Devoir maison

(à rendre le lundi 3 novembre 2014)

Solution proposée

Autour des p. g. c. d. et p. p. c. m. On observera les équivalences $i \in I \iff (i) \subset I$ pour tout idéal $I \subset A$ et tout $i \in A$.

1. Écrivons $a = u\prod p^{\alpha_p}$ et $b = v\prod p^{\beta_p}$ où les p sur lesquels portent les produits sont des irréductibles deux à deux non associés. Alors des p. g. c. d. et p. p. c. m. de a et b sont respectivement $\prod p^{\min\{\alpha_p,\beta_p\}}$ et $\prod p^{\max\{\alpha_p,\beta_p\}}$. Cet argument n'est pas valide si a ou b est nul (l'existence d'une décomposition ne s'applique pas à 0), auquel cas $a \vee b = 0$ (tout multiple commun de a et b est alors multiple de 0, donc est nul) et $a \wedge 0 = a$ et $0 \wedge b = b$ (les éléments divisant 0 formant tout A, intersecter ce dernier avec l'ensemble des diviseurs de a ou de b ne change rien).

2. On a les équivalences

$$\begin{aligned} m \text{ est un multiple commun de } a \text{ et } b &\iff a \mid m \text{ et } b \mid m \\ &\iff (m) \subset (a) \text{ et } (m) \subset (b) \\ &\iff (m) \subset (a) \cap (b)\,, \end{aligned}$$

d'où l'on déduit les équivalences

$$\begin{aligned} m \text{ divise tout multiple commun de } a \text{ et } b &\iff \forall x \in A,\ (x) \subset (a) \cap (b) \Longrightarrow (x) \subset (m) \\ &\overset{\text{car } (a)\cap(b) \text{ et } (m) \text{ sont stables par homothétie}}{\iff} \forall x \in A,\ x \in (a) \cap (b) \Longrightarrow x \in (m) \\ &\iff (a) \cap (b) \subset (m)\,. \end{aligned}$$

On conclut en remarquant que m est un p. p. c. m. de a et de b ssi $\begin{cases} m \text{ est un multiple commun de } a \text{ et } b \\ m \text{ divise tout multiple commun de } a \text{ et} \end{cases}$.

3. On a les équivalences

$$\begin{aligned} d \text{ est un diviseur commun de } a \text{ et } b &\iff d \mid a \text{ et } d \mid b \\ &\iff (a) \subset (d) \text{ et } (b) \subset (d) \\ &\overset{\text{car } (d) \text{ est stable par } +}{\iff} (a) + (b) \subset (d)\,, \end{aligned}$$

d'où l'on déduit l'équivalence

$$\text{tout diviseur commun de } a \text{ et } b \text{ divise } d \iff \forall x \in A,\ (a) + (b) \subset (x) \Longrightarrow (d) \subset (x)\,.$$

On conclut en remarquant que d est un p. g. c. d. de a et de b ssi $\begin{cases} d \text{ est un diviseur commun de } a \text{ et } b \\ \text{tout diviseur commun de } a \text{ et } b \text{ divise } d \end{cases}$.

Lorsque $A = \mathbf{Q}[X,Y]$ et $(a,b) = (X,Y)$, les éléments a et b sont étrangers mais pourtant la somme $(a) + (b) = XA + YA$ ne contient aucun polynôme constant non nul (car tous les éléments de $(a) + (b)$ s'annulent en $(0,0)$), ce qui montre l'inclusion stricte $(a) + (b) \subsetneq (1)$.

4. [micro-analyse : si d est un p. g. c. d. de a et b, on doit avoir $ab \sim dm$, d'où $d \sim \frac{ab}{m}$] Puisque ab est multiple commun à a et b, il est multiple de m.

Regardons d'abord le cas $m = 0$. Alors ab est multiple de 0, donc nul, d'où (par intégrité de A) la nullité de a ou b : si $b = 0$, alors a est un p. g. c. d. de 0 et a ; même argument si $a = 0$.

On supposera à présent a et b non nuls. Le quotient $\delta := \frac{ab}{m}$ (élément de $\operatorname{Frac} A$) fait alors sens est reste dans A. Les égalités $a = \frac{ab}{b} = \frac{ab}{m}\frac{m}{b} = \delta\frac{m}{b}$ et $b = \delta\frac{m}{a}$ montrent que δ divise a et b. On a par ailleurs les équivalences (à $x \in A$ non nul[1])

$$\begin{cases} x \mid a \\ x \mid b \end{cases} \iff \begin{cases} a \mid \frac{\alpha b}{x} \\ b \mid \frac{a\alpha}{x} \end{cases} \iff m \mid \frac{\alpha b}{x} \iff x \mid \frac{ab}{m} = \delta, \quad \begin{matrix} \text{ce qui montre que } \delta \text{ est} \\ \text{un p. g. c. d. de } a \text{ et } b. \end{matrix}$$

[1] Lorsque x est nul, les divisibilités $x \mid a, b$ impliquent les nullités de a et b et de même la divisibilité $x \mid \delta = \frac{ab}{m}$ implique la nullité de ab ; vu que nous avons exclu ces nullités, l'équivalence affirmée est maintenue.

