ANNEXE B

Solutions, indications et corrigés

1. Exercices du chapitre 1

Exercice 1.1. Les nombres 47 et 79 sont premiers $\equiv 3 \bmod 4$, d'où les égalités

$$\left(\frac{47}{79}\right) = -\left(\frac{79}{47}\right) = -\left(\frac{32}{47}\right) = -\left(\frac{2}{47}\right) = -1$$

et donc 49 n'est pas un carré modulo 79.

Exercice 1.3. On a $4(X^2+aX+b) = (2X+a)^2 - D$. Observer aussi que X^2+X+1 est le seul polynôme irréductible de degré 2 dans $\mathbb{Z}/2\mathbb{Z}[X]$.

Exercice 1.5. Observer que l'on a $\prod_{a=1}^{\frac{p-1}{2}}(p-a) \equiv (-1)^{\frac{p-1}{2}}(\frac{p-1}{2})! \bmod p$.

Exercice 1.6. Pour le (ii), on pourra imiter les décompositions dans $\mathbb{C}[X]$

$$X^4+1 = (X^2+i)(X^2-i) = (X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1) = (X^2+i\sqrt{2}X-1)(X^2-i\sqrt{2}-1).$$

Exercice 1.7. Observer que -1 est une puissance 4ème si et seulement si $(\mathbb{Z}/p\mathbb{Z})^\times$ admet un élément d'ordre 8. Conclure par la cyclicité de ce dernier.

Exercice 1.8. (i) Observer que $x \mapsto p-x$ échange les carrés de $\{1,\dots,\frac{p-1}{2}\}$ et ceux de $\{\frac{p+1}{2},\cdots,p-1\}$. Le (ii) découle du (i) car $C+N \equiv 1 \bmod 2$ si $p \equiv 3 \bmod 4$. Pour les (iii) et (iv), écrire

$$A = \sum_{a=1}^{\frac{p-1}{2}} \left[a\left(\frac{a}{p}\right) + (p-a)\left(\frac{p-a}{p}\right)\right] \quad \text{et} \quad A = \sum_{a=1}^{\frac{p-1}{2}} \left[2a\left(\frac{2a}{p}\right) + (p-2a)\left(\frac{p-2a}{p}\right)\right].$$

Exercice 1.9.(i) $\mathrm{N}(x^2=a)$ vaut 1 si $a=0$, 2 si a est un carré, 0 sinon, ce qui coïncide dans tous les cas avec $1+\left(\frac{a}{p}\right)$. Pour le (ii), observer que si $a \neq 0$ on a

$$\left(\frac{a(1-\alpha a)}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{(1-\alpha a)}{p}\right) = \left(\frac{a}{p}\right)^{-1}\left(\frac{(1-\alpha a)}{p}\right) = \left(\frac{a^{-1}-\alpha}{p}\right),$$

puis que $a \mapsto a^{-1}-\alpha$ est une bijection de $(\mathbb{Z}/p\mathbb{Z})^\times$ sur $\mathbb{Z}/p\mathbb{Z}-\{-\alpha\}$. Au (v) on trouve $1+(p-1)(1+\left(\frac{-\alpha\beta}{p}\right))$ solutions.

Exercice 1.10. Si m est un carré modulo n, il l'est aussi modulo tous les premiers divisant n, et donc $\left(\frac{m}{n}\right) = 1$ par définition.

Exercice 1.11. Supposons $x^{\frac{n-1}{2}} = \left(\frac{x}{n}\right)$ pour tout $x \in (\mathbb{Z}/n\mathbb{Z})^\times$. Si n n'est pas premier, on pourra écrire $n = p^\alpha m$ avec $(m,p)=1$ et considérer un x tel que $x \equiv 1 \bmod m$ et $x \bmod p^\alpha$ est un générateur de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. Pour le (ii), observer que $x \mapsto x^{\frac{n-1}{2}}\left(\frac{x}{n}\right)^{-1}$ est un morphisme de groupes non trivial $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$, son noyau est donc de cardinal $\leq \frac{\varphi(n)}{2}$.

Exercice 1.12. Soit $S = \sum_{a=1}^{p-1} a^j$, où $j \geq 1$ est un entier. Observer que $x^j S \equiv S \bmod p$ pour tout $x \in \mathbb{Z}$ premier à p. En considérant une racine primitive modulo p, en déduire $S \equiv 0 \bmod p$ si $j \neq 0 \bmod p-1$.

