9. Corrigé de l'examen 2011-2012

Problème 1. (i) Il suffit de déterminer les formes réduites de Gauss (a,b,c) de discriminant -136. Elles satisfont en particulier $b \equiv 0 \bmod 2$ et $|b| \leq a \leq \sqrt{\frac{136}{3}} < 7$ car $136/3 < 49$. On trouve $(1,0,34)$, $(2,0,17)$ et $(5,\pm 2,7)$.

(ii) Les classes ambigües sont celles de $(1,0,34)$ et $(2,0,17)$. Il y a donc 3 formes à équivalence près : $(1,0,34)$, $(2,0,17)$ et $(5,2,7)$.

(iii) La loi de réciprocité quadratique assure que pour $p \neq 2,17$

$$\left(\frac{-136}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{17}{p}\right) = (-1)^{\frac{p-1}{4}+\frac{p^2-1}{8}}\left(\frac{p}{17}\right)$$

car $17 \equiv 1 \bmod 4$. Si p est comme dans l'énoncé il vient que -136 est un carré modulo p, et donc modulo $4p$ car $-136 \equiv 0 \bmod 4$ et p est impair. Il est donc représenté par l'une des formes $(1,0,34)$, $(2,0,17)$ et $(5,2,7)$ (et même une seule) par le (ii) et le théorème de Lagrange.

Si p est représenté par l'une des deux premières alors soit $p \equiv 2x^2 \bmod 17$, soit $p \equiv x^2 \bmod 17$, ce qui est absurde car p n'est pas un carré modulo 17, alors que 2 l'est ($17 \equiv 1 \bmod 8$).

(iv) A est de Dedekind car -34 est sans facteur carré et $\equiv 2 \bmod 4$.

(v) On a les factorisations $X^2+34 \equiv X^2$ modulo 2, irréductible modulo 3, $\equiv X^2-1$ modulo 5 et 7. On en déduit que (3) est premier. De plus, si $D = 2A+\alpha A$, $C = 5A+(\alpha+1)A$, $C' = 5A+(\alpha-1)A$, $S = 7A+(\alpha+1)A$ et $S' = 7A+(\alpha-1)A$, alors ces idéaux sont premiers distincts et on a : $(2) = D^2$, $(5) = CC'$, $(7) = SS'$.

On a $\alpha+1 \in C,S$ donc les idéaux premiers distincts C et S divisent $(\alpha+1)$. Mais $\mathrm{N}(\alpha+1) = 35 = \mathrm{N}(C)\mathrm{N}(S)$ donc $(\alpha+1) = CS$.

(vi) Minkowski nous dit que toute classe d'idéaux non nuls contient un idéal contenant $1 \leq N \leq 7$, i.e. divisant (N) pour un tel N par la propriété de Dedekind. Ces idéaux sont donc produits d'idéaux premiers contenant $2,3,5$ ou 7. Ainsi, $\mathrm{Cl}(A)$ est engendré par tous les idéaux premiers ci-dessus. Les relations $[C][C'] = 1$, $[S][S'] = 1$ et $[C][S] = 1$ assure que $\mathrm{Cl}(A)$ est engendré par $[C]$ et $[D]$.

(vii) $\mathrm{N}(D) = 2$ et 2 n'est pas de la forme x^2+34y^2 donc D n'est pas principal. Par contre $\mathrm{N}(CD^2) = 2 \cdot 25 = 50$ est la norme des éléments $\pm(\alpha \pm 4)$. Comme $\alpha - 4$ n'est pas dans C' (sinon on aurait aussi $\alpha - 1 - (\alpha-4) = 3 \in C'$ puis $5 - 2 \cdot 3 = -1 \in C'$ ce qui est absurde), la propriété de Dedekind entraîne $DC^2 = (\alpha-4)$.

(viii) On a $[D]^2 = 1$ car $(2) = D^2$, et $[D] \neq 1$, donc $[D]$ est d'ordre 2. De plus, $[D][C]^2 = 1$, donc $[D] = [C]^2$ d'où l'on tire que $\mathrm{Cl}(A)$ est engendré par $[C]$ qui est d'ordre 4.

(ix) Le théorème de Dedekind définit un isomorphisme de groupes entre $\mathrm{Cl}(A)$ avec $\mathrm{Cl}(-136)$, ce dernier étant muni de la loi de composition de Gauss. On a donc $\mathrm{Cl}(-136) \simeq \mathbb{Z}/4\mathbb{Z}$. La classe principale est l'élément neutre, l'autre classe ambigüe $[(2,0,17)]$ est l'élément d'ordre 2, et les classes de $[(5,\pm 2,7)]$ sont donc des générateurs (inverses l'un de l'autre). Cela détermine uniquement la table de multiplication.

(x) En particulier, $[(5,2,7)]^2 = [(2,0,17)]$ et $[(5,2,7)][(5,-2,7)] = 1$. Le résultat s'en déduit car une composée de Gauss est une composée au sens du cours.

(xi) 5 et 7 ont les propriétés requises. On a $35 = 2 \cdot 9 + 17 = 1 + 34$.

Problème 2. (i) Les conjugués sur $\mathbb{Q}$ de ζ sont les racines de $\Pi_{\zeta,\mathbb{Q}} = X^4+1$, i.e. ζ, ζ^3, ζ^5 et ζ^7 qui sont tous complexes non réels, donc l'entier r_2 du corps de nombres $\mathbb{Q}(\zeta)$ est $\frac{4}{2} = 2$. Le discriminant de X^4+1 vaut 4^4 par une formule du cours, le covolume de $\iota(\mathbb{Z}[\zeta])$ vaut donc

$$\frac{1}{2^{r_2}}|4^4|^{1/2} = 4.$$

(ii) D'après Minkowski tout idéal non nul de $\mathbb{Z}[\zeta]$ est équivalent à un idéal contenant un entier N compris entre 1 et $\left(\frac{4}{\pi}\right)^2 \frac{4!}{4^4} \cdot 4 \cdot 4 = 3\frac{8}{\pi^2} < 3$.

(iii) Comme $X^4+1 \equiv (X-1)^4 \bmod 2$, on déduit du cours que les idéaux de $\mathbb{Z}[\zeta]$ contenant 2 sont les 5 idéaux $I_i = (2,(\zeta-1)^i)$ avec $i = 0,\ldots,4$. On a $I_0 = \mathbb{Z}[\zeta]$ (l'anneau tout entier) qui est aussi l'unique idéal contenant 1.

(iv) La dérivée en 1 de $X^8 - 1 = \prod_{i=0}^{7}(X - \zeta^i)$ s'écrit de deux façons

$$8 = \prod_{i=1}^{7}(1 - \zeta^i).$$

Mais $\zeta^2 = i$, $\zeta^4 = -1$ et $\zeta^6 = -i$, donc $(1-\zeta^2)(1-\zeta^4)(1-\zeta^6) = (1-i)(1+i)2 = 4$, ce qui conclut la première formule. Pour la seconde on remarque que pour tout $i = 1, \dots, 7$ on a

$$1 - \zeta^i = (1-\zeta)(\sum_{k=0}^{i-1}\zeta^k) \in (1-\zeta)\mathbb{Z}[\zeta].$$

(v) On déduit du (iv) que $2 \in (1-\zeta^i)$ pour $i \leq 4$, donc $I_i = ((1-\zeta)^i)$ est principal.

(vi) On en déduit que tout idéal de $\mathbb{Z}[\zeta]$ est équivalent à un idéal principal : $\mathbb{Z}[\zeta]$ est principal.

(vii) Principal implique factoriel implique intégralement clos, donc $\mathbb{Z}[\zeta]$ est intégralement clos. Il contient donc l'anneau des entiers de $\mathbb{Q}(\zeta)$, et donc il est égal à ce dernier.

Problème 3. (i) Soient $x, y \in \mathbb{Z}$ tels que $y^2 = x^5 + k$. On a $y \equiv x \bmod 2$ car $k \equiv 0 \bmod 2$. Il suffit donc de montrer que x et y sont premiers entre eux. Si $d > 1$ divse x et y alors d^2 divise k : absurde.

(ii) L'idéal $(y+\alpha, y-\alpha)$ contient $2y$ et $(y-\alpha)(y+\alpha) = x^5$. Mais $2y$ et x^5 sont premiers entre eux par le (i), il contient donc 1 par Bézout.

(iii) On a $(y-\alpha)(y+\alpha) = (x)^5$. Comme les idéaux $(y-\alpha)$ et $(y+\alpha)$ sont premiers entre eux dans l'anneau de Dedekind $\mathbb{Z}[\alpha]$ (car $k \equiv 2 \bmod 4$ est sans facteur carré), on déduit de l'unicité de la décomposition en produit d'idéaux premiers que $(y+\alpha)$ est de la forme I^5 pour un certain idéal I de $\mathbb{Z}[\alpha]$.

(iv) On sait que $\mathrm{h}(4k)$ est le cardinal du groupe $\mathrm{Cl}(A)$. Si il est premier à 5, ce groupe n'a pas d'élément d'ordre 5. Comme $[I]^5 = [I^5] = 1$, il vient que $[I] = 1$.

(v) Ainsi, I est principal, disons engendré par $z \in \mathbb{Z}[\alpha]$. On a donc $(y+\alpha) = (z^5)$ puis $y + \alpha = uz^5$ où u est une unité de A, i.e. $u = \pm 1$ par un résultat du cours. Mais alors $u = u^5$ et donc $y + \alpha = (uz)^5$. Soient $a, b \in \mathbb{Z}$ des entiers tels que $uz = a + b\alpha$. On conclut par la formule du binôme.

(vi) On rappelle que $1, \alpha$ est une $\mathbb{Z}$-base de A. En égalisant le coefficient en α on obtient

$$1 = b(5a^4 + 10a^2b^2k + b^4k^2).$$

Donc $b = \pm 1$ (tous les termes sont entiers), puis $b^2 = b^4 = 1$, d'où la première assertion. En égalisant le coefficient en 1 on constate aussi que $y \equiv a \bmod 2$, donc a est impair. En particulier $a^2 \equiv 1 \bmod 8$. Il vient $5 + k(k+2) \equiv \pm 1 \bmod 8$. Comme k est pair, $k(k+2) \equiv 0 \bmod 8$, puis $5 \equiv \pm 1 \bmod 8$: c'est absurde.

(vii) On regarde les entiers $3^5 - y^2 > 0$ avec y impair, i.e. $y \in \{1, 3, 5, 7, 9, 11, 13, 15\}$. On trouve respectivement $242, 234, 218, 194, 122, 74, 18$. Mais 9 divise 18 et 234, et $11^2 \cdot 2 = 242$. Par contre, $218 = 2 \cdot 109$, $194 = 2 \cdot 97$, $122 = 2 \cdot 67$ et $74 = 2 \cdot 37$ sont sans facteur carré : ces valeurs de k conviennent donc et on en déduit le résultat.

10. Corrigé de l'examen 2012-2013

Problème 1. (i) Les carrés de $(\mathbb{Z}/13\mathbb{Z})^\times$ sont $\pm 1, \pm 3$ et ± 4.

