1. Corrigé de l'examen MAT552 année 2015-2016

Problème 1. (i) D'après un théorème de Gauss, toute forme est proprement équivalente à une et une seule forme réduite (nécessairement de même discriminant). Soit (a,b,c) une forme réduite de discriminant -95. On a $-a < |b| \leq a \leq c$, b impair, et $a \leq \sqrt{95/3} < \sqrt{32} < 6$, donc $b = \pm 1, \pm 2, \pm 3$ et $(b^2 - D)/4 = ac$. Pour $b^2 = 1$ on a $ac = 24$, et on trouve $(1,1,24)$, $(2,\pm 1,12)$, $(3,\pm 1,8)$ et $(4,\pm 1,6)$. Pour $b^2 = 3$ on a $ac = 26$, et aucune forme réduite. Pour $b^2 = 5$ on a $ac = 30$, qui conduit à $(5,5,6)$. Les 8 formes exhibées sont bien réduites, et conviennent donc. Elles sont primitives (conformément au fait que -95 est fondamental).

(ii) Les classes de carré 1 de $\mathrm{P}(D)$ sont les classes ambiguës, i.e. les classes de formes ambiguës. Les formes $(1,1,24)$ et $(5,5,6)$ sont ambiguës (car du type (a,a,c)), et les 6 autres ne le sont manifestement pas. La classe de $(1,1,24)$ est d'ordre 1. La seule classe d'ordre 2 est donc celle de $(5,5,6)$.

(iii) Comme -95 est non carré, sans facteur carré et congru à 1 modulo 4, un résultat du cours assure que A_{-95} est l'anneau des entiers de $\mathbb{Q}(\sqrt{-95})$. C'est donc un anneau de Dedekind, par un autre résultat du cours. Le polynôme minimal $\Pi_{\alpha,\mathbb{Z}}$ de α sur $\mathbb{Q}$ est $(X-\alpha)(X-\overline{\alpha}) = X^2 - X + 24$.

(iv) On a $\Pi_{\alpha,\mathbb{Q}} \equiv X(X-1) \bmod 2$, donc D et $\overline{D}$ sont des "I(Q)" du cours pour $p = 2$ et $Q = X$ et $X - 1$ respectivement. Comme un tel Q est irréductible de degré 1, D et $\overline{D}$ sont premiers de norme $2^1 = 2$. De même, C est premier de norme 5 à cause de la relation $\Pi_{\alpha,\mathbb{Q}} \equiv (X+2)^2 \bmod 5$.

(v) Si $C = (z)$ avec $z \in A$, alors on $\mathrm{N}(C) = \mathrm{N}(z)$ (cours) et donc 5 est représenté par $(1,1,24)$. Mais $5 = x^2 + xy + 24y^2$ avec $x, y \in \mathbb{Z}$ entraine $20 = (2x+y)^2 + 95 \cdot y^2$, puis $y = 0$, puis $5 = x^2$: absurde. Les décomposition cherchées découlent d'un théorème du cours, qui utilise le fait que $\mathbb{Z}[\alpha]$ est l'anneau des entiers de $\mathbb{Q}(\sqrt{-95})$ et les décompositions mod 2 et 5 de $\Pi_{\alpha,\mathbb{Q}}$ données au (iv).

(vi) La bijection de Dedekind est un isomorphisme de groupes $[I] \mapsto \mathrm{q}_I$, entre $\mathrm{Pic}(A) = \mathrm{Cl}(A)$ et $\mathrm{P}(-95)$. D'après le (v), on a $[C]^2 = 1$ et $[C] \neq 1$, donc $[C]$ est d'ordre 2. Il en résulte que q_C est d'ordre 2, c'est donc la classe de $(5,5,6)$ d'après le (ii).

