Université de Rennes 1 Année universitaire 2018-2019
Licence de mathématiques
Module Anneaux et Arithmétique

Contrôle continu n°1
Mercredi 6 mars 2019, 17h15 – 18h15

Exercice 1

Soit A un anneau. Pour tout idéal I de A, on pose

$$\sqrt{I} := \{a \in A, \quad \exists n \in \mathbf{N} \setminus \{0\}, \quad a^n \in I\}.$$

1. Soit I un idéal de A. Montrer que $\sqrt{I}$ est un idéal de A qui contient I.
   Correction : Montrons que $\sqrt{I}$ est un sous-groupe de A.
   On a $0^1 = 0$ or $0 \in I$ car I est un idéal de A, donc $0 \in \sqrt{I}$
   Soit $x \in \sqrt{I}$ et $n \in \mathbf{N} \setminus \{0\}$ tel que $x^n \in I$. Alors $(-x)^n = (-1)^n x$. Comme I est un sous-groupe de A et $x^n \in I$, on a $(-1)^n x \in I$. Donc $-x \in \sqrt{I}$.
   Soit $x, y \in \sqrt{I}$, $n \in \mathbf{N} \setminus \{0\}$ tel que $x^n \in I$ et $m \in \mathbf{N} \setminus \{0\}$ tel que $y^m \in I$.
   Notons que si $r \in \mathbf{N}$, comme $x^{n+r} = x^n x^r$ et I est un idéal, on a $x^{n+r} \in I$. De même $y^{m+r} \in I$.
   D'après la formule du binôme de Newton, on a

$$(x+y)^{n+m} = \sum_{\substack{p,q \in \mathbf{N} \\ p+q=n+m}} \binom{n}{p} x^p y^q.$$

   Soit $p, q \in \mathbf{N}$ tel que $p + q = n + m$. Si $p < n$ et $q < m$, on a $p + q < n + m$ ce qui est absurde. Donc soit $p \geqslant n$, soit $q \geqslant m$. Si $p \geqslant n$, d'après la remarque ci-dessus, on a $x^p \in I$. Comme I est un idéal, on a alors $\binom{n}{p} x^p y^q \in I$. Si $q \geqslant m$, on a $y^q \in I$ et donc là encore $\binom{n}{p} x^p y^q \in I$.
   Ainsi $(x+y)^{n+m}$ s'écrit comme une somme d'éléments de I, donc est dans I. Donc $x+y \in \sqrt{I}$.
   Ainsi $\sqrt{I}$ est bien un sous-groupe de A.
   Soit $x \in \sqrt{I}$, $n \in \mathbf{N} \setminus \{0\}$ tel que $x^n \in I$ et $y \in A$. Alors $(xy)^n = x^n y^n$. Comme $x^n \in I$ et I est un idéal, on a $x^n y^n \in I$. Donc $xy \in \sqrt{I}$.
   Ceci achève de montrer que $\sqrt{I}$ est un idéal de A.
   Montrons que $I \subset \sqrt{I}$. Soit $x \in I$. On a $x^1 = x$ donc $x^1 \in I$ et donc $x \in \sqrt{I}$, ce qui conclut.
   Notons que ce dernier résultat montre que pour établir qu'un idéal I est radical, il suffit de montrer l'inclusion $\sqrt{I} \subset I$. Nous utiliserons cette remarque par la suite.
2. Soit I un idéal premier de A. Montrer que I est radical.
   Correction : Soit $x \in I$. Pour n entier strictement positif, soit $\mathcal{P}_n$ la propriété : « si $x^n \in I$, alors $x \in I$ ».
   $\mathcal{P}_1$ est évidemment vérifiée. Soit $n \geqslant 1$ un entier tel que $\mathcal{P}_n$ est vérifiée. Montrons que $\mathcal{P}_{n+1}$ est vérifiée. Supposons $x^{n+1} \in I$. Comme $x = x^n.x$ et I est un idéal premier, on a $x \in I$ ou $x^n \in I$. Dans le premier cas, on a immédiatemment la conclusion cherchée. Dans le second cas, d'après $\mathcal{P}_n$, on a bien la conclusion cherchée.
   On a donc démontrée par récurrence que $\mathcal{P}_n$ est vraie pour tout n. Ceci montre que si $x \in \sqrt{I}$, alors $x \in I$.
   Finalement, on a montré l'inclusion $\sqrt{I} \subset I$, ce qui conclut.

