USTC - Feuille de TD 1

Diego Izquierdo

1 Anneaux et morphismes

Exercice 1

1) Trouver un exemple d'anneau non commutatif A, et un élément a de A qui est inversible à gauche mais pas à droite, ou le contraire.
2) Trouver un exemple d'anneau non commutatif A, et un élément a de A qui est un diviseur de zéro à gauche mais pas à droite, ou le contraire.

Exercice 2 Soit $n > 0$ un entier.

1) a) Quels sont les diviseurs de 0 de $\mathbb{Z}/n\mathbb{Z}$?
   b) À quelle condition sur n l'anneau $\mathbb{Z}/n\mathbb{Z}$ est-il intègre ?
2) a) Quels sont les éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$?
   b) On dit qu'un anneau est réduit s'il n'a pas de nilpotents autres que 0. À quelle condition sur n l'anneau $\mathbb{Z}/n\mathbb{Z}$ est-il réduit ?
3) Soit $m > 0$ un entier. Quels sont les morphismes d'anneaux :
   a) de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$?
   b) de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}$?
   c) de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$?
   d) de $\mathbb{Q}$ dans $\mathbb{Z}/n\mathbb{Z}$?

Exercice 3 Le but de cet exercice est de calculer le groupe des unités de l'anneau $\mathbb{Z}[\sqrt{2}]$.

1) Vérifier que $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} | \, a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{R}$.
2) Vérifier que $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}, \quad a + b\sqrt{2} \mapsto a^2 - 2b^2$ est multiplicative. En déduire que les unités de $\mathbb{Z}[\sqrt{2}]$ sont les $a + b\sqrt{2}$ tels que $N(a + b\sqrt{2}) = a^2 - 2b^2 = \acute{s} \pm 1$.
3) Montrer que $(1 + \sqrt{2})^n$ est une unité pour tout $n \in \mathbb{Z}$.
4) Montrer que $1 + \sqrt{2}$ est la plus petite (pour l'ordre usuel de $\mathbb{R}$) unité de $\mathbb{Z}[\sqrt{2}]$ qui soit strictement plus grande que 1.
5) Montrer que $\mathbb{Z}[\sqrt{2}] = \{\pm(1 + \sqrt{2})^k, \, k \in \mathbb{Z}\}$.

Exercice 4 Soit A un anneau commutatif.

1) On suppose A intègre.
   a) Si A est intègre, montrer que l'anneau $A[X]$ des polynômes à une indéterminée à coefficients dans A est aussi intègre.
   b) Si A est intègre, quelles sont les unités de $A[X]$?
2) On ne suppose plus A intègre.

a) On rappelle qu'un élément a de A est dit nilpotent s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$. Soit a un élément nilpotent de A, et soit u une unité de A. Montrer que $u + a$ est inversible.

b) Soit $P = a_0 + a_1X + \ldots + a_NX^N$ un polynôme à coefficients dans A. On suppose que a_0 est inversible et que les éléments $a_1, \ldots, a_N$ sont nilpotents. Montrer que P est inversible dans $A[X]$.

c) Réciproquement, montrer que les les unités de $A[X]$ sont les polynômes $P = a_0 + a_1X + \ldots + a_NX^N$ avec a_0 inversible et $a_1, \ldots, a_N$ nilpotents.

d) Dans $(\mathbb{Z}/324\mathbb{Z})[X]$, combien de polynômes de degré n sont des unités ?

Exercice 5 Montrer que tout anneau commutatif intègre fini est un corps.

Exercice 6 On rappelle qu'un nombre complexe x est un *entier algébrique* s'il existe un polynôme $P \in \mathbb{Z}[X]$ unitaire tel que l'on ait $P(x) = 0$. On note $\overline{\mathbb{Z}}$ l'anneau des entiers algébriques.