Montrons les distributivités. Soit $\lambda \in A$. On a les égalités

$$(\lambda a) \cap (\lambda b) \overset{\text{car } A \text{ est}}{\underset{\text{intègre}}{=}} \lambda\left((a) \cap (b)\right) = \lambda\,(m) = (\lambda m)\,,$$

ce qui montre (d'après la question 2) que λm est un p. p. c. m. de λa et λb. On en déduit (d'après le début de la question) que ces derniers admet un p. g. c. d. Δ vérifiant $\lambda a\ \lambda b \sim \lambda m\ \Delta$, d'où (si $\lambda m \neq 0$) $\Delta \sim \lambda \frac{ab}{m} = \lambda\delta$. Reste le cas pénible $\lambda m = 0$. Lorsque $\lambda = 0$, on a (*modulo* $\sim$) les égalités $\Delta \sim \lambda a \wedge \lambda b = 0 \wedge 0 = 0 = \lambda\delta$. Lorsque $m = 0$, on a comme ci-dessus $a = 0$ ou $b = 0$, mettons $b = 0$, et alors a est un p. g. c. d. de 0 et a tout comme λa est un p. g. c. d. de $\lambda 0$ et λa. Dans les deux cas, (*modulo* $\sim$) l'égalité $\Delta \sim \lambda\delta$ est assurée.

Sanity check : $(\lambda a) + (\lambda b) = \lambda\,(a) + \lambda\,(b) = \lambda\,[(a) + (b)] = \lambda\,(d) = (\lambda d)$.

5. Soit d un p. g. c. d. de a et b. Alors $\frac{ab}{d} = a\frac{b}{d} = \frac{a}{d}b$ fait sens et est un multiple commun de a et b. Soit x un multiple commun de a et b. Si $x \mid ab$, alors $\frac{ab}{x}$ fait sens et est (comme ci-dessus) un diviseur commun de a et b, d'où $\frac{ab}{x} \mid d$, *i. e.* $\frac{ab}{d} \mid x$, *i. e.* $m \mid x$. Sinon, on passe par un $x \wedge ab$ (autorisé par hypothèse) : ce dernier divise ab, il s'écrit[2] $a\left(\frac{x}{a} \wedge b\right) = b\left(\frac{x}{b} \wedge a\right)$ et est donc un multiple commun de a et b. On peut par conséquent appliquer ce qui précède et obtenir $m \mid (x \wedge ab) \mid x$.

Remarque. On bien utilisé l'hypothèse que tout couple admettait un p. g. c. d., pas seulement a et b. Et pour cause : si $A = \mathbf{Z}\left[i\sqrt{5}\right]$, $a = 2$ et $b = 1 - i\sqrt{5}$, alors a et b admettent un p. g. c. d. (ils sont irréductibles) mais n'admettent pas de p. p. c. m.

Remonter depuis l'unicité des facteurs irréductibles.

1. Supposons que A vérifie le lemme d'Euclide. On raisonne par récurrence sur le nombre de facteurs irréductibles. Nous présentons ici *juste pour l'exemple* une preuve extrêmement détaillée – beaucoup trop pour une rédaction de croisière, pour laquelle est adaptée la preuve du cours traitée dans le cas $A = \mathbf{Z}$.

Notons $\mathbf{P}$ l'ensemble des irréductibles de A. Soit[3] $u \in A^\times$. Pour tout naturel n, on note U_n l'énoncé

$$\begin{array}{c}\forall v \in A^\times,\ \forall r \in \mathbf{N},\\ \forall\,(\overrightarrow{p}, \overrightarrow{q}) \in \mathbf{P}^n \times \mathbf{P}^r,\end{array} \quad \left[u\prod_{i=1}^{n} p_i = v\prod_{j=1}^{r} q_j\right] \Longrightarrow \left[n = r \text{ et } \exists\sigma \in \mathfrak{S}_n,\ \forall i \in \{1,2,...,n\}\,,\ q_i \sim p_{\sigma(i)}\right].$$

Montrons U_0. Soient $v \in A^\times$, $r \in \mathbf{N}$ et $(\overrightarrow{p}, \overrightarrow{q}) \in \mathbf{P}^0 \times \mathbf{P}^r$ tels que $u\prod_{i=1}^{0} p_i = v\prod_{j=1}^{r} q_j$. Le membre de gauche vaut u (le produit est vide), donc est inversible, donc le membre de droite aussi, *a fortiori* tous ses diviseurs ; or aucun q_j n'est inversible (ils sont irréductibles), il n'y en a donc aucun, ce qui force $r = 0$. Montrons l'autre partie de la conjonction souhaitée, à savoir[4] $\exists\sigma \in \mathfrak{S}_0,\ \forall i \in \{1,2,...,0\}\,,\ q_i = p_{\sigma(i)}$. La quantification $\forall i \in \emptyset$ étant tautologique, il revient à montrer $\exists\sigma \in \mathfrak{S}_0$, ce qui est vrai puisque $\mathfrak{S}_0$ contient au moins l'application vide.