Exercice 1.13. On a $\sum_{a=0}^{p-1}\zeta^{a^2} = 1 + 2\sum_{a\in C(p)}\zeta^a = 2\sum_{a\in C(p)}\zeta^a - \sum_{a=1}^{p-1}\zeta^a = G$.

Exercice 1.14. Soit $a \leq k \leq b-1$ un entier. On applique le théorème de convergence de Dirichlet (en analyse de Fourier) à la fonction 1-périodique nulle aux entiers et coïncidant avec f sur $]k, k+1[$. On en déduit

$$\frac{f(k)+f(k+1)}{2} = \lim_{A\to\infty} \sum_{n=-A}^{A} \int_k^{k+1} f(t)e^{2i\pi nt}dt.$$

Le (i) en découle en sommant sur $k = a, \ldots, b-1$, la sommation dans l'énoncé étant à prendre au sens ci-dessus. Pour le (ii), on applique le (i) à la fonction $f(t) = e^{2i\pi t^2/N}$ sur le segment $[0, N]$. Un changement de variables $u = t + \frac{nN}{2}$ montre

$$\int_0^N f(t)e^{2i\pi nt}dt = i^{-n^2}N \int_{\frac{nN}{2}}^{\frac{(n+2)N}{2}} e^{\frac{2i\pi u^2}{N}}du,$$

le (ii) s'en déduit en séparant les n pairs et impairs. On en déduit enfin $I = (1-i)^{-1} = \frac{1+i}{2}$ en prenant $N = 1$, car dans ce cas on a $G_1 = 1$.

Exercice 1.15. Pour le (ii), observer que si $p-1 = 2\ell$ avec $\ell = \frac{p-1}{2}$ premier, un élément x de $(\mathbb{Z}/p\mathbb{Z})^\times$ est une racine primitive si et seulement si son ordre n'est pas $1, 2$ ou $\ell = \frac{p-1}{2}$.

Exercice 1.16. Un élément du groupe additif $\mathbb{Z}/2^n\mathbb{Z}$ est générateur si et seulement si il n'est pas congru à 0 modulo 2, le (i) s'ensuit en considérant une racine primitive modulo p. Pour le (ii), observer que si $p > 3$ alors $p \equiv 1 \bmod 4$ et $p \equiv 2 \bmod 3$, donc $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$.

Exercice 1.17. En utilisant l'exercice précédent, vérifier que 10 est une racine primitive modulo 65537. Le résultat est donc 65536.

Exercice 1.18. Considérons la $\mathbb{R}$-algèbre $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ des quaternions de Hamilton. Le sous-groupe fini $\{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{H}^\times$ n'est pas cyclique (ni même commutatif).

Exercice 1.19. Remarquer que $(\mathbb{Z}/2\mathbb{Z})^r$ n'est pas cyclique si $r > 1$. Si p est premier et $n \geq 1$, observer que $(\mathbb{Z}/p^n\mathbb{Z})^\times$ admet un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z}$, même à $(\mathbb{Z}/2\mathbb{Z})^2$ si $p = 2$ et $n \geq 3$. La condition nécessaire du (ii) se déduit alors du (i) et de l'isomorphisme chinois des restes.

Exercice 1.21. Considérer par exemple les $\sqrt[2^i]{N}$ pour $i \geq 1$.

Exercice 1.22. Si p et q sont premiers impairs, la relation d'Eisenstein montre $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^s$ où s est le nombre de points à coordonnées entières à l'intérieur du rectangle OP'S'Q'. En effet, les seuls points à coordonnées entières sur la diagonale $y = qx/p$ du rectangle OPSQ sont O et S car p et q sont premiers entre eux. On conclut le (i) car on a $s = \frac{p-1}{2}\frac{q-1}{2}$.

