Généralités sur les anneaux et modules

Travaux dirigés du 18 et du 21 novembre 2025

Exercice 1. Anneaux simples

Un anneau A est dit *simple* s'il est non nul, et si ses seuls idéaux bilatères sont $\{0\}$ et A.

1. Montrer qu'un corps gauche est simple.
   Soit k un corps gauche, soit I un idéal bilatère de k contenant un élément x non nul. Alors x est inversible dans k, donc il existe $y \in k$ avec $yx = 1$. On a alors $1 = yx \in I$, puis $a = a \cdot 1 \in I$ pour tout $a \in k$, et enfin $I = k$.
2. Pour un anneau A quelconque, montrer que les idéaux bilatères de $M_n(A)$ sont les $M_n(I)$ avec I idéal bilatère de A.
   Si I est un idéal bilatère de A, $M_n(I)$ est un idéal bilatère de $M_n(A)$ par expression des coefficients. Réciproquement, soit J un idéal bilatère de $M_n(A)$. Notant $E_{i,j}$ les matrices élémentaires usuelles, pour tout $X \in J$, $1 \leq i, j \leq n$ et $1 \leq p, q \leq n$ on a $E_{p,i} X E_{j,q} = X_{i,j} E_{p,q} \in J$ car J est bilatère. On en déduit que l'ensemble I des coefficients des matrices de J est un idéal bilatère de A et que $J = M_n(I)$.
3. En déduire que si $A = k$ est un corps gauche, l'anneau $M_n(k)$ est simple.
   Par la question précédente, les idéaux bilatères de $M_n(k)$ sont les $M_n(I)$ avec I idéal bilatère de k, c'est-à-dire par la question 1 $I = 0$ ou k, et donc $M_n(k)$ est simple.

Exercice 2. Une construction du corps des réels

Soit A l'ensemble des suites de Cauchy de rationnels. On regarde le sous-ensemble $I \subseteq A$ constitué des suites (x_n) qui tendent vers 0.

1. Vérifier que A est un sous-anneau de l'anneau produit $\mathbb{Q}^{\mathbb{N}}$, et que I est un idéal de A.
   La suite constante égale à 1 est bien de Cauchy, la somme de deux suites de Cauchy est de Cauchy (on utilise la majoration $|(x_p + y_p) - (x_q - y_q)| \leq |x_p - x_q| + |y_p - y_q|$) et le produit de deux suites de Cauchy est de Cauchy (on utilise la majoration $|x_p y_p - x_q y_q| = |x_p y_p - x_p y_q + x_p y_q - x_q y_q| \leq |x_p||y_p - y_q| + |x_p - x_q||y_q|$ ainsi que le fait que les suites de Cauchy sont bornées), ce qui fait de A un sous-anneau de $\mathbb{Q}^{\mathbb{N}}$. Le fait que I est un idéal de A est une conséquence des opérations sur les limites.
2. Montrer que I est maximal.
   On a $I \neq A$ car la suite constante égale à 1 n'appartient pas à I. Montrons que si $x = (x_n)$ est un élément de $A - I$, alors on a $I + (x) = A$. Il suffit de voir que $1 \in I + (x)$, ou encore qu'il existe $y = (y_n) \in A$ telle que $xy - 1 \in I$. Mais le fait que x ne tend pas vers 0 est équivalent à l'existence d'un $\varepsilon > 0$ tel que pour tout $N \in \mathbb{N}$, il existe un entier $\varphi(N) \geq N$ tel que $|x_{\varphi(N)}| \geq \varepsilon$. De plus comme x est de Cauchy on sait qu'on peut choisir $N \in \mathbb{N}$ tel que pour tous $p, q \geq N$, $|x_p - x_q| < \varepsilon/2$, donc on a pour tout $n \geq N$ que $|x_n| \geq |x_{\varphi(N)}| - |x_n - x_{\varphi(N)}| \geq \varepsilon/2$ et donc la suite $y = (y_n)$ définie par $y_n = 0$ pour $n < N$, et $y_n = 1/x_n$ pour $n \geqslant N$, est une suite de Cauchy, et on a bien $yx - 1 \in I$, ce qui conclut.
3. En déduire une construction du corps des réels.
   On a vu en cours que si A est commutatif, un idéal $I \subsetneq A$ est maximal si et seulement si l'anneau quotient A/I est un corps, ce qui conclut.

