrt{5}] = \left\{a + i\sqrt{5}b \mid (a, b) \in \mathbb{Z}^2\right\}$, les éléments 3 et $2 + i\sqrt{5}$ n'ont pas de ppcm et que 9 et $2 + i\sqrt{5}$ n'ont pas de pgcd.

Théorème 11 (Théorème de Bézout dans un anneau principal)**.**

✓
- S'il existe $u_1, \dots, u_n$ tels que : $\sum_{i=1}^{n} a_i u_i = d$, que dire de d ? (C'est très facile si on raisonne en termes d'idéaux.)
- Comparer avec la démonstration du théorème de Bézout dans $\mathbb{Z}$ et $K[X]$ avec les outils de 1re année. Lorsque, plus tard, nous aurons démontré que $\mathbb{Z}$ et $K[X]$ sont principaux : quelle démonstration du théorème de Bézout est la plus simple ? Néanmoins, j'affirme que l'autre démonstration conserve un intérêt : lequel ?

☢
- Est-ce que réciproquement, si ce théorème est vrai, alors A est principal ? (Je pense qu'il est trop tôt pour répondre à cette question : l'exemple que j'ai en tête nécessite d'avoir *a minima* vu la théorie des séries entières.)

Proposition 12 (Lemme d'Euclide et théorème de Gauß dans un anneau principal)**.**

★
- Réciproquement, montrer que le lemme d'Euclide implique le théorème de Gauß. À faire éventuellement après avoir lu le reste de la section.
- J'affirme que le théorème de Gauß dit quelque chose d'intéressant concernant les éléments inversibles et les diviseurs de zéro de A/aA. Quoi donc ? Même chose avec le lemme d'Euclide si a est irréductible.

☢ Est-ce que réciproquement, cet énoncé implique le théorème de Bézout ?

Théorème 13 (Existence, unicité de la décomposition en éléments irréductibles dans un anneau principal)**.**

✓
- Pourquoi exclut-on $a = 0$ de ce théorème ?
- Pourquoi l'élément inversible n'est-il pas uniquement défini, dans la décomposition en facteurs irréductibles d'un élément non nul ? À ce stade, comprendre pourquoi on veut qu'un élément irréductible soit non inversible.
- Revoir la démonstration de ce théorème dans le cas de $\mathbb{Z}$ et $K[X]$, afin de comprendre comment le lemme 14 permet de les imiter (faire un parallèle, étape par étape, entre les démonstrations dans $\mathbb{Z}$ et $K[X]$ et celle dans A principal). Pourquoi ne pouvait-on pas se passer de passer par des idéaux pour imiter les raisonnements de minimalité dans $\mathbb{Z}$ et $K[X]$?
- Achever la démonstration de l'unicité, si je l'ai laissée en suspens. Soit par une récurrence soignée, soit *via* le commentaire ★ plus bas.

★	— Se convaincre que l'existence, dans ce théorème, équivaut exactement à l'énoncé : « tout élément non inversible admet un diviseur irréductible ». Démontrer cet énoncé équivalent à l'aide du lemme 14 (s'inspirer de la démonstration dans $\mathbb{Z}$ et $K[X]$ si vous manquez d'idée, et l'adapter en vous souvenant de la reformulation des relations de divisibilité en termes d'idéaux). — On a utilisé le lemme 14 pour l'existence. L'utiliser également pour l'unicité, afin d'éviter la rédaction elliptique à la « et ainsi de suite » en fin de démonstration. — Observer que plus généralement, le lemme 14 permet d'imiter les raisonnements par récurrence dans des ensembles autres que $\mathbb{N}$, ainsi que les raisonnements par l'absurde utilisant un plus petit ou plus grand élément. Ce parallèle devient d'autant plus évident si l'on se souvent comment fut démontré le principe de récurrence. L'illustrer en démontrant cet énoncé : « dans un anneau principal, tout idéal est intéressant ». — On a démontré l'unicité à l'aide du lemme d'Euclide. Réciproquement, montrer que l'existence et, surtout, l'unicité de la décomposition en facteurs irréductibles impliquent le lemme d'Euclide (de sorte que, finalement : théorème de Gauß, lemme d'Euclide et unicité de la décomposition, sont trois énoncés équivalents).
☢	— On a utilisé le lemme d'Euclide pour démontrer l'unicité. Cela semble indiquer que l'existence d'une décomposition n'utilise pas ce lemme, et donc pourrait être valable hors d'un anneau principal. Pourriez-vous donner des exemples d'anneaux vérifiant l'existence de la décomposition en irréductibles, sans l'unicité ? (Chercher des exemples proches de ceux que vous connaissez.) — Il reste un résultat classique non énoncé dans un anneau principal A, et pourtant valable dans $\mathbb{Z}$ et $K[X]$: l'infinité des éléments irréductibles (quoique ceci ne soit pas totalement évident dans $K[X]$ si K est fini). Qu'en pensez-vous ? On écartera rapidement les cas triviaux (A de cardinal fini, A un corps).