Montrons la relation d'Eisenstein. Comme q est premier à p, la multiplication par q est injective dans $\mathbb{Z}/p\mathbb{Z}$; on a donc $|R| = |X| = \frac{p-1}{2}$. Pour montrer le (ii) il suffit alors de voir que l'application de l'énoncé est injective. Soient $r, r' \in R$ de parités différentes et tels que $r + r' = p$. On écrit $r \equiv qx \bmod p$ et $r' \equiv qx' \bmod p$ pour $x, x' \in X$. Il vient $x + x' \equiv 0 \bmod p$ car q est premier à p, puis $x + x' = p$, ce qui est absurde modulo 2.

Le (ii) entraîne $\prod_{x\in X} x \equiv \prod_{r\in R}(-1)^r r \bmod p$. Le (iii) s'en déduit car on a $\prod_{r\in R} r \equiv q^{\frac{p-1}{2}} \prod_{x\in X} x \bmod p$ (le produit sur X est non nul car p est premier).

Le (iv) est immédiat car x est pair et p est impair. On a déjà observé que la droite $y = qx/p$ ne contient aucun point (x, y) avec $y \in \mathbb{Z}$ et $x \in X$ car q est premier à p, on a donc $f = \sum_{x\in X}[qx/p]$ en dénombrant abscisse par abscisse, ce qui prouve le (v) d'après le (iv).

Pour le (vi), on raisonne abscisse par abscisse en observant qu'il y a $q-1$ entiers compris strictement entre 0 et q, et $q - 1 \equiv 0 \bmod 2$. La symétrie $(x, y) \mapsto (p - x, q - y)$ identifie les points à coordonnées entières et d'abscisse paire intérieurs au triangle S'SQ", aux points à coordonnées entières et d'abscisse impaire intérieurs au triangle OP'S'. Le (vii) se déduit alors de (v) et (vi).

Le premier point du (viii) découle du (v) pour $q = 2$. Si $n \in \mathbb{Z}$ est un entier impair, notons $f(n)$ le nombre d'entiers pairs compris entre $n/2$ et n. On a $f(1) = 0$, $f(3) = 1$, $f(5) = 1$ et $f(7) = 2$. On observe de plus $f(n + 8) = f(n) + 2$. Ainsi, on a $f(n) \equiv \frac{n^2-1}{8} \bmod 2$.

2. Exercices du chapitre 2

Exercice 2.1. $(a,b) = b\,(m,1) + \frac{a-mb}{n}\,(n,0)$.

Exercice 2.2. Ce groupe abélien L est un réseau car il est compris entre $\mathbb{Z}^3$ et $10\mathbb{Z}^3$. C'est le noyau du morphisme de groupes $\mathbb{Z}^3 \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(a,b,c) \mapsto (a-b \bmod 5, b-a-c \bmod 2)$. Ce morphisme est surjectif, comme on le voit en considérant les éléments $(0,0,1)$ et $(1,0,1)$. Le réseau L est donc de covolume 10. Une base est donnée par les éléments $(1,1,0)$, $(0,5,1)$ et $(0,0,2)$. En effet, on a $(a,b,c) = a\,(1,1,0) + \frac{b-a}{5}\,(0,5,1) + \frac{5c-(b-a)}{10}\,(0,0,2)$.

Exercice 2.5. D'après le cours, le covolume de $L(e)$ est $|\det(e_1,\dots,e_n)|$. De plus, l'indice de $L(e)$ dans L est l'entier $\mathrm{covol}(L)/|\det(e_1,\cdots,e_n)|$. Ainsi, on a $L = L(e)$ si et seulement si cet indice est 1, i.e. $\mathrm{covol}(L) = |\det(e_1,\cdots,e_n)|$.

Exercice 2.6. Pour le (i), notons (e_i) la $\mathbb{Z}$-base canonique de $\mathbb{Z}^n$. On constate que pour tout (x_i) élément de $\mathbb{Z}^n$, il existe une unique partie $I \subset \{1,\dots,n\}$, et un unique $y \in 2\mathbb{Z}^n$, vérifiant $x - y = \sum_{i\in I} e_i$. L'indice en question est donc $|\mathcal{P}(I)| = 2^n$.