3. Soit I et J des idéaux radicaux de A. Montrer que $I \cap J$ est un idéal radical de A.
   Correction : Il suffit de montrer qu'on a $\sqrt{I \cap J} \subset I \cap J$. Soit $x \in \sqrt{I \cap J}$ et $n \in \mathbf{N} \setminus \{0\}$ tel que $x^n \in I \cap J$. En particulier on a $x^n \in I$, donc $x \in \sqrt{I}$. Or par hypothèse $\sqrt{I} = I$, donc $x \in I$. De même on montre $x \in J$. Donc $x \in I \cap J$, d'où le résultat cherché.
4. L'idéal $12\mathbf{Z}$ est-il un idéal radical de $\mathbf{Z}$? Même question pour l'idéal $15\mathbf{Z}$.
   Correction : L'entier $36 = 6^2$ est divisible par 12 mais 6 n'est pas divisible par 12. Donc $6 \in \sqrt{12\mathbf{Z}} \setminus 12\mathbf{Z}$, et $12\mathbf{Z}$ n'est pas un idéal radical de $\mathbf{Z}$.
   Montrons que $15\mathbf{Z}$ est un idéal radical de $\mathbf{Z}$. La méthode la plus rapide est d'exploiter les questions précédentes en en constatant que comme $15 = 3.5$ et 3 et 5 sont premiers entre eux, on a $15\mathbf{Z} = 3\mathbf{Z} \cap 5\mathbf{Z}$. Par ailleurs comme 3 et 5 sont des nombres premiers $3\mathbf{Z}$ et $5\mathbf{Z}$ sont des idéaux premiers. D'après les questions 2 et 3, $3\mathbf{Z} \cap 5\mathbf{Z}$ est un idéal radical.
   On pouvait bien sûr s'en tirer « à la main » comme suit : il suffit de montrer que $\sqrt{15\mathbf{Z}} \subset 15\mathbf{Z}$. Soit $m \in \sqrt{15\mathbf{Z}}$. Il existe donc $n \in \mathbf{N} \setminus \{0\}$ tel que 15 divise m^n. En particulier, 3 et 5 divisent m^n. Comme 3 et 5 sont premiers, le lemme d'Euclide montre que 3 et 5 divisent m. Comme 3 et 5 sont premiers entre eux, on en déduit que 15 divise m. Donc $m \in 15\mathbf{Z}$. On a donc bien $\sqrt{15\mathbf{Z}} \subset 15\mathbf{Z}$.
5. Soit n un entier strictement positif. Déterminer une condition nécessaire et suffisante sur n, portant sur la décomposition de n en facteurs premiers, pour que l'idéal $n\mathbf{Z}$ soit radical. En déduire que tout idéal radical propre de $\mathbf{Z}$ est une intersection finie d'idéaux premiers de $\mathbf{Z}$.
   Correction : Montrons le résultat suivant : $n\mathbf{Z}$ est radical si et seulement si n est sans facteur carré, c'est-à-dire tous les nombres premiers apparaissant dans la décomposition de n en facteurs premiers ont un exposant 1 (de manière équivalente : pour tout nombre premier p, p^2 ne divise pas n).
   Supposons que n n'est pas sans facteur carré et montrons que $n\mathbf{Z}$ n'est pas un idéal radical. D'après l'hypothèse sur n, il existe un nombre premier p, un entier $r \geqslant 2$ et un entier m non divisible par p tel que $n = p^r m$. On a $(pm)^r = nm^{r-1}$ ce qui montre que $pm \in \sqrt{n\mathbf{Z}}$. Mais n ne divise pas pm car l'exposant de p dans la décomposition en facteurs premiers de n (respectivement de pm) est r (respectivement 1) et on a $r \geqslant 2 > 1$. Donc $pm \in \sqrt{n\mathbf{Z}} \setminus n\mathbf{Z}$, et $n\mathbf{Z}$ n'est pas un idéal radical.
   Supposons à présent que n est sans facteur carré et montrons que $n\mathbf{Z}$ est un idéal radical. D'après l'hypothèse sur n, on a soit $n = 1$, soit il existe un entier $s \geqslant 1$ et des nombres premiers deux à deux distincts $p_1, \ldots, p_s$ tels que $n = \prod_{i=1}^{s} p_i$.
   Dans ce dernier cas, là encore, la méthode la plus rapide est d'exploiter les questions 2 et 3, même si on pouvait raisonner aussi « à la main ». Cette méthode rapide a en outre l'avantage de donner presque aussitôt la réponse à la question suivante. Comme les p_i sont deux à deux premiers entre eux, on a (cas particulier de l'énoncé du théorème chinois avec un nombre quelconque d'idéaux vu en cours, ou directement)

