Correction séance 6 (20 octobre)

† *Nombres quadratiques*

Exercice 1.
1. Soit x un nombre quadratique, on a
$$\alpha x^2 + \beta x + \gamma = 0$$
avec $\alpha, \beta, \gamma \in \mathbb{Z}$.

- Si $\alpha = 0$, alors l'équation est de la forme $\beta X + \gamma = 0$, on a alors $\beta \neq 0$ (sans quoi l'équation est vide). On divise alors par β pour obtenir $x + \frac{\gamma}{\beta} = 0$. C'est un polynôme de degré 1 unitaire dans $\mathbb{Q}[X]$ dont x est racine.
- Si $\alpha \neq 0$, alors on a $x^2 + \frac{\beta}{\alpha}x + \frac{\gamma}{\alpha} = 0$, c'est un polynôme unitaire de degré 2 dans $\mathbb{Q}[X]$ dont x est une racine.

Réciproquement, si x est racine d'un polynôme unitaire de degré $\leqslant 2$ dans $\mathbb{Q}[X]$:
$$X^2 + \frac{p}{q}X + \frac{a}{b} = 0$$
En multipliant par qb, on obtient que x est solution du polynôme dans $\mathbb{Z}[X]$:
$$qbX^2 + pbX + aq = 0$$
ce qui prouve que x est un nombre quadratique.

2. Reprenons l'équation (1). Si $\Delta = 0$, alors les solutions sont de la forme $\frac{-\beta}{\alpha}$, qui est bien de la forme voulue pour $a = \frac{-\beta}{\alpha}$ et $d = 0$. Si $\Delta > 0$, alors les solutions sont $\frac{-\beta \pm \sqrt{\Delta}}{2\alpha}$, qui est également de la forme voulue.

3. Soit $x = a + b\sqrt{d}$, on a $x^2 = a^2 + b^2 d + 2ab\sqrt{d}$ et $2ax = 2a^2 + 2ab\sqrt{d}$ donc
$$x^2 - 2ax = a^2 + b^2 d + 2ab\sqrt{d} - 2a^2 - 2ab\sqrt{d} = b^2 d - a^2$$
Donc $x^2 - 2ax + a^2 - b^2 d = 0$, voila un polynôme unitaire de degré 2 dans $\mathbb{Q}[X]$ qui prouve que x est quadratique.

Exercice 2.
1. Soit x un nombre quadratique. L'ensemble des polynômes de $\mathbb{Q}[X]$ dont x est racine forme un idéal de $\mathbb{Q}[X]$. Comme $\mathbb{Q}$ est un corps, $\mathbb{Q}[X]$ est principal, et cet idéal est engendré par un polynôme unitaire bien défini : c'est le polynôme minimal.

2. Le polynôme minimal de x dans $\mathbb{Q}[X]$ est de degré 1 si et seulement si il est de la forme $X + b$ avec $b \in \mathbb{Q}$. Ce polynôme admet une seule racine $-b = x$, qui est donc rationnel.

3. Les racines du polynôme minimal sont les racines (éventuellement complexes) de b. Il y en a 2 et elles sont opposées l'une de l'autre, d'où le résultat.

4. Dans l'écriture $x = a + b\sqrt{d}$, on a que x est rationnel si et seulement si $d = 0$. Sinon, le poylnôme minimal de x est donné par $X^2 - 2ax + a^2 - b^2 d$ d'après l'exercice précédent. On a $\Delta = 4a^2 - 4a^2 + 4b^2 d = 4b^2 d > 0$, les solutions de ce polynôme sont alors
$$\frac{2a \pm 2b\sqrt{d}}{2} = 2a \pm b\sqrt{d}$$
On obtient donc que l'autre racine x_c est égale à $a - b\sqrt{d}$.

4. Si x n'est pas rationnel et son polynôme minimal P est de degré 2, on a
$$P = (X - x)(X - x_c) = X^2 - xX - x_c X + x x_c = X^2 - T(x)X + N(x)$$

5. Soit $x = a + b\sqrt{d}$, on a $ux + v = ua + v + bu\sqrt{d}$, dont le conjugué est $ua + v - bu\sqrt{d} = ux_c + v$. De même, on a

$$\frac{1}{x} = \frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 - b^2 d}$$

dont le conjugué est $\frac{a+b\sqrt{d}}{a^2-b^2d} = \frac{1}{x_c}$.

† *Équation de Pell-Fermat*

Exercice 3.
1. Si $d = a^2 d'$, l'équation devient

$$h^2 - d'(ak)^2 = \pm 1$$

Donc (h,k) est une solution de E_d si et seulement si (h, ak) est une solution de $E_{d'}$, voila la bijection voulue.
2. En divisant par k^2, on obtient que E_d équivaut à $\frac{h^2}{k^2} - d = \frac{\pm 1}{k^2}$, on conclut avec une identité remarquable. Ensuite, si (h,k) est une solution, alors $h > k$ et $\frac{h}{k} > 1$, par ailleurs $\sqrt{d} > 1$ également, d'où

$$2\left|\frac{h}{k} - \sqrt{d}\right| \leqslant \left|\frac{h}{k} - \sqrt{d}\right|\left|\frac{h}{k} + \sqrt{d}\right| = \frac{1}{k^2}$$

et le résultat voulu.