Lemme 14 (Un lemme qui remplace les arguments de minimalité des entiers ou polynômes)**.**

✓	— Réviser la définition d'élément maximal, pour la distinguer du plus grand élément d'un ensemble. — Prendre des exemples simples $\mathcal{I}$ d'ensembles d'idéaux dans $\mathbb{Z}$, et décrire ses éléments maximaux, afin de vous convaincre de la justesse de cette proposition. Qu'observez-vous de remarquable ?
☢	Comparer cet énoncé au lemme de Zorn (vu en Informatique, me semble-t-il : tout ensemble inductif non vide admet un élément maximal). Est-ce que ce lemme est une conséquence directe du lemme de Krull ?

Exercice 1.

✓	Le démontrer dans les cas particuliers $\mathbb{Z}$ et $K[X]$, sans utiliser le fait qu'ils soient principaux.
★	Le faire.
☢	Est-ce que réciproquement, un anneau vérifiant cette propriété est principal ?

Proposition 15 (Caractérisation des éléments premiers entre eux)**.**

✓	— Démontrer cette proposition, si je ne l'ai pas fait. Si vous séchez : il suffit de reprendre la démonstration vue dans $\mathbb{Z}$ ou $K[X]$. — Plus généralement : reprendre TOUS les résultats d'arithmétique vus en 1re année (existence des valuations p-adiques, caractérisation de la divisibilité en termes de valuations, expression des ppcm et pgcd à l'aide de facteurs irréductibles, etc.) et qui découlent du théorème fondamental de l'arithmétique, et vérifier qu'ils se généralisent à tout anneau principal.
★	Pourquoi la dernière caractérisation (avec les diviseurs irréductibles) est très souvent préférable quand on veut montrer que des éléments sont premiers entre eux en raisonnant par l'absurde ?

Montrer qu'un anneau est principal.

✓	Réviser les démonstrations que $\mathbb{Z}$ et $K[X]$ admettent une division euclidienne. On réfléchira en particulier à la façon de définir le quotient (une fois que le quotient est correctement défini, le reste est trivial à obtenir : pourquoi ?). Cela servira d'inspiration pour tous les autres anneaux où vous voulez montrer l'existence d'une division euclidienne.

Après votre révision de cette partie

Récapituler toutes les conséquences arithmétiques de la principalité d'un idéal. Les mettre en parallèle des résultats connus dans $\mathbb{Z}$ et $K[X]$. Réviser comment vous les utilisiez dans ces deux anneaux, pour forger votre intuition dans tout anneau.

2 Arithmétique des entiers et des polynômes

2.1 Arithmétique dans $\mathbb{Z}$

Motivation de cette partie

On redémontre en seulement quelques lignes tous les résultats connus d'arithmétique dans $\mathbb{Z}$. Ce nouveau point de vue permet de prendre plus de hauteur sur ce qui fait la spécificité des entiers.

Théorème 16 ($\mathbb{Z}$ est un anneau principal)**.**

↘ III lem. 19

✓	Revoir la démonstration du lemme auquel on renvoie, et comparer à la dernière remarque de la section précédente.

Corollaire 17 (On peut faire de l'arithmétique dans $\mathbb{Z}$)**.**

✓	Comparer avec les démonstrations de ces différents résultats en 1re année. Qu'est-ce que la démonstration de cette année apporte comme plus-value ? Pourquoi, pour autant, les démonstrations de 1re année ne sont pas obsolètes ?

2.2 Structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$

Motivation de cette partie

Pour le moment, seul le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$ fut étudié. Nous passons à l'étude de $\mathbb{Z}/n\mathbb{Z}$ en tant qu'anneau, et c'est autrement plus intéressant pour l'arithmétique : en effet, l'arithmétique considère plutôt les produits que les sommes d'entiers. Lorsqu'on étudie un anneau, on s'intéresse à sa commutativité, ses inversibles, ses diviseurs de zéro, ses éléments nilpotents. Notre étude permet de recouvrir tous ces aspects, et de donner une condition nécessaire et suffisante remarquable pour que $\mathbb{Z}/n\mathbb{Z}$ soit un corps. Nous allons aussi généraliser le petit théorème de Fermat et donner un moyen de calculer l'indicatrice d'Euler.

Quand p est premier, $\mathbb{Z}/p^k\mathbb{Z}$ est considérablement plus simple à manipuler. Nous donnerons un théorème permettant de toujours s'y ramener : le théorème chinois.

Proposition 18 (Inversibles de $(\mathbb{Z}/n\mathbb{Z})^\times$)**.**

↘ III prop. 24

✓	— Démontrer cette équivalence sans recourir au résultat sur les générateurs de $\mathbb{Z}/n\mathbb{Z}$. — Démontrer cette équivalence en passant par d'autres implications, par exemple : $(iii) \Rightarrow (ii) \Rightarrow (i) \Rightarrow (iii)$. — Vérifier que $u \cdot \bar{x} = \bar{u} \cdot \bar{x}$ pour tout $u \in \mathbb{Z}$. — Est-ce que le même résultat serait vrai dans l'anneau $K[X]/PK[X]$? Pourquoi ?
★	Comment peut-on caractériser l'aspect générateur de $\bar{x}$ à l'aide de l'application $\bar{a} \mapsto \bar{a}\bar{x}$ de multiplication par $\bar{x}$? En déduire une équivalence entre : être diviseur de zéro dans $\mathbb{Z}/n\mathbb{Z}$, et : être inversible dans $\mathbb{Z}/n\mathbb{Z}$. On fait ainsi le lien entre deux propriétés que l'on n'aurait pas forcément rapprochées immédiatement, au vu de leurs définitions. On doit se poser régulièrement cette question, même hors du contexte de ce chapitre : les propriétés des applications de multiplication par un élément $x \in A$ fixé peuvent être étudiées grâce à des théorèmes sur les applications, afin d'en déduire des propriétés de x.