$$n\mathbf{Z} = \bigcap_{i=1}^{s} p_i\mathbf{Z}.$$

   Comme les p_i sont premiers, les idéaux $p_i\mathbf{Z}$ sont premiers, donc radicaux d'après la question 2. La question 3 (ou plutôt son extension immédiate à une intersection finie d'idéaux) montre alors que $n\mathbf{Z}$ est radical.
   Dans le cas où $n = 1$, comme $\sqrt{\mathbf{Z}} \subset \mathbf{Z}$ est de toute façon vérfiée, $\mathbf{Z}$ est un idéal radical (et de manière générale, si A est un anneau, l'idéal A est toujours un idéal radical de A).
   Considérons à présent un idéal radical propre I de $\mathbf{Z}$. Si $I = 0\mathbf{Z}$, I est premier (car $\mathbf{Z}$ est intègre) et on a terminé. Sinon d'après ce qui précède il existe un entier $s \geqslant 1$ et des nombres

premiers deux à deux distincts $p_1, \ldots, p_s$ tels que $n = \prod_{i=1}^{s} p_i$. Et on a déjà montré que $n\mathbf{Z}$ était une intersection finie d'idéaux premiers.

6. Soit B et C des anneaux non nuls. Montrer que $\sqrt{0}$ (le radical de l'idéal nul) n'est *pas* un idéal premier de $B \times C$.
   Correction : On a $(0_B, 1_C)(1_B, 0_C) = (0_B, 0_C)$ et $(0_B, 0_C) \in \sqrt{0}$. Cependant, ni $(0_B, 1_C)$ ni $(1_B, 0_C)$ ne sont des éléments de $\sqrt{0}$. En effet, si n est un entier strictement positif, on a $(0_B, 1_C)^n = (0_B^n, 1_C^n) = (0_B, 1_C)$ et $(0_B, 1_C) \neq (0_B, 0_C)$ car C n'est pas l'anneau nul. Même raisonnement pour $(1_B, 0_C)$. Donc $\sqrt{0}$ n'est pas un idéal premier de $B \times C$
7. Donner un exemple d'un anneau A non intègre tel que $\sqrt{0}$ est un idéal premier de A.
   Correction : Prenons $A = \mathbf{Z}/4\mathbf{Z}$. On a $[2]_2^2 = [0]_2$. Par ailleurs, pour tout entier n strictement positif $[1]_2^n = [1]_2 \neq [0]_2$ et $[3]_2^n = [-1]_2^n = [(-1)^n]_2 \neq [0]_2$.
   Donc $\sqrt{0} = \{[0]_2, [2]_2\}$, qui est bien un idéal premier : en effet il est propre et on vérifie aussitôt que si $\{a, b\} = \mathbf{Z}/4\mathbf{Z} \setminus \sqrt{0}$ on a $\{a^2, b^2, ab\} \cap \sqrt{0} = \varnothing$. Plus conceptuellement, on pouvait montrer que $(\mathbf{Z}/4\mathbf{Z})/\sqrt{0}$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$. En effet on vérifie facilement que l'unique morphisme d'anneaux $\mathbf{Z}/4\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z}$ est surjectif et de noyau $\sqrt{0}$.
8. **(hors-barême)** Donner un exemple d'un anneau A non intègre, non nul, tel que $\sqrt{0}$ n'est *pas* un idéal premier de A et A n'est *pas* isomorphe à un produit $B \times C$, où B et C sont des anneaux non nuls.
   Correction (indication) : On pourra essayer de montrer que l'anneau $A = \mathbf{C}[X, Y]/\langle XY \rangle$ fournit un tel exemple. Pour montrer que A n'est pas isomorphe à un produit non trivial, on montrera que A ne contient pas d'élément $e \notin \{0_A, 1_A\}$ tel que $e^2 = e$ et on se reportera à la correction du premier contrôle continu d'ANAR de l'an dernier.
   Remarques : Sans la condition (oubliée dans la rédaction de l'énoncé distribué lors de l'examen) que A n'est pas l'anneau nul, l'anneau nul fournit un exemple immédiat mais guère intéressant.
   Par ailleurs la condition « non intègre » était superflue dans l'énoncé dans le sens où elle est entraînée par la condition « $\sqrt{0}$ n'est pas un idéal premier de A ». En effet, si A est intègre, l'idéal nul est intègre et coïncide avec $\sqrt{0}$.