Soit $n \in \mathbf{N}$ tel que U_n. Montrons U_{n+1}. Soient $v \in A^\times$, $r \in \mathbf{N}$, $(\overrightarrow{p}, p) \in \mathbf{P}^{n+1}$ et $\overrightarrow{q} \in \mathbf{P}^r$ tels que $u\prod_{i=1}^{n+1} p_i = v\prod_{j=1}^{r} q_j$. L'irréductible p divise le membre de gauche, donc celui de droite, donc (par Euclide) divise ou bien v (mais il serait alors inversible comme tout diviseur d'un inversible, ce qui est exclu puisque p est irréductible) ou bien l'un des q_j : on a donc $r \geq 1$ et l'on peut invoquer un $k \in \{1,2,...,r\}$ tel que $p \mid q_k$. Puisque q_k est également irréductible, cette divisibilité devient une égalité *modulo* $\sim$. Soit π une bijection $\{1,2,...,r-1\} \xrightarrow{\sim} \{1,2,...,r\}\setminus\{k\}$. Définissons $\begin{cases} Q := q \circ \pi \text{ dans } \mathbf{P}^{r-1} \\ V := v\frac{q_k}{p} \text{ dans } A^\times \end{cases}$. Simplifier l'égalité $u\prod_{i=1}^{n+1} p_i = v\prod_{j=1}^{r} q_j$ par p (on peut car p est non nul et A intègre) donne[5] $u\prod_{i=1}^{n} p_i = V\prod_{j=1}^{r-1} Q_j$. D'après U_n, on peut affirmer $n = r - 1$ et invoquer un $\sigma \in \mathfrak{S}_n$ tel que $\forall i \in \{1,2,...,n\}\,,\ Q_i \sim p_{\sigma(i)}$, ce qui se réécrit $\forall i \in \{1,2,...,n\}\,,\ q_{\pi(i)} \sim p_{\sigma(i)}$, ou encore $\forall j \in \{1,2,...,n+1\}\setminus\{k\}\,,\ q_j \sim p_{\sigma(\pi^{-1}(j))}$. En complétant la bijection $\sigma \circ \pi^{-1} : \{1,2,...,n+1\}\setminus\{k\} \xrightarrow{\sim} \{1,2,...,n\}$ par $k \mapsto n+1$, on définit une permutation Σ de $\{0,1,...,n\}$ qui convient (puisque $q_k \sim p = p_{n+1}$).

[2] l'écriture $\frac{x}{a}$ dénote tout λ tel que $x = \lambda a$: elle est donc légtime – bien qu'abusive – lorsque $a = 0 = x$

[3] On serait tenté d'alléger la rédaction en fixant les *deux* inversibles des deux décompositions. Une note prochaine explique pourquoi on ne peut pas se passer de quantifier sur au moins l'un d'entre eux.

[4] on le montre vraiment uniquement pour la forme

[5] Ici apparaît la raison (subtile) pour laquelle on ne peut pas se passer de quantifier sur u ou sur v dans l'énoncé U_n. On serait tenter d'y échapper en gardant *les mêmes* u et v quand on descend "au rang d'avant", ce qui suppose d'envoyer l'inversible $\frac{p}{q_k}$ dans les $p_{i\leq n}$ ou les $q_{j\neq k}$ (par exemple en définissant $p'_1 := p_1\frac{p}{q_k}$ et $p'_{i>1} := p_i$). Or, si n est nul (ce qui est possible puisqu'on l'a invoqué dans $\mathbf{N}$), il n'y a aucun $p_{i\leq n}$ ou $q_{j\neq k}$! (Un produit vide vaut 1 et non l'inversible de notre choix.) C'est cette même raison qui fait que, dans la définition d'un anneau factoriel, *on ne doit pas oublier les inversibles* comme facteur possible devant les irréductibles. (Sinon, les produits d'irréductibles – même vides – rateront les inversibles autres que 1.)

2. Supposons le théorème de Gauss vérifié dans A. Soient $a, b, p \in A$ avec p irréductible et divisant ab. Si p ne divise pas a, alors ils sont étrangers, d'où (d'après Gauss) l'implication $p \mid ab \implies p \mid b$, ce qui conclut par disjonction des cas.

3. Supposons le théorème de Gauss 1. Soient $d, d', a \in A$ où d et d' sont deux diviseurs de a étrangers. Soit $\lambda \in A$ tel que $\lambda d = a$. Alors d' divise λd, donc (par Gauss 1) d' divise λ : soit $\mu \in A$ tel que $\lambda = \mu d'$. On obtient alors $a = \lambda d = \mu d' d$, ce qui montre que dd' divise a.

