M64 : Groupes, anneaux, corps 2

Licence de Mathématiques L3 S6 – Université de Lille – Année 2020-2021

Feuille de TD 2. Anneaux

Exercice 1. Pour un anneau K, démontrez l'équivalence des propriétés suivantes :

1. K est un corps.
2. $K \neq \{0\}$ et les idéaux de K sont $\{0\}$ et K.

Exercice 2. Soient A un anneau, I un idéal de A et $\pi : A \to A/I$ la surjection canonique.

1. Montrer que pour un morphisme d'anneaux $\varphi : A \to B$, l'image réciproque de chaque idéal de B est un idéal de A, mais l'image d'un idéal de A n'est pas forcément un idéal de B.
2. Montrer que si J est un ideal de A, alors $\pi(J)$ est un idéal de A/I.
3. Montrer que A/I est un corps si et seulement si I est un idéal maximal.

Exercice 3. Montrer qu'un anneau fini est intègre si et seulement si il est un corps.

Exercice 4. (i) Montrer que le produit direct de deux anneaux non nuls n'est pas intègre.

(ii) Donner un exemple d'un anneau non intègre qui ne soit pas isomorphe au produit de deux anneaux non nuls.

(iii) Soient A un anneau et I un idéal de A. Montrer que A/I est intègre si et seulement si I est un idéal premier.

(iv) Montrer que tout idéal maximal est premier et donner un exemple d'un idéal premier non maximal.

(v) Pour un idéal non nul I d'un anneau principal A, démontrer les équivalences suivantes :

$$I \text{ premier} \iff I \text{ maximal} \iff I = (a) \text{ pour un élément irréductible } a \text{ de } A.$$

Exercice 5. (i) Montrer que pour tout anneau intègre A, l'ensemble des éléments inversibles de $A[X]$ coïncide avec $A^\times$.

(ii) Donner un contre-exemple à (i) sans l'hypothèse que A soit intègre.

Exercice 6. Décrire les idéaux maximaux des anneaux $\mathbb{C}[X]$, $\mathbb{R}[X]$, $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$.

Exercice 7. Soient A un anneau et $I_1, \dots, I_n$ des idéaux de A tels que $I_i + I_j = A$ pour tous i, j, $1 \leq i < j \leq n$. Démontrer les généralisations suivantes du lemme chinois :

1. $A/I_1 \cap \ldots \cap I_n = A/I_1 \ldots I_n \simeq A/I_1 \times \ldots \times A/I_n$;
2. $A/I_1^{m_1} \cap \ldots \cap I_n^{m_n} = A/I_1^{m_1} \ldots I_n^{m_n} \simeq A/I_1^{m_1} \times \ldots \times A/I_n^{m_n}$ pour tous $m_1 \geq 1, \dots, m_n \geq 1$.

Exercice 8. Expliciter l'antécédent $x \in A/I_1 \ldots I_n$ d'un élément $(a_1, \dots, a_n) \in A/I_1 \times \ldots \times A/I_n$ par l'isomorphisme du lemme chinois généralisé de l'exercice précédent dans les exemples suivants :

1. $n = 3$, $A = \mathbb{Z}$, $I_1 = (17)$, $I_2 = (11)$, $I_3 = (8)$, $(a_1, a_2, a_3) = (6 + I_1, 4 + I_2, -3 + I_3)$;
2. $A = \mathbb{R}[X]$, $I_k = (X - t_k)$, $a_k = y_k + I_k$, $k = 1, \dots, n$, où $(t_1, \dots, t_n)$, $(y_1, \dots, y_n) \in \mathbb{R}^n$ et $t_1, \dots, t_n$ sont disctincts.

Exercice 9. Démontrer : (a) $\mathbb{Q}[X]/(X^2-1) \simeq \mathbb{Q}\times\mathbb{Q}$; (b) de façon plus générale, pour tout corps K et pour tout polynôme P de $K[X]$ de degré n ayant n racines distinctes dans K, on a $K[X]/(P) \simeq K^n$ (produit direct de n copies de l'anneau K).

Exercice 10. Les anneaux A, B sont-ils isomorphes ? Si c'est oui, donner explicitement un isomorphisme.

1. $A = \mathbb{R}[X]/(X^2+1)$, $B = \mathbb{R}[X]/(X^2+X+1)$;
2. $A = \mathbb{C}[X]/(X-1)^2$, $B = \mathbb{C}[X]/(X^2-1)$;
3. $A = \mathbb{C}[X,Y]/(X-Y, XY-1)$, $B = \mathbb{C}[X]/(X^2-1)$;
4. $A = \mathbb{C}[X,Y]/(X-Y^m)$, $B = \mathbb{C}[X]/(Y-X^n)$;
5. $A = \mathbb{C}[X,Y]/(X^2-Y^3)$, $B = \mathbb{C}[X]/(X^2-Y^4)$.