Pour aller plus loin

- *Sur les questions 2,3 et 5 :* On a déjà utilisé le fait que le résultat de la question 3 s'étend immédiatement à une intersection finie, et en fait un raisonnement quasiment identique montre qu'une intersection quelconque d'idéaux radicaux est encore un idéal radical. En particulier, compte tenu de la question 2, une intersection quelconque d'idéaux premiers est radicaux. Réciproquement, on peut montrer que tout idéal radical propre est une intersection d'idéaux premiers. Plus généralement, si I est un idéal propre de A, on peut montrer que $\sqrt{I}$ est l'intersection des idéaux premiers de A contenant I. Vous pouvez essayer de montrer ce qui précède soit directement si vous connaissez le lemme de Zorn, soit en admettant le résultat de la question 7 de l'exerice 10 et en quotientant astucieusement. Le résultat de la question 5 dans le cas de l'anneau $\mathbf{Z}$ est plus fort en ce sens qu'on obtient une intersection est finie. En fait un tel résultat vaut de manière générale pour une classe beaucoup plus large d'anneaux, à savoir les anneaux noetheriens, que l'on peut définir comme étant les anneaux dont tout idéal est engendré par un nombre fini d'éléments. La notion d'anneau noetherien est absolument fondamentale en algèbre commutative, et constitue en en sens la « grande absente » du programme du module (mais il faut bien faire des choix compte tenu du volume horaire imparti).
- *Sur la question 7 :* On pourra montrer plus généralement que pour tout nombre premier p et tout entier strictement positif r, l'idéal $\sqrt{0}$ est un idéal premier de $A = \mathbf{Z}/p^r\mathbf{Z}$ engendré par $[p]_{p^r}$ et que $A/\sqrt{0}$ est isomorphe à $\mathbf{Z}/p\mathbf{Z}$.

- *Sur la question 8 :* Telle quelle la question est évidemment extrêmement difficile. Notons qu'au vu de ce qui précède sur la question 7 et du théorème chinois, il est sans espoir de trouver un tel exemple parmi les anneaux $\mathbf{Z}/n\mathbf{Z}$.
  Je peux tâcher d'expliquer d'où vient le type d'exemple proposé. Cela nécessite quelques notions de topologie et de géométrie algébrique.
  Soit E un espace topologique. Vous connaissez a priori la notion de connexité, qui formalise l'idée intuitive d'« espace d'un seul tenant ». L'espace E est dit connexe s'il n'est pas la réunion de deux fermés disjoints (ici je prends donc la convention que l'espace vide n'est pas connexe).
  La notion de connexité peut être renforcée en la notion d'irréductibilité. L'espace E est dit irréductible s'il est non vide et n'est pas la réunion de deux fermés propres. Clairement, un espace irréductible est nécessairement connexe. Pour les espaces topologiques « usuels » tels que $\mathbf{R}$, la notion d'irréductibilité est en fait trop forte pour être pertinente. Ainsi une partie de $\mathbf{R}$ (avec la topologie induite) est irréductible si et seulement si c'est un singleton. Cependant, la notion d'irréductibilité devient un renforcement pertinent de la notion de connexité pour d'autres topologies. Les espaces connexes non irréductibles correspondent alors intuitivement à des espaces qui, bien que « d'un seul tenant », admettent une décomposition raisonnable en « morceaux » plus élémentaires.
  Un exemple important de type de topologie pour laquelle la notion d'irréductibilité est pertinente est la topologie de Zariski, fondamentale en géométrie algébrique. C'est une topologie sur l'ensemble $\mathrm{Spec}(A)$ des idéaux premiers d'un anneau A, dont les fermés sont les ensembles de la forme