(ii) On a $-104 = -8 \cdot 13$. En particulier -104 est un carré modulo 13. Si $p \neq 2, 13$, on a

$$\left(\frac{-104}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{13}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{p}{13}\right)$$

Ainsi -104 est un carré modulo p si et seulement si $\left(\frac{-2}{p}\right) = \left(\frac{p}{13}\right)$. Mais $\left(\frac{-2}{p}\right) = (-1)^{\frac{p-1}{4}+\frac{p^2-1}{8}}$ vaut 1 si et seulement si $p \equiv 1, 3 \bmod 8$. On conclut par le (i).

(iii) Il suffit de déterminer les formes réduites de Gauss (a, b, c) de discriminant -104. Elles satisfont en particulier $b \equiv 0 \bmod 2$ et $|b| \leq a \leq \sqrt{\frac{104}{3}} < 6$ car $104/3 < 35 < 6^2$. On trouve $(1, 0, 26)$ et $(2, 0, 13)$ pour $b = 0$, $(3, \pm 2, 9)$ pour $b = \pm 2$, et $(5, \pm 4, 6)$ pour $b = \pm 4$.

(iv) Les classes ambiguës sont celles de $(1, 0, 26)$ et $(2, 0, 13)$. Il y a donc 4 formes à équivalence (non nécessairement propre) près : $(1, 0, 34)$, $(2, 0, 13)$, $(3, 2, 9)$ et $(5, 4, 6)$.

(v) Si $p \equiv 1, 3 \bmod 8$ et p est un carré modulo 13, alors -104 est un carré modulo p d'après le (ii). Il l'est donc également modulo $4p$ car $-104 \equiv 0 \bmod 4$ et p est impair. Il est donc représenté par l'une des 4 formes précédentes, et même par une seule, d'après un résultat du cours dû à Lagrange. Si p est de la forme $2x^2 + 13y^2$ alors $p \equiv 2x^2$ modulo 13, ce qui est absurde car 2 n'est pas un carré modulo 13 (observer que $p \neq 13$). Si p est de la forme $5x^2 + 4xy + 6y^2$, alors x est impair et donc $p \equiv 5, -1 \bmod 8$ (selon que y est pair ou impair). C'est encore absurde.

(vi) La forme $(3, 2, 9)$ représente 3 et la forme $(1, 0, 26)$ représente le nombre premier $107 = 9^2 + 26$.

(vii) A est l'anneau des entiers de $\mathbb{Q}(\alpha)$ car -26 est sans facteur carré et $\equiv 2 \bmod 4$.

(viii) On a les factorisations $X^2 + 26 \equiv X^2$ modulo 2, $X^2 + 26 \equiv X^2 - 1 = (X - 1)(X + 1)$ modulo 3, et $X^2 + 26 \equiv X^2 - 4 = (X - 2)(X + 2)$ mod 5. D'après le cours, les idéaux premiers cherchés sont donc $D = (2, \alpha)$, $T_\pm = (3, \alpha \pm 1)$ et $C_\pm = (5, \alpha \pm 2)$.

(ix) Si un idéal I de A est principal engendré par $z \in A$, on sait que $\mathrm{N}(z) = \mathrm{N}(I)$. En particulier, $\mathrm{N}(I)$ est de la forme $x^2 + 26y^2$. D'après le cours, les idéaux premiers précédents sont de norme respective $2, 3, 3, 5, 5$. Mais aucun de ces entiers n'est représenté par $x^2 + 26y^2$.

(x) D'après le cours, (vii) et (viii), on a $(2) = D^2$, $(3) = T_+T_-$ et $(5) = C_+C_-$. Le nombre $\alpha + 2$ est de norme $4 + 26 = 30 = 2 \cdot 3 \cdot 5$. De plus, $\alpha + 2$ est dans les trois idéaux premiers distincts D, T_- et C_+. La propriété de Dedekind montre alors que $(\alpha + 2)$ est divisible par DT_-C+. Ce dernier étant également de norme 30, on a l'égalité $(\alpha + 2) = DT_-C_+$. De même, $(\alpha - 2) = DT_+C_-$.

(xi) Minkowski nous dit que toute classe d'idéaux non nuls de A contient un idéal contenant un entier $1 \leq n \leq \frac{2}{\pi}\sqrt{104} < 2\sqrt{104/9} < 2\sqrt{12} = \sqrt{48} < 7$. Par la propriété de Dedekind, un tel idéal est un diviseur de (2), (3), (4) = (2)(2), (5) ou (6) = (2)(3), ses facteurs premiers étant donc parmi ceux du (viii). On en déduit que $\mathrm{Cl}(A)$ est engendré comme groupe par les classes de D, $T_\pm$ et $C_\pm$.

(xii) On a $[T_+][T_-] = 1$, $[C_+][C_-] = 1$, et $[D][T_-][C_+] = 1$ par le (x). Ainsi, $\mathrm{Cl}(A) = \langle [D], [T] \rangle$ où $T = T_+$.

(xiii) L'énoncé suggère que T^3 est principal, auquel cas il doit être engendré par un élément $z \in A$ tel que $N(z) = 3^3 = 27$. Il n'y a que deux tels éléments, à savoir $\pm\alpha + 1$. Les diviseurs premiers de $(\pm\alpha + 1)$ sont ceux contenant 3, donc T_- et $T = T_+$. Mais comme $\alpha + 1 \in T$ mais $\alpha + 1$ n'est pas dans T^-, car sinon $-1 = \alpha + 1 - (\alpha - 1) - 3$ serait dans T^-, il vient que $(\alpha + 1) = T^a$ puis $a = 3$ en prenant la norme.

On aurait aussi pu calculer directement. Comme $(\alpha + 1)^2 = 2(\alpha + 1) - 27$, on a $T^2 = (9, 3(\alpha + 1), 2(\alpha + 1)) = (9, \alpha + 1)$ et puis $T^3 = (27, 18(\alpha + 1), 2(\alpha + 1)) = (27, \alpha + 1) = (\alpha + 1)$.

(xiv) On a vu que $\mathrm{Cl}(A) = \langle [D], [T] \rangle$ avec $[D]^2 = 1$ et $[T]^3 = 1$. Ainsi, $[DT]^3 = [D]$ et $[DT]^4 = [T]$, donc $\mathrm{Cl}(A)$ est engendré par $[DT]$. On a $[DT]^6 = 1$, donc $[DT]$ est d'ordre divisant 6. Comme ni T, ni D ne sont principaux, les relations $[DT]^3 = [D]$ et $[DT]^2 = [T]^{-1}$ montrent $[DT]$ est d'ordre 6, ce qui conclut.

(xv) D'après la question précédente, un système de représentants des classes non triviales est donné par les $[DT]^i$ avec $i = 1, \ldots, 5$. Mais on constate que $[DT] = [C_-]^{-1} = [C_+]$, $[DT]^2 = [T]^2 = [T_-]$, $[DT]^3 = [D]$, $[DT]^4 = [T]$, $[DT]^5 = [DT]^{-1} = [C_-]$.

(xvi) Par un argument vu en classe, $2, \alpha$ est une $\mathbb{Z}$-base de D. De même, $3, \alpha \pm 1$ en est une de $T_\pm$, et $5, \alpha \pm 2$ en est une de $C_\pm$. Un calcul direct de la forme associée à ces $\mathbb{Z}$-base, montre que si $I = D$, $T_\pm$, $C_\pm$, alors la classe q_I est respectivement celle de $(2, 0, 13)$, $(3, \pm 2, 9)$ et $(5, \pm 4, 6)$. On conclut par (xv) et (iii).

(xvii) On a $q_T = [(3, 2, 9)]$, donc l'ordre de $[(3, 2, 9)]$ dans $\mathrm{Cl}(-104)$ est celui de $[T]$ dans $\mathrm{Cl}(A)$, i.e. 3. De même, $q_D = [(2, 0, 13)]$ donc $q_{DT} = q_D q_T = q_{C_+} = [(5, 4, 6)]$.

(xviii) Sous l'hypothèse sur p, on a vu au (v) que p est représenté par une forme q qui est soit la forme principale soit $(3, 2, 9)$. Dans tous les cas, $[q]^3$ est la classe de la forme principale par le (xvii), donc p^3 est représenté par la forme principale.

Problème 2. (i) La relation $x^p + y^p = 1$ s'écrit aussi $(x + y)(\sum_{i=0}^{p-1} x^i(-y)^{p-1-i}) = 1$, la somme entre parenthèse étant dans A, donc $x + y \in A^\times$.

(ii) Si $x + y = -1$, on a la congruence $(-1)^p \equiv x^p + y^p = 1$ modulo $p\overline{\mathbb{Z}}$. On en tire la congruence traditionnelle $(-1)^p \equiv 1 \bmod p$, ce qui est absurde car $p \neq 2$.

(iii) On part de $x^p + (1 - x)^p = 1$, l'énoncé s'en déduit pour $P = \frac{1}{p} \sum_{i=1}^{p-2} (-X)^{i-1} \binom{p}{i+1} \in \mathbb{Z}[X]$.

(iv) De $x(xP(x) - 1) = 0$ on tire que soit $x = 0$, soit $xP(x) = 1$ et donc $x \in A^\times = \{\pm 1\}$. Si $x = 0$ alors $y = 1 - x = 1$, si $x = 1$ alors $y = 1 - x = 0$, si $x = -1$ alors $y = 1 - x = 2$, ce qui est absurde car alors $x^p + y^p = -1 + 2^p \neq 1$ (car $p \neq 1$).

(v) On a $DN^2 \equiv 1 \bmod 8$. En particulier, N est impair, et donc $N^2 \equiv 1 \bmod 8$, puis $D \equiv 1 \bmod 8$.

(vi) On a $K = \mathbb{Q}(\sqrt{D})$, et comme D est sans facteur carré et $D \equiv 1 \bmod 4$, le cours assure que $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$, et $\mathcal{O}_K^\times = \{\pm 1\}$ car $D \equiv 1 \bmod 4$ est sans facteur carré, $D < 0$, et $D \neq -3$.

(vii) Le théorème de Dedekind assure que $h_K = |\mathrm{P}(D)|$ car $\mathcal{O}_K = A_D$. Mais $D \equiv 1 \bmod 4$ est sans facteur carré, donc $\mathrm{Cl}(D) = \mathrm{P}(D)$.

Si $p = 2$ alors $D = 1 - 2^4 = -15$. Les réduites de Gauss (a, b, c) de ce discriminant satisfont $b \equiv 1 \bmod 2$ et $b^2 \leq 15/3 < 3^2$, donc $b = \pm 1$. On trouve $(1, 1, 4)$ et $(2, 1, 2)$. Ainsi, $|\mathrm{Cl}(-15) = 2|$, ce qui conclut si $p = 2$.

(viii) On a $2^p = \frac{1-N^2D}{4} = \frac{1-N\sqrt{D}}{2} \frac{1+N\sqrt{D}}{2} = z(1 - z)$ si $z = \frac{1-N\sqrt{D}}{2}$. Comme N est impair (cf. (v)), $z \in \mathcal{O}_K$.

