Leonid Monin
Léo Navarro Chafloque

Solutions – Semaine 6

Exercice 1.
On considère $d > 0$. On considère l'anneau $\mathbb{Z}[i\sqrt{d}]$.

1. Montrez que
$$\mathbb{Z}[i\sqrt{d}] \cong \mathbb{Z}[t]/(t^2 + d).$$
2. On considère $N\colon \mathbb{Z}[i\sqrt{d}] \to \mathbb{N}$ qui envoie $a + bi\sqrt{d}$ sur $a^2 + b^2 d$. Montrez que si $x \in \mathbb{Z}[i\sqrt{d}]$ est inversible, alors $N(x) = 1$. De cette observation déduisez quels sont les inversibles de cet anneau.
3. Prenons $d = 5$. En utilisant la norme N, montrez que $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ sont irréductibles.
4. Montrez que $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.

Solution. Le premier point se montre en utilisant le morphisme d'évaluation, qu'il n'y a pas de polynôme de degré 1 qui annule $i\sqrt{d}$, et en menant une division euclidienne pour montrer que le noyau de l'évaluation est $(t^2 - d)$. Pour le deuxième point : comme la fonction N est multiplicative, a une image dans le monoïde multiplicatif $(\mathbb{N}, \cdot)$, et qu'un inversible est envoyé sur un inversible par un morphisme de monoïde, et que le seul inversible de $\mathbb{N}$ est 1, cela conclut.* Dès lors, si $x = a + bi\sqrt{d}$ est inversible
$$a^2 + b^2 d = 1,$$
c'est que si $d > 1$ alors $x = \pm 1$, et que si $d = 1$ alors on a également $x = \pm i$ comme possibilités.

Maintenant, prenons $d = 5$. Notons que tous les éléments présentés ont une norme 6, 4 ou 9. On montre plus généralement que tout élément de norme 6, 4 ou 9 est irréductible. Si x est tel que $N(x) = 6, 4, 9$ et si $x = yz$ et qu'aucun des deux n'est inversible, alors $6 = N(x) = N(y)N(z)$ avec $N(y)$, sans perte de généralité, égal à 2 ou 3. Mais on voit qu'il n'est pas possible d'avoir des éléments de norme 2 ou 3.

Notons qu'aucun des éléments listés en 3. ne sont associés car les seuls éléments inversibles sont $1, -1$. Maintenant
$$2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$
montre que 6 n'a pas de décomposition unique en irréductibles.

Exercice 2.
On pousse plus loin l'exercice précédent. Soit $d > 1$. On note $A = \mathbb{Z}[i\sqrt{d}]$. On note $N(a + bi\sqrt{d}) = a^2 + db^2$.

1. Lister les éléments $x \in A$ tel que $N(x) \leq d + 1$.
2. Montrer que $i\sqrt{d}$, $1 + i\sqrt{d}$ et $1 - i\sqrt{d}$ sont irréductibles.
3. Si $d + 1$ n'est pas premier *dans* $\mathbb{Z}$, alors A n'est pas factoriel.
4. Si $q = d + 1$ est premier *dans* $\mathbb{Z}$ alors celui-ci admet une factorisation unique en irréductibles dans A.

Solution.

*C'est d'ailleurs un si et seulement si.

1. Soit $x = a + bi\sqrt{d} \in A$ avec $a^2 + b^2 d \leq d + 1$. Donc

$$a^2 + (b^2 - 1)d \leq 1.$$

On voit dès lors que $|b| \leq 1$. On distingue deux cas. Tout d'abord traitons le cas où $b = \pm 1$. Alors on a nécessairement $a = 0$ ou $a = \pm 1$, c'est à dire

$$x = \pm i\sqrt{d} \quad x = \pm(1 - i\sqrt{d}) \quad x = \pm(1 + i\sqrt{d}).$$

Traitons maintenant le cas où $b = 0$. On alors $x = a \in \mathbb{Z}$ avec la condition que $|a| \leq \sqrt{1 + d}$.