  $$V(I) := \{\mathfrak{p} \in \mathrm{Spec}(A), I \subset \mathfrak{p}\}$$

  où I parcourt l'ensemble des idéaux de A. Les deux résultats suivants sont alors raisonnablement faciles à montrer :
  — $\mathrm{Spec}(A)$ est connexe si et seulement si A est non nul et n'est pas isomorphe au produit de deux anneaux non nuls ;
  — $\mathrm{Spec}(A)$ est irréductible si et seulement si $\sqrt{0}$ est un idéal premier.
  L'exemple demandé correspond donc géométriquement à la recherche d'un exemple d'espace connexe non irréductible parmi les $\mathrm{Spec}(A)$. Maintenant, en me permettant un certain nombre de raccourcis, l'intuition qui soutient le fait que $\mathrm{Spec}(\mathbf{C}[X,Y]/\langle XY\rangle)$ est connexe et non irréductible est le fait que l'ensemble

  $$\{(x,y) \in \mathbf{C}^2, \quad xy = 0\}$$

  est connexe, mais est réunion de deux fermés *algébriques* (c'est-à-dire définis par des équations polynomiales) propres, à savoir ceux définis par les équations $x = 0$ et $y = 0$. Dit autrement, on a deux droites (complexes) qui ont un point d'intersection, ce qui garantit la connexité de leur réunion ; mais par ailleurs cette réunion admet une décomposition naturelle dont les morceaux sont chacune des deux droites.

Exercice 2

Soit $\mathbf{Z}[i\sqrt{2}]$ l'image de l'unique morphisme d'anneaux $\varphi\colon \mathbf{Z}[X] \to \mathbf{C}$ qui envoie X sur $i\sqrt{2}$. Pour tout $z \in \mathbf{Z}[i\sqrt{2}]$, on pose $N(z) := z\bar{z}$.

1. Montrer que $\mathbf{Z}[i\sqrt{2}]$ est isomorphe à l'anneau quotient $\mathbf{Z}[X]/(X^2+2)\mathbf{Z}[X]$.
   Correction : D'après l'un des « théorèmes d'isomorphisme » du cours, il suffit de montrer que $\mathrm{Ker}(\varphi) = (X^2+2)\mathbf{Z}[X]$.

Montrons l'inclusion $(X^2+2)\mathbf{Z}[X] \subset \mathrm{Ker}(\varphi)$. Soit $Q \in \mathbf{Z}[X]$. Comme φ est un morphisme d'anneaux, on a $\varphi((X^2+2)Q) = \varphi(X^2+2)\varphi(Q)$. Or $\varphi(X^2+2) = (i\sqrt{2})^2 + 2 = 0$. Donc $\varphi((X^2+2)Q) = 0$. Ceci montre l'inclusion annoncée.
Montrons à présent l'inclusion $\mathrm{Ker}(\varphi) \subset (X^2+2)\mathbf{Z}[X]$, ce qui permettra de conclure. Soit $P \in \mathrm{Ker}(\varphi)$. Comme X^2+2 est unitaire, il existe, d'après le théorème de la division euclidienne vue en cours, $(Q,R) \in \mathbf{Z}[X]^2$ vérifiant $P = (X^2+2)Q + R$ et $\deg(R) < \deg(X^2+2) = 2$. Comme φ est un morphisme d'anneaux et $\varphi(X^2+2) = 0$, on a

$$0 = \varphi(P) = \varphi(Q)\varphi(X^2+2) + \varphi(R) = \varphi(R).$$

Soit $(a,b) \in \mathbf{Z}^2$ tel que $R = aX + b$. Le nombre complexe $\varphi(R) = a + i\sqrt{2}b$ est donc nul, donc ses parties réelles et imaginaires également, ce qui donne aussitôt $a = b = 0$ donc $R = 0$. Finalement $P = (X^2+2)Q$ est bien un élément de $(X^2+2)\mathbf{Z}[X]$