   Supposons le théorème de Gauss 2. Soient $d, a, b \in A$ où d est un diviseur de ab étranger à a. Alors a et d divisent tous deux ab, donc (par Gauss 2) leur produit le divise : soit λ tel que $ab = \lambda ad$. Lorsque a est non nul, l'intégrité de A permet de simplifier par a, ce qui donne $b = \lambda d$, d'où la divisibilité $d \mid b$. Sinon, d divise trivialement $0 = a$, donc l'extranéité de a et d impose l'inversibilité du divisieur commun d, d'où on tire immédiatement la divisibilité $d \mid b$.

4. Soient $d, a, b \in A$ où d est un diviseur de ab étranger à a. Soit $d' \in A$ tel que $ab = d'd$.

   Supposons que tout couple de A^2 admet un p. g. c. d. On peut alors écrire

$$d' = d' \left(d \wedge a\right) = d'd \wedge d'a = ab \wedge d'a = a \left(b \wedge d'\right),$$

   d'où l'on déduit $ab = a \left(b \wedge d'\right) d$ et (par intégrité) $b = \left(b \wedge d'\right) d$, d'où la divisibilité $d \mid b$.

   Supposons que A vérifie le théorème de Bézout. Soient $\lambda, \mu \in A$ tels que $1 = \lambda a + \mu d$. Multiplier par b donne $b = \lambda ab + \mu db = \lambda d'd + \mu bd = d \left(\lambda d' + \mu b\right)$, d'où la divisibilité $d \mid b$.

5. Supposons A bézoutien. La question 3 des préliminaires montre alors que tout couple de A^2 admet un p. g. c. d. Pour deux éléments étrangers a et b, ce p. g. c. d. vaut 1, d'où l'appartenance $1 \in (1) = (a) + (b)$, laquel valide le théorème de Bézout pour a et b.

   Supposons réciproquement que A vérifie le théorème de Bézout et que tout couple de A^2 admet un p. g. c. d. Soient a et b dans A. S'ils sont étrangers, le théorème de Bézout montre que l'idéal $(a) + (b)$ contient 1, donc vaut l'idéal plein $A = (1)$, ce qui conclut. Ramenons-nous à ce cas. Soit δ un p. g. c. d. de a et b. Si δ est nul, alors a et b aussi et l'on conclut aussitôt $(a) + (b) = (0) + (0) = (0)$. On supposera donc $\delta \neq 0$. Soient $\alpha, \beta \in A$ tels que $\begin{cases} a = \delta\alpha \\ b = \delta\beta \end{cases}$. Vu les égalités $\delta \sim a \wedge b = (\delta\alpha) \wedge (\delta\beta) = \delta \left(\alpha \wedge \beta\right)$, diviser par δ donne $1 \sim \alpha \wedge \beta$. On peut alors écrire

$$(a) + (b) = (\delta\alpha) + (\delta b) = \delta \left(\alpha\right) + \delta \left(\beta\right) = \delta \left(\left(\alpha\right) + \left(\beta\right)\right) \underset{\text{étrangers}}{\overset{\alpha \text{ et } \beta}{=}} \delta \left(1\right) = \left(\delta\right), \text{ ce qui conclut.}$$

6. Soient $a, b \in A$ étrangers. Si l'idéal $(a) + (b)$ vaut A, on a terminé. Sinon, il est inclus dans un idéal maximal : soit d engendrant cet idéal. Alors d divise a et b, donc d est inversible et (d) est l'idéal plein, ce qui contredit son caractère *strict*.

   Soit a non inversible. L'idéal (a) est alors strict, donc inclus dans un maximal (p). Si p n'était pas irréductible, il admettrait un diviseur d associé ni à p ni à 1, d'où les inclusions strictes $(p) \subsetneq (d) \subsetneq (1)$, ce qui contredirait la maximalité de (p).

De la noethérianité

1. Les idéaux d'un corps étant en nombre fini (il n'y a que (0) et (1)), il est impossible d'en tirer une suite injective, *a fortiori* strictement croissante.

2. Supposons que tout idéal est de type fini. Soit (I_n) une suite d'idéaux croissante. Alors la réunion $I := \bigcup_{n \in \mathbf{N}} I_n$ est un idéal (vérifier !), donc est de type fini, mettons $I = \sum_{k=1}^{n} \left(i_k\right)$ pour certains $i_k \in I$. Chaque i_k tombant dans un I_{n_k}, tous tombent dans un même I_N (définir les n_k minimaux puis définir $N := \max n_k$), d'où les inclusions $\left(i_k\right) \subset I_N$ et $\sum_k \left(i_k\right) \subset I_N$, *i. e.* $I \subset I_N$, ce qui montre que la suite (I_n) stationne à partir du rang N.

   Soit I un idéal qui n'est jamais somme finie d'idéaux principaux. On a en particulier : $\forall n \in \mathbf{N},\ \forall \overrightarrow{i} \in I^n,\ \exists j \in I \setminus \sum_{k=1}^{n} \left(i_k\right)$. En utilisant une fonction de choix c sur A, ce dernier énoncé permet de construire par récurrence une suite $(i_n) \in I^{\mathbf{N}}$ telle que $i_0 = 0$ et $\forall n \in \mathbf{N},\ i_{n+1} = c \left(I \setminus I_n\right)$ où l'on a abrégé $I_n := \sum_{k=0}^{n} \left(i_k\right)$. Alors la suite (I_n) croît strictement vu les appartenances $c \left(I \setminus I_n\right) \in \left(i_{n+1}\right) \setminus I_n \subset I_{n+1} \setminus I_n$, ce qui montre que A n'est pas noethérien.