Exercice 11. (i) Soit B un anneau, $A\subset B$ un sous-anneau. On dit qu'un élément b de B est entier sur A s'il existe un polynôme unitaire $P\in A[X]$ tel que $P(b)=0$. Montrer que l'ensemble $\hat{A}$ des éléments de B entiers sur A est un sous-anneau de B contenant A. Ce sous-anneau s'appelle fermeture intégrale de A dans B. *Indication : truc déterminantal.* 1) Si $a,b\in\hat{A}$ et $P,Q\in A[X]$ sont des polynômes unitaires de degrés respectifs m,n tels que $P(a)=Q(b)=0$, alors $A[a,b]=Az_1+\ldots+Az_N$, où $N=mn$ et $(z_i)_{i=1,\ldots,N}$ est la famille $(a^ib^j)_{0\le i<m, 0\le j<n}$, renumérotée par un indice simple. 2) Pour tout $x\in A[a,b]$, il existe $c_{ij}\in A$ tels que $xz_j=\sum_{i=1}^N c_{ij}z_i$, $1\le j\le N$, de sorte que la matrice $M=(x\delta_{ij}-c_{ij})\in M_N(A)$ satisfait à $(z_1\ldots z_N)M=(0\ldots 0)\in A^n$. 3) Multiplier à droite par $\operatorname{comat}(M)$ pour voir que $\det M=0$, ce qui donne un polynôme unitaire de $A[X]$ annulant x ; l'application de ce truc à $x=a-b$ et à $x=ab$ permet de conclure.

(ii) Soient A,C des anneaux tels que $A\subset C$. On dit que C est fini sur A s'il existe $x_1,\ldots,x_r\in C$ tels que $C=Ax_1+\ldots+Ax_r$. Dans les notations du point (i), montrer que tout sous-anneau de B, fini sur A, est contenu dans $\hat{A}$, et en déduire que $\hat{\hat{A}}=\hat{A}$.

(iii) Au cas où A est intègre et $B=K$ est le corps des fractions de A, $\hat{A}$ est appelé clôture intégrale de A. Si $\hat{A}=A$, on dit que A est intégralement clos. Montrer que tout anneau factoriel est intégralement clos.

(iv) Soit $d\in\mathbb{Z}^*\smallsetminus\{1\}$ sans carrés, c'est à dire, p^2 ne divise d pour aucun premier p, et soit K_d le corps quadratique $\mathbb{Q}[\sqrt{d}]=\mathbb{Q}+\mathbb{Q}\sqrt{d}$. Si $d<0$, le symbole $\sqrt{d}$ désigne le nombre complexe $i\sqrt{|d|}$. On note σ l'automorphisme involutif de K_d défini par $a+b\sqrt{d}\mapsto a-b\sqrt{d}$, où $a,b\in\mathbb{Q}$, et on définit les applications de la norme et de la trace :

$$\operatorname{tr} : K_d \to K_d\ ,\quad z\mapsto z+\sigma(z),$$

$$N : K_d\to K_d\ ,\quad z\mapsto z\sigma(z).$$

Les éléments de K_d entiers sur $\mathbb{Z}$ sont appelés entiers de K_d ; l'anneau $\mathfrak{o}_d$ des entiers de K_d n'est autre que la fermeture intégrale de $\mathbb{Z}$ dans K_d. Démontrer :

(a) $\mathfrak{o}_d=\{z\in K_d \mid \operatorname{tr}(z)\in\mathbb{Z},\ N(z)\in\mathbb{Z}\}$.

(b) Si $d\not\equiv 1 \bmod 4$, alors $\mathfrak{o}_d=\mathbb{Z}+\mathbb{Z}\sqrt{d}$.

(c) Si $d\equiv 1\bmod 4$, alors

$$\mathfrak{o}_d=\mathbb{Z}+\mathbb{Z}\tfrac{1+\sqrt{d}}{2}=\left\{\frac{n_1+n_2\sqrt{d}}{2}\ \middle|\ (n_1,n_2)\in\mathbb{Z}^2,\ n_1\equiv n_2 \bmod 2\right\}.$$

(d) L'anneau $\mathfrak{o}_d$ est euclidien de stathme $\varphi : \mathfrak{o}_d \to \mathbb{N},\ z \mapsto |N(z)|$ si

$$d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 13\}.$$

Remarque. Cette liste n'est pas exhaustive. Pour une liste complète, il faut rajouter $d = 6, 7, 11, 17, 19, 21, 29, 33, 37, 41, 57, 73,$ mais la démonstration de la propriété euclidienne pour ces valeurs de d nécessite des arguments plus astucieux que ceux dont l'usage est supposé dans cet exercice.

