Correction des problèmes de révisions

PROBLÈME 1. (i) Comme $D = -132$ est < 0 toute classe d'équivalence propre de formes de discriminant D contient une et une seule forme réduite au sens de Gauss. Déterminons les formes réduites (a, b, c) telles que $D = b^2 - 4ac = -132 = -4 \cdot 3 \cdot 11$ suivant la méthode du cours. On rappelle notamment que $|b| \leq a \leq c$, $a \leq \sqrt{\frac{|D|}{3}}$ et $b \equiv D \bmod 2$. Comme $132/3 = 44 < 7^2$ on a donc $a < 7$, puis $b = \pm 6, \pm 4, \pm 2, 0$. On résoud alors $ac = \frac{b^2 - D}{4}$. Si $b = 0$ alors $ac = 3 \cdot 11$, ce qui donne les formes

$$(3, 0, 11) \quad \text{et} \quad (1, 0, 33).$$

Si $b = \pm 2$ alors $a \geq 2$, puis $ac = 33 + 1 = 34 = 2 \cdot 17$, ce qui donne simplement

$$(2, 2, 17)$$

(car $(2, -2, 17)$ n'est pas réduite). Si $b = \pm 4$ alors $a \geq 4$ et $ac = 33 + 4 = 37$: il n'y a pas de telle forme réduite. Si $b = \pm 6$ alors $a \geq 6$ et $ac = 33 + 9 = 42 = 6 \cdot 7$, ce qui donne simplement la forme

$$(6, 6, 7)$$

(car $(6, -6, 7)$ n'est pas réduite). On a donc pour formes réduites de discriminant -132 les formes $(1, 0, 33)$, $(2, 2, 17)$, $(3, 0, 11)$ et $(6, 6, 7)$, puis $|\mathrm{Cl}(-132) = 4|$. On constate que toutes ces formes sont ambiguës (voir le premier point du théorème sur les formes ambiguës).

(ii) $C = \{0, 1, 4, 9, 5, 3\}$.

(iii) Soit n un entier. Si $n = x^2 + 33y^2$ alors n est un carré modulo 3, donc $n \equiv 0, 1 \bmod 3$. De même, si $n = 6x^3 + 6xy + 7y^2$ alors $n \equiv 7y^2 \equiv y^2 \bmod 3$, et donc n est aussi un carré modulo 3. Enfin, si $n = 3x^2 + 11y^2$ alors $n \equiv 3x^2 \bmod 11$ et donc n est un carré modulo 11 car $3 \in C$.

(iv) Supposons que $p \equiv 5 \bmod 12$ et que $\left(\frac{p}{11}\right) = -1$. Vérifions d'abord que p est représenté par une forme de discriminant -132. Comme $p > 2$ il faut vérifier que -132 est un carré modulo p. Par multiplicativité du symbole de Legendre on a

$$\left(\frac{-132}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{3}{p}\right) \left(\frac{11}{p}\right)$$

et par la loi de réciprocité quadratique $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right)$ et $\left(\frac{11}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{11}\right)$ car $11 \equiv 3 \bmod 4$. Si p est comme dans l'énoncé, alors $p \equiv 1 \bmod 4$, $\left(\frac{3}{p}\right) = \left(\frac{11}{p}\right) = -1$, puis $\left(\frac{-132}{p}\right) = 1$.

Le théorème de Lagrange assure alors qu'un tel p est représenté par l'une des formes $(1, 0, 33)$, $(2, 2, 17)$, $(3, 0, 11)$ et $(6, 6, 7)$. D'après le (iii), le seul cas possible est d'être représenté par $(2, 2, 17)$.

Les trois premiers nombres premiers concernés sont $p = 17, 29$ et 41, qui sont bien de la forme $2x^2 + 2xy + 17y^2$: prendre $y = 1$ et respectivement $x = 0, 2, 3$.

PROBLÈME 2. (i) Soit (a, b, c) une forme réduite de discriminant $D = 1 - 4k$ (< 0). On a $b \equiv 1 \bmod 2$, de sorte que l'on peut écrire $|b| = 1 + 2x$ avec x entier ≥ 0, et aussi $|b| \leq \sqrt{\frac{|D|}{3}} < 2\sqrt{k/3}$, et donc $0 \leq x \leq \sqrt{k/3} - 1/2$. La relation $(b^2 - D)/4 = ac$ s'écrit aussi $x^2 + x + k = ac$. Les inégalités $|b| \leq a \leq c$ et la propriété (b) entraînent donc $a = 1$ et $b = 1$, puis $c = k$: (a, b, c) est la forme principale. On a montré $(b) \Rightarrow (c)$.

(ii) Écrivons $n = x^2 + xy + ky^2$ avec x, y dans $\mathbb{Z}$. On a $4n = (2x + y)^2 + (4k - 1)y^2$. Comme n n'est pas un carré dans $\mathbb{Z}$ on a $y \neq 0$, et donc $4n \geq 4k - 1$, ce qui entraîne $n \geq k$.

(iii) D'après Lagrange, une forme q représente primitivement un entier n si, et seulement si, $\operatorname{disc} q$ est un carré modulo $4n$. On conclut car si D est un carré modulo $4n$, et si m divise n, alors D est un carré modulo $4m$.