Exercice 3. Idéaux premiers

Soient A un anneau commutatif et $\mathfrak{p}$ un idéal de A. On dit que $\mathfrak{p}$ est *premier* si on a $\mathfrak{p} \neq A$ et si pour tout $x, y \in A$ tels que $xy \in \mathfrak{p}$, on a soit $x \in \mathfrak{p}$, soit $y \in \mathfrak{p}$.

1. Montrer que $\mathfrak{p}$ est premier si et seulement si l'anneau quotient $A/\mathfrak{p}$ est intègre.
   Pour tous $x, y \in A$, on a

   $$(xy = 0 \bmod \mathfrak{p} \Rightarrow (x = 0 \bmod \mathfrak{p} \text{ ou } y = 0 \bmod \mathfrak{p})) \Leftrightarrow (xy \in \mathfrak{p} \Rightarrow (x \in \mathfrak{p} \text{ ou } y \in \mathfrak{p})),$$

   d'où le résultat.
2. Montrer que si $\mathfrak{p}$ est maximal alors $\mathfrak{p}$ est premier.
   On sait que $\mathfrak{p}$ est maximal si et seulement si $A/\mathfrak{p}$ est un corps, ce qui conclut.
3. Donner un exemple d'idéal premier non maximal.
   Pour tout anneau A on a $A/(0) = A[X]/(X) = A$. Si A est intègre mais pas un corps (par exemple $A = \mathbb{Z}$), il suit que (0) est un idéal premier non maximal de A, et que (X) est un idéal premier non maximal de $A[X]$.

4. Montrer que si $\mathfrak{p}$ est premier, et si $A/\mathfrak{p}$ est fini, alors $\mathfrak{p}$ est maximal.

   C'est une conséquence du fait qu'un anneau intègre fini est un corps gauche (voir TD n°1).

Exercice 4. Modules sur un anneau de polynômes

Soient k un corps et $n \geq 1$ un entier. Montrer qu'il est équivalent de se donner un $k[X_1,\dots,X_n]$-module et de se donner un k-espace vectoriel V muni de n endomorphismes $u_1,\dots,u_n \in \mathrm{End}(V)$ vérifiant $u_i u_j = u_j u_i$ pour tout $1 \leq i,j \leq n$.

On constate que si M est un $k[X_1,\dots,X_n]$-module, c'est *a fortiori* un k-module i.e. un k-espace vectoriel. De plus, les applications $u_i : M \to M$, $m \mapsto X_i \cdot m$ sont des endomorphismes pour cette structure d'espace vectoriel, et on a bien que u_i et u_j commutent pour tous i et j. Réciproquement, si on se donne un k-espace vectoriel V muni de n endomorphismes $u_1,\dots,u_n \in \mathrm{End}(V)$ vérifiant $u_i u_j = u_j u_i$ pour tout $1 \leq i,j \leq n$, alors on définit une application $k[X_1,\dots,X_n] \times V \to V$, $(P,v) \mapsto P \cdot v$ par $X_i \cdot v = u_i(v)$, ce qui fait de V un $k[X_1,\dots,X_n]$-module.

Exercice 5. Modules sur un corps gauche

Pour tout module M sur un anneau A et toute famille finie $e = (e_1,\dots,e_n)$ d'éléments de M, on dispose de l'application A-linéaire

$$u : A^n \to M,\ (a_i) \mapsto \sum_{i=1}^{n} a_i e_i.$$

On dit que e est une *famille génératrice* de M si u est surjective, on dit que e est *libre* si u est injective, et on dit enfin que e est une *base* si u est un isomorphisme. Un A-module est dit *de type fini* s'il possède une famille finie génératrice, et *libre* de rang n s'il possède une base à n éléments.

Soit k un corps gauche.

1. Montrer que tout k-module de type fini est libre.

   Soit M un k-module de type fini et soit $e = (e_1,\dots,e_n)$ une famille génératrice. Comme pour les corps, on regarde une sous-famille génératrice de e de cardinal minimal : quitte à réordonner les éléments de e on peut supposer que cette sous-famille est $(e_1,\dots,e_r)$ avec $r \leq n$. Alors cette famille est libre : sinon, on trouve $(a_i) \in k^r - \{0\}$ telle que $\sum_{i=1}^{r} a_i e_i = 0$, et il existe j tel que $a_j \neq 0$ donc on a $e_j = -a_j^{-1} \sum_{i \neq j} a_i e_i$, ce qui contredit la minimalité de r.