3. Supposons A noéthérien et bézoutien. Observer que le caractère bézoutien implique (suite à une récurrence immédiate) que tout idéal de type fini est principal. Puisque le caractère noethérien implique que tout idéal est de type fini, il en découle immédiatement que A est principal.

   Supposons A principal. Alors A est tautologiquement bézoutien. Par ailleurs, un idéal principal étant de type fini, la question 2 montre que A est noethérien.

4. Soit $\mathcal{I}$ un ensemble non vide d'idéaux sans élément maximal. Alors la partie $\{I \in \mathcal{I} \ ; \ J \subsetneq I\}$ est non vide pour tout idéal $J \in \mathcal{I}$: en invoquant une fonction de choix c sur $\mathcal{I}$, on en déduit que la fonction $J \mapsto c(\{I \in \mathcal{I} \ ; \ J \subsetneq I\})$ stabilise $\mathcal{I}$, ce qui légitime la construction d'une suite $(I_n) \in \mathcal{I}^{\mathbf{N}}$ telle que $I_0 = c(\mathcal{I})$ et $\forall n \in \mathbf{N}, \ I_{n+1} = c(\{I \in \mathcal{I} \ ; \ I_n \subsetneq I\})$. Par construction, la suite (I_n) croît strictement, ce qui montre que A n'est pas noethérien.

   Supposons que toute famille non vide d'idéaux admet un élément maximal. Soit (I_n) une suite croissante idéaux. Soit I_N un élément maximal de l'ensemble des termes de cette suite. Alors tous les $I_{n \geq N}$, étant plus grands que I_N, doivent égaler ce dernier par maximalité, ce qui montre que la suite (I_n) stationne à partir du rang N.

   Les deux paragraphes précédents s'adaptent sans changement au cas d'idéaux principaux.

5. Supposons A principalement noéthérien. Supposons par l'absurde que la partie E de A formée des éléments ne s'écrivant pas de la forme désirée soit non vide. Alors l'ensemble des idéaux (e) pour e parcourant E admet un élément maximal, mettons (ε). Puisque $\varepsilon \in E$, il ne peut être ni inversible ni irréductible, donc se décompose $\varepsilon = ab$ avec les inclusions strictes $(\varepsilon) \subsetneq (a)$ et $(\varepsilon) \subsetneq (b)$. Par maximalité de (ε), ni a ni b ne peut apppartenir à E, donc chacun s'écrit de la forme voulue et il est alors immédiat que leur produit également, ce qui montre $\varepsilon \in E$: contradiction.

   Supposons A factoriel. Soit[6] $((a_n))$ une suite croissante d'idéaux principaux. Puisque a_0 n'admet qu'un nombre *fini* de diviseurs *modulo* $\sim$, il ne peut y avoir qu'un nombre *fini* d'inclusions strictes dans la chaîne $(a_0) \subset (a_1) \subset (a_2) \subset \cdots$, donc ces inclusions sont toutes des égalités à partir d'un certain rang, *c. q. f. d.*

6. Supposons A principal, *i. e.* (*cf.* question 2) noethérien et bézoutien. Il est alors principalement noethérien, d'où l'existence d'une décomposition en produit d'irréductibles. Il vérifie par ailleurs (d'après la section précédente) le théorème de Bézout, donc le théorème de Gauss, le lemme d'Euclide et l'unicité de la décomposition.

   Supposons A factoriel et bézoutien. Soit par l'absurde I un idéal non principal. Montrons que I ne peut contenir aucun idéal principal, ce qui contredira l'inclusion $(0) \subset I$. Soit $a \in A$ tel que $(a) \subset I$. Puisque I n'est pas principal, l'inclusion est stricte. Soit $a' \in I \setminus (a)$. On a alors les inclusions $(a) \subsetneq (a) + (a') \subset I$. D'après le caractère bézoutien, on peut invoquer un $b \in A$ tel que $(a) + (a') = (b)$. On peut alors itérer l'argument[7] et construire une suite strictement croissante $(a) \subsetneq (b) \subsetneq (c) \subsetneq \cdots \subsetneq I$; or A est factoriel, donc principalement noethérien, ce qui est absurde.

   Supposons enfin A factoriel et vérifiant le théorème de Bézout. Étant factoriel, tout couple de A^2 admet un p. p. c. m., donc (d'après la question 5) Aest bézoutien, donc (d'après ce qui précède) principal.

   Interprétation. Les anneaux principaux sont par conséquent "les anneaux intègres (commutatifs unitaires non nuls) auxquels on peut étendre deux théorèmes qui, au sens strict, concernent l'anneau des entiers relatifs : le théorème de Bachet-Bézout et le théorème fondamental de l'arithmétique."