Exemple 2.

✓	Varier les exemples pour s'approprier la méthode. La *Banque des Cent* vous le permet aussi.
★	S'en inspirer pour calculer des inverses dans $K[X]/PK[X]$. Quand on applique la méthode à un élément $a+bi = \overline{a+bX}$ de $\mathbb{C} = \mathbb{R}[X]/(X^2+1)\mathbb{R}[X]$ (défini au chapitre III), qu'obtient-on ? À comparer avec ce que vous savez être $(a+bi)^{-1}$.

Corollaire 19 (Théorème d'Euler)**.**

↘ III th. 22

★	Et si x n'est pas premier avec n, peut-on dire quelque chose malgré tout ? Varier les exemples. Constater que le comportement « asymptotique » des puissances dépend de certaines choses (mais quoi ?). À la fin de la section, démontrer ce que vous avez constaté.

Corollaire 20 ($\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier, notation $\mathbb{F}_p$)**.**

✓	Il est possible de démontrer cette équivalence de plein de façons différentes. Les varier. Je trouve que dans la suite d'implications : $(iii) \Rightarrow (ii) \Rightarrow (i) \Rightarrow (iii)$, chaque raisonnement est très instructif.
★	— Caractériser les points (i) et (ii) à l'aide des applications $\bar{a} \mapsto \bar{a}\bar{x}$ de multiplication par un entier. Quelle équivalence remarquable démontre-t-on, reformulée ainsi ? — Montrer plus généralement que tout anneau commutatif fini et intègre est un corps. — Montrer que ces équivalences et la démonstration s'adaptent à $K[X]/PK[X]$, avec P polynôme non nul : c'est un corps (et un anneau intègre) si et seulement si P est irréductible. Même si cet anneau quotient n'est jamais étudié dans le programme de classes préparatoires, c'est probablement l'anneau quotient le plus riche et instructif qui soit (autant voire plus que $\mathbb{Z}/n\mathbb{Z}$). Il permet notamment de bien comprendre les anneaux de la forme $K[u]$ avec u élément d'une algèbre, *via* le théorème d'isomorphisme (voir plus loin la définition du polynôme minimal pour approfondir ce commentaire). Vous gagnerez donc en recul si vous l'étudiez systématiquement lorsque j'en fais la mention. — Montrer que ces équivalences et la démonstration s'adaptent à A/aA avec A principal et $a \in A \setminus (\{0\} \cup A^\times)$.
☢	Connaissez-vous d'autres corps finis que $\mathbb{Z}/p\mathbb{Z}$ pour p premier ?

Remarque.

✓	— Comparer avec la démonstration « antique » du petit théorème de Fermat. Selon votre façon de le démontrer en 1re année (soit par un calcul de $\prod_{i=1}^{n-1} i \bmod n$ de deux manières différentes *via* une bijection, soit avec une récurrence et la formule du binôme de Newton), la démonstration de 2e année n'en est qu'une bête reformulation : le remarquer. — On sait que le théorème de Fermat peut se reformuler : $\forall x \in \mathbb{Z}$, $x^n \equiv x \bmod n$ (pour n premier), ce qui a l'avantage de ne pas nécessiter d'hypothèse sur x. J'affirme pourtant que l'égalité $x^{n-1} \equiv 1 \bmod n$, pour x premier avec n, est préférable, par exemple en vue de simplifier des puissances de x arbitrairement grandes. Pourquoi ?
★	Si n n'est pas premier, peut-on proposer un énoncé du théorème d'Euler pour tout $x \in \mathbb{Z}$, sans hypothèse sur x ?

Théorème 21 (Théorème chinois)**.**

✓	— Pour n entier naturel non nul quelconque, qu'est-ce que cet énoncé nous dit que $\mathbb{Z}/n\mathbb{Z}$? — Faire une liste de toutes les propriétés qui vous viennent en tête, qui sont vérifiées par $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ ou $\mathbb{Z}/p_i\mathbb{Z}$ pour p_i premier, et qui ne sont pas vérifiées par $\mathbb{Z}/n\mathbb{Z}$ en général. Comprendre pourquoi l'intérêt de cet énoncé est de pouvoir s'y ramener. Se poser la question plus tard éventuellement. — Vérifier que si m_1 et m_2 sont premiers entre eux, alors effectivement : $\mathrm{ppcm}(m_1, m_2) = m_1 m_2$. C'est la clé du raisonnement ! — Pour la récurrence : vérifier que si $m_1, \dots, m_r$ sont premiers entre eux dans leur ensemble, et non deux à deux, alors $m_1 \cdots m_{r-1}$ et m_r ne sont pas forcément premiers entre eux. Vérifier que sous l'hypothèse plus forte de l'énoncé, c'est vrai (je n'ai pas détaillé ce point).