(vii) On a $\mathrm{N}(7+\alpha) = 7^2 + 7 + 24 = 80$. Les idéaux premiers de A contenant $7+\alpha$, et donc $(7+\alpha)\overline{(7+\alpha)} = 80 = 2^4 \cdot 5$, contiennent donc 2 ou 5. Mais A étant Dedekind, les relations $(2) = D\overline{D}$ et $(5) = C^2$ montrent que ces idéaux sont parmi D, $\overline{D}$ et C, puis l'existence d'une décomposition $(7+\alpha) = D^a \overline{D}^b C^c$. Par multiplicativité de la norme dans $A = \mathcal{O}_{\mathbb{Q}(\sqrt{-95})}$, on a $80 = 2^{a+b}5^c$ donc $c = 1$ et $a + b = 4$. Si D divise $7+\alpha$, alors on a $7 + \alpha = 1 + 2 \cdot 3 + 2\alpha$ puis $1 \in D$ et $D = A$, ce qui est faux car $\mathrm{ND} = 2$. Donc $a = 0$ et $b = 4$.

(viii) Le (vii) entraîne $1 = [\overline{D}]^4[C]$ dans $\mathrm{Cl}(A)$. On a aussi $[D][\overline{D}] = 1$ car $(2) = D\overline{D}$, donc $[D]^4 = [C]$ dans $\mathrm{Cl}(A)$. Comme $[C]$ est d'ordre 2, l'ordre de $[D]$ est exactement 8 (il divise 8, mais pas 4). Ainsi, $[D]$ engendre un sous-groupe cyclique d'ordre 8 dans $\mathrm{Cl}(A)$. On a déjà justifié $\mathrm{Cl}(A) \simeq \mathrm{P}(-95)$, donc $|\mathrm{Cl}(A)| = 8$ par le (i), ce qui conclut.

(ix) Le groupe $2\mathbb{Z} + \alpha\mathbb{Z}$ est clairement d'indice 2 dans A, et inclus dans D, qui est aussi d'indice (=norme) 2 par le (iv), on a donc $D = 2\mathbb{Z} + \alpha\mathbb{Z}$. La base $2, \alpha$ est directe (on conserve les conventions du cours), donc q_D est la classe d'équivalence propre de la forme

$$\mathrm{q}_{2,\alpha}(x,y) = \frac{1}{2}\mathrm{N}(2x + y\alpha) = \frac{1}{2}(4x^2 + 2xy + 24y^2),$$

i.e. de $(2,1,12)$.

(x) On a $C^2 = \langle 2,\alpha\rangle^2 = \langle 4, 2\alpha, \alpha^2\rangle$. Les relations $\alpha^2 = \alpha - 24$ et $24 = 4\cdot 6$ montrent successivement $C^2 = \langle 4, 2\alpha, \alpha\rangle = \langle 4,\alpha\rangle$. Ensuite, on constate de même les égalités

$$C^2C = \langle 4,\alpha\rangle\langle 2,\alpha\rangle = \langle 8, 2\alpha, \alpha^2\rangle = \langle 8, 2\alpha, \alpha\rangle = \langle 8,\alpha\rangle$$

(on a utilisé $8\cdot 3 = 24$). On a $\mathrm{N}(C^n) = 2^n$ ($A = \mathcal{O}_{\mathbb{Q}(\sqrt{-95})}$ et $\mathrm{N}(C) = 2$). Un calcul immédiat montre $\mathrm{q}_{4,\alpha} = (4,1,6)$ et $\mathrm{q}_{8,\alpha} = (8,1,3)$. En utilisant que (a,b,c) est proprement équivalent à $(c,-b,a)$, on en déduit que q_{C^2} et q_{C^3} sont les classes respectives de $(4,1,6)$ et $(3,-1,8)$. On conclut car on a $\mathrm{q}_{C^n} = (\mathrm{q}_C)^n$ par définition de la loi de groupe sur $\mathrm{P}(D)$.

(xi) D'après (viii) et (ix), l'application $\mathbb{Z}/8\mathbb{Z} \to \mathrm{P}(-95)$, $i \mapsto (\mathrm{q}_C)^i$ est un isomorphisme de groupe. Il suffit donc de déterminer $(\mathrm{q}_C)^i$ pour tout entier $0 \le i \le 7$. Ces classes sont respectivement : celle de $(1,1,24)$ pour $i = 0$ (forme principale, ordre 1), celle de $(4,1,6)$ pour $i = 2$ et celle de $(3,-1,8)$ pour $i = 3$ d'après (x), celle de $(5,5,6)$ pour $i = 4$ d'après (vi). On conclut car $(\mathrm{q}_C)^5 = (\mathrm{q}_C)^{-3} = (\mathrm{q}_C^3)^{\mathrm{opp}}$ est donc la classe de $(3,1,8)$, et de même $(\mathrm{q}_C)^6 = (\mathrm{q}_C)^{-2}$ est celle de $(4,-1,6)$ et $(\mathrm{q}_C)^7 = (\mathrm{q}_C)^{\mathrm{opp}}$ est celle de $(2,-1,12)$.