2. Montrer que l'on a un isomorphisme de k-modules $k^n \simeq k^m$ si et seulement si $n = m$.

   On fait une récurrence sur n pour montrer qu'il ne peut pas y avoir de famille libre de $n+1$ éléments dans k^n. Pour $n = 1$, une famille (e_1,e_2) d'éléments de $k^\times$ n'est pas libre car $e_1 = e_1 e_2^{-1} e_2$. Supposons la propriété vraie au rang n. Soit $(e_1,\dots,e_{n+2})$ une famille libre d'éléments de k^{n+1}. Si tous les éléments sont dans $k^n \times \{0\}$, on obtient une famille libre de k^n à $n+2$ éléments, donc *a fortiori* une famille libre de k^n à $n+1$ éléments, ce qui est impossible par hypothèse de récurrence. On peut donc supposer que l'un des éléments de la famille, disons e_{n+1}, a sa dernière coordonnée $e_{n+1,n+1}$ non nulle donc inversible. Pour tous i et j, notons $e_{i,j}$ le j-ième coefficient de e_i. On regarde alors la famille des $e'_i := e_i - (e_{i,n+1} e_{n+1,n+1}^{-1}) e_{n+1}$ pour $i \leq n$. Cette famille est incluse dans $k^n \times \{0\}$, et libre car le morphisme k-linéaire $u' : k^n \to M$, $(a_i) \mapsto \sum_{i=1}^{n} a_i e'_i$ est la composée $u \circ \varphi$ des morphismes injectifs $u : k^{n+1} \to M$, $(a_i) \mapsto \sum_{i=1}^{n+1} a_i e_i$ et $\varphi : k^n \to k^{n+1}$, $(a_i) \mapsto (a_1,\dots,a_n, -e_{n+1,n+1}^{-1} \sum_{i=1}^{n} e_{i,n+1} a_i)$. On conclut par hypothèse de récurrence. (On a essentiellement appliqué le pivot de Gauss.)

Exercice 6. Localisation

Dans un anneau commutatif A, on dit qu'un sous-ensemble S de A est une *partie multiplicative* si S est stable par multiplication, contient 1 mais ne contient pas 0. Par exemple, on peut citer l'ensemble $S = A - \{0\}$ quand A est intègre, l'ensemble $S = \{f^n, n \in \mathbb{N}\}$ des puissances de f si $f \in A$ n'est pas nilpotent et l'ensemble complémentaire $A \backslash \mathfrak{p}$ si $\mathfrak{p}$ est un idéal premier (voir définition à l'exercice 3).

Soit donc S une partie multiplicative de A. On munit l'ensemble $A \times S$ de la relation d'équivalence suivante :

$$(a,s) \sim (a',s') \Leftrightarrow \exists t \in S,\ t(as' - a's) = 0$$

On notera $S^{-1}A := (A \times S)/\sim$ l'ensemble quotient, et $\frac{a}{s}$ la classe d'équivalence de (a,s).

1. Montrer que l'application $(A \times S) \times (A \times S) \to A \times S$ qui envoie $((a,s),(b,r))$ sur $(ar+bs, sr)$ induit une loi associative et commutative

$$+ : \quad S^{-1}A \times S^{-1}A \to S^{-1}A, \quad \left(\frac{a}{s}, \frac{b}{r}\right) \mapsto \frac{a}{s} + \frac{b}{r} = \frac{ar+bs}{sr},$$

   d'élément neutre $0 := \frac{0}{s}$ pour tout s.

Vérifions d'abord que la loi est bien définie. Soit $(a',s') \sim (a,s)$ et $(b',r') \sim (b,r)$. Il existe donc $t,u \in S$ tels que $t(as'-a's) = 0 = u(br'-b'r)$. On a alors

$$ut\big((ar+bs)s'r' - (a'r'+b's')sr\big) = ut(as'-a's)rr' + ut(br'-b'r)ss' = 0$$

et il s'ensuit que $(ar+bs,sr) \sim (a'r'+b's',s'r')$, ce qui montre que la loi + est bien définie sur $S^{-1}A$. La commutativité de cette loi découle de la commutativité de A. L'associativité et le fait que $\frac{0}{s}$ en est un élément neutre (indépendant de s) résultent de calculs identiques à ceux dans $\mathbb{Q}$.