★	— Le théorème de factorisation des morphismes devrait plutôt impliquer que $\Phi : \mathbb{Z}^2/(m_1\mathbb{Z} \times m_2\mathbb{Z}) \to \mathbb{Z}/m_1m_2\mathbb{Z}$ est bien définie, pourtant ce n'est pas ce que j'ai écrit. Se convaincre que l'anneau de départ donne bien la même chose que $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$. — On a montré la surjectivité par un argument sur les cardinaux. Pouvait-on la démontrer directement sans cela ? — Réciproquement, si m et n ne sont pas premiers entre eux, comparer $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. — On peut démontrer par des moyens élémentaires que si m et n sont premiers entre eux, alors $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est cyclique, engendré par (1,1), et est donc isomorphe à $\mathbb{Z}/mn\mathbb{Z}$. J'affirme cependant que cet énoncé en dit bien davantage. Pourquoi ? — Déduire de cet énoncé quelques conséquences de base sur l'intégrité, les éléments nilpotents, les diviseurs de zéro, etc. (la seule limite est votre imagination), de $\mathbb{Z}/n\mathbb{Z}$ en fonction de ses diviseurs premiers. — Montrer que le théorème chinois a une version dans $K[X]$: si P_1 et P_2 sont premiers entre eux, alors $K[X]/P_1P_2K[X]$ est isomorphe à $K[X]/P_1K[X] \times K[X]/P_2K[X]$, de même avec r polynômes P_i. En particulier, pour $P_i = X - a_i$, j'affirme que l'existence et l'unicité d'un antécédent de $(b_1 \bmod X - a_1, \dots, b_r \bmod X - a_r)$ vous renvoie à un résultat de 1re année bien connu ! Lequel ? Pourquoi la reformulation que je vous propose est-elle plus riche de conséquences ? — Vérifier que si $m_1, \dots, m_r$ ne sont pas supposés premiers entre eux deux à deux, alors le morphisme est toujours correctement défini, mais qu'il n'est plus injectif (ni surjectif).
☢	Généraliser l'énoncé à tout anneau principal.

Interprétation en termes de congruence.

✓	— Comprendre cette reformulation. Que dit précisément l'injectivité sur ce système ? Et la surjectivité ? — Pourquoi cette reformulation, certes très concrète, n'est pas aussi riche d'implications que celle avec un isomorphisme ? — Donner des systèmes de congruence CONCRETS n'ayant pas de solution.

Exemple 3. ♡

✓	— Se convaincre de l'implication : $a^{561} \equiv a \bmod 561 \Rightarrow a^{561} \equiv a \bmod 3$ (ou 11, ou 17), et qu'elle ne nécessite pas le théorème chinois. Plus généralement, vérifier que si : $a \equiv b \bmod n$, et si m divise n, alors : $a \equiv b \bmod m$. — Se convaincre que le fait d'avoir une équivalence, et non une implication directe, est bien une conséquence du théorème chinois. *C'est très important.* — Comprendre pourquoi je n'ai pas utilisé le petit théorème de Fermat sous la forme : $a^3 \equiv a \bmod 3$, préférant la fastidieuse distinction de cas que nécessite la congruence $a^2 \equiv 1 \bmod 3$ (de même avec 11 et 17). Faire le lien avec un commentaire plus haut sur le petit théorème de Fermat (après l'avoir déduit du théorème d'Euler).
☢	En observant quelles propriétés arithmétiques de 561 ont permis ce contre-exemple au petit théorème de Fermat, conjecturer une généralisation (que vous ne serez pas en mesure de démontrer : il faut pour cela la cyclicité du groupe $(\mathbb{Z}/p\mathbb{Z})^\times$) : à quelle condition suffisante (voire nécessaire) un entier n vérifie : $\forall a \in \mathbb{Z}$, $a^n \equiv a \bmod n$?

Remarque. ♡

✓	Comprendre pourquoi Φ^{-1} vérifie effectivement la propriété de « $\mathbb{Z}$-linéarité » suivante : $\Phi^{-1}(a \bmod m, b \bmod n) = a\Phi^{-1}(1 \bmod m, 0 \bmod n) + b\Phi^{-1}(0 \bmod m, 1 \bmod n)$. Cette stratégie pour déterminer un morphisme de groupes à l'aide de son image d'une « base » se généralise-t-elle ?
★	— Peut-on construire de même la bijection réciproque de l'isomorphisme entre $\mathbb{Z}/m_1 \cdots m_r\mathbb{Z}$ et $\prod_{i=1}^{r} \mathbb{Z}/m_i\mathbb{Z}$? — On a dit plus haut que le théorème chinois est valable avec $K[X]/(P)$. Construire la bijection réciproque sur le même modèle. Dans le cas : $P_i = X - a_i$, que reconnaissez-vous de très connu ? — Si vous avez réussi l'item précédent : comprendre pourquoi le théorème chinois avec $K[X]/(P)$ permet de créer des polynômes interpolateurs dont les évaluations ET les évaluations des dérivées (à un certain ordre), en un nombre fini de points, ont des valeurs prescrites.

Exemple 4.