1) En exhibant un polynôme annulateur, montrer que le nombre $\sqrt{2} + \sqrt[3]{11}$ est un entier algébrique.
2) Soit $a = \sqrt[3]{2} + \sqrt[3]{3}$. Montrer que $\mathbb{Z}[\sqrt[3]{2}]$ et $\mathbb{Z}[\sqrt[3]{3}]$ sont des groupes abéliens libres de type fini. En déduire qu'il en est de même de $\mathbb{Z}[a]$ puis que a est un entier algébrique.
3) Généraliser le raisonnement précédent pour montrer que $\overline{\mathbb{Z}}$ est un anneau.

2 Sous-anneaux et idéaux

Exercice 7 Soit A un anneau. Soit I un idéal bilatère de A.

1) Montrer que $I = A$ si et seulement si I contient un élément inversible. En déduire que si l'anneau A est à division, alors ses seuls idéaux bilatères sont $\{0\}$ et A.
2) La réciproque est-elle vraie ? On pourra regarder l'exemple de $\mathcal{M}_2(\mathbb{R})$.
3) Et si A est commutatif ?

Exercice 8 Soit A un anneau commutatif.

1) Supposons que A s'écrit sous la forme $A_1 \times .... \times A_n$ où $A_1, ..., A_n$ sont des anneaux non nuls. Montrer que A possède des idempotents non nuls $e_1, ..., e_n$ tels que $e_ie_j = 0$ pour $i \neq j$ et $e_1 + ... + e_n = 1$.
2) Réciproquement, montrer que si A possède des idempotents non nuls $e_1, ..., e_n$ tels que $e_ie_j = 0$ pour $i \neq j$ et $e_1 + ... + e_n = 1$, alors A s'écrit sous la forme $A_1 \times .... \times A_n$ où $A_1, ..., A_n$ sont des anneaux non nuls. Décrire alors les idéaux de A.
3) Soit $m > 0$ un entier. Quel est le plus grand entier n tel qu'il existe des anneaux non nuls A_1, ..., A_n vérifiant $\mathbb{Z}/m\mathbb{Z} = A_1 \times ... \times A_n$?

Exercice 9 Soient $a, b \in \mathbb{Z}$. Donner des générateurs de $(a) + (b)$, de $(a)(b)$ et de $(a) \cap (b)$.

Exercice 10 Soient A un anneau commutatif et I un idéal de A. On appelle radical de I l'ensemble $\sqrt{I} = \{a \in A | \exists n \in \mathbb{N}^*, a^n \in I\}$.

1) Montrer que $\sqrt{I}$ est un idéal.
2) Reconnaître $\sqrt{A}$ et $\sqrt{(0)}$.
3) Soit J un idéal de A. Déterminer si les assertions suivantes sont vraies ou fausses. Corriger celles qui sont fausses.
   (a) $\sqrt{\sqrt{I}} = \sqrt{I}$.
   (b) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.
   (c) $\sqrt{IJ} = \sqrt{I} \cdot \sqrt{J}$.
   (d) $\sqrt{I + J} = \sqrt{I} + \sqrt{J}$.
4) Prenons $A = \mathbb{Z}$ et $I = N\mathbb{Z}$. Calculer $\sqrt{I}$.

Exercice 11 Soient A un anneau commutatif et I et J deux idéaux.

1) On suppose que $I + J = A$. Montrer que $I^n + J^n = A$ pour tout $n > 0$.
2) On suppose que $I + J = A$. Soit L un idéal tel que $IL \subseteq J$. Montrer que $L \subseteq J$.
3) On suppose que $I \cap J = IJ$. A-t'on forcément $I + J = A$?

3 Quotients d'anneaux

Exercice 12 Soit k un corps.

1) Montrer que la k-algèbre $k[X, Y]/(X^2 - Y^3)$ est isomorphe à $k[T^2, T^3]$.
2) Montrer que la k-algèbre $k[X, Y]/(X^2 - Y)$ est isomorphe à $k[T]$.
3) Plus généralement, soient a et b deux entiers naturels non nuls. Réaliser l'anneau $k[T^a, T^b]$ comme quotient de $k[X, Y]$.
4) Montrer que la k-algèbre $k[X, Y]/(XY - 1)$ n'est pas isomorphe à $k[T]$.
5) Réaliser les anneaux $\mathbb{Z}[i\sqrt{7}]$ et $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ comme quotients de $\mathbb{Z}[X]$.