2. Montrer que l'application $(A\times S)\times(A\times S) \to A\times S$ qui envoie $((a,s),(b,r))$ sur (ab,sr) induit une loi associative, commutative, et distributive par rapport à +,

$$\cdot : \quad S^{-1}A \times S^{-1}A \to S^{-1}A, \quad \left(\frac{a}{s},\frac{b}{r}\right) \mapsto \frac{a}{s}\cdot\frac{b}{r} = \frac{ab}{sr},$$

d'élément neutre $1 := \frac{1}{1}$. Ainsi $(S^{-1}A,+,\cdot)$ est un anneau que l'on appelle le *localisé* de A en S.
Soit $(a',s') \sim (a,s)$ et $(b',r') \sim (b,r)$, il existe $t,u \in S$ tels que $t(as'-a's) = 0 = u(br'-b'r)$. On a alors

$$ut(as'-a's)br' - ut(br'-b'r)a's = ut(abs'r' - a'b'sr) = 0$$

et donc $(ab,sr) \sim (a'b',s'r')$, et la loi $\cdot$ est bien définie sur $S^{-1}A$. La commutativité de cette loi découle de la commutativité de A. L'associativité, la distributivité par rapport à + et le fait que $\frac{1}{1}$ en est un élément neutre résultent de calculs identiques à ceux dans $\mathbb{Q}$.

3. Montrer que l'application $A \xrightarrow{\iota} S^{-1}A$, $a \mapsto \frac{a}{1}$ est un morphisme d'anneaux. Quel est son noyau ?
Les calculs sont encore une fois comme dans $\mathbb{Q}$. Le noyau du morphisme est constitué des éléments a tels que $(a,1) \sim (0,1)$. On voit donc que $\mathrm{Ker}(\iota) = \{a \in A, \exists t \in S, at = 0\}$ est constitué en particulier de diviseurs de 0.

4. Montrer que si est A est intègre et $S = A - \{0\}$, $S^{-1}A$ est un corps qui contient A. C'est le *corps des fractions* de A.
Dans ce cas, tout élément non nul de $S^{-1}A$ est de la forme $\frac{a}{b}$ avec $a,b \neq 0$, et donc est inversible d'inverse $\frac{b}{a}$. Ainsi, $S^{-1}A$ est un corps qui contient A (via ι).

Exercice 7. Unités des anneaux d'entiers quadratiques

Fixons $d \in \mathbb{Z}$ non carré, ainsi qu'une racine carrée $\sqrt{d} \in \mathbb{C}$ de d. Pour fixer les idées on suppose $\sqrt{d} > 0$ pour $d > 0$ (cas dit réel), et $\sqrt{d}$ de partie imaginaire > 0 pour $d < 0$ (cas dit imaginaire). On considère les sous-groupes additifs de $\mathbb{C}$

$$\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Q}[\sqrt{d}] \subseteq \mathbb{C}$$

avec $\mathbb{Z}[\sqrt{d}] := \mathbb{Z} + \mathbb{Z}\sqrt{d}$ et $\mathbb{Q}[\sqrt{d}] := \mathbb{Q} + \mathbb{Q}\sqrt{d}$.

1. Vérifier que $\mathbb{Z}[\sqrt{d}]$ et $\mathbb{Q}[\sqrt{d}]$ sont des sous-anneaux de $\mathbb{C}$.
On utilise la formule $(x+y\sqrt{d})(x'+y'\sqrt{d}) = \big(xx'+dyy'\big) + \big(xy'+x'y\big)\sqrt{d}$.

Pour $x,y \in \mathbb{Q}$, et $z := x + y\sqrt{d}$, on pose

$$\begin{cases} \overline{z} = x - y\sqrt{d}, & \text{le } \textit{conjugué} \text{ de } z \\ \mathrm{T}(z) = z + \overline{z} = 2x, & \text{la } \textit{trace} \text{ de } z \\ \mathrm{N}(z) = z\overline{z} = x^2 - dy^2, & \text{la } \textit{norme} \text{ de } z \end{cases}$$

On a donc l'identité de Cayley-Hamilton $z^2 - \mathrm{T}(z)z + \mathrm{N}(z) = 0 = (z-z)(z-\overline{z})$.