✓	— Bien comprendre pourquoi $\bar{x}^2 = \bar{1} \Rightarrow \bar{x} = \pm\bar{1}$ nécessite de raisonner modulo un nombre premier (d'ailleurs, cet exemple permet bien de démontrer que c'est faux modulo 51). — Vérifier que $x^2 \equiv 1 \bmod p_1 \cdots p_r$ admet bien 2^r solutions si les p_i sont distincts, premiers et impairs, et 2^{r-1} solutions sans l'hypothèse de parité.
★	Varier les exemples. La *Banque des Cent* fournit (fournira ?) d'autres équations analogues.
☢	Donner tous les anneaux $\mathbb{Z}/n\mathbb{Z}$ dans lesquels $x^2 \equiv 1 \bmod n$ admet uniquement pour solutions 1 et -1 modulo n.

Corollaire 22 (Indicatrice d'Euler : calcul effectif)**.**

✓	— Vérifier *vraiment* l'isomorphisme entre $(\mathbb{Z}/mn\mathbb{Z})^\times$ et $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. — Vérifier le dénombrement de l'ensemble des éléments non inversibles : pourquoi y a-t-il bien $p^k - p^{k-1}$ classes dans $\mathbb{Z}/p^k\mathbb{Z}$ de la forme $\overline{ap}$ avec $a \in \mathbb{Z}$? — Pourquoi ce même dénombrement dans $\mathbb{Z}/n\mathbb{Z}$ directement, avec n quelconque, est-il plus compliqué, et justifie l'approche suivie ?
★	À l'aide de ce corollaire, démontrer l'identité $n = \sum_{d\mid n} \varphi(d)$ autrement que *via* l'approche suivie en travaux dirigés. Pourquoi la démonstration que j'ai proposée en exercice est-elle conceptuellement plus instructive ?

Exemple 5.

✓	— Poursuivre le calcul pour d'autres valeurs de n. On pourra les représenter graphiquement et essayer de comprendre ce que l'on observe, effectuer différentes conjectures sur le comportement asymptotique de φ, etc. — Qu'observe-t-on sur la parité de $\varphi(n)$? L'expliquer.
★	— Quelles sont les solutions apparentes de $\varphi(n) = 2$ et $\varphi(n) = 4$? Proposer une démonstration. Ces deux équations sont intéressantes pour diverses préoccupations algébriques, dont deux que j'énonce dans proposer de démonstration : la première, pour que le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$ soit égal à 2 (ce qui permet de démontrer sans outil sophistiqué le cas particulier suivant de la progression arithmétique de Dirichlet : il existe une infinité de nombres premiers p tels que $p \equiv -1 \bmod n$), la seconde, pour que la dimension sur $\mathbb{Q}$ de $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ soit égale à 4, et donc la dimension de $\mathbb{Q}\left[\cos\left(\frac{2\pi}{n}\right)\right]$ égale à 2 (ce qui implique concrètement que cela donne tous les angles remarquables dont le cosinus s'exprime à l'aide de rationnels et de la racine carrée d'un rationnel). — Proposer un encadrement explicite de $\varphi(n)$ pour tout $n \geqslant 1$, en fonction de n.
☢	Est-ce que φ induit une surjection de $\mathbb{N} \setminus \{0,1,2\}$ dans $2\mathbb{N} \setminus \{0\}$?

Après votre révision de cette partie

1. Commencer à comprendre quel fut l'intérêt d'introduire l'ensemble $\mathbb{Z}/n\mathbb{Z}$: après tout, en 1re année, vous saviez déjà faire du calcul modulo n, donc l'introduction de $\mathbb{Z}/n\mathbb{Z}$ pouvait d'abord s'apparenter à un simple changement de vocabulaire.
2. Effectuer les *Savoir-faire à vérifier* sur l'arithmétique des entiers, sauf celui exploitant la structure cyclique de $(\mathbb{Z}/p\mathbb{Z})^\times$ (attendre de l'avoir vue en travaux dirigés).

2.3 Arithmétique dans $K[X]$

Motivation de cette partie

Même motivation que dans $\mathbb{Z}$. Mais ici la situation est un peu plus nouvelle, puisque le programme de 1re année se borne à l'étude dans $\mathbb{R}[X]$ ou $\mathbb{C}[X]$. Or l'étude des polynômes dans $\mathbb{Q}[X]$ est très présente dès qu'on s'intéresse aux nombres *algébriques* (c'est-à-dire aux solutions des équations polynomiales non triviales à coefficients entiers ou rationnels). On approfondit donc l'étude des polynômes irréductibles, en donnant une classe importante de polynômes irréductibles :

les polynômes minimaux, qui donnent en quelque sorte les équations polynomiales minimales vérifiées par des nombres algébriques, et donnent un moyen inédit (propre aux polynômes et sans analogue dans $\mathbb{Z}$) de montrer des relations de divisibilité.