(iv) Supposons $|\mathrm{Cl}(1-4k)| = 1$. Soient $0 \leq x < k-1$ entier et $n := x^2 + x + k$. Comme n est représenté primitivement par la forme principale de discriminant $1-4k$, le (iii) montre que tout diviseur de n est représenté primitivement par une forme de discriminant $1-4k$. Par l'hypothèse $|\mathrm{Cl}(1-4k)| = 1$, tout diviseur de n est donc représenté par la forme principale de discriminant $1-4k$. Soit ℓ un diviseur premier de n. D'après le (ii), on a $\ell \geq k$. Mais l'inégalité $x < k-1$ entraîne $n = x(x+1) + k < k(k-1) + k = k^2$. On en déduit que n est premier.

Problème 3. (i) Soit $\psi : \mathbb{Z}^n \longrightarrow A$ l'application $(x_i) \mapsto \sum_i x_i e_i$. C'est un isomorphisme de groupes abéliens par hypothèse. Soit u' l'endomorphisme de $\mathbb{Z}^n$ défini par $u' = \psi^{-1} \circ u \circ \psi$, on a $\psi \circ u' = u \circ \psi$. L'application ψ induit un isomorphisme de groupes abéliens $\mathbb{Z}^n/u'(\mathbb{Z}^n) \simeq A/u(A)$. La matrice de u' dans la base canonique de $\mathbb{Z}^n$ coincide avec la matrice U. En conclusion, on peut supposer que l'on a $A = \mathbb{Z}^n$ et que e_i est la $\mathbb{Z}$-base canonique. L'hypothèse $\det U \neq 0$ montre que les éléments $u(e_i)$, vus dans $\mathbb{R}^n$, forment une $\mathbb{R}$-base. Le sous-groupe discret $u(\mathbb{Z}^n) \subset \mathbb{Z}^n$ est donc le réseau de $\mathbb{R}^n$ engendré par cette $\mathbb{R}$-base. D'après le cours, il est d'indice fini dans $\mathbb{Z}^n$, d'indice $\mathrm{covol}(u(\mathbb{Z}^n))/\mathrm{covol}(\mathbb{Z}^n) = |\det_{e_1,\dots,e_n}(u(e_1),\dots,u(e_n))| = |\det U|$.

(ii) Si α est comme dans le cours, on a $A_D = \mathbb{Z} + \mathbb{Z}\alpha$. Comme $1, \alpha$ est une $\mathbb{R}$-base de $\mathbb{C}$, c'est évidemment une $\mathbb{Z}$-base de A_D. Si $z \in A_D$ on considère l'application $u : x \mapsto zx, A_D \to A_D$. Elle est bien $\mathbb{Z}$-linéaire. Un petit calcul montre que le déterminant de la matrice de u dans la base $1, \alpha$ est $\mathrm{N}(z)$. On conclut par le (i).

Problème 4. (i) $\mathrm{I}_{a,b}$ est un idéal de A si, et seulement si, on a $\sqrt{d}\,\mathrm{I}_{a,b} \subset \mathrm{I}_{a,b}$. Il est équivalent de demander que l'on a $a\sqrt{d} \in \mathrm{I}_{a,b}$ et $(b+\sqrt{d})\sqrt{d} = d + b\sqrt{d} \in \mathrm{I}_{a,b}$. La relation $a\sqrt{d} = a(\sqrt{d}-b) + ba$ montre que l'on a toujours $a\sqrt{d} \in \mathrm{I}_{a,b}$. L'identité $d + b\sqrt{d} = (d-b^2) + b(\sqrt{d}+b)$, et le fait que $1, \sqrt{d}$ est une $\mathbb{R}$-base de $\mathbb{C}$, montrent que l'on a $d + b\sqrt{d} \in \mathrm{I}_{a,b}$ si, et seulement si, $d - b^2 \in a\mathbb{Z}$.

(ii) On constate que si $\beta := b + \sqrt{d}$, alors $1, \beta$ est une $\mathbb{Z}$-base de A. En effet, on a $x + y\sqrt{d} = (x - by) \cdot 1 + y\beta$. De plus, $a \cdot 1$ et β est une $\mathbb{Z}$-base de $\mathrm{I}_{a,b}$. On a donc $A/\mathrm{I}_{a,b} \simeq \mathbb{Z}/a\mathbb{Z}$ (considérer par exemple l'application $\mathbb{Z}$-linéaire $A \to \mathbb{Z}/a\mathbb{Z}, x + y\beta \mapsto x \bmod a$.)

(iii) Si I est un idéal principal de A, alors il existe z dans A avec $I = Az$. On a vu en cours $\mathrm{N}(I) = \mathrm{N}(zA) = \mathrm{N}(z)$. Mais $\mathrm{N}(x + y\sqrt{d}) = x^2 + dy^2$. Donc si $\mathrm{N}(I)$ n'est pas un carré alors $\mathrm{N}(I) \geq d$.

(iv) D'après le (i), (ii) et (iii), pour tout entier $b \in \mathbb{Z}$ et tout entier $a > 0$ non carré tell que a divise $b^2 - d$, on a $a \geq d$. Pour $b = 0$, cela montre que soit $-d = 1$ ou 2, soit $-d$ est premier impair. Dans ce dernier cas, on réapplique l'observation à $b = 1$, de sorte que $1 - d$ est pair, et $a = 2$. On en déduit $|d| \leq 2$.