2. Montrer que $z \mapsto \overline{z}$ est un automorphisme des anneaux $\mathbb{Q}[\sqrt{d}]$ et $\mathbb{Z}[\sqrt{d}]$, que $\mathbb{Q}[\sqrt{d}]$ est le corps des fractions (voir exercice précédent) de $\mathbb{Z}[\sqrt{d}]$, que $N : \mathbb{Q}[\sqrt{d}]^\times \to \mathbb{Q}^\times$ est un morphisme de groupes et qu'on a $\mathrm{N}(\mathbb{Z}[\sqrt{d}]) \subseteq \mathbb{Z}$.
L'application $z \mapsto \overline{z}$ est un endomorphisme $\mathbb{Q}$-linéaire de $\mathbb{Q}[\sqrt{d}]$ vérifiant $\overline{1} = 1$. De plus, pour $a,b \in \mathbb{Q}[\sqrt{d}]$ la formule écrite pour la question précédente montre $\overline{ab} = \overline{a}\,\overline{b}$, puis le premier point. Pour $b \neq 0$, on a $\mathrm{N}(b) \in \mathbb{Q}^\times$ puis $a/b = ab/\mathrm{N}(b) \in \mathbb{Q}[\sqrt{d}]$, ce qui montre le deuxième point. Le premier point montre aussi $\mathrm{N}(ab) = ab\overline{ab} = ab\overline{a}\,\overline{b} = \mathrm{N}(a)\mathrm{N}(b)$, puis le troisième point. Le dernier point vient de la définition de N.

3. Montrer qu'on a $\mathbb{Z}[\sqrt{d}]^\times = \{z \in \mathbb{Z}[\sqrt{d}] \mid N(z) = \pm 1\}$.
En effet, si $ab = 1$ dans $\mathbb{Z}[\sqrt{d}]$ on a $\mathrm{N}(a)\mathrm{N}(b) = \mathrm{N}(1) = 1$, puis $\mathrm{N}(a),\mathrm{N}(b) \in \mathbb{Z}^\times = \{\pm 1\}$. Réciproquement, si on a $\mathrm{N}(a) = \varepsilon$ avec $a \in \mathbb{Z}[\sqrt{d}]$ et $\varepsilon = \pm 1$, on a $a\overline{a} = \varepsilon$ avec $\overline{a} \in \mathbb{Z}[\sqrt{d}]$, et donc $\varepsilon\overline{a} = a^{-1} \in \mathbb{Z}[\sqrt{d}]$.

4. Déterminer $\mathbb{Z}[i]^\times$ et $\mathbb{Z}[\sqrt{d}]^\times$ pour $d<-1$.
   On a
   $$\mathbb{Z}[i]^\times = \{a+bi \in \mathbb{Z}[i] \mid a^2+b^2 = \pm 1\} = \{\pm 1, \pm i\}$$
   et pour $d<-1$,
   $$\mathbb{Z}[\sqrt{d}]^\times = \{a+b\sqrt{d} \in \mathbb{Z}[\sqrt{d}] \mid a^2+|d|b^2 = \pm 1\} = \{\pm 1\}.$$

Traitons maintenant le cas $d>0$.

5. *(Principe de Dirichlet)* Montrer que pour tout $\alpha \in \mathbb{R}$, et tout entier $N \geq 1$, il existe $p \in \mathbb{Z}$ et $1 \leq q \leq N$ tels que $|p-q\alpha| < 1/N$.
   C'est un argument dû à Dirichlet. On regarde les $N+1$ éléments $k\alpha - \lfloor k\alpha \rfloor$ de $[0,1[$, avec $0 \leq k \leq N$. Considérant la partition de $[0,1[$ en les N parties $[q/N,(q+1)/N[$ avec $0 \leq q < N$, on en déduit qu'il existe $0 \leq i < j \leq N$ avec $|(j\alpha - \lfloor j\alpha \rfloor) - (i\alpha - \lfloor i\alpha \rfloor)| < 1/N$. Posons $q = j-i$ et $p = \lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor$, on a $1 \leq q < N$ et $|p-q\alpha| < 1/N$.

6. Montrer qu'il existe une suite d'éléments $x_n \in \mathbb{Z}[\sqrt{d}]$ non nuls avec $x_n \to 0$ dans $\mathbb{R}$ et $(\mathrm{N}(x_n))_{n\geq 1}$ bornée.
   Pour $n \geq 1$, on choisit $p_n \in \mathbb{Z}$ et $q_n \geq 1$ avec $\left|p_n - q_n\sqrt{d}\right| < 1/n$ et $1 \leq q_n \leq n$. On a donc
   $$|p_n| < \frac{1}{n} + |q_n|\sqrt{d} \leq \frac{1}{n} + n\sqrt{d}$$
   puis
   $$\left|\mathrm{N}\left(p_n - q_n\sqrt{d}\right)\right| = \left|p_n - q_n\sqrt{d}\right|\left|p_n + q_n\sqrt{d}\right| < \frac{1}{n}\left(\frac{1}{n} + 2n\sqrt{d}\right) \leq 1 + 2\sqrt{d}.$$
   On conclut en posant $x_n = p_n - q_n\sqrt{d}$ (nécessairement non nul car $q_n \neq 0$).