(ix) Les idéaux (z) et $(1 - z)$ sont premiers entre eux. En effet, s'ils possèdent un facteur commun Q, alors $z, 1 - z \in Q$, et donc $1 \in Q = \mathcal{O}_K$. La relation $(z)(1 - z) = (2)^p$, ainsi que la propriété de Dedekind, entraîne alors que (z) et $(1 - z)$ dont des puissances p-èmes d'idéaux de $\mathcal{O}_K$.

(x) Si $I^p = (z)$, alors $[I]^p = 1$ dans $\mathrm{Cl}(\mathcal{O}_K)$. En particulier, l'ordre de $[I]$ divise p, c'est donc 1 ou p car p est premier. Si p ne divise pas h_K, cet ordre est 1, i.e. I est principal. Le raisonnement est le même pour J.

(xi) Si p ne divise pas h_K on peut trouver $x \in \mathcal{O}_K$ tels que $I = (x)$ d'après le (x). En particulier, $(x^p) = (z)$ et donc x^p et z sont associés dans $\mathcal{O}_K$. Ainsi, $x^p = \pm z$ car $\mathcal{O}_K^\times = \{\pm 1\}$ par le (vi). Il vient que $z = (\pm x)^p$ car $p \neq 2$. Quitte à remplacer x en $-x$ on peut donc supposer que $z = x^p$. De même, on peut trouver y tel que $1 - z = y^p$.

(xii) Pour conclure, on peut supposer $p > 2$ d'après le (vi). Si p ne divise pas h_K, alors on peut trouver $x, y \in \mathcal{O}_K$ tels que $x^p + y^p = 1$ et $2^p = x^p(1 - x^p)$ d'après les questions précédentes. Le (iv) s'applique à $A = \mathcal{O}_K$ car on a vu au (vi) que $\mathcal{O}_K^\times = \{\pm 1\}$. Il montre que $x = 0$ ou $x = 1$, ce qui est absurde car cela conduit à $2^p = 0$.

(xiii) Pour $p = 7$, on a $1 - 2^9 = -511 = -7 \cdot 73$ (sans facteur carré..). En particulier, $|\mathrm{Cl}(-511)| = h_K$ est multiple de 7. Mais d'autre part, on sait que $|\mathrm{Cl}(-511)|$ est pair d'après Gauss, car le nombre impair -511 n'est pas puissance d'un nombre premier. Ainsi, $|\mathrm{Cl}(-511)|$ est multiple de 14. Si l'on ne veut pas invoquer le théorème de Gauss, on peut aussi vérifier qu'il y a un élément d'ordre 2 dans $\mathrm{P}(-511) = \mathrm{Cl}(-511)$, i.e. une forme ambiguë réduite non triviale. Comme -511 est impair, une telle forme est nécessairement de la forme (a, a, c) avec $1 < a < c$ et satisfait $a^2 - 4ac = -511$. La seule solution est $a = 7$, $a - 4c = -73$, i.e. $(7, 7, 20)$. Avec un peu d'acharnement, on pourrait en fait voir que $|\mathrm{Cl}(-511)| = 14$.

11. Corrigé de l'examen 2013-2014

Problème 1. (i) On détermine les réduites de Gauss (a,b,c) de discriminant -55 par l'algorithme du cours. En particulier b est impair et $|b| \leq [\sqrt{55/3}] = 4$. On a $(55+1)/4 = 14 = 1*14 = 2*7$ d'où $(1,1,14)$ et $(2,\pm 1,7)$, puis $(55+9)/4 = 16 = 4*4$ d'où $(4,3,4)$ (car $(4,-3,4)$ n'est pas réduite). Sont ambigües $(1,1,14)$ et $(4,3,4)$ par la caractérisation de Gauss.

(ii) $\mathrm{P}(-55) = \mathrm{Cl}(-55)$ car toutes les formes de discriminant -55 sont primitives (d'après le (i), ou plus généralement car -55 est fondamental). C'est donc un groupe d'ordre 4 pour la loi de Gauss. On sait que le neutre correspond à la classe de la forme principale et que les éléments de carré 1 correspondent aux classes ambiguës. Ainsi, la classe x de la forme non ambiguë $(2,1,7)$, dont l'ordre divise 4, est nécessairement d'ordre exactement 4. De plus, $x^2 = [(4,3,4)]$ (car d'ordre 2), $x^4 = [(1,1,14)]$ (élément neutre), et $x^3 = x^{-1} = x^{\mathrm{opp}} = [(2,-1,7)]$. La table de multiplication de $\mathrm{P}(-55) = \langle x \rangle$ s'en déduit.

(iii) On a vu que le carré de $[(2,1,7)]$ est $[(4,3,4)]$, donc $(4,3,4)$ est une composée de Gauss de $(2,1,7)$ par elle-même. On a aussi vu que $[(2,-1,7)]$ est l'inverse de $[(2,1,7)]$, de sorte que $[(2,1,7)][(2,-1,7)] = [(1,1,14)]$. Mais $(2,-1,7)$ est (non proprement) équivalente à $(2,1,7)$, de sorte que $(1,1,14)$ est également une composée (qui n'est pas de Gauss !) de $(2,1,7)$ par lui-même. On conclut car $(4,3,4)$ et $(1,1,14)$ sont non équivalentes, étant toutes deux ambiguës et non proprement équivalentes.

(iv) D'après Lagrange p est représenté par une forme q de discriminant -55 si et seulement si -55 est un carré modulo $4p$. Vérifions que c'est équivalent à la condition de l'énoncé. C'est vrai si $p = 2$ car $-55 \equiv 1 \bmod 8$ est un carré modulo 8, et 2 n'est ni un carré modul 5, ni modulo 11. Supposons $p > 2$, -55 est donc un carré mod. $4p$ ssi $\left(\frac{-55}{p}\right) = \left(\frac{5}{p}\right)\left(\frac{-11}{p}\right) = 1$, ou ce qui revient au même ssi $\left(\frac{5}{p}\right) = \left(\frac{-11}{p}\right)$. Par hypothèse $p \neq 5, 11$. La loi de réciprocité quadratique montre que $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ (car 5 est premier $\equiv 1 \bmod 4$) et $\left(\frac{-11}{p}\right) = \left(\frac{p}{11}\right)$ (car 11 est premier $\equiv 3 \bmod 4$).

(v) Le (i) montre que q est équivalente à $(1,1,14)$, $(2,1,7)$ ou $(4,3,4)$. Mais q représente $p \neq 5$ donc $\varepsilon_5(q) = \left(\frac{p}{5}\right) = -1$. Comme $(1,1,16)$ et $(4,3,4)$ représentent respectivement 1 et 4, qui sont des carrés premiers à 5, on a $\varepsilon_5(1,1,14) = \varepsilon_5(4,3,4) = 1$. La seule possibilité est donc que q est équivalente à $(2,1,7)$. Exemples : $p = 2, 7, 13, 17, \ldots$.

Problème 2. (i) Si $(\pi) \subset (x)$ alors $x|\pi$, donc x est soit une unité, soit associé à π, i.e $(x) = A$ ou $(x) = (\pi)$. Le second point est du cours.

(ii) L'idéal (π) n'est pas premier par π n'est pas premier. Il est non nul et strict car $\pi \neq 0$ et π n'est pas une unité par définition. Par la propriété de Dedekind, il est donc divisible par un produit de deux idéaux premiers P et Q de $\mathcal{O}_K$. En particulier, (π) est inclus dans P, Q et PQ, ces trois idéaux étant distincts de $\mathcal{O}_K$. Comme π n'est pas premier, P et Q ne sont pas principaux d'après le (i). Comme $|\mathrm{Cl}(\mathcal{O}_K)| = 2$, il vient que $[P] = [Q]$ (classe non principale). Mais alors PQ est principal car $[PQ] = [P][Q] = [P]^2 = 1$ dans le groupe $\mathrm{Cl}(\mathcal{O}_K) \simeq \mathbb{Z}/2\mathbb{Z}$. Donc PQ et principal, puis $PQ = (\pi)$ par le (i).

(iii) Il existe une et une seule telle fonction f car tout idéal est produit unique d'idéaux premiers. On peut la définir ainsi. Si $P \in \mathcal{I}$ est premier, posons $e_P = 2$ si P est principal, $e_P = 1$ sinon. Pour $I \in \mathcal{I}$, on pose alors $f(I) = \sum_P v_P(I) e_P$ (où $v_P(I)$, introduit en cours, est la plus grande puissance de P divisant I).

(iv) Soit $\pi \in \mathcal{O}_K$ irréductible. Si π est premier alors $f((\pi)) = 2$ par définition. Sinon, $(\pi) = PQ$ où P et Q sont premiers non principaux d'après le (ii). On a donc encore $f((\pi)) = 1+1 = 2$. Ainsi, $f((\pi)) = 2$ pour tout irréductible π de $\mathcal{O}_K$. Il s'ensuit que $f((\pi_1 \cdots \pi_n) = f(\prod_{i=1}^n (\pi_i)) = \sum_{i=1}^n f((\pi_i)) = 2n$ et de même $f((\pi'_1 \cdots \pi'_m)) = 2m$, d'où $2n = 2m$ puis $n = m$.

(v) -31 est sans facteur carré et $\equiv 1 \bmod 4$, donc $\mathcal{O}_K = \mathbb{Z}[\alpha]$ où α est comme dans l'énoncé. Comme $\Pi_{\alpha,\mathbb{Q}} = X^2 + X + 8$, il vient que $\mathrm{disc}(\mathcal{O}_K) = \mathrm{disc}(\Pi_{\alpha,\mathbb{Q}}) = 1 - 32 = -31$.

(vi) $X^2 - X + 8 \equiv X(X-1) \bmod 2$ (produit de deux polynômes irréductibles unitaires distincts), donc les idéaux de $\mathcal{O}_K$ contenant 2 sont, d'après le cours, les 4 idéaux distincts $(2), D_1 := (2,\alpha), D_2 = (2,\alpha+1)$ et $\mathbb{Z}[\alpha]$. Parmi-ceux là, les idéaux premiers sont ceux correspondants aux facteurs irréductibles, i.e. D_1 et D_2 (qui sont de norme $2^1 = 2$). De plus, $X^2 - X + 8$ est irréductible modulo 3, car on constate par évaluation en 0, 1 et -1 qu'il n'a pas de racine dans $\mathbb{Z}/3\mathbb{Z}$, donc les idéaux de $\mathbb{Z}[\alpha]$ contenant 3 sont $(3) = (3, \Pi_{\alpha,\mathbb{Q}}(\alpha))$ et $\mathbb{Z}[\alpha]$ d'après le cours, seul (3) étant premier. Les idéaux

premiers trouvés sont donc exactement D_1, D_2 et (3). De plus, (2), (3) et $\mathbb{Z}[\alpha]$ sont tautologiquement principaux. Mais 2 n'est pas de la forme $x^2+xy+8y^2$ (forme principale de discriminant -31), car 8 n'est pas de la forme $4*(x^2+xy+8y^2)=(2x+y)^2+31y^2$, donc ni D_1 ni D_2 n'est principal (on utilise $\mathrm{N}((z))=|\mathrm{N}_{K/\mathbb{Q}}(z)|=z\overline{z}$).