(xii) Si n est représenté par $(2,1,12)$, dont la classe est q_C, alors n^i est représenté par toute forme dans la classe de q_C^i, ainsi que par toute forme équivalente à une telle forme. On conclut par le (xi). En guise d'exemple, l'assertion est manifestement satisfaite pour $n = 2$ (noter $5{+}5{+}6 = 16$).

Problème 2. (i) Comme I est inversible, il existe un idéal J non nul de A tel que IJ est principal, disons $IJ = (z)$. L'inclusion $aI \subset bI$ entraine $aIJ \subset bIJ$, c'est-à-dire $(az) \subset (bz)$. En multipliant par $1/z$ (noter $z \neq 0$), il reste $(a) \subset (b)$: $a.1 \in bA$ et donc b divise a.

(ii) Comme A est un ordre de K, il contient une $\mathbb{Q}$-base de K. On en déduit $K = \bigcup_m \frac{1}{m}A$, la réunion portant sur les $m \in \mathbb{Z}$ avec $m \ge 1$. Écrivons $E = \{e_1, \ldots, e_n\}$ et choisissons $m_i \in \mathbb{Z} - \{0\}$ tel que $m_i e_i \in A$. Alors l'entier $m = m_1 m_2 \cdot m_n$ est non nul et vérifie $mE \subset A$.

(iii) Comme x est dans $\mathcal{O}_K$, il existe $m_0, m_1, \ldots, m_{n-1}$ dans $\mathbb{Z}$ tels que $x^n = \sum_{i=0}^{n-1} m_i x^i$. D'après un énoncé du cours (chapitre 1), tout élément de $A[x]$ s'écrit alors sous la forme $\sum_{i=0}^{n} a_i x^i$ avec $a_i \in A$. Il suffit donc de montrer qu'il existe $m \in \mathbb{Z} - \{0\}$ avec $mx^i \in A$ pour tout $i \in \{0, 1, \ldots, n-1\}$. Cela résulte du (ii) appliqué à l'ensemble fini $E = \{x^i,\ 0 \le i \le n-1\}$.

(iv) $A[x]$ est un sous-anneau de K. En particulier, c'est un sous-groupe additif stable par multiplication par A et par x. Il en va donc de même de $aA[x]$ pour tout $a \in A$. Soit $m \in \mathbb{Z} - \{0\}$ tel que $mA[x] \subset A$, un tel $a = m$ existe par (iii). La remarque précédente assure que $mA[x]$ est un idéal de A. Il est non nul : il contient $m.1 = m \neq 0$.

(v) Supposons (c) vérifiée. Soit x dans $\mathcal{O}_K$ non nul. En particulier, x est dans K, donc s'écrit sous la forme a/b avec $b = m$ non nul dans $\mathbb{Z}$ (par le (ii)). Soit I comme au (iv). On a $a/bI \subset I$, donc $aI \subset bI$. D'après (c), I est inversible. Le (i) entraîne donc que b divise a dans A, i.e. $x \in A$. Ainsi, on a $\mathcal{O}_K \subset A$, puis $A = \mathcal{O}_K$.

(vi) C'est le cas $\alpha = 1$ du Lemme 7.4, dont la démonstration ne nécessite pas que A soit l'anneau des entiers de K, comme nous l'avions observé en cours.

(vii) Supposons (b) vérifié mais qu'il existe un idéal non nul de A non inversible. Considérons un tel idéal I de norme minimale. L'idéal I n'est pas maximal, d'après (b). Il est donc inclus dans un idéal maximal P de A. Mais P est premier donc inversible d'après (b), on a donc $I = JP$ pour un idéal J de A. On a $I = JP \subsetneq J$ d'après le (vi), donc $\mathrm{N}(J) < \mathrm{N}(I)$. Donc J est inversible.