Exercice 12. Trouver les éléments inversibles des anneaux $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{3}]$, $\mathbb{Z}[j]$ et $\mathbb{Z}[\sqrt{2}]$, où $j = e^{\frac{2\pi i}{3}}$. *Indication.* Montrer qu'un élément de chacun des anneaux donnés est inversible si et seulement si sa norme vaut ± 1.

Exercice 13. Soit A un anneau intègre, $a, b, c \in A,\ abc \neq 0$. Démontrer :
(i) p.g.c.d. $(a, b) \sim a \iff a|b$.
(ii) p.g.c.d. $(ta, tb) \sim t$p.g.c.d. (a, b) $\forall t \in A, t \neq 0$, si les deux p.g.c.d. existent.
(iii) p.g.c.d. (p.g.c.d. $(a, b), c) \sim$ p.g.c.d. $(a,$ p.g.c.d. $(b, c))$.
Soit A en plus factoriel. Alors :
(iv) Si p.g.c.d. $(a, b) \sim 1$ et p.g.c.d. $(a, c) \sim 1$, alors p.g.c.d. $(a, bc) \sim 1$.
(v) Si $a|bc$ et p.g.c.d. $(a, b) \sim 1$, alors $a|c$.
(vi) Si $b|a$, $c|a$ et p.g.c.d. $(b, c) \sim 1$, alors $bc|a$.

Exercice 14. (a) Trouver toutes les factorisations de 4 en irréductibles dans l'anneau $A = \mathbb{Z}[i\sqrt{3}]$. En déduire que $\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel.
(b) Montrer, que les propriétés (iv)-(vi) du p.g.c.d. (Exercice 13) ne sont pas vérifiées dans $\mathbb{Z}[i\sqrt{3}]$.
(c) Trouver trois éléments non-nuls a, b, t de A, tels que p.g.c.d.(a, b) existe, mais p.g.c.d.(ta, tb) n'existe pas.
(d) Donner un exemple d'un idéal principal non premier, engendré par un élément irréductible de A.
(e) Donner un exemple d'un idéal non principal de A.

Exercice 15. (i) Montrer que tout anneau euclidien A possède un stathme δ qui peut être étendu en 0 de telle façon qu'il satisfasse à la condition :

$$\text{(a)} \qquad \forall\ (a, b) \in A \times A^* \ \exists\ (q, r) \in A \times A, \big(a = qb + r,\ \delta(r) < \delta(b)\big).$$

Un tel stathme étendu est dit total.
(ii) On peut munir l'ensemble $\mathscr{E}$ des stathmes totaux $\delta : A \to \mathbb{N}$ d'une relation d'ordre partielle comme suit : $\delta_1 \leq \delta_2$ si $\forall a \in A,\ \delta_1(a) \leq \delta_2(a)$. Montrer que $\mathscr{E}$ possède le plus petit élément δ, et que ce plus petit stathme total satisfait aux conditions suivantes :

$$\text{(b)} \qquad \delta(0) = 0, \big(\forall u \in A^\times,\ \delta(u) = 1\big),\ \text{et}\ \big(\forall\ (a, b) \in A^* \times A^*,\ \delta(ab) \geq \delta(a)\big).$$

Un stathme satisfaisant à (a) et (b) est dit normalisé. *Indication.* Considérer la suite croissante $(A_n)_{n\mathbb{N}}$ de parties de A, définie de façon récurrente par

$$A_0 = \{0\},\ A_{n+1} = A_n \cup \{x \in A \mid (x) + A_n = A\} \text{ pour } n \geq 0;$$

montrer que pour tout stathme total $\varphi \in \mathscr{E}$, $\varphi(x) = n \implies x \in A_n$; en déduire que $A = \cup_{n\in\mathbb{N}} A_n$ et que $\delta(x) = \min\{n \in \mathbb{N} \mid x \in A_n\}$ pour tout $x \in A$.

(iii) Présenter un stathme normalisé sur $\mathbb{C}[X]$.
(iv) Montrer que le plus petit stathme total sur $\mathbb{Z}$ est donné par $\delta(0) = 0$ et $\delta(n) = \mathbb{E}(\log_2 |n|)+1$ pour tout $n \neq 0$, où $\mathbb{E}$ désigne la partie entière.

