4. Exercices du chapitre 4

Exercice 4.1. Comme $\mathrm{N}(1+i)=2$ est premier, $1+i$ est irréductible. Si p est premier et $p=a^2+b^2$ avec $a,b\in\mathbb{Z}$, alors $p=\mathrm{N}(a+bi)=\pi\overline{\pi}$ où $\pi=a+bi$ est irréductible car de norme première. Les unités de $\mathbb{Z}[i]$ sont $\pm1,\pm i$, donc les associés de $a+bi$ sont $a+bi,-a-bi,-b+ai,b-ai$. Cette liste ne contient pas $a-bi$ sauf si $b=0$ ou $a=\pm b$. Le premier cas ne se produit jamais, et le second uniquement si $p=a^2+b^2=2$. Pour le (ii), observer que si p est un nombre premier et si π est un facteur irréductible de p dans $\mathbb{Z}[i]$, alors $\mathrm{N}(\pi)$ est un diviseur propre de $\mathrm{N}(p)=p^2$, donc $\mathrm{N}(\pi)=p$, et p est somme de deux carrés. Si π est irréductible dans $\mathbb{Z}[i]$, alors $(\pi)\cap\mathbb{Z}$ est un idéal de $\mathbb{Z}$ dont le générateur est par définition le plus petit nombre entier N divisible par π dans $\mathbb{Z}[i]$. Mais π est premier dans $\mathbb{Z}[i]$ car ce dernier est factoriel, donc N est nécessairement premier. Ainsi, chaque irréductible de π divise un unique nombre premier de $\mathbb{Z}$, et sont donc dans la liste (i), (ii) et (iii).

Exercice 4.2 Les éléments $z=a+bi\in\mathbb{Z}^2$ tels que $\mathrm{N}(z)=p$ sont exactement les diviseurs de p qui ne sont pas des unités. Si $p=\pi\overline{\pi}$ avec $\pi\in\mathbb{Z}[i]$ fixé, on a vu que π et $\overline{\pi}$ sont deux irréducibles non associés. La factorisation unique dans $\mathbb{Z}[i]$ donne donc exactement 8 solutions, à savoir les 4 associés de π et les 4 de $\overline{\pi}$. Autrement dit, si $p=a^2+b^2$, les seules autres écritures de p comme somme de deux carrés sont celles obtenues en remplaçant (a,b) par $(\pm a,\pm b)$ et $(\pm b,\pm a)$.

Exercice 4.3 On a $-3+15i=3(-1+5i)$ et le nombre 3 est premier dans $\mathbb{Z}[i]$. De plus, $\mathrm{N}(-1+5i)=26=2\cdot13$, on s'attend donc (étant donnée la propriété de factorisation unique et la classification des irréductibles) que $-1+5i$ soit de la forme $(1+i)\pi$ où $\mathrm{N}(\pi)=13$ (premier congru à 1 modulo 4). On constate en effet que $(-1+5i)=(1+i)(2+3i)$.

Exercice 4.4 Pour le (i), observer que $4=-2i(1+i)^2$ est bien dans l'idéal en question, et que de plus $i\cdot2(1+i)=2(-1+i)=2(1+i)-4$. Pour le (ii), écrire $a+bi=a-b+b(1+i)$, de sorte que $a+bi\equiv3 \bmod 2(1+i)$ si et seulement si $b\equiv0 \bmod 2$ et $a-b\equiv3 \bmod 4$. Pour le (iii), observer que tout élément inversible de l'anneau $\mathbb{Z}[i]/2(1+i)\mathbb{Z}[i]$ s'écrit de manière unique sous la forme $3u$ où $u\in\mathbb{Z}[i]^\times$.

Exercice 4.5 On a $(a+b\alpha)(c+d\alpha)=ac-pbd+(ad+bc)\alpha$. Mais p divise $ac-pbd$ si et seulement si p divise a ou p divise c.