Mais alors $I = JP$ est inversible (produit de deux inversibles) : absurde. Il ne reste que (a) $\Rightarrow$ (b) (ou (c)), qui est un théorème du cours.

(viii) On a $\mathrm{I}(P) = pA + \Pi_{\alpha,\mathbb{Q}}(\alpha)A = pA$.

(ix) D'après Bézout, il existe V, V' dans $(\mathbb{Z}/p\mathbb{Z})[X]$ tels que $UQ + U'Q' = 1$. Soient $U, U' \in \mathbb{Z}[X]$ arbitraires tels que $U \equiv V \bmod p$ et $U' \equiv V' \bmod p$. On a $U\widetilde{Q} + U'\widetilde{Q} \equiv 1 \bmod p\mathbb{Z}[X]$, et conclut en évaluant en $X = \alpha$.

(x) On a $\mathrm{I}(Q) = (p, \widetilde{Q}(\alpha))$ et $\mathrm{I}(Q') = (p, \widetilde{Q'}(\alpha)$, donc $\mathrm{I}(Q)\mathrm{I}(Q')$ est l'idéal $p(p, \widetilde{Q}(\alpha), \widetilde{Q'}(\alpha)) + (\widetilde{Q}(\alpha)\widetilde{Q'}(\alpha))$. D'après le (ix) on a $1 \in (p, \widetilde{Q'}(\alpha), \widetilde{Q}(\alpha))$, donc l'idéal ci-dessus est $\mathrm{I}(QQ')$.

(xi) On écrit $P = \prod_i P_i$ avec les P_i irréductibles distincts. Le (x) montre par récurrence $\mathrm{I}(P) = \prod_i \mathrm{I}(P_i)$. Le $\mathrm{I}(P_i)$ sont les idéaux premiers de A contenant p par le cours, et leur produit est principal : ce sont des idéaux inversibles.

Problème 3. (i) On a $\Phi_\ell(\zeta) = 0$ et Φ_ℓ est irréductible dans $\mathbb{Q}[X]$, donc $\Phi_\ell = \Pi_{\zeta,\mathbb{Q}}$. En particulier, on a $\ell - 1 = \deg \Phi_\ell = [K : \mathbb{Q}]$. Les racines de Φ_ℓ sont les éléments de $\mu = \{\zeta^i, i = 1, \ldots, \ell - 1\}$. On en déduit d'une part l'assertion sur $\Sigma(K)$ (cours), et d'autre part, comme ℓ est impair, que tous ces éléments sont complexes non réels. On a donc $r_1 = 0$ et $r_2 = (\ell - 1)/2$.

(ii) On a $\Phi_\ell(X) = \prod_{i=1}^{\ell-1}(X - \zeta^i)$, puis $\ell = \Phi_\ell(1) = \prod_{i=1}^{\ell-1}(1 - \zeta^i)$ en faisant $X = 1$. On conclut par la relation $\mathrm{N}_{K/\mathbb{Q}}(x) = \prod_{\sigma\in\Sigma(K)} \sigma(x)$ et la description de $\Sigma(K)$ en (i).

(iii) D'après le cours on a $\mathrm{N}((1 - \zeta)) = |\mathrm{N}_{K/Q}(1 - \zeta)|$. Donc l'idéal $(1 - \zeta)$ de A est de norme ℓ, i.e. d'indice ℓ dans A. Un sous-groupe d'indice premier ℓ dans A est forcément maximal pour l'inclusion, car $A/\ell A \simeq \mathbb{Z}/\ell\mathbb{Z}$ n'a pas d'autres sous-groupes que 0 et $\mathbb{Z}/\ell\mathbb{Z}$. Ainsi, $(1 - \zeta)$ est un sous-groupe maximal de A, donc un idéal maximal de A en particulier.