Exercice 4.
1. Par construction, les nombres h_n et k_n sont des entiers, en particuliers ils sont égaux à leurs conjuqués. On a alors $(xk_{n-1} - h_{n-1})_c = (x_c k_{n-1} - h_{n-1})$.
Pour alléger les notations, on pose $k := k_{n-1}, h := h_{n-1}$, $h' = h_{n-2}, k' = k_{n-2}$. On sait que $hk' - kh' = (-1)^n$. On a alors

$$\begin{aligned}
(-1)^n V_n x_n &= -N(xk - h)\frac{xk' - h'}{xk - h} \\
&= -(xk - h)(x_c k - h)\frac{xk' - h'}{xk - h} \\
&= -(x_c k - h)(xk' - h') \\
&= -(x_c x k k' - xhk' - x_c h' k + hh') \\
&= -N(x)kk' + hh' + xhk' + x_c h' k \\
&= -N(x)kk' + hh' + xhk' - xh'k \\
&= -N(x)kk' + hh' + x(-1)^n
\end{aligned}$$

Et on a bien que $-N(x)kk' + hh'$ est un rationnel (c'est même un entier).
2. Si V, V' sont deux rationnels tels que $Vx_n - \sqrt{d}$ et $V'x_n - \sqrt{d}$ sont des rationnels. Par soustraction, on a $Vx_n - \sqrt{d} - V'x_n + \sqrt{d} = x_n(V - V') \in \mathbb{Q}$. Si $V - V' \neq 0$, alors par division (comme $V - V' \in \mathbb{Q}$) on obtient que $x_n \in \mathbb{Q}$, ce qui est faux : $x_n = [a_n, a_{n+1}, \ldots]$ est un développement en fraction continue infini.
3. Comme $V_n x_n - \sqrt{d}$ est un rationnel, il est égal à son conjugué :

$$V_n x_n - \sqrt{d} = (V_n x_n - \sqrt{d})_c = V_n (x_n)_c + \sqrt{d}$$

On en déduit

$$V_n(x - x_c) = 2\sqrt{d} \Leftrightarrow V_n = \frac{2\sqrt{d}}{x - x_c} > 0$$

car $x > x_c$ par hypothèse. On sait déjà que $N(xk_{n-1} - h_{n-1}) = \pm 1 \Leftrightarrow V_n = (-1)^n N(xk_{n-1} - h_{n-1}) = \pm 1$, comme V_n est positif, $V_n = \pm 1$ si et seulement si $V_n = 1$.

4. La périodicité du développement de x en fraction continue donne $x_1 = [\overline{a_1, \ldots, a_p}] = x_{mp+1}$ pour $m \in \mathbb{N}$. Si $n = mp$ est un multiple de p, on a

$$x_n - x = a_{mp} + \frac{1}{x_{mp+1}} - a_0 - \frac{1}{x_1} = a_{mp} - a_0 \in \mathbb{N}$$

Le nombre $V = 1$ est donc tel que $x_n - x = Vx_n - \sqrt{d}$ est rationnel (entier). Par la question 2, on trouve alors $V_n = 1$.

5. On développe

$$\begin{aligned}
(-1)^n V_n &= N(xk_{n-1} - h_{n-1}) \\
&= (xk_{n-1} - h_{n-1})(xk_{n-1} - h_{n-1})_c \\
&= (xk_{n-1} - h_{n-1})(x_c k_{n-1} - h_{n-1}) \\
&= xx_c k_{n-1}^2 - x_c h_{n-1} k_{n-1} - x h_{n-1} k_{n-1} + h_{n-1}^2 \\
&= N(x) k_{n-1}^2 - T(x) h_{n-1} k_{n-1} + h_{n-1}^2
\end{aligned}$$

Le polynôme minimal de $x = \sqrt{d}$ est $X^2 - d$, on a alors $x_c = -\sqrt{d}, N(x) = -d, T(x) = 0$. Donc $(-1)^n V_n = -dk_{n-1}^2 + h_{n-1}^2$. Si $V_n = 1$ (ce qui arrive pour $n = mp$ d'après la question précédente) on trouve

$$(-1)^n = h_{n-1}^2 - dk_{n-1}^2$$

soit des solutions de l'équation de Pell-Fermat.

Exercice 5. On calcule les décompositions en fractions rationnelles de 11 et de 41 comme dans l'exercice 3. On trouve $\sqrt{11} = [3, \overline{3, 6}]$ et $\sqrt{41} = [6, \overline{2, 2, 12}]$. Deux solutions de la première équation sont alors données par

$$[3, 3] = \frac{10}{3}, \quad [3, 3, 6, 3] = \frac{199}{60}$$

Deux solutions de la deuxième sont données par

$$[6, 2, 2] = \frac{32}{5}, \quad [6, 2, 2, 12, 2, 2] = \frac{2049}{320}$$