Exercice 2.7. Si $e_1,\dots,e_m$ engendre A comme groupe abélien, alors $\mathrm{Vect}_{\mathbb{Q}}(A) = \mathrm{Vect}_{\mathbb{Q}}(e_1,\dots,e_m)$ est de dimension finie $\leq m$. Pour le (ii), extraire de $\{e_i\}$ une $\mathbb{Q}$-base de $\mathrm{Vect}_{\mathbb{Q}}(A)$, disons $e_1,\dots,e_n$ quitte à renuméroter les e_i. Décomposer les e_j dans la $\mathbb{Q}$-base des e_i avec $i \leq n$ et prendre pour N le ppcm des dénominateurs des $n \cdot m$ coordonnées obtenues. Considérer enfin les inclusions $\mathbb{Z}^n \subset f^{-1}(A) \subset \frac{1}{N}\mathbb{Z}^n$ (injectivité de f).

Exercice 2.8. Soit p un nombre premier impair tel que $\left(\frac{-6}{p}\right) = 1$. Comme $\frac{4\sqrt{6}}{\pi} < \frac{10}{\pi} < 4$ au moins l'un de p, $2p$ ou $3p$ est de la forme a^2+6b^2. Si p est de la forme a^2+6b^2 on constate que a est impair, puis $p \equiv \pm 1 \bmod 8$. Si $2p$ est de la forme a^2+6b^2 alors $a = 2c$ est pair et on a donc $p = 2c^2+3b^2$. De même si $3p = a^2+6b^2$ alors $a = 3c$ est multiple de 3 et $p = 3c^2+2b^2$. Pour conclure, il suffit de remarquer que si p est de la forme $2a^2+3b^2$ alors b est impair, puis $p \equiv \pm 3 \bmod 8$.

Exercice 2.9. Pour le (i), observer que si $3n = a^2+11b^2$ alors $\pm a \equiv b \bmod 3$. Se ramener au cas $a \equiv b \bmod 3$ et poser $a = b+3u$. Pour l'assertion concernant $4n$ raisonner modulo 2. Pour le (ii), distinguer selon que a est pair, b est pair, ou a et b sont impairs, et utiliser les secondes identités remarquables. Le (iii) se déduit de $4\frac{\sqrt{11}}{\pi} < \frac{14}{\pi} < 5$ et de (i) et (ii). Pour le (iv), appliquer le (i) à $3p$ ou $4p$.

Exercice 2.10. Les ensembles $P(N)$ et $Q(N)$ sont non vides. En effet, le premier contient 1, et pour le second on peut par exemple invoquer le lemme 8.16. Donnons une autre méthode, basée sur l'observation que 3 et 4 sont de la forme $3a^2+2ab+4b^2$, mais ne sont pas toujours inversibles modulo N. Soient M et N des entiers premiers entre eux. On observe que l'isomorphisme chinois $\mathbb{Z}/MN\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ induit une bijection $Q(MN) \xrightarrow{\sim} Q(M) \times Q(N)$. En particulier, il suffit de montrer que $Q(N)$ est non vide lorsque N est impair, et lorsque N est une puissance de 2. Mais si N est impair (resp. non divisible par 3), la classe de 4 (resp. 3) est dans $Q(N)$.

Montrons $P(N) = Q(N)$. Les premières et dernières identités remarquables montrent respectivement que $P(N)$ et $Q(N)$ sont stables par multiplication, ce sont donc des sous-groupes du groupe $(\mathbb{Z}/N\mathbb{Z})^\times$ car ce dernier est fini. En particulier, 1 est dans $P(N)$ et $Q(N)$. Les secondes et troisièmes identités montrent respectivement $P(N)\cdot Q(N) \subset P(N)$ et $P(N)\cdot Q(N) \subset Q(N)$. Comme $1 \in P(N), Q(N)$, on en tire $Q(N) \subset P(N)$ et $P(N) \subset Q(N)$, *i.e.* $P(N) = Q(N)$. Le (ii) découle des identités remarquables données et du corollaire 2.37.

Exercice 2.12. Pour le (i), la considération de l'homothétie de rapport r montre $\mu(C_n(r)) = r^n c_n$. Si $n \geq 2$ on calcule c_n par tranches selon la coordonnée $t = x_n$:

$$c_n = \int_{-1}^{1} \mu(C_{n-1}(\sqrt{1-t^2}))dt.$$

Pour le (ii), on intègre deux fois par parties.