7. (suite) Montrer que quitte à extraire une sous-suite de x_n, on peut supposer qu'il existe $k \in \mathbb{Z}$ tel que $\mathrm{N}(x_n) = k$ et $x_n\overline{x_m} \in k\mathbb{Z}[\sqrt{d}]$, pour tout $n,m \geq 1$.
   Comme l'ensemble des $\mathrm{N}(x_n)$ est fini (des entiers bornés), quitte à extraire (x_n) on peut supposer qu'il existe $k \in \mathbb{Z}$ avec $\mathrm{N}(x_n) = k$ pour tout n et $x_n \to 0$. De même, comme on a $\mathbb{Z}[\sqrt{d}]/k\mathbb{Z}[\sqrt{d}] = (\mathbb{Z}/k\mathbb{Z})1 \oplus (\mathbb{Z}/k\mathbb{Z})\sqrt{d}$, un ensemble fini, on peut supposer que $x_n \bmod k\mathbb{Z}[\sqrt{d}]$ est constante. Comme $k\mathbb{Z}[\sqrt{d}]$ est un idéal de $\mathbb{Z}[\sqrt{d}]$, on peut multiplier les congruences, et on en déduit que la classe $x_m\overline{x_n} \bmod k\mathbb{Z}[\sqrt{d}]$ ne dépend pas de $n,m \geqslant 1$. Pour $m=n$ on a $x_n\overline{x_n} = \mathrm{N}(x_n) = k \equiv 0 \bmod k\mathbb{Z}[\sqrt{d}]$. On a donc $x_m\overline{x_n} \in k\mathbb{Z}[\sqrt{d}]$ pour tout $m,n \geqslant 1$.

8. En déduire que $\mathbb{Z}[\sqrt{d}]^\times$ est infini.
   Posons $x_m\overline{x_n} = ky_{m,n}$ pour un certain $y_{m,n} \in \mathbb{Z}[\sqrt{d}]$. En prenant la norme on a $k^2 = \mathrm{N}(x_m)\mathrm{N}(x_n) = k^2\,\mathrm{N}(y_{m,n})$, puis $y_{m,n} \in \mathbb{Z}[\sqrt{d}]^\times$ pour tout m,n. On a $y_{m,n} \to 0$ et $y_{m,n} \neq 0$, on a donc construit une infinité d'unités.

9. Montrer que tout élément >1 de $\mathbb{Z}[\sqrt{d}]^\times$ est de la forme $x+y\sqrt{d}$ avec $x,y \geq 1$, qu'il existe un unique plus petit tel élément η_d, appelé *unité fondamentale* de $\mathbb{Z}[\sqrt{d}]$, et qu'on a $\mathbb{Z}[\sqrt{d}]^\times = \langle -1, \eta_d \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. Calculer η_2.
   Soit $u = x+y\sqrt{d}$ dans $\mathbb{Z}[\sqrt{d}]^\times - \{\pm 1\}$. Quitte à remplacer u par $-u$, on peut supposer $u>0$, puis quitte à le remplacer par $1/u$ on peut supposer $u>1$. Mais l'ensemble de 4 inversibles $\{u,u^{-1},-u,-u^{-1}\} = \{\pm u, \pm\overline{u}\} = \{\pm x \pm y\sqrt{d}\}$ rencontre chacun des intervalles $]-\infty,-1[$, $]-1,0[$, $]0,1[$ et $]1,+\infty[$ en un point. Le plus grand des 4 est u, ce qui montre $x,y>0$, et la première assertion. On en déduit que le sous-groupe des inversibles >0 de $\mathbb{Z}[\sqrt{d}]$ est discret dans le groupe multiplicatif $\mathbb{R}_+^*$, qui est isomorphe par le log au groupe additif $\mathbb{R}$. Comme il est non trivial par la question précédente, il est monogène engendré par η_d. Enfin, pour $d=2$, on a $1+\sqrt{2}>1$ et $\mathrm{N}(1+\sqrt{2}) = -1$ donc $\eta_2 = 1+\sqrt{2}$. On en déduit par exemple $\eta_2^6 = (1+\sqrt{2})^6 = 99+70\sqrt{2}$ et donc $99^2 - 2\cdot 70^2 = 1$.