(vii) D'après le cours (ou par une vérification directe), $(2)=D_1D_2$. De plus (3) étant premier, sa décomposition est simplement ... $(3)=(3)$! Enfin, $\mathrm{N}(\alpha)=8$, dont 2 est l'unique facteur premier, donc les seuls facteurs premiers de (α) sont parmi D_1 et D_2. Le premier est effectivement un facteur car $\alpha\in D_1=(2,\alpha)$ (contenir = diviser). Ce n'est pas le cas du second car $\alpha\in(2,1+\alpha)$ entraînerait $1=(1+\alpha)-\alpha\in(2,\alpha+1)$ ce qui est absurde (on sait que $(2,\alpha+1)\neq\mathbb{Z}[\alpha]$, cf. (vi)). Ainsi $(\alpha)=D_1^m$ puis $m=3$ en prenant la norme.

(viii) D'après Minkowski, tout idéal non nul de $\mathcal{O}_K$ est équivalent à un idéal contenant un entier $1\leq m\leq\frac{2}{\pi}\sqrt{31}<4$ (par exemple, par la table du cours). D'après le (vi), ces idéaux sont soit principaux, soit équivalents à D_1 ou D_2, ces deux derniers étant non principaux. Comme $D_1D_2=(2)$, il s'ensuit que $\mathrm{Cl}(\mathcal{O}_K)$ est engendré par $[D_1]$. Comme $D_1^3=(\alpha)$ est principal d'après (vii), et D_1 n'est pas principal, la classe $[D_1]$ est d'ordre 3.

(ix) Vérifions que $2,\alpha$ est une $\mathbb{Z}$-base (clairement directe) de D_1. Soit $J=2\mathbb{Z}+\alpha\mathbb{Z}$. On a $J\subset D_1$. De plus, $2\alpha\in J$ et $\alpha^2=\alpha-8\in J$, donc $\alpha J\subset J$. Cela montre que J est un idéal de $\mathcal{O}_K$, puis que $D_1\subset J$ et $D_1=J$. Comme D_1 est de norme 2, on a $q_{2,\alpha}=\frac{1}{2}(\mathrm{N}(2)x^2+\mathrm{Tr}(2\overline{\alpha})xy+\mathrm{N}(\alpha)y^2)=2x^2+xy+4y^2$. La bijection de Dedekind est donc $[\mathcal{O}_K]\mapsto[(1,1,8)]$, $[D_1]\mapsto[(2,1,4)]$ et $[D_1]^{-1}\mapsto[(2,1,4)]^{\mathrm{opp}}=[(2,-1,4)]$. (Il serait aisé de vérifier que $(1,1,8)$, $(2,1,4)$ et $(2,-1,4)$ sont bien les seules réduites de Gauss de discriminant -31).

(x) Si p est réductible alors $p=uv$ avec $u,v\in\mathcal{O}_K$ non unités, i.e. de norme >1 d'après le cours, et donc $\mathrm{N}(u)=\mathrm{N}(v)=p$. Vérifions que p n'est pas une norme de $\mathcal{O}_K$. En effet, cela signifie que p est représenté par la forme principale de discriminant -31 (en particulier, -31 est un carré modulo $4p$). Mais ceci est absurde d'après le théorème de Lagrange car p est déjà représenté par la forme $(2,1,4)$, qui n'est pas équivalente à la forme principale (c'est une réduite de Gauss distincte de la forme principale). En revanche, comme $[(2,1,4)]^3=[(1,1,8)]$ d'après le (ix), donc p^3 est représenté par la forme principale, i.e. $p^3=\mathrm{N}(\pi)=\pi\overline{\pi}$ pour un certain $\pi\in\mathcal{O}_K$. Un tel π est nécessairement irréductible, car si $\pi=uv$ où u et v ne sont pas des unités, alors soit $\mathrm{N}(u)=p$ soit $\mathrm{N}(v)=p$, qui sont impossible comme on l'a déjà vu. Exemple : $8=\mathrm{N}(\alpha)$.

(xi) Le (x) montre que l'hypothèse $|\mathrm{Cl}(\mathcal{O}_K)|=2$ est nécessaire dans le (iv).

Problème 3. (i) Si $I=mJ^2$ alors $\mathrm{N}(I)=\mathrm{N}((m))\mathrm{N}(J)^2=m^2\mathrm{N}(J)^2$.

(ii) Écrivons $\mathcal{O}_K=\mathbb{Z}[\alpha]$; on dispose d'un α explicite en fonction de d d'après le cours mais ce ne sera pas utile, en revanche on va utiliser que $R:=\Pi_{\alpha,\mathbb{Q}}$ est de la forme $X^2+aX+b\in\mathbb{Z}[X]$. Si $\overline{R}=R \bmod p$ admet une racine double dans $\mathbb{Z}/p\mathbb{Z}$, i.e. $\overline{R}=(X-t)^2$ avec $t\in\mathbb{Z}/p\mathbb{Z}$, alors $\mathcal{O}_K$ admet un unique idéal premier P contenant p, à savoir $(p,\alpha-t)$, tel que $\mathrm{N}(P)=p$, et donc $(p)=P^2$ par la propriété de Dedekind. Si $\overline{R}$ admet deux racines distinctes, i.e. $\overline{R}=(X-t)(X-t')$ avec $t\neq t'\in\mathbb{Z}/p\mathbb{Z}$, alors $\mathcal{O}_K$ admet exactement deux idéaux premiers distincts contenant p, à savoir $P=(p,\alpha-t)$ et $Q=(p,\alpha-t')$, tous deux de norme $p^1=p$, et donc $(p)=PQ$. Dans le dernier cas, $\overline{R}$ est irréductible donc (p) est premier dans $\mathcal{O}_K$ (de norme p^2).

(iii) Si $\mathrm{N}(I)=p^{2n}$, tout idéal premier divisant I est de norme une puissance de p, donc contient p. Si on est dans le cas 1., on a donc $I=P^a$, puis $p^{2n}=\mathrm{N}(P)^a=p^a$ et donc $a=2n$. Dans ce cas I est le carré de P^n. Dans le cas 2., on a donc $I=P^aQ^b$ pour $a,b\geq0$. Quitte a échanger les rôles de P et Q supposons $a\leq b$. Comme $(p)=PQ$, on peut aussi écrire $I=(p^a)Q^{b-a}$, puis en prenant les normes $p^{2n}=p^{2a+b-a}$. Il s'ensuit que $b-a$ est pair, et donc $I=(p^a)(Q^{(b-a)/2})^2$. Enfin dans le cas 3., $I=(p)^n=(p^n)$.

(iv) Supposons que $\mathrm{N}(I)$ est un carré. Écrivons $\mathrm{N}(I)=\prod_{i=1}^n p_i^{\alpha_i}$ où les p_i sont premiers et distincts. Par multiplicativité de la norme et le fait que les idéaux premiers sont de norme une puissance d'un nombre premier, la propriété de Dedekind permet d'écrire $I=I_1I_2\cdots I_n$ où $\mathrm{N}(I_i)=p_i^{\alpha_i}$. Si $\mathrm{N}(I)$ est un carré, alors α_i est pair pour tout i, donc I_i est de la forme $m_iJ_i^2$ pour tout i par le (iii), et donc $I=(\prod_i m_i)(\prod_i J_i)^2$.

(v) Si $x\in I$ est non nul alors I divise (x) (contenir = diviser), i.e. il existe un idéal J tel que $(x)=IJ$. En prenant la norme il vient que $\mathrm{N}(J)=|\mathrm{N}_{K/\mathbb{Q}}(x)|/\mathrm{N}(I)$ est un entier. Si c'est un carré, alors $\mathrm{N}(J)$ est un carré, et en particulier $[J]$ un carré dans $\mathrm{Cl}(\mathcal{O}_K)$ d'après le (iv). On conclut car $[I]=[J]^{-1}$.

(vi) C'est la caractérisation du cours des discriminants fondamentaux combinée à la description de l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$.

(vii) (3) Si $[q]$ est un carré dans $\mathrm{P}(D)$, disons $[q] = [q']^2$, alors q représente le carré de tout entier représenté par q', car q est une composée de q' par elle-même. Réciproquement, si q représente un carré m^2, et si $I \in \mathrm{Pic}(A_D) = \mathrm{Cl}(A_D)$ est un idéal dont la classe correspond à $[q]$ par le théorème de Dedekind, alors il existe $x \in I$ tel que $m^2 = \frac{\mathrm{N}(x)}{\mathrm{N}(I)}$ par définition. Le (v) assure que $[I]$ est un carré dans $\mathrm{Pic}(A_D)$ et donc $[q]$ est un carré dans $\mathrm{P}(D)$.

12. Corrigé de l'examen 2014-2015

Problème 1. (i) $-p$ est sans facteur carré et $\equiv 3 \bmod 4$, on conclut par la proposition 5.22.

(ii) Si $P = \Pi_{\sqrt{-p},\mathbb{Q}}$ alors $P = X^2 + p$. De plus $P \equiv (X+1)^2 \bmod 2$; la proposition 6.11 montre que Q est de norme 2. Le théorème 7.17, qui s'applique par le (i), montre que $(2) = Q^2$.

(iii) Supposons $D = (z)$ avec $z \in A$. Alors $\mathrm{N}(D) = z\overline{z}$ (proposition 4.12.3). Écrivons $z = a + b\sqrt{-p}$ avec $a, b \in \mathbb{Z}$. Le (ii) entraîne $2 = a^2 + pb^2$, puis $b = 0$ (car $p > 2$) : absurde.

(iv) D'après le (i), $\mathrm{Cl}(A)$ est un groupe. D'après (ii) et (iii), $[D]$ est d'ordre 2 dans $\mathrm{Cl}(A)$. On conclut par Lagrange.

(v) Soit $J \subset D$ le sous-groupe engendré par 2 et $\alpha = 1 + \sqrt{-p}$. Comme $1, \alpha - 1$ est une $\mathbb{Z}$-base de A, il en va de même de $1, \alpha$, ce qui montre que $|A/J| = 2$. Comme d'autre part $|A/D| = 2$ d'après le (ii), on a $J = D$. On constate que $1, \alpha$ est une $\mathbb{R}$-base directe de $\mathbb{C}$ (comme dans le cours, on prend la convention que $\sqrt{-p} = i\sqrt{p}$). Ainsi,

$$\mathrm{q}_{1,\alpha}(x,y) := \frac{1}{2}\mathrm{N}(2x + \alpha y) = \frac{1}{2}((2x+y)^2 + py^2) = 2x^2 + 2xy + \frac{p+1}{2}y^2.$$

La forme $(2, 2, \frac{p+1}{2})$ est réduite au sens de Gauss car $\frac{p+1}{2} > 2$ si $p \equiv 1 \bmod 4$.