Théorème 23 (L'anneau des polynômes sur un corps est un anneau principal)**.**

✓	— Comprendre pourquoi, au moment de chercher un polynôme qui engendre I, il était *naturel* de le prendre de degré minimal (par analyse-synthèse par exemple). — Vérifier l'inclusion réciproque « évidente ». — Il y a plusieurs choix possibles de polynôme de degré minimal. Pourtant ils engendrent le même idéal : pourquoi ? — Comparer avec la démonstration que $\mathbb{Z}$ est principal. Essayer d'en déduire une stratégie générale pour montrer que tout anneau intègre ayant une division euclidienne (en termes qu'on laisse vague : la difficulté est de généraliser la condition sur le reste) est principal. — Dans le cas de $\mathbb{Z}$, on a même montré mieux : tous les sous-groupes de $\mathbb{Z}$ sont engendrés par un seul élément. Se convaincre que ce n'est pas le cas dans $K[X]$, et comprendre ce qui empêche la démonstration de se généraliser de $\mathbb{Z}$ à $K[X]$ (cela apparaît de manière presque voilée dans la démonstration de cette proposition).
☢	— Si l'on veut adapter la démonstration à $A[X]$ où A n'est pas un corps (par exemple $\mathbb{Z}[X]$), qu'est-ce qui coince ? Peut-on malgré tout démontrer que $A[X]$ est principal ? — Si l'on remplace $K[X]$ par $K[[X]]$ (c'est $K^{\mathbb{N}}$ munit de la même addition et multiplication que $K[X]$), obtient-on toujours un anneau principal ? (J'affirme que les propriétés arithmétiques de cet anneau sont très étonnantes, et répondent à des questions pertinentes qu'on pourrait se poser sur les irréductibles d'un anneau.))

Rappel.

✓	— Se convaincre de ce que j'affirme très brièvement. — Au regard de tout ce qui a été dit dans la section précédente sur les éléments associés : comprendre en quoi ce rappel permet de dire : « on peut toujours se ramener à des polynômes unitaires quand on fait de l'arithmétique dans $K[X]$. »

Corollaire 24 (On peut faire de l'arithmétique avec les polynômes)**.**

✓	— J'affirme que cet énoncé contient davantage que ce que vous aviez déjà démontré en 1re année (même si cela reste très proche). Quoi donc ? — Vérifier effectivement l'unicité de la constante, dans la décomposition en facteurs irréductibles unitaires. — Comprendre la plus-value de la remarque qui précède.
☢	Bien qu'on ne puisse pas montrer que $A[X]$ est principal par la méthode utilisée plus haut, j'affirme qu'on peut obtenir l'existence et unicité de la décomposition en facteurs irréductibles dans $A[X]$ si A est intègre. Pourquoi ? Prendre $A = \mathbb{Z}$ si cela vous aide à y voir clair.

Proposition 25 (Condition nécessaire pour être un polynôme irréductible)**.**

✓	Pourquoi j'exclus le degré 1 de la condition nécessaire ? Où apparaît cette nécessité dans la démonstration ?
★	— J'affirme que dans la démonstration, il apparaît subtilement, en *deux* endroits, le fait que les coefficients des polynômes soient dans un corps. Où ? (L'un de ces deux endroits ne nécessite que l'intégrité.) — Que donne cet énoncé si l'on est dans $A[X]$ avec A qui n'est pas un corps ?

☢	— Montrer que si $P \in K[X]$ est irréductible, alors il existe toujours un corps contenant K et une racine de P (s'inspirer de la construction de $\mathbb{C}$ au chapitre III ; pour vérifier que vous obtenez ainsi un corps, vous aurez besoin de mes commentaires formulés au corollaire 20). Ainsi, il faut toujours préciser dans quel corps le polynôme qu'on étudie n'admet pas de racine. Montrer de plus que la dimension minimale d'un tel corps (vu comme K-espace vectoriel) est égale au degré de P (vous aurez besoin de la construction *explicite* qui précède et du théorème d'isomorphisme). Un tel corps s'appelle un *corps de rupture* de P. Le faire pour $X^2+\bar{1} \in \mathbb{Z}/3\mathbb{Z}[X]$ et $X^2+X+\bar{1} \in \mathbb{Z}/2\mathbb{Z}[X]$: qu'obtenez-vous comme corps ? On peut obtenir tous les corps finis possibles par ce procédé ! — Que donne le point précédent si P n'est pas irréductible ?

Exemple 6.

✓	Fournir facilement une infinité de contre-exemples dans $\mathbb{R}[X]$.
★	Que dire d'un anneau $K[X]$ vérifiant l'équivalence entre l'irréductibilité (pour un polynôme de degré au moins 2) et l'absence de racine ? Connaissez-vous de tels anneaux ?
☢	Montrer néanmoins qu'on obtient une condition nécessaire et suffisante si l'on tient compte des corps contenant K, c'est-à-dire : montrer que si $P \in K[X]$, alors P est irréductible si et seulement si, pour tout corps L contenant K, le polynôme P n'admet pas de racine dans L. La démonstration de cette équivalence nécessite de montrer l'existence des corps de rupture mentionnée ci-dessus. Retrouver, alors, grâce à cet énoncé, le fait que les polynômes irréductibles dans $\mathbb{R}[X]$ soient exactement les polynômes de degré 1 et ceux de degré 2 sans racine.