Sur les anneaux euclidiens.

1. Le corps k est euclidien pour n'importe quel stathme, l'anneau $k[X]$ est euclidien pour stathme deg et l'anneau $\mathbf{Z}$ est euclidien pour stathme $|\cdot|$.

   Soit $(a, b) \in \mathbf{Z}[i] \times \mathbf{Z}[i]^*$. Le complexe $\frac{a}{b}$ fait sens et tombe dans un carré du réseau $\mathbf{Z}[i]$, donc est à distance < 1 de l'un des coins d'un tel carré, mettons $\left|\frac{a}{b} - q\right| < 1$ pour un certain $q \in \mathbf{Z}[i]$. Posons $r := a - bq$. On a d'une part $a = bq + r$, d'autre part ou bien $r = 0$ ou bien $|r| = |a - bq| = |b| \left|\frac{a}{b} - q\right| < |b|$.

2. Supposons A euclidien. Soit I un idéal non nul de A. La partie $s(I \setminus \{0\})$ de $\mathbf{N}$ est non vide, donc admet un minimum $s(i_0) = \min_{i \in I^*} s(i)$ pour un certain $i_0 \in I^*$. Montrons que $I = (i_0)$. Soit $i \in I$. Puisque $i_0 \neq 0$, on peut effectuer la division euclidienne de i par i_0 : soit $(q, r) \in A^2$ tel que $i = qi_0 + r$. Si $r = 0$, on obtient $i = qi_0 \in (i_0)$, *c. q. f. d.*. Sinon, on doit avoir d'une part $r \in I^*$ (puisque $r = i - qi_0 \in I$), d'autre part $s(r) < s(i_0)$, ce qui contredit la minimalité de i_0.

3. Soit $(a, b) \in A^2$ tels que $ab = 0$. Si $b \neq 0$, on a deux divisions euclidiennes $ab + 0 = 0 = 0b + 0$, d'où l'égalité des quotients $a = 0$.

[6] en toute rigueur, on devrait invoquer une suite (I_n) d'idéaux principaux puis utiliser AC pour invoquer une suite $(a_n) \in A^{\mathbf{N}}$ telle que $\forall n \in \mathbf{N}, \ I_n = (a_n)$

[7] Proprement, en utilisant une fonction c de choix sur A, on définirait une suite $(a_n) \in A^{\mathbf{N}}$ telle que $a_0 = 0$ et $\forall n \in \mathbf{N}, \ a_{n+1} = c(\{d \in A \ ; \ (a_n) + (a'_n) = (d)\})$ où l'on a abrégé $a'_n := c(I \setminus (a_n))$. La condition $a'_n \notin (a_n)$ implique la stricte croissance $(a_n) \subsetneq (a_n) + (a'_n) = (a_{n+1})$, ce qui contredit le caractère principalement noethérien.

4. Soit $(a,b) \in A^{*2}$ tels que $a \mid b$. Si $s(a) > s(b)$, on a deux divisions $a\frac{b}{a} + 0 = b = a0 + b$, donc les restes 0 et b coïncident, ce qui n'est pas. On en déduit $s(a) \leq s(b)$. La comparaison réciproque viendrait de même de l'hypothèse $b \mid a$.

5. Puisque 1 divise tout élément, $s(1)$ vaut $\min s$. Puisque 1 est associé à toute unité, les unités sont de stathme $\min s$. Soit réciproquement $a \in A^*$ tel que $s(a) = \min s$. Puisque $a \neq 0$, on peut diviser $1 = qa + r$: la comparaison $s(r) < s(a)$ contredisant la minimalité de $s(a)$, on doit avoir $r = 0$, ce qui montre que a est inversible (d'inverse q).

6. Vérifions que K est un corps, *i. e.* que K est un groupe additif et que K^* est un groupe multiplicatif (la distributivité découle de celle de A). La partie $K^* = K \setminus \{0\} = A^\times$ est bien un groupe abélien. La partie K contient 0 et est stable par opposition (il contient $-1 \in A^\times$), donc il suffit de montrer sa stablilité par $+$.

   Soit $(a,b) \in K^2$. Si a ou b est nul, il est clair que $a+b \in K$. On peut donc supposer a et b inversibles. Vu l'égalité $a + b = a\left(1 + \frac{b}{a}\right)$ et la stabilité de K par $\times$, il suffit de montrer $\forall u \in A^\times,\ 1 + u \in K$. Soit par l'absurde $u \in A^\times$ tel que $1 + u \notin K$. Alors $1 + u$ est non nul et non inversible, donc $s(1+u)$ fait sens et est $> \min s$. On obtient alors deux divisions euclidiennes $0(1+u) + 1 = 1 = \frac{1}{u}(1+u) + \left(-\frac{1}{u}\right)$, ce qui force l'égalité absurde des quotients $0 = \frac{1}{u}$.