(vi) Soit (a,b,c) une réduite de Gauss de discriminant $-4p$, i.e. $b^2 - 4ac = -4p$. En particulier, $b = 2b'$ est pair et $b'^2 - ac = -p$. D'après le théorème 3.29 (i), (a,b,c) est ambiguë si et seulement si on a $b = 0$, ou $a = b$, ou $a = c$.

Si $b = 0$, alors $ac = p$. Comme p est premier, le seul cas possible est $(1, 0, p)$ (forme principale). Si $b = a$ $(= 2b')$, alors $b'(2c - b') = p$, les deux cas $b' = 1, p$ conduisent aux deux possibilités $(2, 2, \frac{p+1}{2})$, $(2p, 2p, \frac{p+1}{2})$, seule la première étant réduite. Si $a = c$, alors $(a - b')(a + b') = p$ (avec $a - b' \geq 0$). La seule possibilité est $a - b' = 1$ et $a + b' = p$, i.e. $(a,b,c) = (\frac{p+1}{2}, p-1, \frac{p+1}{2})$, qui n'est pas réduite car $p > 3$.

(vii) On a $A = A_{-4p}$ avec la notation du cours. La bijection de Dedekind $\mathrm{Cl}(A) \xrightarrow{\sim} \mathrm{Cl}(-4p) = \mathrm{P}(-4p)$ (la denière égalité vient du (i)) fait correspondre éléments de carré 1 et classes ambiguës (Lemme 8.19), et envoie $[A]$ et $[D]$ sur $[(1,0,p)]$ et $[(2, 2, \frac{p+1}{2})]$ (cours + question (v)). On conclut par le (vi).

(viii) G étant abélien, l'application $g \mapsto g^2$ est un morphisme de groupes $G \to G$ de noyau $\langle z \rangle$ et d'image $\mathcal{C}(G)$. Ainsi $|\mathcal{C}(G)| = |G|/|\langle z \rangle| = |G|/2$. Si $z = g^2$ alors g est d'ordre 4 et donc $|G| \equiv 0 \bmod 4$ (Lagrange). Réciproquement, si $|G| \equiv 0 \bmod 4$ alors $|\mathcal{C}(G)| = |G|/2$ est pair et donc $\mathcal{C}(G)$ possède un élément d'ordre 2 (Cauchy), nécessairement égal à z.

(ix) $(2, 2, \frac{p+1}{2})$ représente 2 qui est premier à p, donc $\varepsilon_p((2, 2, \frac{p+1}{2})) = \left(\frac{2}{p}\right)$.

(x) Si $|\mathrm{Cl}(A)| \equiv 0 \bmod 4$, alors $[D]$ est un carré dans $\mathrm{Cl}(A)$ (question (viii)), ou ce qui revient au même $[(2, 2, \frac{p+1}{2})]$ est un carré dans $\mathrm{P}(-4p)$. Comme ε_p est un morphisme de groupes, cela entraîne $\varepsilon_p(2, 2, \frac{p+1}{2}) = 1$. I.e. $p \equiv \pm 1 \bmod 8$ d'après le (ix) et la loi supplémentaire. Comme $p \equiv 1 \bmod 4$, on a même $p \equiv 1 \bmod 8$.

(xi) Comme $p > 2$ il existe au moins un entier $m \in \mathbb{Z}$ tel que m n'est pas un carré modulo p (en particulier m est premier à p). Par le lemme chinois des restes, il existe un entier a tel que $a \equiv 3 \bmod 4$ et $a \equiv m \bmod p$. En particulier, a est premier à $b := 4p$. Par le théorème de la progression arithmétique de Dirichlet, il existe un premier ℓ tel que $\ell \equiv a \bmod b$, il convient.

(xii) Soit ℓ comme au (xii). Montrons qu'il existe une forme de discriminant $-4p$ qui représente ℓ. Par Lagrange, il faut voir que $-4p$ est un carré modulo 4ℓ, i.e. modulo 4 et modulo ℓ car ℓ est impair. Il est évident que $-4p$ est un carré mod 4 (c'est 0). De plus, en utilisant la loi quadratique et le symbole de -1 (ℓ et p sont impairs) on a

$$\left(\frac{-4p}{\ell}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{\ell}\right) = (-1) \times (-1) = 1$$

la seconde égalité découlant du (xi). D'après Lagrange, il existe une forme q de discriminant $-4p$ qui représente ℓ. En particulier, $\varepsilon_p(q) = \left(\frac{\ell}{p}\right) = -1$.

(xiii) Le (xii) montre que le morphisme ε_p est surjectif. Son noyau est donc de cardinal $|\mathrm{P}(-4p)|/2$, et contient évidemment $\mathcal{C}(\mathrm{P}(-4p))$. On conclut car ce dernier est de cardinal $|\mathrm{P}(-4p)|/2$ d'après le (vii) et le (viii).

(xiv) On a déjà vu que $\mathrm{Cl}(A) \equiv 0 \bmod 4$ si et seulement si $(2,2,\frac{p+1}{2})$ est un carré dans $\mathrm{P}(-4p)$. D'après le (xiii), il est équivalent de demander $\varepsilon_p(2,2,\frac{p+1}{2}) = 1$, i.e. $p \equiv 1 \bmod 8$ d'après le (ix).

Problème 2. (i) $x \mapsto P(x)$ est strictement croissante sur $\mathbb{R}$ car $P'(X) = 3X^2 + d$ ne s'annule pas ($d > 0$). On a $P(-1/d) = (-1/d)^3 < 0$ et $P(-1/d + 1/d^2) = \frac{(1-d)^3+d^5}{d^6} > 0$. Le (i) se déduit du théorème des valeurs intermédiaires.

(ii) L'assertion $-\mathrm{disc}\ P = 4d^3 + 27$ suit du formulaire du Chap. 5 §2. Comme P est de degré 3, il est irréductible dans $\mathbb{Q}[X]$ si et seulement si il admet une racine rationelle. Comme il est unitaire à coefficients entiers, une telle racine serait nécessairement dans $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. Cela contredit le (i) car $-1 < \alpha < 0$.

(iii) D'après (ii), $\Pi_{\alpha,\mathbb{Q}} = P$ et donc $[K : \mathbb{Q}] = \deg P = 3$. D'après le cours, $\sigma \mapsto \sigma(\alpha)$ induit une bijection entre $\Sigma(K)$ et les plongements de K, de sorte que r_1 est le nombre de racines réelles de P, i.e. 1, et $r_2 = ([K : \mathbb{Q}] - r_1)/2 = 1$ également.

L'existence de σ suit de l'explication précédente : soit $\beta \neq \alpha$ une racine de P, non dans $\mathbb{R}$ d'après (i), l'unique $\sigma \in \Sigma(K)$ tel que $\sigma(\alpha) = \beta$ convient. La racine restante de P est $\overline{\beta}$. Ainsi, $\Sigma(K) = \{\mathrm{id}, \sigma, \overline{\sigma}\}$.

(iv) La question (iii) montre que $\mathrm{N}_{K/\mathbb{Q}}(x) = x\sigma(x)\overline{\sigma(x)} = x|\sigma(x)|^2$. Si x est dans $\mathcal{O}_K$, alors $\chi_{x,K/\mathbb{Q}} = X^3 + aX^2 + bX + c$ avec $c = -\mathrm{N}_{K/\mathbb{Q}}(x)$ et $a, b, c \in \mathbb{Z}$ (théorème 5.20). L'équation $\chi_{x,K/\mathbb{Q}}(x) = 0$ s'écrit donc aussi

$$x(x^2 + ax + b - |\sigma(x)|^2) = 0.$$

Si $x = 0$ il n'y a rien à démontrer, et sinon on en tire $|\sigma(x)|^2 = x^2 + ax + b \in \mathbb{Z}[x]$.

(v) A^1 est un sous-groupe de $A^\times$ car $\mathbb{R}_{>0}$ est un sous-groupe de $\mathbb{R}^\times$. On a $\alpha(\alpha^2 + d) = -1 \in A^\times$, et $\alpha^2 + d \in A$, donc $\alpha \in A^\times$. On conclut car $\alpha < 0$ par le (i).

(vi) Si $x \in A$ satisfait $x|\sigma(x)|^2 = 1$ alors $x > 0$ et $x \in A^*$ car $|\sigma(x)|^2 \in A$ (question (v)), donc $x \in A^1$. Réciproquement, si $x \in A^1$ alors il existe $y \in A$ tel que $xy = 1$. En appliquant la multiplicativité de la norme de $K/\mathbb{Q}$, et le fait que $\mathrm{N}_{K/\mathbb{Q}}(A) \subset \mathbb{Z}$, il vient que $\mathrm{N}_{K/\mathbb{Q}}(x) \in \mathbb{Z}^\times = \{\pm 1\}$. On conclut car $\mathrm{N}_{K/\mathbb{Q}}(x) = x|\sigma(x)|^2 > 0$.

(vii) Soit $x \in A^1$. Si $\frac{1}{\rho} \leq x \leq \rho$ alors $|\sigma(x)| = 1/\sqrt{x}$ d'après le (vi), il vérifie donc $\frac{1}{\sqrt{\rho}} \leq |\sigma(x)| \leq \sqrt{\rho}$. D'après le (iii), on constate donc que $|\tau(x)| \leq \rho$ pour tout $\tau \in \Sigma(K)$. On applique la prop. 5.14.(iii) : les relations coefficients racines montrent que les coefficients du polynôme $\chi_{x,K/\mathbb{Q}}$ sont tous $\leq$ à un réel $\mathrm{C}(\rho)$ qui ne dépend que de ρ (et non de x) ; on peut prendre $\mathrm{C}(\rho) = 3\rho^3$. Ces coefficients sont de plus entiers car $x \in \mathcal{O}_K$. Ainsi, à $\rho > 1$ fixé l'ensemble des $\chi_{x,K/\mathbb{Q}}$, avec $x \in A^1$ tel que $\frac{1}{\rho} \leq x \leq \rho$, est fini, ainsi donc que l'ensemble des tels x car un polynôme n'a qu'un nombre fini de racines.

(viii) Le logarithme $\log : \mathbb{R}_{>0} \to \mathbb{R}$ est un isomorphisme de groupes, donc $\log A^1$ est un sous-groupe de $\mathbb{R}$. Soit $r > 0$, l'ensemble $\{x \in A^1, |\log x| < r\} = \{x \in A^1, e^{-r} < x < e^r\}$ est fini par le (vii), donc $\log A^1$ est discret dans $\mathbb{R}$. Enfin, $-\alpha \in A^1$ d'après (v) et $-\alpha < 1$ d'après le (i), donc $\log A^1$ est non réduit à 0 : c'est un réseau.

(ix) Le (viii) montre que $\log A^1 = \mathbb{Z}\log\varepsilon$ pour un unique $\varepsilon \in A^1$ tel que $\varepsilon > 1$. En prenant l'exponentielle, on en déduit que A^1 est le groupe monogène infini engendré par ε (isomorphe à $\mathbb{Z}$). On conclut car l'application $\{\pm 1\} \times A^1 \to A^\times, (u, x) \mapsto ux$, est un isomorphisme de groupes.