Exercice 16. Soient A un anneau et S une partie multiplicative (c'est à dire, stable par multiplication) de A, contenant 1 et ne contenant pas 0. Alors le localisé $S^{-1}A$ de A suivant S est défini comme le quotient du produit cartésien $S \times A$ par la relation d'équivalence

$$(s, a) \sim (s', a') \iff \exists t \in S, ts'a = tsa'.$$

La classe d'équivalence d'une paire (s, a) est notée $\frac{a}{s}$; $S^{-1}A$ a une structure naturelle d'un anneau, et l'application naturelle $\varphi = \varphi_S : A \to S^{-1}A$, $a \mapsto \frac{a}{1}$ est un morphisme d'anneaux possédant la propriété universelle suivante : pour tout morphisme d'anneaux $f : A \to B$ tel que $f(S) \subset B^{\times}$, il existe un unique morphisme d'anneaux $g : S^{-1}A \to B$ tel que $f = g\varphi$, et on a :

$$\forall s \in S\ \forall a \in A,\ g\left(\tfrac{a}{s}\right) = f(s)^{-1}f(a).$$

Lorsque S contient des diviseurs de 0, φ est non injectif : $\ker\varphi = \{a \in A \mid \exists s \in S, sa = 0\}$. Au cas où A est supposé intègre, la définition de la relation d'équivalence peut être simplifiée :

$$(s, a) \sim (s', a') \iff s'a = sa';$$

dans ce cas φ est injectif et $S^{-1}A$ est un sous-anneau du corps des fractions $\mathrm{Fr}(A) = T^{-1}A$, où $T = A \setminus \{0\}$.

1. On définit le saturé de S par $\hat{S} = \{x \in A \mid \exists s \in S,\ x \text{ divise } s\}$. Montrer que l'application naturelle $\varphi_{S,\hat{S}} : S^{-1}A \to \hat{S}^{-1}A$, $\frac{a}{s} \mapsto \frac{a}{s}$ est un isomorphisme d'anneaux.
2. Pour un idéal I de A, on définit son localisé suivant S par $S^{-1}I = \{\frac{a}{s} \mid s \in S, a \in I\}$. Montrer : (a) $J = S^{-1}I$ est un idéal de $S^{-1}A$ et $\varphi^{-1}(J) = \hat{I} \supset I$ est le plus grand idéal de A dont le localisé est J ; (b) $S^{-1}I = S^{-1}A$ si et seulement si $I \cap S \neq \varnothing$; (c) dans le cas où $I \cap S = \varnothing$, I est premier $\iff$ $S^{-1}I$ est premier ; (d) l'application $I \mapsto S^{-1}I$ induit une bijection de l'ensemble des idéaux premiers de A tels que $I \cap S = \varnothing$ sur l'ensemble des idéaux premiers de $S^{-1}A$.
3. Montrer que si $P \subset A$ est un idéal premier, alors $S_P = A \setminus P$ est une partie multiplicative, contenant 1 et ne contenant pas 0, et le localisé $S_P^{-1}A$ possède un unique idéal maximal. Ce localisé s'appelle *localisé de A en P*. Un anneau possédant un unique idéal maximal est dit local (ce qui explique le terme « localisé »).
4. Montrer que si A est factoriel, alors $S^{-1}A$ l'est aussi (on pourra se ramener au cas ou $\hat{S} = S$).
5. Montrer que si A est euclidien, $S^{-1}A$ aussi.
6. Soit $\Bbbk$ un corps. Donner une définition de l'anneau des polynômes de Laurent $\Bbbk[X, X^{-1}]$ en une variable comme l'anneau des suites $(a_n)_{n\in\mathbb{Z}}$ d'éléments de $\Bbbk$ presque nulles, puis établir un isomorphisme naturel de cet anneau avec le localisé $S^{-1}A$ pour $A = \Bbbk[X]$, $S = \{1, X, X^2, \ldots\} = \{X^n\}_{n\in\mathbb{N}}$ et montrer que $\Bbbk[X, X^{-1}]$ est euclidien.
7. L'anneau total des fractions $\mathrm{Fr}\,A$ de A est défini comme le localisé $S^{-1}A$, où S est l'ensemble de tous les éléments non nuls de A qui ne sont pas des diviseurs de zéro. Montrer que si A est factoriel et $f \in A$ est un élément non inversible, alors $\mathrm{Fr}\,(A/(f))$ est produit direct d'un nombre fini de corps.
8. Soient L un corps, A un sous-anneau de L, S une partie multiplicative de A contenant 1 et ne contenant pas 0. Si $\tilde{A}$ est la fermeture intégrale de A dans L, alors $S^{-1}\tilde{A}$ est la fermeture intégrale de $S^{-1}A$ dans L. En particulier, le localisé de la clôture intégrale de A est la clôture intégrale du localisé de A.