7. Soit $(a,k) \in A \setminus A^\times \times K^*$ (le cas $k = 0$ est trivial). Vu les équivalences $s(a) = s(a+k) \iff s\left(k\frac{a}{k}\right) = s\left(k\left(\frac{a}{k} + 1\right)\right) \iff s\left(\frac{a}{k}\right) = s\left(\frac{a}{k} + 1\right)$, on peut supposer $k = 1$. On veut $s(a+1) = s(a)$. L'élément $1+a$ est hors de K (car K est stable par soustraction et contient 1), donc est non nul et tel que $s(1+a) > \min s$, ce qui montre que l'égalité $1 = 0(1+a)+1$ est une division euclidienne. L'égalité $1 = 1(1+a) - a$ ne pouvant être également une division euclidienne (un reste est inversible et pas l'autre), on obtient $s(a) \geq s(a+1)$. Nous avons donc montré $\forall a \in A \setminus K\ ,\ s(a) \geq s(a+1)$. Montrons pour conclure la comparaison réciproque. Soit $b \in A \setminus K$. On applique ce qui précède en remplaçant a par $-1-b$, ce qui donne $s(1+b) \geq s(b)$, *c. q. f. d.*.

8. Nous avons déjà vu que les corps étaient euclidiens. Supposons donc que A n'est pas un corps.

   (Micro analyse si $A = K[X]$. On a $A^\times = K^*$, ce qui impose $K = A^\times \cup \{0\}$. Par ailleurs, X est de stathme minimal autre que $\min s$. Fin de l'analyse.) Puisque A n'est pas un corps, il y a un $x \in A$ hors de K. Invoquons-en un de stathme minimal et montrons que le morphisme d'anneaux $\begin{cases} K[X] & \longrightarrow & A \\ P & \longmapsto & P(x) \end{cases}$ est bijectif.

   Injectivité. Soit $P \in K[X]$ tel que $P(x) = 0$, mettons $0 = P(x) = x\left(a_1 + a_2x + \cdots + a_nx^{n-1}\right) + a_0$. Puisque $a_0 \in K$, il est ou bien nul ou bien de stathme minimal $\min s < s(x)$: l'égalité précédente est donc une division euclidienne (de 0 par x). Par unicité, le quotient $a_1 + a_2x + \cdots + a_nx^{n-1}$ est nul et le reste a_0 aussi. Par récurrence (sur le degré de P), P est nul, (pas de problème si P est constant), *c. f. q. d.*.

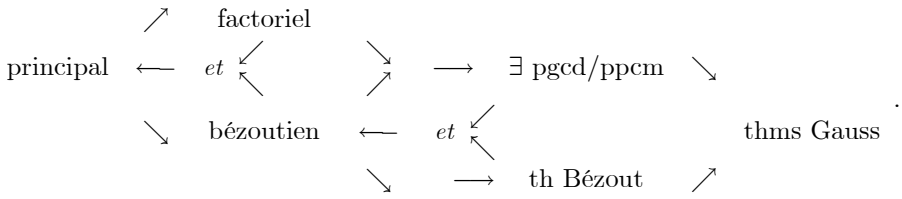
   Surjectivité. Les éléments de K sont des polynômes constants en x. Soit donc $a \in A \setminus K$: on divise $a = qx + r$. Si $r \neq 0$, on a $s(r) < s(x)$, d'où (par minimalité de x) $r \in K$. Dans tous les cas, on a $r \in K$ et il suffit de montrer $q \in K[x]$: si l'on montre $s(q) < s(a)$, on pourra récurrer sur $s(a)$ (le cas $s(a)$ minimal est englobé par le cas $a \in K$ déjà traité). La question 7 permettant d'écrire $s(qx) = s(a-r) = s(a)$, il suffit de montrer $s(qx) > s(q)$. Pour cela, on divise $q = q'(qx) + r'$ (le dividende qx est non nul par intégrité de A car : d'une part x est non nul, d'autre part la nullité de q impliquerait $a = r \in K$). D'une part, l'élément $r' = q(1 - q'x)$ est multiple de q, d'où $s(r') \geq s(q)$. D'autre part, si $r' = 0$, l'intégrité de A nous donne alors $1 = x'q'$, ce qui est absurde puisque x n'est pas inversible, d'où l'on déduit $s(r') < s(xq)$. Mettre bout à bout les deux comparaisons précédentes conclut.

   Remarque. Il peut sembler étrange que $\mathbf{Z}$ ne soit pas fortement euclidien au vu de l'unicité connue du quotient/reste. Mais cette dernière devient fausse une fois formulée en termes de sthame vu que "la division euclidienne" de 1 par 2 possède (exactement) deux couples "quotient/reste" au sens du stathme $|\cdot|$, à savoir $(0,1)$ et $(1,-1)$.