(x) Comme $-\alpha^{-1} \in A^1$ il existe un unique entier $n \in \mathbb{Z}$ tel que $-\alpha^{-1} = \varepsilon^n$, d'après le (ix). Mais $-\alpha < 1$, donc $-1/\alpha > 1$, et donc $n > 1$. Il est évident que $\mathbb{Z}[\varepsilon] \subset \mathbb{Z}[\alpha]$. Comme $\varepsilon^{-1} = |\sigma(\varepsilon)|^2 \in \mathbb{Z}[\varepsilon]$ (question (iv)), on a aussi $\mathbb{Z}[\alpha] \subset \mathbb{Z}[\varepsilon]$.

(xi) De même (c'est seulement plus simple), $\mathbb{Q}(\alpha) = \mathbb{Q}(\varepsilon)$. Soit $Q = \chi_{\varepsilon,K/\mathbb{Q}}$. Alors $Q \in \mathbb{R}[X]$ est unitaire. Il vérifie $Q(0) = -\varepsilon|\sigma(\varepsilon)|^2 = -1$ (question (vi)). Comme $K = \mathbb{Q}(\varepsilon)$ le fait que $r_1 = 1$ (prouvé au (iii)) montre que ε a un $\mathbb{Q}$-conjugué réel (lui-même) et deux autres non réels : $\sigma(\varepsilon)$ et $\overline{\sigma(\varepsilon)}$. Comme $K = \mathbb{Q}(\varepsilon)$ on a aussi $Q = \Pi_{\varepsilon,\mathbb{Q}}$. Ainsi, $\mathrm{disc}\ Q = \mathrm{disc}\ \mathbb{Z}[\varepsilon] = \mathrm{disc}\ A = \mathrm{disc}P$.

(xii) L'inégalité d'Artin montre que $4d^3 + 27 = |\mathrm{disc}P| = |\mathrm{disc}Q| < 4(-\alpha^{-3})^{1/n} + 24$. En particulier, $(-\alpha^{-1})^{1/n} > d$. Mais $\alpha < (1-d)/d^2$ d'après le (i), donc $-1/\alpha < \frac{d^2}{d-1}$ si $d > 1$. On conclut par passage aux log. Pour une démonstration de l'inégalité d'Artin, voir par exemple le livre *Algebraic number theory*, A. Fröhlich & M. J. Taylor, Cambridge adv. math. studies 27, Chap. V, §3, fomrule (3.2).

(xiii) Il suffit de voir que $\log(\frac{d^2}{d-1}) < 2\log(d)$, soit encore $\frac{d^2}{d-1} < d^2$ pour $d > 1$, ce qui est évident. Cela montre $n = 1$, puis que $\varepsilon = -\alpha^{-1}$. On conclut par (ix) et (v).

Observer que si $d = 1$ alors $P(-2/3) = 1 - \frac{26}{27} > 0$ donc $\alpha < -2/3$, puis $-\alpha^{-1} < 3/2$. L'inégalité d'Artin montre plus précisément que $4\,(-\alpha^{-1})^{3/n} + 24 > |\mathrm{disc}(P)| = 31$, i.e. $(-\alpha^{-3})^{1/n} > 7/4$. Ainsi, $n < 3\frac{\log 3/2}{\log 7/4}$. Un petit calcul montre alors que $n = 1$ ou 2. Cependant, on peut montrer que dans ce cas par un argument de congruences modulo 13 que $-\alpha$ n'est pas un carré dans $\mathbb{Z}[\alpha]$, et conclure également $n = 1$ dans ce cas.

(xiv) C'est la proposition-définition 6.15 : pour tout $x \in \overline{\mathbb{Z}}$, $\mathbb{Z}[x]$ contient une $\mathbb{Q}$-base de $L = \mathbb{Q}(x)$ et donc $\mathrm{disc}\ \mathbb{Z}[x] = |\mathcal{O}_K/\mathbb{Z}[x]|\mathrm{disc}\ \mathbb{Z}[x]$. On a $\mathrm{disc}\ A = \mathrm{disc}\ P = -4^4 - 27 = -283$. Mais 283 est sans facteur carré (c'est un nombre premier, cf l'annexe). Comme $|\mathcal{O}_K/A|$ est un entier ≥ 1, c'est 1, i.e. $\mathcal{O}_K = A$.

(xv) On rappelle que $r_2 = 1$ et $\mathrm{disc}\ A = -283$. D'après Minkowski, tout idéal non nul de A est équivalent à un idéal de A contenant un entier n tel que $1 \leq n \leq (4/\pi)3!/3^2\sqrt{283} < 5$ d'après l'énoncé. On conclut car "contenir c'est diviser", puisque A est égal à $\mathcal{O}_K$ par le (xiv).

(xvi) On applique le théorème 7.17 (car $A = \mathcal{O}_K$) et la prop. 6.11. On conclut car $X^3 + 4X + 1 \equiv (X-1)(X^2+X+1) \bmod 2$ (décomposition en irréductibles dans $\mathbb{Z}/2[X]$) et $X^3 + 4X + 1 \equiv (X-1)(X^2+X-1) \bmod 3$ (idem). Ainsi, $D_1 = (2, \alpha - 1)$, $D_2 = (2, \alpha^2 + \alpha + 1)$, $T_1 = (3, \alpha - 1)$ et $T_2 = (3, \alpha^2 + 2\alpha - 1)$.

(xvii) On rappelle que si Q est un idéal premier de $\mathcal{O}_K$ alors $\mathrm{N}(Q)$ est une puissance de l'unique nombre premier p appartenant à Q (thm. 7.16 (ii)). Comme contenir = diviser, on a de plus $p \in Q$ si et seulement si Q divise (p). On conclut par le (xvi).

(xviii) Si $m \in \mathbb{Q}$, alors

$$\mathrm{N}_{K/\mathbb{Q}}(m - \alpha) = (m - \alpha)(m - \sigma(\alpha))(m - \overline{\sigma(\alpha)}) = P(m).$$

On a donc $\mathrm{N}_{K/\mathbb{Q}}(1 + \alpha) = -P(-1) = 4$ et $\mathrm{N}_{K/\mathbb{Q}}(1 - \alpha) = P(1) = 6$. En particulier, les facteurs premiers de $(1+\alpha)$ et $(1-\alpha)$ sont parmi $\{D_1, D_2, T_1, T_2\}$. Par multiplicativité de la norme, la seule possibilité pour $(1 - \alpha)$ est donc $(1 - \alpha) = D_1T_1$. De même, les deux possibilités pour $(1 + \alpha)$ sont D_1^2 et D_2. Mais $1 + \alpha = 1 - \alpha + 2 \in D_1$, donc D_1 divise $(1 + \alpha)$. Ainsi, $(1 + \alpha) = D_1^2$.

(xix) D'après la question (xv), tout idéal non nul de A est équivalent à un idéal divisant (1), (2), (3) ou $(2)^2$. Comme $A = \mathcal{O}_K$, un tel idéal est donc un produit (éventuellement vide) d'idéaux parmi $\{D_1, D_2, T_1, T_2\}$. Ainsi, le groupe $\mathrm{Cl}(A)$ est engendré par les classes de ces 4 idéaux premiers. Mais $[D_1][D_2] = [T_1][T_2] = 1$ d'après le (xvi), et $[D_1][T_1] = 1$ d'après le (xviii). Donc le groupe $\mathrm{Cl}(A)$ est engendré par $[D_1]$, qui est de carré 1 par la relation $D_1^2 = (1 + \alpha)$.

(xx) On observe que 2 est une racine de $P = X^3 + 4X + 1$ modulo 17. Ainsi, le morphisme d'anneaux $\mathbb{Z}[X] \to \mathbb{Z}/17$, $P(X) \mapsto P(2) \bmod 17$, est nul sur l'élément $X^3 + 4X + 1$, il se factorise donc en un morphisme d'anneaux $\mathbb{Z}[X]/(P) \to \mathbb{Z}/17$. Mais P est le polynôme minimal de α (question (ii)) et donc $\mathbb{Z}[X]/(P)$ est naturellement isomorphe à $\mathbb{Z}[\alpha]$ d'après le cours.

(xix) $\varphi(-1) = -1$ est un carré non nul dans $\mathbb{Z}/17\mathbb{Z}$ car $17 \equiv 1 \bmod 4$. $\varphi(\alpha) = 2$ est également un carré non nul modulo 17 car $17 \equiv 1 \bmod 8$. Comme $A^\times = \langle -1, \alpha \rangle$, $\varphi(A^\times)$ est inclus dans le groupe des carrés de $(\mathbb{Z}/17)^\times$. Mais $\varphi(1 + \alpha) = 3$ et $\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{-1}{3}\right) = -1$, ce qui conclut.

(xxii) Si $D_1 = (z)$ avec $z \in A$ alors $D_1^2 = (z^2) = (1+\alpha)$, donc $z^2 = (1+\alpha)x$ avec $x \in A^\times$. En particulier, $\varphi((1 + \alpha)x) = \varphi(z)^2$ est un carré : absurde. Ainsi, D_1 n'est pas principal, et $\mathrm{Cl}(A) \simeq \mathbb{Z}/2\mathbb{Z}$.

13. Corrigé de l'examen 2015-2016

Problème 1. (i) D'après Gauss, il suffit de déterminer les formes réduites (a,b,c) de discriminant $D=-127$. On a $|b|\leq a\leq \sqrt{127/3}<7$ et $b\equiv 1 \bmod 2$, donc b vaut $\pm 1,\pm 3,\pm 5$. On applique l'algorithme du cours : $(b^2-D)/4=ac$ vaut respectivement $32,34,38$. Les deux derniers cas ne conduisent à aucune forme réduite ($|b|\leq a\leq c$), et le cas $b=\pm 1$ donne les formes $(1,1,32)$, $(2,\pm 1,16)$, $(4,\pm 1,8)$. Ainsi, $\mathrm{Cl}(-127)$ a exactement 5 éléments, représentés par ces 5 formes.

(ii) L'anneau A est l'anneau A_{-127} du cours car $-127\equiv 1 \bmod 4$. Comme 127 est premier (Annexe B !), donc sans facteur carré, c'est aussi l'anneau des entiers de $\mathbb{Q}(\sqrt{-127})$. Ainsi, on sait que $\mathrm{Cl}(A)$ est un groupe. D'après Dedekind, on a $|\mathrm{Cl}(A)|=|\mathrm{Cl}(-127)|$, qui vaut 5 par le (i). Mais un groupe d'ordre premier p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, car un élément distinct de 1 est nécessairement d'ordre p d'après Lagrange.