2. On montre d'abord que $i\sqrt{d}$ est irréductible. On a $N(i\sqrt{d}) = d$. Ainsi si $x \mid i\sqrt{d}$ avec x ni inversible ni associé, il faut que $1 < N(x) < d$. Selon la liste établie au point 1, on a alors $x = a \in \mathbb{Z}$ avec $|a| < \sqrt{d}$. Mais comme on a supposé que $x \mid i\sqrt{d}$, il existe $e, f \in \mathbb{Z}$ tel que

$$a(e + fi\sqrt{d}) = i\sqrt{d}.$$

Donc $e = 0$ et $fa = 1$ ce qui contredit $N(a) > 1$.

On montre maintenant que $1 + i\sqrt{d}$ est irréductible. Comme la conjugaison complexe est un automorphisme d'anneau qui envoie $1 + i\sqrt{d}$ sur $1 - i\sqrt{d}$ cela montrera que $1 - i\sqrt{d}$ est également irréductible. Comme $N(1 + i\sqrt{d}) = 1 + d$, si $x \mid 1 + i\sqrt{d}$ avec x ni irréductible ni associé à $1 + i\sqrt{d}$, alors $1 < N(x) < 1 + d$. Comme il faut aussi que $N(x) \mid 1 + d$, on voit que $N(x) < d$. Ainsi un argument similaire à celui au-dessus conclut.

3. Supposons que $1 + d$ n'est pas premier dans $\mathbb{Z}$. Alors on a

$$1 + d = (1 + i\sqrt{d})(1 - i\sqrt{d}) = p_1 \cdots p_r$$

pour $p_1, \ldots, p_r$ des premiers avec $p_i \leq d$ comme on a supposé $d + 1$ pas premier. Comme $1 + i\sqrt{d}$ est irréductible, si $1 + d$ admet une factorisation *unique* en produit d'irréductibles (en supposant par l'absurde que A est factoriel) cela impliquerait que $1 + i\sqrt{d} \mid p_j$ pour un indice j. Mais dès lors il existerait $e, f \in \mathbb{Z}$ avec

$$(1 + i\sqrt{d})(e + fi\sqrt{d}) = p_j$$

Donc $e + f = 0$ et $p_j = e - df = (1 + d)e$. Comme $p_j \leq d$, c'est une contradiction. Ainsi on conclut que $1 + d$ n'admet pas de factorisation unique en produit d'irréductibles. En particulier, on conclut que dans ce cas A n'est pas factoriel.

4. Supposons maintenant $q := 1 + d$ premier dans $\mathbb{Z}$. On a

$$1 + d = (1 + i\sqrt{d})(1 - i\sqrt{d}),$$

qui est une décomposition en irréductibles. On veut montrer que si $x \mid 1 + d$ et est ni inversible ni associé à $1 + d$, alors x est associé à $1 + i\sqrt{d}$ ou $1 - i\sqrt{d}$. Comme $N(1 + d) = (1 + d)^2 = q^2$, un tel diviseur x satisfait forcément $N(x) = q = 1 + d$. Selon la liste au-dessus on a dès lors

$$x = \pm(1 - i\sqrt{d}) \quad x = \pm(1 + i\sqrt{d}).$$

ou $x \in \mathbb{Z}$ avec $x^2 = q$, mais cela n'est pas possible comme q est premier.

Exercice 3.
L'anneau $\mathbb{Z}[\sqrt{5}]$.

1. Montrer que la norme $N \colon \mathbb{Z}[\sqrt{5}] \to \mathbb{Z}$ définie par $N(a + b\sqrt{5}) = a^2 - 5b^2$ est une fonction multiplicative (donc que $N(xy) = N(x)N(y)$ – noter que si l'on définit $\overline{a + b\sqrt{5}} = a - b\sqrt{5}$, alors $N(x) = x\overline{x}$) et que $a + b\sqrt{5}$ est inversible si et seulement si $N(a + b\sqrt{5}) = \pm 1$.