Exercice 13

1) On considère les anneaux :

$$\mathbb{C}[X], \mathbb{R}[X]/(X^2 + X + 1), \mathbb{R}[X]/(X^3 - 6X^2 + 11X - 6), \mathbb{R}[X]/(X^4 - 1).$$

   Déterminer les morphismes de $\mathbb{R}$-algèbres de ces anneaux à valeurs dans $\mathbb{R}$ (resp. $\mathbb{C}$).
2) On considère l'anneau $\mathbb{R}[X]/(X^5)$. Déterminer les morphismes de $\mathbb{R}$-algèbres de cet anneau à valeurs dans $\mathbb{R}$ (resp. $\mathbb{C}$).

Exercice 14

1) Soit k un corps. Montrer qu'il existe une k-algèbre commutative A telle que, pour chaque k-algèbre B, on ait une bijection $\mathrm{Hom}_{k-\mathrm{alg}}(A, B) \cong B^\times$.
2) Même question pour $\mathrm{Hom}_{k-\mathrm{alg}}(A, B) \cong GL_n(B)$.
3) Même question pour $\mathrm{Hom}_{k-\mathrm{alg}}(A, B) \cong \mu_n(B)$ où $\mu_n(B)$ désigne l'ensemble des racines n-ièmes de l'unité dans B.

4 Idéaux premiers et maximaux

Exercice 15 Soit A un anneau commutatif. Montrer l'égalité

$$\bigcup_{\mathfrak{M} \text{ idéal maximal de} A} \mathfrak{M} = A \setminus A^\times.$$

Exercice 16 Soient $f : A \to B$ un morphismes d'anneaux commutatifs. Montrer que l'image réciproque d'un idéal premier de B est un idéal premier de A. Est-ce encore vrai pour un idéal maximal ?

Exercice 17 Soient A un anneau commutatif et I un idéal.

1) Montrer que les idéaux de A/I sont en bijection avec les idéaux de A contenant I.
2) Soit $J \supseteq I$ un idéal de A. Montrer que A/J est canoniquement isomorphe au quotient de A/I par J/I.
3) On dit que I est un idéal premier (resp. maximal) si A/I est intègre (resp. un corps). Montrer que les idéaux premiers (resp. maximaux) de A/I sont en bijection avec les idéaux premiers (resp. maximaux) de A contenant I.
4) Soit $n > 0$ un entier. Quels sont les idéaux de $\mathbb{Z}/n\mathbb{Z}$? Lesquels sont premiers ? Et maximaux ?
5) Déterminer les idéaux des anneaux suivants :

$$\mathbb{R}[X]/(X^2 + X + 1), \mathbb{R}[X]/(X^3 - 6X^2 + 11X - 6), \mathbb{R}[X]/(X^4 - 1), \mathbb{R}[X]/(X^5).$$

   Lesquels sont premiers ? Et maximaux ?
6) Combien l'anneau $\mathbb{R}[X]/(X^5(X^4 - 1))$ possède-t'il d'idéaux ? d'idéaux premiers ? d'idéaux maximaux ?

Exercice 18 Soit A un anneau commutatif.

1) On suppose que A est intègre et ne possède qu'un nombre fini d'idéaux. Montrer que A est un corps.
2) On suppose que A ne possède qu'un nombre fini d'idéaux. Montrer que tout idéal premier est maximal.
3) On suppose que tout idéal propre de A est premier. Montrer que A est un corps.

Exercice 19 Soit A un anneau commutatif.

1) Soient $\mathfrak{p}$ un idéal premier et $I_1, ..., I_n$ des idéaux. On suppose que $\mathfrak{p}$ contient $\prod_{k=1}^n I_k$. Montrer que $\mathfrak{p}$ contient l'un des I_k.
2) Soient I un idéal et $\mathfrak{p}_1, ..., \mathfrak{p}_n$ des idéaux premiers. On suppose que I est contenu dans $\bigcup_{k=1}^n \mathfrak{p}_k$. Montrer que I est contenu dans l'un des $\mathfrak{p}_k$.