(iii) On a $\Pi_{\alpha,\mathbb{Q}}=X^2-X+32$, donc $\mathrm{disc}A=\mathrm{disc}\,(X^2-X+32)=-127$ (et en général, $\mathrm{disc}\,A_D=D$). D'après Minkowski, tout idéal non nul de A est équivalent à un idéal contenant un entier $N\leq 1$ tel que $N\leq \frac{4}{\pi}\cdot\frac{1}{2}\cdot\sqrt{127}<8$. En effet, le corps $K=\mathbb{Q}(\alpha)$ et de degré 2 et n'a pas de plongement réel.

(iv) On a déjà justifié au (ii) le fait que A est l'anneau des entiers de $\mathbb{Q}(\alpha)$, et donc que $\mathrm{Cl}(A)$ est un groupe. D'après le (iii), tout idéal de A est équivalent à un idéal contenant, un idéal (N) avec $1\leq N\leq 7$. Comme un tel idéal est produit d'idéaux premiers ayant la même propriété (par la propriété de Dedekind de $A=\mathcal{O}_{\mathbb{Q}(\alpha)}$), le groupe $\mathrm{Cl}(A)$ est a fortiori engendré par les classes des idéaux premiers P de A contenant un entier ≤ 7, et donc un nombre premier $p\leq 7$.

(v) Le polynôme X^2-X+32 est congru à $X(X-1)$ modulo 2. D'après le cours (Prop. 6.11), les idéaux de $A=\mathbb{Z}[\alpha]$ contenant 2 sont donc les quatre idéaux $A, 2A, (2,\alpha)$ et $(2,\alpha-1)$. Parmi ceux-là, les idéaux premiers sont (disons) $I:=(2,\alpha)$ et $J:=(2,\alpha-1)$ (les $\mathrm{I}(Q)$ avec Q facteur irréductible unitaire de $X(X-1)$, cf l'exemple suivant la définition 7.7) et sont de norme $2^1=2$. Comme A est l'anneau des entiers de $\mathbb{Q}(\alpha)$ (cf (ii)), un théorème du cours montre que l'on a $(2)=IJ$ (Thm. 7.17). Pour voir que ni I, ni J, n'est principal, il suffit de voir que A n'admet aucun idéal principal de norme 2, i.e. aucun élément de norme 2 (car $\mathrm{N}(z)=\mathrm{N}((z))$. Mais si $x,y\in\mathbb{Z}$ on a $\mathrm{N}(x+y\alpha)=x^2+xy+32y^2$ (forme principale de discriminant -127). Elle ne représente pas 2, car $4(x^2+xy+32y^2)=(2x+y)^2+127y^2$ ne représente pas 8.

(vi) Observons que la réduction modulo p du polynôme $\Pi_{\alpha,\mathbb{Q}}=X^2-X+32$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$ pour $p=3,5,7$. Il suffit de voir que dans chacun des cas, il n'a pas de racine dans $\mathbb{Z}/p\mathbb{Z}$. D'après la relation $4(X^2-X+32)=(2X-1)^2+127$, et $p>2$, il est équivalent de voir que -127 n'est pas un carré modulo p. Mais $-127=2 \bmod 3$ (non carré), $-127\equiv -2 \bmod 5$ (non carré), et $-127\equiv -1 \bmod 7$ (non carré car $7\equiv 3 \bmod 4$). Ainsi, pour ces 3 valeurs de p, l'idéal $(p)=\mathrm{I}(X^2-X+32)$ est premier d'après la proposition 6.11 (et l'exemple suivant la définition 7.7).

(vii) Soit P un idéal premier de A contenant un nombre premier p, ou ce qui revient au même divisant (p), avec $p\leq 7$. Si $p\neq 2$, alors $P=(p)$ d'après le (v). Un tel P est donc principal. D'autre part, si $p=2$ on a $P=I$ ou $P=J$ d'après le (v), ainsi que $IJ=(2)$. Cette dernière relation montrer que $[I]=[J]^{-1}$ dans $\mathrm{Cl}(A)$. D'après la question (iv), $\mathrm{Cl}(A)$ est donc engendré par $[I]$ (et aussi par $[J]$).

(viii) L'équation $\alpha(1-\alpha)=\mathrm{N}(\alpha)=2^5$ montre que l'idéal (α) est de norme 2^5. En particulier, d'après la propriété de Dedekind et le (iv), ses facteurs premiers sont parmi $\{I,J\}$. On a clairement $\alpha\in I$. Si $\alpha\in J$, alors $1=\alpha-(\alpha-1)\in J$, ce qui est absurde car $J\neq A$ (il est de norme 2). Donc $\alpha\notin J$, i.e. J ne divise pas (α). La seule possibilité est donc $(\alpha)=I^5$. En particulier, $[I]^5=1$ dans $\mathrm{Cl}(A)$. L'ordre de $[I]$ est donc 1 ou 5. Ce n'est pas 1 car I est non principal (question (iv)).

Problème 2. (i) Par hypothèses, D est sans facteur carré et $\equiv 1 \bmod 4$, donc $\mathcal{O}_K=A_D$ d'après le cours (Prop. 5.22).

(ii) On a $\overline{\alpha}=1-\alpha$, et donc $\overline{I}=(\overline{\alpha})=(1-\alpha)$. Ainsi, $1=\alpha+1-\alpha\in I+\overline{I}$, d'où l'énoncé.

(iii) On a $\alpha\overline{\alpha}=\alpha(1-\alpha)=n^g$, et donc $I\overline{I}=(\alpha)(1-\alpha)=(\alpha(1-\alpha))=(n^g)=(n)^g$. Comme les idéaux I et $\overline{I}$ n'ont pas de facteurs premier commun (ou ce qui revient au même, ne sont pas inclus dans un même idéal premier) d'après le (x), la propriété de factorisation unique des idéaux montre que I (et $\overline{I}$) est la puissance g-ème d'un (unique) idéal, on le note J.

(iv) Si $\overline{J}^m=\overline{\mathrm{J}^m}$, alors en élevant à la puissance g on a $I^m=\overline{I}^m$, ce qui est absurde car I et $\overline{I}$ sont premiers entre eux par le (ii). Si $J^m=(x)$ avec $x\in\mathbb{Z}$, alors $\overline{x}=x$ et donc on a les égalités $\overline{J}^m=\overline{\mathrm{J}^m}=\overline{(x)}=(x)=J^m$: on est ramené au cas précédent.

(v) La forme principale de discriminant D est $q(x,y) = x^2 + xy + n^g y^2$. En particulier on a $4\,q(x,y) = (2x+y)^2 + (4\,n^g - 1)y^2$. Ainsi, si on a $(x,y) \in \mathbb{Z}^2$ et $q(x,y) = n^m$ avec $y \neq 0$, on a l'inégalité $4n^g - 1 \leq 4n^m$, i.e. $n^g \leq n^m$ car $n, g \geq 1$, et donc $m \geq g$.

(vi) Soit $m \geq 1$ l'ordre de $[J]$ dans $\mathrm{Cl}(A)$. La relation $J^g = I = (\alpha)$, i.e. $[J]^g = 1$, montre m divise g. De plus, il existe $z \in A$ tel que $J^m = (z)$. En particulier, on a $\mathrm{N}(J)^m = \mathrm{N}(z)$. La relation $J^g = (\alpha)$ montre que $\mathrm{N}(J)^g = n^g$, i.e. $\mathrm{N}(J) = n$. Écrivons $z = x + y\alpha$ avec $x, y \in \mathbb{Z}$. On a $\mathrm{N}(z) = n^m$, ou ce qui revient au même $q(x,y) = n^m$ (avec q principale de discriminant D). Le (v) montre que $y = 0$ ou $m \geq g$ (et donc $m = g$). Mais si $y = 0$ on a $J^m = (x)$, ce qui est absurde par le (iv).

(vii) On a déjà vu $\mathrm{N}(J) = n$, i.e. J est d'indice n dans A. Le théorème de Lagrange montre alors $n \in J$. Soit $J' \subset J$ le sous-groupe $\mathbb{Z}n + \mathbb{Z}\alpha$. Comme $1, \alpha$ est une $\mathbb{Z}$-base de A, J' est un sous-groupe d'indice n dans A, donc d'indice 1 dans J, i.e. $J = J'$.

(viii) n, α est une $\mathbb{Z}$-base de l'idéal J d'après la question précédente, manifestement directe relativement à la $\mathbb{R}$-base $1, \alpha$ de $\mathbb{C}$. Calculons la forme binaire associée à cette base par Dedekind. On a $q_{n,\alpha}(x,y) = \frac{1}{n}(n^2x^2 + nxy + n^g y^2) = nx^2 + xy + n^{g-1}y^2$. Ainsi, l'isomorphisme de groupes $\mathrm{P}(D) \xrightarrow{\sim} \mathrm{Cl}(A)$ fait correspondre la classe d'équivalence propre de $(n, 1, n^{g-1})$ avec la classe de l'idéal J. On conclut par la question (vi).

(ix) On a $-2047 = 1 - 2 \cdot 2^9 = -23 \cdot 89$ sans facteur carré, donc on est dans le cas particulier $n = 2$ et $g = 9$. Le groupe $\mathrm{P}(-2047)$ admet un élément d'ordre 9 d'après le (viii). La classe de la forme réduire ambiguë $(23, 23, 28)$ (non principale), qui est bien de discriminant -2047 par la donnée de l'énoncé, est d'ordre 2 d'après le cours. On conclut car si un groupe abélien G possède un élément a d'ordre m et un élément b d'ordre n premier à n, l'élément ab est d'ordre mn (Lemme 1.30).

Pour la question bonus, on observe que d'après le cours, le sous-groupe $V = 23\mathbb{Z} + \frac{23+\sqrt{D}}{2}\mathbb{Z} = 23\mathbb{Z} + (\alpha + 11)\mathbb{Z}$ est un idéal de A dont la classe correspond à la classe d'équivalence propre de $(23, 23, 28)$. Il s'agit de déterminer la classe de formes associées à l'idéal VJ (où $J = \mathbb{Z}2 + \mathbb{Z}\alpha$). Mais VJ est engendré $\mathbb{Z}$-linéairement par $46, 23\alpha, 2(\alpha+11), \alpha(\alpha+11) = 12\alpha - 512$. Une petite analyse montre que $VJ = \mathbb{Z}46 + \mathbb{Z}(\alpha - 12)$. La forme associée à la base $46, \alpha - 12$ convient : on trouve $(46, -23, 14)$. On a les équivalences propres $(46, -23, 14) \overset{+}{\sim} (14, 23, 46) \overset{+}{\sim} (14, -5, 37)$ (cette dernière est réduite).