(iv) D'après le (i), on a la formule $\mathrm{disc}\Phi_\ell = \prod_{1\le i<j\le \ell-1}(\zeta^i - \zeta^j)^2$. En particulier, $\pm\mathrm{disc}\Phi_\ell$ est le produit sur tous les couples (i, j) avec $i \neq j$, des $(\zeta^i - \zeta^j)$. On a donc $\mathrm{disc}|\Phi_\ell| = \prod_{1\le i\le \ell-1} m_i$ avec

$$m_i = |\prod_{j\neq i}(\zeta^i - \zeta^j) = |\prod_{j\neq i}(1 - \zeta^{j-i})| = \ell|1 - \zeta^{-i}|^{-1},$$

(la seconde égalité utilise (ii)), ce qui conclut par (ii) encore.

(v) On a $\Phi_\ell \equiv (X - 1)^{\ell-1} \bmod \ell$, donc d'après le cours il existe un et un seul idéal premier de A contenant ℓ, à savoir l'idéal $\mathrm{I}(X - 1) = (\ell, \zeta - 1)$. Mais on a vu que $(\zeta - 1)$ est maximal, de sorte que l'inclusion évidente $(\zeta - 1) \subset \mathrm{I}(X - 1)$ entraîne $\mathrm{I}(X - 1) = (\zeta - 1)$.

(vi) Soit p premier $\neq \ell$. La réduction modulo p du polynôme $X^\ell - 1$ est sans facteur carré. En effet, si $P \in \mathbb{Z}/p\mathbb{Z}[X]$ est tel que P^2 divise $X^\ell - 1$, alors P divise le polynôme dérivé de $X^\ell - 1$, qui vaut $\ell X^{\ell-1}$, et donc $X^\ell - 1$ car ℓ est premier à p. C'est absurde, car X ne divise pas $X^\ell - 1$. Ainsi, Φ_ℓ (qui divise $X^\ell - 1$) est sans facteur carré également.

(vii) D'après le (vi) et le problème 2 (xi), les idéaux premiers de A contenant un premier $p \neq \ell$ sont inversibles. D'après le (v), l'unique idéal premier de A contenant ℓ est $(1 - \zeta)$, qui est aussi inversible (car principal...). Mais d'après le cours, tout idéal premier de A contient un premier p de $\mathbb{Z}$. Ainsi, tous les idéaux premiers de A sont inversibles. Le (b) $\Rightarrow$ (a) du problème 2 entraîne donc $A = \mathcal{O}_K$.

(viii) D'après Minkowski, (i) et (iv), tout déal de A est équivalent à un idéal contenant un entier N avec $1 \le N \le C(3, 6)\sqrt{7^5} \simeq 4.12$ d'après l'énoncé.

(ix) On a démontré que A est l'anneau des entiers de $\mathbb{Q}(\zeta)$ (donc de Dedekind). Le (viii) montre donc que $\mathrm{Cl}(A)$ est engendré par les classes des idéaux premiers de A contenant un entier $1 \leq N \leq 4$, i.e. un entier $1 \leq N \leq 3$. D'après les données, l'unique idéal premier contenant 3 est l'idéal principal (3). De plus, on constate que $X^3 + X + 1$ et $X^3 + X^2 + 1$ n'ont pas de racine dans $\mathbb{Z}/2\mathbb{Z}$, ils sont donc irréductibles dans $\mathbb{Z}/2\mathbb{Z}[X]$. Les idéaux premiers contenant 2 sont donc $I = (2, \zeta^3 + \zeta + 1)$ et $J = (2, \zeta^3 + \zeta^2 + 1)$, et on a $IJ = (2)$ car A est l'anneau des entiers de $\mathbb{Q}(\zeta)$. La relation $1 = [I][J]$ entraîne bien que $\mathrm{Cl}(A)$ est engendré par $[I]$.

(x) On constate que la multiplication par $1 + \zeta + \zeta^3$ a pour matrice dans la base $1, \zeta, \cdots, \zeta^5$ la matrice indiquée dans les données. Le déterminant de cette matrice est 8, et aussi $\mathrm{N}_{K/\mathbb{Q}}(1+\zeta+\zeta^3)$ par définition. Mais la norme de I vaut $2^{\deg(X^3+X+1)} = 8$, et I contient $(1 + \zeta + \zeta^3)$ qui est aussi de norme 8, on a donc $I = (1 + \zeta + \zeta^3)$: c'est un idéal principal, et A est principal d'après le (ix).