Théorème 26 (Théorème de D'Alembert-Gauß, et polynômes irréductibles sur $\mathbb{C}$)**.**

✓	Vérifier l'équivalence entre les deux formulations de ce théorème.
★	Vérifier que cet énoncé est faux avec $\mathbb{Q}[i] = \left\{a+bi \mid (a,b) \in \mathbb{Q}^2\right\}$ à la place de $\mathbb{C}$. Cela permet de comprendre pourquoi toute démonstration du théorème de D'Alembert-Gauß repose sur un argument d'analyse réelle : il nécessite $\mathbb{R}$ pour être vrai, or $\mathbb{R}$ fut construit analytiquement (soit pour avoir l'axiome de la borne supérieure, soit pour faire converger les suites de Cauchy, ce qui est équivalent).
☢	On pourrait penser que le problème avec $\mathbb{Q}(i)$ est sa dimension finie sur $\mathbb{Q}$, ou sa dénombrabilité, qui en fait un corps « trop petit » pour contenir les racines de tous les polynômes. Montrer qu'il n'en est rien, en remplaçant $\mathbb{Q}$ par l'un de ces deux corps (qui contredisent soit la dimension finie, soit la dénombrabilité, soit les deux) : 1° le plus petit sous-corps de $\mathbb{R}$ stable par $x \mapsto \sqrt{x}$ (c'est le corps des *nombres constructibles*, dont je ne demande pas de montrer l'existence ici), 2° l'élément maximal de l'ensemble $\{K \subseteq \mathbb{R} \mid K \text{ corps}, \sqrt{2} \notin K\}$ pour la relation d'inclusion, qui existe par le lemme de Zorn. Ainsi vous serez convaincus de la singularité du corps $\mathbb{R}$.

Corollaire 27 (Polynômes irréductibles sur $\mathbb{R}$)**.**

✓	Proposer une autre démonstration. Constater que dans tous les cas, on a besoin du théorème fondamental de l'algèbre, ce qui peut paraître étonnant alors que l'énoncé du corollaire ne fait pas intervenir $\mathbb{C}$.
★	Démontrer ce que j'ai laissé en suspens : *a priori* $(X-\alpha)(X-\bar{\alpha}) = X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2$ divise P dans $\mathbb{C}[X]$ (c'est-à-dire : le quotient est dans $\mathbb{C}[X]$), et pourtant j'utilise ensuite l'irréductibilité de P dans $\mathbb{R}[X]$: pourquoi puis-je passer de $\mathbb{C}[X]$ dans $\mathbb{R}[X]$? Démontrer plus généralement que si A et B sont deux polynômes de $K[X]$, et si L est un corps contenant K, alors A divise B dans $K[X]$ si et seulement si c'est le cas dans $L[X]$. Cet énoncé a plein d'analogues (le pgcd ne dépend pas du corps K, etc.). Vous aurez probablement besoin d'utiliser l'unicité du quotient et du reste dans la division euclidienne.

☢
- Montrer plus généralement que si K et L sont deux corps tels que : $L = K(\alpha)$, où $\alpha \in L \setminus K$ est annulé par un polynôme de $K[X]$ de degré 2, alors il n'existe qu'un seul automorphisme de corps de L non trivial qui fixe les éléments de K et que, si l'on note σ cet automorphisme, alors $(X-x)(X-\sigma(x))$ est dans $K[X]$ pour tout $x \in L$, et irréductible si $x \in L \setminus K$.
  Achever de généraliser ce corollaire en notant que si L est algébriquement clos (c'est-à-dire : tout polynôme de $L[X]$ non constant est scindé), alors les irréductibles de $K[X]$ sont exactement les polynômes de degré 1 et ceux de degré 2 sans racine dans K.
- Et si l'on reprend l'énoncé ci-dessus en supposant que α est annulé par un polynôme de $K[X]$ de degré d (où d est le plus petit degré à convenir), qu'obtient-on à la place ?

Exemple 7.

✓
- Proposer une autre démonstration que l'égalité : $\sqrt[3]{2} = \frac{a}{b}$, avec a et b entiers premiers entre eux, est impossible. Par exemple : montrer que b doit diviser a, ce qui n'est possible que si $b = \pm 1$, et conclure immédiatement.
- Produire une infinité d'autres exemples, de degré supérieur à 3 et irréductibles dans $\mathbb{Q}[X]$, puis en faire autant dans $\mathbb{Z}/p\mathbb{Z}[X]$ (avec p explicite). Cela appuie mon commentaire ci-dessus concernant la forme très remarquable des irréductibles de $\mathbb{R}[X]$ (ils vous sont si familiers que le caractère exceptionnel de la proposition peut échapper).

☢ Produire des exemples de degré 4, 5, 6, etc. Certains exercices de travaux dirigés permettraient d'en produire pour des degrés quelconques.

Définition-Proposition 28 (Un idéal important : l'idéal annulateur, polynôme minimal)**.**

✓
- Connaissez-vous des exemples concrets où l'idéal I est réduit à $\{0\}$?
- Définir alternativement $\pi_{z,K}$ comme le plus petit polynôme unitaire *au sens du degré*, dans $K[X]$, ayant z pour racine, et essayer de retrouver toutes ses propriétés données dans cette proposition. Comprendre pourquoi notre définition est plus satisfaisante.
- Rédiger autrement notre démonstration de l'irréductibilité de $\pi_{z,K}$, pour que ce soit un raisonnement direct et non par l'absurde.
- Quel aspect de la proposition nous permet de trouver le polynôme minimal d'un élément *en pratique* ?