2. Montrer que $9+4\sqrt{5}$ est inversible et en déduire que $(\mathbb{Z}[\sqrt{5}])^\times$ est infini.

3. Montrer qu'il n'existe aucun élément de norme 2 ou -2, si bien que tout élément de norme 4 est irréductible.

4. Trouver deux décompositions de 4 en produit d'irréductibles dans $\mathbb{Z}[\sqrt{5}]$.

5. L'idéal $(3+\sqrt{5})$ est-il premier?

Solution.

1. We define $\overline{a+b\sqrt{5}} = a-b\sqrt{5}$ and note that for all $z \in \mathbb{Z}[\sqrt{5}]$, the norm $N(z) = z\overline{z}$. The fact that N is a multiplicative function then follows from the fact that $\forall y, z \in \mathbb{Z}[\sqrt{5}]$, it holds that $\overline{yz} = \overline{y}\,\overline{z}$. With this, we get that $N(yz) = yz\overline{yz} = yz\overline{y}\,\overline{z} = y\overline{y}z\overline{z} = N(y)N(z)$.

   Furthermore, if $z \in \mathbb{Z}[\sqrt{5}]$ is invertible, then $N(z) = \pm 1$ is necessary. If we denote its inverse by z^{-1}, then $N(z)N(z^{-1}) = N(1) = 1$, and therefore, $N(z) = \pm 1$. On the other hand, if $N(z) = \pm 1$ for some $z \in \mathbb{Z}[\sqrt{5}]$, then $\pm 1 = N(z) = z\overline{z}$ and hence $\pm\overline{z}$ is the inverse of z.

2. We note that $N(9+4\sqrt{5}) = 9^2 - 5\cdot 4^2 = 1$, and so by the first point, $9+4\sqrt{5}$ is invertible. Furthermore, by the multiplicative property of the norm, the norm of $(9+4\sqrt{5})^n$ is 1 as well, for $n \in \mathbb{N}$. This means that we have created infinitely many invertible elements, and $(\mathbb{Z}[\sqrt{5}])^\times$ is infinite.

3. We first show that no elements of norm 2 exist. For this, we note that $N(a+\sqrt{5}b) = a^2 - 5b^2$, which is equal to a^2 modulo 5, a square. But all squares in $\mathbb{Z}/5\mathbb{Z}$ are either 0,1 or 4, as one checks by taking the square of all elements in $\mathbb{Z}/5\mathbb{Z}$.

   Now let $z \in \mathbb{Z}[\sqrt{5}]$ be of norm 4, and we assume that $z = v \cdot w$ for $v, w \in \mathbb{Z}[\sqrt{5}]$. Then $4 = N(z) = N(v)N(w)$. But as there are no elements of norm 2, we have that either $N(v) = \pm 1, N(w) = \pm 4$ or $N(v) = \pm 4, N(w) = \pm 1$. In either cases one of the two elements is of norm ± 1, which means that that element is invertible. Hence z is irreducible.

4. We have

   - $4 = 2\cdot 2$ and $N(2) = 4$, hence by the previous part, 2 is irreducible
   - $4 = (1+\sqrt{5})(-1+\sqrt{5})$ and $N(1+\sqrt{5}) = -4, N(-1+\sqrt{5}) = -4$, hence both $1+\sqrt{5}, -1+\sqrt{5}$ are irreducible.
   - $4 = (3+\sqrt{5})(3-\sqrt{5})$ and $N(3+\sqrt{5}) = 4, N(3-\sqrt{5}) = 4$, hence both $3+\sqrt{5}, 3-\sqrt{5}$ are irreducible.

5. As we see from the previous point, $2\cdot 2 = 4 = (3+\sqrt{5})(3-\sqrt{5})$, from which it follows that $2\cdot 2 \in (3+\sqrt{5})$. But as $2 \notin (3+\sqrt{5})$, the ideal $(3+\sqrt{5})$ is not prime.