2. Soit $z \in \mathbf{Z}[i\sqrt{2}]$. Montrer que $z \in \mathbf{Z}[i\sqrt{2}]^\times$ si et seulement si $N(z) = 1$.
Correction : Commençons par montrer que pour tout $z \in \mathbf{Z}[i\sqrt{2}]$ on a $N(z) \in \mathbf{N}$ et $\bar{z} \in \mathbf{Z}[i\sqrt{2}]$. Soit $P \in \mathbf{Z}[X]$ tel que $z = P(i\sqrt{2})$. En reprenant le raisonnement de la question précédente faisant intervenir la division euclidienne (en ne supposant plus nécessairement $P \in \mathrm{Ker}(\varphi)$), on constate qu'il existe $a, b \in \mathbf{Z}$ tel que $z = ai\sqrt{2} + b$. Donc $N(z) = |z|^2 = a^2 + 2b^2 \in \mathbf{N}$ et $\bar{z} = -ai\sqrt{2} + b = (-aX + b)(i\sqrt{2})$ ce qui montre que $\bar{z} \in \mathbf{Z}[i\sqrt{2}]$.
Soit $z \in \mathbf{Z}[i\sqrt{2}]^\times$. Montrons que $N(z) = 1$. Soit $z' \in \mathbf{Z}[i\sqrt{2}]$ tel que $zz' = 1$. On a donc $N(zz') = N(1) = 1$ or

$$N(zz') = zz'\bar{z}\bar{z'} = zz'\bar{z}\bar{z'} = z\bar{z}z'\bar{z'} = N(z)N(z').$$

Ainsi $N(z)N(z') = 1$. Sachant que par ailleurs $N(z)$ et $N(z')$ sont des entiers positifs, on en tire aussitôt $N(z) = N(z') = 1$.
Soit $z \in \mathbf{Z}[i\sqrt{2}]$ tel que $N(z) = 1$. Montrons que $z \in \mathbf{Z}[i\sqrt{2}]^\times$. Par hypothèse $z\bar{z} = 1$. Or d'après ce qui précède, on a $\bar{z} \in \mathbf{Z}[i\sqrt{2}]$. Donc z est bien un élément inversible de $\mathbf{Z}[i\sqrt{2}]$ (d'inverse $\bar{z}$).

3. 9 est-il un élément irréductible de $\mathbf{Z}[i\sqrt{2}]$? Même question pour 3 et 5.
Correction : On a $9 = 3.3$ or $N(3) = 3^2 \neq 1$. Donc 9 s'écrit comme le produit de deux éléments non inversibles et n'est donc pas irréductible.
On a $3 = (1+i\sqrt{2})(1-i\sqrt{2})$ or $N(1+i\sqrt{2}) = N(1-i\sqrt{2}) = 3 \neq 1$. Donc 3 s'écrit comme le produit de deux éléments non inversibles et n'est donc pas irréductible.
On a $N(5) = 5^2 \neq 1$, donc 5 n'est pas inversible dans $\mathbf{Z}[i\sqrt{2}]$. Soit $z, z' \in \mathbf{Z}[i\sqrt{2}]$ tels que $zz' = 5$. En particulier $25 = N(5) = N(zz') = N(z)N(z')$. Comme $N(z)$ et $N(z')$ sont des entiers positifs et vu la décomposition en facteurs premiers de 25, on a donc $\{N(z), N(z')\} = \{1, 25\}$ ou $\{N(z), N(z')\} = \{5\}$. Cependant si $(a,b) \in \mathbf{Z}^2$, on a toujours $a^2 + 2b^2 \neq 5$. En effet si $b = 0$, $a^2 \neq 5$ car 5 n'est pas un carré, et si $|b| = 1$ $a^2 \neq 3$ car 3 n'est pas un carré. Par ailleurs si $|b| \geqslant 2$, on a $a^2 + 2b^2 \geqslant 2.4 > 5$. Finalement on a nécessairement $\{N(z), N(z')\} = \{1, 25\}$, en particulier $N(z) = 1$ ou $N(z') = 1$. D'après la question précédente, on a $z \in \mathbf{Z}[i\sqrt{2}]^\times$ ou $z' \in \mathbf{Z}[i\sqrt{2}]^\times$. Ceci montre que 5 est un élément irréductible de $\mathbf{Z}[i\sqrt{2}]$.