★
- On savait déjà que $X - z$ divise P si et seulement si $P(z) = 0$. Pourquoi la relation de divisibilité de cette proposition est-elle plus instructive ? Plusieurs réponses sont possibles (y réfléchir éventuellement après avoir fini cette section ou traité quelques exercices). Quel est son *seul* défaut, par rapport à la divisibilité par $X - z$?
- Le polynôme minimal d'un élément est irréductible. Réciproquement, est-ce que tout polynôme irréductible de $K[X]$ est le polynôme minimal sur K d'un élément ?
- Que donne le théorème d'isomorphisme appliqué au morphisme d'évaluation ? Si vous avez bien suivi tout ce que je vous ai demandé, tout au long des commentaires de ce chapitre, vous pouvez notamment en déduire à moindre frais : une condition nécessaire et suffisante pour que $K[z]$ soit de dimension finie sur K, ou soit un corps (et le cas échéant, comment calculer un inverse en s'inspirant de ce que l'on fait dans $\mathbb{Z}/n\mathbb{Z}$). Vous pouvez aussi en déduire une démonstration élégante et très rapide que le polynôme minimal de z sur K est irréductible dans $K[X]$. C'est un des isomorphismes les plus utiles de l'algèbre.
- Si K' est un autre corps tel que : $K \subseteq K' \subseteq L$, quelle relation peut-on donner entre $\pi_{z,K}$ et $\pi_{z,K'}$?
- Si, au lieu de prendre $z \in L$, on prenait z dans une K-algèbre A quelconque, on pourrait toujours définir l'idéal I, et donc $\pi_{z,K}$. Quelles propriétés se généraliseraient toujours, et lesquelles disparaîtraient ? Cette observation aura une très grande importance en algèbre linéaire.
- Toujours en remplaçant L par A : donner une condition suffisante simple pour que le polynôme minimal existe pour tout $z \in A$ (penser à une condition qui assurerait que le morphisme d'évaluation a un noyau non trivial).

Exemple 8.

✓
- Varier les exemples. Essayer de donner des exemples de polynômes minimaux de degré plus élevé.
- Plus généralement, à quelle condition nécessaire et suffisante sur z a-t-on : $\deg(\pi_{z,K}) = 1$?
- Pourquoi $X^2 - 2$ est bien irréductible ?

★	En considérant le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$ trouvé : comprendre pourquoi la relation de divisibilité par le polynôme minimal, dans la proposition précédente, est plus instructive que la simple divisibilité par $X - z$. Que nous enseigne la relation $P = \pi_{z,K} Q$, que ne nous enseignerait pas la relation $P = (X - z)Q$?

Exemple 9.

✓	— Et si $\theta \in \pi\mathbb{Z}$, que dire ? — Plus généralement, si $z \in \mathbb{C} \setminus \mathbb{R}$, quel est le polynôme minimal sur $\mathbb{R}$ de z ?
☢	Peut-on de même proposer un polynôme minimal sur $\mathbb{Q}$ de $e^{i\theta}$?

Remarque.

★	Essayer de construire une « dérivation » sur $\mathbb{Z}$, c'est-à-dire une application $d : \mathbb{Z} \to \mathbb{C}$ additive et vérifiant : $\delta(ab) = a\delta(b) + \delta(a)b$, pour tout $(a, b) \in \mathbb{Z}^2$. Qu'en pensez-vous ? Peut-on imiter la dérivation sur $K[X]$?
☢	Contrairement à ce que j'affirme, il y a bien une sorte de généralisation de la propriété vis-à-vis de l'évaluation : si A est un anneau principal (pour simplifier) contenant $\mathbb{Z}$, et si p est un élément irréductible de A, montrer que $pA \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$ engendré par un nombre premier q, et que p divise $a \in \mathbb{Z}$ si et seulement si q divise a. Pourquoi est-ce un analogue de la propriété du polynôme minimal ?

Exemple 10.

★	Démontrer ce résultat sans recourir aux polynômes minimaux, pour apprécier la valeur ajoutée du polynôme minimal quand on veut démontrer des relations de divisibilité.

Exemple 11.

✓	Vérifier les réductions que je n'ai pas détaillées en cours (le fait de pouvoir supposer P, Q et R premiers entre eux deux à deux, et que R est le polynôme de degré maximal).
☢	Démontrer cet autre énoncé qui est résolu dans $\mathbb{C}[X]$ mais un problème ouvert important dans $\mathbb{Z}$ (et qui implique d'ailleurs le dernier théorème de Fermat) : pour tous polynômes P, Q et R de $\mathbb{C}[X]$ premiers entre eux tels que : $P + Q = R$, on a : $\max(\deg(P), \deg(Q), \deg(R)) \leqslant N - 1$, où N est le nombre de racines distinctes de PQR (théorème de Mason-Stothers). L'analogue entier s'appelle la *conjecture abc* et est l'une des conjectures les plus importantes de l'arithmétique, avec l'hypothèse de Riemann et le problème de Langlands. Ne pas croire l'annonce récente que le mathématicien japonais Mochizuki l'aurait démontrée.

Après votre révision de cette partie

1. Bien cerner les subtilités de l'irréductibilité dans $K[X]$, en évitant toutes les généralisations hâtives (concernant le lien avec le degré et les racines).
2. Faire les *Savoir-faire à vérifier* sur l'arithmétique des polynômes.

Table des matières