   We remark (all these notions will be defined later in the course) that irreducible does not imply prime in a ring that is not factorial or principal.

Exercice 4.
On dit qu'un anneau commutatif A est *Noetherien* si tout idéal de A admet un nombre fini de générateurs.

1. Montrez qu'un anneau commutatif est Noetherien si et seulement si toute chaîne croissante d'idéaux
$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$$
   stabilise.

2. En mettant ensemble les définitions et les théorèmes du cours montrez qu'un anneau intègre et Noetherien est factoriel si et seulement si tout élément irréductible est premier.

3. Montrez qu'un quotient d'un anneau Noetherien est encore Noetherien.

4. Montrez que les anneaux suivants ne sont pas Noetheriens.

   (a) $A[x_1, \dots, x_n, \dots]$ l'anneau de polynôme sur A avec une infinité de variables pour un anneau non-nul A.

   (b) Les fonctions continues $C(X, \mathbb{R})$ où X est un espace topologique compact (=séparé et quasi-compact) infini.

   On pourra prendre une suite convergente avec une infinité de points distincts $(x_n)_{n\in\mathbb{N}}$. *On pourra comprendre comment utiliser le théorème de prolongement de Tietze pour avoir l'existence pour chaque* $n \in \mathbb{N}$ *d'une fonction* $f_n \colon X \to \mathbb{R}$ *avec* $f_n(x_m) = 0$ *si* $m \geq n$ *et* $f_n(x_m) = 1$ *si* $m < n$. *On construira une chaîne infinie d'idéaux qu'on montrera ne pas stabiliser pas à l'aide des fonctions* f_n.

Solution.

Pour le 1. on montre les deux directions. Si tout chaîne stabilise on montre que tout idéal est finement généré. On montre la contraposée. Soit I un idéal pas finement généré. Soit $i_1 \in I$. Alors $(i_1) \subsetneq I$ sinon l'idéal est finement généré. Dès lors il existe $i_2 \in I \setminus (i_1)$. Mais alors $(i_1, i_2) \subsetneq I$ par le même argument. On peut par induction alors créer une chaîne d'idéaux qui ne stabilise pas.

Supposons que tout idéal est finement généré et considérons une chaîne croissante d'idéaux $(I_n)_{n\in\mathbb{N}}$. Une union croissante d'idéaux étant encore un idéal, on considère

$$I_\infty = \bigcup_{n\in\mathbb{N}} I_n$$

Maintenant $I_\infty = (a_1, \dots, a_n)$ comme A est Noetherien. Alors il existe $N \in \mathbb{N}$ avec $a_i \in I_N$ pour tout i. Alors pour tout $n \in \mathbb{N}$ on a

$$I_n \subset I_\infty \subset I_N \subset I_n.$$

ce qui montre que la chaîne stabilise.

Pour le (2), on rappelle qu'un anneau intègre est factoriel si et seulement tout chaîne d'idéaux principaux stabilise, ce qui va être vérifié pour un anneau Noethérien et que tout élément irréductible est premier.

Pour le 3., cela suit du théorème du correspondance.

Pour le 4.(a) on considère la chaîne d'idéaux

$$(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots.$$

Pour le 4.(b). Soit (x_n) une suite infinie d'élément deux à deux distincts de X. Comme X est compact, sans perte de généralité la suite a une limite x. On considère le fermé

$$Z = \{x\} \cup \{x_n\}_{n\in\mathbb{N}}$$

Pour chaque $n \in \mathbb{N}$ on a une décomposition ouverte-fermée de Z

$$Z = Z_{\geq n} \sqcup Z_{<n}$$

avec $Z_{\geq n} = \{x\} \cup \{x_m\}_{m\geq n}$ et $Z_{<n} = \{x_m\}_{m<n}$. Ainsi on peut définir une fonction continue $f'_n \colon Z \to \mathbb{R}$ pour chaque $n \in \mathbb{N}$ avec la propriété que $f'_n(x_m) = 0$ si $m \geq n$ et $f'_n(x_m) = 1$ si $m < n$. Maintenant, en utilisant le théorème de prolongement de Tietze on obtient des fonctions f_n avec la propriété désirée. Maintenant, on voit que la suite croissante d'idéaux $(I_n)_{n\in\mathbb{N}}$ avec

$$I_n = \{f \in C(X, \mathbb{R}) \mid f(x_m) = 0 \mid m \geq n\},$$

ne stabilise.