Exercice 20 Soit p un nombre premier et soit $\alpha = i\sqrt{p}$. On considère l'anneau $A = \mathbb{Z}[\alpha]$. Montrer que l'idéal (α) de A est $\{a + b\alpha | a \in p\mathbb{Z},\ b \in \mathbb{Z}\}$. En déduire que α est premier dans A.

Exercice 21

1) Soient A un anneau commutatif et I un idéal de A. Notons J l'intersection des idéaux premiers de A contenant I. Le but de cette question est de montrer que $\sqrt{I} = J$.
   (a) Montrer que $\sqrt{I}$ est contenu dans J.
   (b) Réciproquement, soit $a \in A \setminus \sqrt{I}$, et considérons $\mathcal{E}$ la famille constituée des idéaux qui contiennent I mais qui ne contiennent aucune puissance de a. Montrer que $\mathcal{E}$ possède un élément maximal (pour l'inclusion), qui est un idéal premier de A. En déduire que $a \notin J$.
   (c) Conclure.

Soit $\mathcal{C}$ l'anneau des fonctions continues de $[0,1]$ dans $\mathbb{R}$.

2) Montrer que les idéaux maximaux de $\mathcal{C}$ sont les
$$I_x = \{f \in \mathcal{C} \mid f(x) = 0\}$$
pour $x \in [0,1]$.
3) Soit $I = \{f \in \mathcal{C} \mid \forall m \in \mathbb{N}, \lim_{x\to 0} \frac{f(x)}{x^m} = 0\}$. Montrer que $I = \sqrt{I}$ (on dit que I est un idéal radical). L'idéal I est-il premier ?
4) En déduire que $\mathcal{C}$ possède des idéaux premiers non maximaux.

5 Unités de $\mathbb{Z}/n\mathbb{Z}$

Exercice 22 Dans cet exercice, nous voulons étudier la structure du groupe des unités d'un groupe cyclique. On rappelle que tout sous-groupe fini du groupe des unités d'un corps est cyclique. Cela entraîne en particulier que $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ pour tout nombre premier p.

1) Rappeler quel est l'ordre de $(\mathbb{Z}/n\mathbb{Z})^\times$.
2) Soient p un nombre premier impair et $m > 1$ un entier.
   (a) Montrer que $(1+p)^{p^{m-2}} \equiv 1 + p^{m-1} \mod p^m$, puis que $1+p$ est d'ordre p^{m-1} dans $(\mathbb{Z}/p^m\mathbb{Z})^\times$.
   (b) En déduire que le noyau de la projection naturelle $(\mathbb{Z}/p^m\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ est isomorphe à $\mathbb{Z}/p^{m-1}\mathbb{Z}$.
   (c) Montrer qu'il existe $x_0 \in (\mathbb{Z}/p^m\mathbb{Z})^\times$ d'ordre $p-1$.
   (d) Montrer que $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z} \to (\mathbb{Z}/p^m\mathbb{Z})^\times, (a,b) \mapsto x_0^a(1+p)^b$ est un isomorphisme. En déduire que $(\mathbb{Z}/p^m\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p^{m-1}\mathbb{Z}$.
3) Soit $m > 2$ un entier.
   (a) Montrer que $5^{2^{m-3}} \equiv 1 + 2^{m-1} \mod 2^m$, puis que 5 est d'ordre 2^{m-2} dans $(\mathbb{Z}/2^m\mathbb{Z})^\times$.
   (b) En déduire que le noyau de la projection naturelle $(\mathbb{Z}/2^m\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$ est isomorphe à $\mathbb{Z}/2^{m-2}\mathbb{Z}$.
   (c) En s'inspirant de la question 2.(d), montrer que $(\mathbb{Z}/2^m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$.
4) Quelle est la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$? Quand ce groupe est-il cyclique ?

Exercice 23

1. Donner un générateur du groupe $(\mathbb{Z}/162\mathbb{Z})^\times$.
2. Donner un élément d'ordre maximal dans $(\mathbb{Z}/2592\mathbb{Z})^\times$.