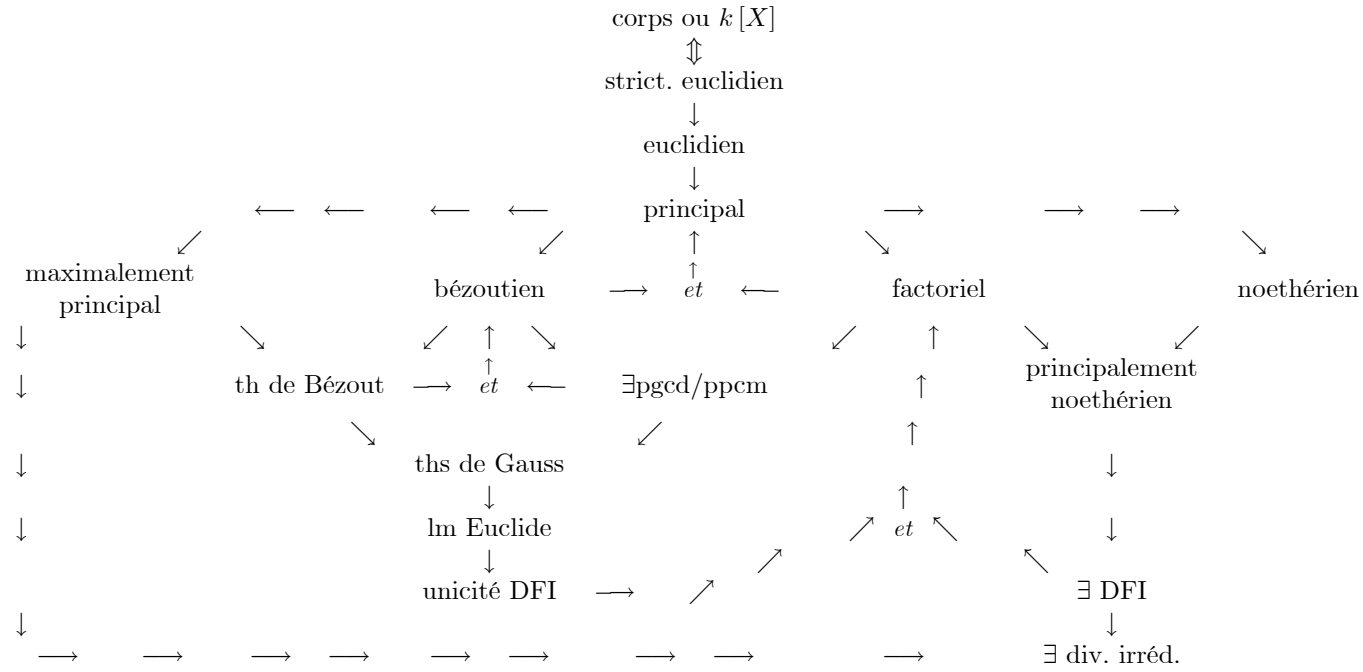
Résumé. Une première partie concerne les conséquences de la factorialité (et commenter y remonter) :

$$\begin{array}{ccccccccccc} & \nearrow & \exists \text{ pgcd/ppcm} & \longrightarrow & \text{ths de Gauss} & \longrightarrow & \text{lm Euclide} & \longrightarrow & \text{unicité DFI} \\ \text{factoriel} & \longleftarrow & \longleftarrow \quad \longleftarrow & \longleftarrow & \longleftarrow \quad \textit{et} \quad \longleftarrow & \longleftarrow & \longleftarrow & \longleftarrow & \swarrow \\ & & & & \uparrow & & & & \\ & \searrow & \begin{array}{c}\text{principalement} \\ \text{noethérien}\end{array} & \longrightarrow & \exists \text{ DFI} & \longrightarrow & \exists \text{ div. irréd} & & \end{array}$$

Une seconde partie concerne Bézout :



Il reste enfin à rajouter les considérations euclidiennes :



On peut *remonter vers "principal" depuis la conjonction de "th Bézout" et "∃ DFI"* (en effet, le th de Bézout implique l'unicité de la DFI, donc (avec l'existence) la factorialité et une question 6. permet alors de remonter à la principalité).

On lirait également comment *remonter vers "principal" depuis la conjonction de "noethérien" et "bézoutien"*, ou encore *de "noethérien" et "maximalement principal"*.

Quelques contre-exemples (pas tous faciles).

$\mathbf{Z}$ et $\mathbf{Z}[i]$ sont euclidiens mais pas fortement euclidiens.

$\mathbf{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais pas euclidien.

$\mathbf{Q}[X_n]_{n>0}$ est factoriel mais pas noethérien (donc pas principal), $\mathbf{Z}\left[i\sqrt{5}\right]$ est noethérien mais pas factoriel (donc pas principal).

$\mathbf{Z} + X\mathbf{Q}[X]$ est bézoutien mais pas principal (donc ni factoriel ni noethérien), tout comme l'anneau des fonctions holomorphes.

$\mathbf{Q}[X, Y]$ est factoriel et noethérien mais ne vérifie pas le théorème de Bézout (donc n'est ni bézoutien ni principal ni maximalement principal).

L'exercice 20 du chapitre 7 du tome d'*Algèbre commutative* de Bourbaki décrit un anneau bézoutien où aucun premier (non nul) n'est de type fini. Cet anneau vérifie donc le théorème de Bézout sans être maximalement principal.