Exercice 2.13. Pour le (i), on constate sur la table 3 que si $n \leq 4$ alors $\sqrt{2}^n c_n > 2^n$. Ainsi, pour un $0 < r < \sqrt{2}$ assez proche de $\sqrt{2}$, on a $\mu(C_n(r)) > 2^n \mathrm{covol}(L)$. Le lemme du corps convexe de Minkowski assure donc que L contient un élément v non nul tel que $v\cdot v < 2$, on conclut car $v\cdot v$ est entier par hypothèse. Pour le (ii), on pose $u = x - (x\cdot v)v$. Pour le (iii) on observe que si l'espace euclidien $\mathbb{R}^n$ est somme directe orthogonale de deux sous-espaces U_1 et U_2, et si L_i est un réseau de U_i, alors $\mathrm{covol}(L_1 \oplus L_2) =$

covol(L_1)covol(L_2), où tous ces covolumes sont calculés de sorte que le pavé fondamental d'une base orthonormée soit de volume 1.

Exercice 2.14. Pour le (i), observer que D_8 est d'indice 2 dans $\mathbb{Z}^8$, donc de covolume 2. Pour le (ii), observer que tout élément de E_8 est soit dans D_8, soit de la forme $u+e$ avec $u \in \mathrm{D}_8$. Autrement dit, D_8 est d'indice 2 dans E_8, qui est donc de covolume 1. Pour le (iii), observer que $e \cdot e = 2$ et que $e \cdot u \in \mathbb{Z}$ si $u \in \mathrm{D}_8$. Pour le (iv), remarquer que 1 n'est pas pair, donc ne peut pas être de la forme $v \cdot v$.

3. Exercices du chapitre 3

Exercice 3.1. La forme $(5, 16, 13)$ est de discriminant -4. D'après le cours il n'y a qu'une telle forme de ce discriminant à équivalence près (équivalente à $(1, 0, 1)$). Si $p \equiv 1 \bmod 4$ alors -4 est un carré modulo p, et donc $(5, 16, 13)$ représente p par Lagrange.

Exercice 3.4. (vu en cours) On a $\sqrt{44/3} < 4$. Les formes réduites de discriminant -20 sont les trois formes $(1, 0, 11)$ et $(3, \pm 2, 4)$. Seule la première est ambiguë, les deux autres étant opposées. À équivalence près, les deux formes de discriminant -44 sont donc $(1, 0, 11)$ et $(3, 2, 4)$.

Exercice 3.5. On a $\sqrt{84/3} < 6$. Les formes réduites de discriminant $-84 = -3 \cdot 4 \cdot 7$ sont les formes $(1, 0, 21)$, $(3, 0, 7)$, $(2, 2, 11)$ et $(5, 4, 5)$, qui sont toutes ambiguës.

Exercice 3.6. On a $\sqrt{56/3} < 5$. Les formes réduites de discriminant $-56 = -8 \cdot 7$ sont donc $(1, 0, 14)$, $(2, 0, 7)$ et $(3, \pm 2, 5)$.

Exercice 3.7. Si $D \equiv 0 \bmod 4$, les couples $(x, y) \in \mathbb{Z}^2$ tels que $x^2 - \frac{D}{4}y^2 = 1$ sont $(\pm 1, 0)$, sauf si $D = -4$ auquel cas il y a aussi $(0, \pm 1$. Si $D \equiv 1 \bmod 4$. Les couples $(x, y) \in \mathbb{Z}^2$ tels que $x^2 + xy + \frac{1-D}{4}y^2 = 1$, soit encore tels que $(2x + y)^2 - Dy^2 = 4$, sont $(\pm 1, 0)$, sauf si $D = -3$ auquel cas il y a aussi $\pm(1, -1)$. Pour le (ii), observer que $(1 + \sqrt{2})(1 - \sqrt{2}) = -1$ puis que $a_n^2 - 2b_n^2 = (-1)^n$ pour tout entier $n \in \mathbb{Z}$.

Exercice 3.9 Le (i) est immédiat. Observer que si $c, d \in \mathbb{R}$ et $\tau \in \mathbb{H}$, alors $c\tau + d \neq 0$. L'action naturelle de $\mathrm{GL}_2(\mathbb{C})$ sur $\mathbb{C}^2$ définit par restriction une action de $\mathrm{GL}(2, \mathbb{R})$ sur $\mathbb{C}^2$. Si $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, et si $\tau \in \mathbb{H}$, on constate que

$$g \begin{pmatrix} \tau \\ 1 \end{pmatrix} = (c\tau + d) \begin{pmatrix} g \cdot \tau \\ 1 \end{pmatrix}.$$

Le (ii) s'ensuit (sans calcul !). Pour le (iii) considérer les éléments $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ de $\mathrm{SL}_2(\mathbb{Z})$.