Problème 3. (i) On rappelle que d'après le cours, si $x \in A$ alors $\mathrm{N}_{K/\mathbb{Q}}(x) \in \mathbb{Z}$. Si $x \in A^\times$ il existe $y \in A$ tel que $xy = 1$, puis par multiplicativité de $\mathrm{N}_{K/\mathbb{Q}}$: $1 = \mathrm{N}_{K/\mathbb{Q}}(1) = \mathrm{N}_{K/\mathbb{Q}}(xy) = \mathrm{N}_{K/\mathbb{Q}}(x)\mathrm{N}_{K/\mathbb{Q}}(y)$, et donc $\mathrm{N}_{K/\mathbb{Q}}(x) \in \mathbb{Z}^\times = \{\pm 1\}$. Réciproquement, si $x \in A$ vérifie $\mathrm{N}_{K/\mathbb{Q}}(x) = \pm 1$, on sait qu'il existe un polynôme unitaire P dans $\mathbb{Z}[X]$ tel que $P(x) = 0$ et $P(0) = \mathrm{N}_{K/\mathbb{Q}}(x)$: par exemple, $P = \chi_{x,K/\mathbb{Q}}$ convient d'après le cours. On écrit $P = QX \pm 1$. On en tire $\pm 1 = Q(x)x$, i.e. $\pm\mathrm{Q}(x) \in A$ est un inverse de x dans A.

(ii) La norme d'un idéal non nul est un entier ≥ 1, il suffit donc de voir qu'il n'y a qu'un nombre fini d'idéaux de A de norme $M \geq 1$ donnée. Par Lagrange, un idéal de norme $M \geq 1$ contient M. On conclut car on a vu que A/MA est fini (et n'a donc qu'un nombre fini d'idéaux) : Lemme 6.8.

(iii) On rappelle que si $x \in A$, on a $\mathrm{N}((x)) = |\mathrm{N}_{K/\mathbb{Q}}(x)|$. L'hypothèse et le (ii) montrent donc qu'il existe un idéal I et une infinité d'entiers $m \geq$ tels que l'on a $I = (x_m)$. L'idéal I est évidement non nul et principal, disons $I = (x)$ avec $x \in A - \{0\}$. De plus, si $y \in A$ on a $(y) = (x)$ si et seulement si y et x sont associés, i.e. $y/x \in A^\times$. Cela conclut.

(iv) Dans les notations du cours, on a $n = r_1$ et $r_2 = 0$ (et ι est bien le plongement canonique choisi dans le cours). On conclut car on sait que $\iota(A)$ est un réseau de covolume $2^{-r_2}|\mathrm{disc}(A)|^{1/2}$ (Prop.-Déf. 6.15).

(v) Soit $\epsilon > 0$. On onsidère le sous-ensemble B_ϵ de $\mathbb{R}^\Sigma$ constitué des n-uples (x_τ) tels que $|x_\tau| \leq 1$ pour $\tau \notin \{\sigma, \sigma'\}$, $|x_\sigma| \leq \epsilon$ et $|x_{\sigma'}| \leq |\mathrm{disc}A|^{1/2}/\epsilon$. C'est un convexe compact symétrique de mesure $2^n \cdot |\mathrm{disc}A|^{1/2} = 2^n \mathrm{covol}\iota(A)$. D'après le lemme du corps convexe de Minkowski, on peut donc trouver $x \in A - \{0\}$ tel que $\iota(x) \in B_\epsilon$.

(vi) On applique la question précédente à une suite de réels ϵ_m tendant vers 0. On en tire une suite x_m d'éléments de A tels que $|\tau(x_m)| \leq 1$ pour tout $m \geq 1$ et $\tau \notin \{\sigma, \sigma'\}$, $|\sigma(x_m)|$ tend vers 0 quand m tend vers l'infini, et $|\sigma(x_m)\sigma'(x_m)| \leq |\mathrm{disc}(A)|^{1/2}$. En particulier, on a

$$|\mathrm{N}_{K/\mathbb{Q}}(x_m)| \leq |\mathrm{disc}(A)|^{1/2}$$

pour tout m, à cause de la formule du cours $\mathrm{N}_{K/\mathbb{Q}}(x) = \prod_{\tau\in\Sigma} \tau(x)$ pour tout $x \in K$. On peut donc appliquer le (iii) à la suite (x_m). Il montre que quitte à la remplacer par une sous-suite, il

existe $x \in A - \{0\}$ tel que $x_m/x \in A^\times$ pour tout $m \geq 1$. On pose $u_m = x_m/x$. Si $\tau \in \Sigma$ on a $|\tau(u_m)| = |\tau(x_m)|/|\tau(x)|$. On en déduit le (vi) avec pour constante C tout majorant de l'ensemble fini $\{\frac{1}{|\tau(x)|}, \tau \in \Sigma\} \cup \{\frac{|\mathrm{disc}\, A|^{1/2}}{|\tau(x)\tau'(x)|}, (\tau, \tau') \in \Sigma^2\}$.

(vii) Soit $y \in A^\times$ et $I \subset \Sigma$. D'après le (i) on a l'égalité

$$\prod_{\tau \in I} \tau(x) = \prod_{\tau \in \Sigma - I} \frac{1}{\tau(x)}.$$

En particulier $\frac{1}{|\tau(y)|} = \prod_{\tau' \in \Sigma\{\tau\}} |\tau'(y)|$. On en tire $1/|\tau(u_m)| \leq C^{n-2}$ pour tout $m \geq 1$ et $\tau \notin \{\sigma, \sigma'\}$. De même (pour $I = \{\sigma, \sigma'\}$), on a $1/|\sigma(u_m)\sigma'(u_m)| \leq C^{n-2}$. Autrement dit, la constante $c = C^{2-n}$ convient.

(viii) Supposons qu'il existe $(a_\sigma) \in \mathbb{R}^\Sigma$ tel que $\sum_{\sigma \in \Sigma} a_\sigma \log|\sigma(u)| = 0$ pour tout $u \in A^\times$. Soient σ, σ' deux éléments distincts de Σ. Il faut voir $a_\sigma = a'_\sigma$. D'après les questions (v)-(vii), il existe une suite d'unités $(u_m)_{m \geq 1}$ de A telle que, lorsque m tends vers l'infini on a :

(a) $\log|\tau(u_m)| = O(1)$ si $\tau \neq \sigma, \sigma'$,

(b) $\log|\sigma'(u_m)| = -\log|\sigma'(u_m)| + O(1)$,

(c) $\log|\sigma(u_m)|$ tends vers $-\infty$.

On a $\sum_{\sigma \in \Sigma} a_\sigma \log|\sigma(u_m)| = 0$ pour tout $m \geq 1$. En faisant tendre m vers l'infini, (a) et (b) montrent que l'on a la relation $(a_\sigma - a_{\sigma'})\log|\sigma(u_m)| = O(1)$. Enfin, (c) montre $a_\sigma = a'_\sigma$.

(ix) Le fait que λ est un morphisme de groupes est évident. Enfin, si $x \in A^\times$ la relation $1 = |\mathrm{N}_{K/\mathbb{Q}}(x)| = \prod_{\sigma \in \Sigma} |\sigma(x)|$ montre après passage au logarithme $0 = \sum_{\sigma \in \Sigma} \log|\sigma(x)|$.

(x) Si $x \in \mathrm{E}_r$, alors $x \in A$ et $e^{-r} \leq |\sigma(x)| \leq e^r$ pour tout $\sigma \in \Sigma$. L'ensemble E_r est donc fini car $\iota(A)$ est un réseau d'après le cours (question (iv)).

(xi) Soient $||.|| : \mathbb{R}^\Sigma \to \mathbb{R}_{\geq 0}$ la norme définie par $||(x_\sigma)|| = \mathrm{Sup}_\sigma |x_\sigma|$ et $\mathrm{D}_r = \{x \in \mathbb{R}^\Sigma, ||x|| \leq r\}$. On a $\mathrm{D}_r \cap \mathrm{Im}\, \lambda = \lambda(\mathrm{E}_r)$, qui est fini d'après le (x). De même, $\ker \lambda = \mathrm{E}_0$ est fini. C'est un sous-groupe de $A^\times \subset K^\times \subset \mathbb{R}^\times$.

(xii) On a déja vu que $\mathrm{Im}\, \lambda$ est un sous-groupe discret de $\mathbb{R}^\Sigma$, inclus dans H, c'est donc un sous-groupe discret de H (la restriction de $||.||$ à H est une norme...). D'autre part, la question (viii) montre que $\mathrm{Im}\, \lambda$ n'est inclus dans aucun hyperplan de $\mathbb{R}^\Sigma$ distinct de H, ainsi $\mathrm{Im}\, \lambda$ engendre $\mathbb{R}$-linéairement H : c'est un réseau de H.

(xiii) Il est clair que si $x \in \mathbb{R}^\times$ vérifie $x^m = 1$ avec $m \geq 1$, alors $x = \pm 1$. En particulier, tout sous-groupe fini de $\mathbb{R}^\times$ est inclus dans $\{\pm 1\}$. Comme on a évidemment $\{\pm 1\} \subset \ker \lambda$, le (xi) (et Lagrange !) montre $\ker \lambda = A^\times$.

(xiv) On note f l'application de l'énoncé. C'est clairement un morphisme de groupes. Vérifions qu'il est injectif. Soit $(e, (m_1, \ldots, m_{n-1})) \in \{\pm 1\} \times \mathbb{Z}^{n-1}$ tel que $e u_1^{m_1} \cdots u_{n-1}^{m_{n-1}} = 1$. En appliquant le morphisme λ à cette identité, on trouve $0 = \sum_{i=1}^{n-1} m_i \lambda(u_i)$. Comme les $\lambda(u_i)$ forment une $\mathbb{Z}$-base de $\mathrm{Im}\, \lambda$, on a donc $m_i = 0$ pour tout $i = 1, \ldots, n-1$. La relation de départ s'écrit donc $e = 1$: on a montré que f est injectif. Il ne reste qu'à voir que f est surjectif. Soit $x \in A^\times$. On regarde $\lambda(x) \in \mathrm{Im}\, \lambda = \sum_i \mathbb{Z}\lambda(u_i)$. On peut donc trouver $(m_1, \ldots, m_{n-1}) \in \mathbb{Z}^{n-1}$ tel que $\lambda(x) = \lambda(\prod_{i=1}^{n-1} u_i^{m_i})$, autrement dit $x \prod_{i=1}^{n-1} u_i^{-m_i} \in \ker \lambda$. On conclut car $\ker \lambda = \{\pm 1\}$.

(xv) Par hypothèse sur d, le corps $\mathbb{Q}(\sqrt{d})$ est de degré 2 sur $\mathbb{Q}$ et totalement réel : les deux racines de $X^2 - d$ sont dans $\mathbb{R} - \mathbb{Q}$. Soit $A = \mathbb{Z}[\sqrt{d}]$. Si $(x, y) \in \mathbb{Z}^2$, un exemple du cours montre $\mathrm{N}_{K/\mathbb{Q}}(x + y\sqrt{d}) = x^2 - dy^2$. D'après le (i), il s'agit de voir qu'il y a une infinité de $z \in A^\times$ tels que $\mathrm{N}_{K/\mathbb{Q}}(z) = 1$. Mais d'après le (xiv), on a $A^\times \simeq \{\pm 1\} \times \mathbb{Z}$. En particulier, $A^\times$ est infini. Il en va donc de même du noyau du morphisme $A^\times \to \{\pm 1\}$, $z \mapsto \mathrm{N}_{K/\mathbb{Q}}(z)$.