Remarque. Le dernier point peut être mis en contexte. Remarquons que l'idéal I_n est l'idéal des fonctions qui s'annule sur le fermé $Z_{\geq n}$. En géométrie algébrique cette transition "idéal-fermé" est au cœur de la théorie. Si maintenant on pense à vouloir démontrer qu'il existe une suite croissante infinie d'idéaux, on peut chercher une suite *dé*croissante de fermés infinie. Ensuite on considère les idéaux des fonctions qui s'annule sur ces fermés.

Exercice 5.
Soit A un anneau commutatif Noetherien. Le but de cet exercice est de démontrer que $A[t]$ est Noetherien également. Soit $J \subset A[t]$ un idéal. Le but est de montrer qu'il est finiment généré.

On définit pour $d \in \mathbb{N}$

$$I_d = \{a \in A \mid a \text{ est le coeff. dominant d'un polynôme de degré } d \text{ dans } J\} \cup \{0\}$$

1. Montrer que les I_d sont des idéaux de A et que $I_d \subset I_{d'}$ dès que $d \leq d'$.

2. En utilisant que A est Noetherien, déduire qu'il existe $d_0 \in \mathbb{N}$ tel que J est généré par des polynômes de J de degré $\leq d_0$.

3. Montrez par récurrence sur $d \in \mathbb{N}$ que les polynômes de degré au plus d de J sont générés par un nombre fini d'éléments de J. Montrer cela en utilisant que chaque I_d est finement généré.

4. Conclure.

Solution.

1. Si $a \in I_d$ alors on a $at^d + \cdots \in J$. Si $b \in A$ alors $bat^d + \cdots \in J$ également. On voit similairement que I_d est stable par somme. Si $d \leq d'$ alors soit $a \in I_d$ avec $at^d + \cdots \in J$. Alors $t^{d'-d}(at^d + \dots) \in J$ ce qui montre $a \in J_{d'}$.

2. Comme A est Noetherien la chaîne d'idéaux I_d stabilise. Prenons d_0 avec si $d \geq d_0$ alors $I_d = I_{d_0}$. Soit $f(t) \in J$ de degré d avec $d \geq d_0$. Soit a le coefficient dominant de $f(t)$. Comme $a \in I_d = I_{d_0}$, il existe $g(t) \in J$ de degré d_0 avec comme coefficient dominant a. Alors $f(t) - t^{d-d_0}g(t) \in J$ est de degré strictement plus petit que d. En répétant l'opération, on conclut après un nombre fini d'itérations que $f(t)$ est dans l'idéal généré par les éléments de J de degré d_0.

   On déduit alors que J est généré par les polynômes de J de degré au plus d_0.

3. On montre cela par récurrence. Les polynômes de degré 0 sont égaux à I_0. C'est un idéal finement généré car c'est un idéal de A. On procède maintenant au pas de récurrence. Soit $a_1, \dots, a_r$ des générateurs de I_d. Soit $f_1, \dots, f_r \in J$ de degré d tel que f_i a coefficient dominant a_i pour $i = 1, \dots, r$. Soit $f \in J$ de degré d et notons a son coefficient dominant. Comme $a \in I_d$ on a
$$a = \sum_i b_i a_i$$
   pour des $b_i \in A$. Maintenant $f - \sum_i b_i f_i$ est de degré strictement plus petit que d – ainsi le principe de récurrence conclut.

4. On conclut que J est généré par le nombre fini de générateurs des polynômes en degré $\leq d_0$.