Le (iv) est plus délicat. Fixons $\tau_0 \in \mathbb{H}$ et considérons son orbite $O = \mathrm{SL}_2(\mathbb{Z}) \cdot \tau_0 \subset \mathbb{H}$. Montrons que $\tau \mapsto \mathrm{Im}(\tau)$ atteint son maximum sur O en un élément de $O \cap D$. Observons que $\mathbb{Z} + \tau_0\mathbb{Z}$ est un réseau de $\mathbb{C}$: il n'a donc qu'un nombre fini d'éléments dans le disque unité. Il résulte de ceci et du (i) que l'ensemble des $\mathrm{Im}(\tau)$ avec $\tau \in O$ admet un plus grand élément, disons $\mathrm{Im}(\tau)$. Quitte à user des translations (inverses l'une de l'autre et préservant O), $\tau \mapsto \tau \pm 1$, on peut supposer sans changer $\mathrm{Im}(\tau)$ que $-\frac{1}{2} < \mathrm{Re}(\tau) \leq \frac{1}{2}$. Par maximalité on a encore, $|c\tau + d| \geq 1$ pour tout $(c, d) \in \mathbb{Z}^2$ premiers entre eux. Pour $(c, d) = (1, 0)$ on obtient $|\tau| \geq 1$. Si $|\tau| > 1$ alors $\tau \in D$. Si $|\tau| = 1$, alors quitte à remplacer τ par $-1/\tau \in O$, ce qui ne change pas $\mathrm{Im}(\tau)$, on peut encore supposer que $\tau \in D$, ce que l'on voulait.

Pour vérifier l'unicité, observons que si $z \in D$ et $|cz + d| \leq 1$ avec $c, d \in \mathbb{Z}$ premiers entre eux, alors soit $(c, d) = (0, \pm 1)$, soit $(c, d) = (\pm 1, 0)$ et $|z| = 1$, soit $(c, d) = \pm(1, -1)$ et $z = \rho := e^{i\pi/3}$ (observer que $|c| \geq 2$ est impossible car $\mathrm{Im}(z) \geq \frac{\sqrt{3}}{2} > \frac{1}{2}$). Supposons maintenant que $g \cdot \tau \in D \cap O$ avec τ comme précédemment et $g^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Par maximalité de $\mathrm{Im}(\tau)$, et $\tau = g^{-1} \cdot (g \cdot \tau)$, on a $|c\, g \cdot \tau + d| \leq 1$. On applique l'observation à $z = g \cdot \tau$. Si $c = 0$ et $d = \pm 1 = a$, alors g^{-1} est la translation $\tau \mapsto \tau + ab$, et donc $b = 0$ et $\tau = z$ à cause des conditions sur la partie réelle. Si $c = \pm 1$, $d = 0$, et $|z| = 1$, alors $b = -c$ et donc $g^{-1}.z = a/c - \frac{1}{z} = \tau \in D$. Par définition de D cela entraîne $z = \tau = \rho$ et $a/c = 1$. Enfin, si $c = -d = \pm 1$, donc $(a + b)d = 1$, alors $\tau = \frac{az+b}{cz+d} = \frac{a/d\,(z-1)+1}{1-z} = -a/d + \frac{1}{1-z}$. Dans ce cas on a vu que $z = \rho$, de sorte que $1/(1 - z) = z$, d'où l'on tire que $a = 0$ et encore $\tau = z$.

Pour le (v), on a $\tau(q) = -\frac{b}{2a} + \frac{\sqrt{D}}{2a}$ où $D < 0$ est le discriminant de (a, b, c) et $\sqrt{D} \in \mathbb{H}$. Un calcul sans difficulté montre que $\tau(q \cdot P) = P^{-1} \cdot \tau(q)$. Pour le (vii), on observe d'abord que q est réduite au sens de Gauss si et seulement si $\tau(q) \in D$, et on conclut par le (iv).