Exercice 4.6 Montrons le (i). $\mathrm{I}_{a,b}$ est un idéal de A si, et seulement si, on a $\sqrt{d}\,\mathrm{I}_{a,b}\subset\mathrm{I}_{a,b}$. Il est équivalent de demander que l'on a $a\sqrt{d}\in\mathrm{I}_{a,b}$ et $(b+\sqrt{d})\sqrt{d}=d+b\sqrt{d}\in\mathrm{I}_{a,b}$. La relation $a\sqrt{d}=a(\sqrt{d}-b)+ba$ montre que l'on a toujours $a\sqrt{d}\in\mathrm{I}_{a,b}$. L'identité $d+b\sqrt{d}=(d-b^2)+b(\sqrt{d}+b)$, et le fait que $1,\sqrt{d}$ est une $\mathbb{R}$-base de $\mathbb{C}$, montrent que l'on a $d+b\sqrt{d}\in\mathrm{I}_{a,b}$ si, et seulement si, $d-b^2\in a\mathbb{Z}$.

Pour le (ii), on constate que si $\beta:=b+\sqrt{d}$, alors $1,\beta$ est une $\mathbb{Z}$-base de A. En effet, on a $x+y\sqrt{d}=(x-by)\cdot1+y\beta$. De plus, $a\cdot1$ et β est une $\mathbb{Z}$-base de $\mathrm{I}_{a,b}$. On a donc $A/\mathrm{I}_{a,b}\simeq\mathbb{Z}/a\mathbb{Z}$ (considérer par exemple l'application $\mathbb{Z}$-linéaire $A\to\mathbb{Z}/a\mathbb{Z},x+y\beta\mapsto x \bmod a$.)

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

D'après le (i), (ii) et (iii), pour tout entier $b\in\mathbb{Z}$ et tout entier $a>0$ non carré tell que a divise b^2-d, on a $a\geq d$. Pour $b=0$, cela montre que soit $-d=1$ ou 2, soit $-d$ est premier impair. Dans ce dernier cas, on réapplique cette observation à $b=1$, de sorte que $1-d$ est pair, et $a=2$. On en déduit $|d|\leq2$.

Exercice 4.7 On raisonne dans l'anneau euclidien $\mathbb{Z}[\alpha]$ avec $\alpha=\frac{1+\sqrt{-7}}{2}$. On constate en effet que $y^2+y=x^3-2$ s'écrit aussi $\mathrm{N}(y+\alpha)=x^3$. Pour le (i), on pourra observer que $\pi=\sqrt{-7}$ est irréductible (car de norme7) et donc premier car $\mathbb{Z}[\alpha]$ est euclidien donc factoriel. On pourrait aussi raisonner comme dans l'Exercice 4.5. Pour le (ii), on observe que π et $\overline{\pi}=-\pi$ sont associés, de sorte que $v_\pi(y+\alpha)=v_\pi(y+\overline{\alpha})$. Comme $y+\alpha-(y+\overline{\alpha})=\sqrt{-7}=\pi$, on a de plus $v_\pi(y+\alpha)\leq1$. Mais on a aussi $2v_\pi(y+\alpha)=3v_\pi(x)$, de sorte que $v_\pi(y+\alpha)$ est multiple de 3, d'où $v_\pi(y+\alpha)=0$. On en déduit que $y+\alpha$ et $y+\overline{\alpha}$ sont premiers entre eux, et donc $y+\alpha=(a+b\alpha)^3$ pour certains $a,b\in\mathbb{Z}$. On conclut comme dans l'exemple du cours.

Exercice 4.9 Le (i) est tautologique. Pour le (ii), observer que si $x\in A$ est tel que $m=bx$ est multiple de a, alors $a|x$, puis ab divise m.

Exercice 4.10 (i) L'élément $\sqrt{-5}$ est premier et ne divise pas $1+\sqrt{-5}$, ils sont donc premiers entre eux, et on conclut donc par le (i) de l'Exercice 4.9.

(ii) Un ppcm m de 2 et $1+\sqrt{-5}$ serait de norme multiple de $\mathrm{N}(2)=4$ et $\mathrm{N}(1+\sqrt{-5})=6$, donc multiple de 12. D'autre part m diviserait $2(1+\sqrt{-5})$ dont la norme est 24, ainsi que $2\cdot 3=(1-\sqrt{-5})(1+\sqrt{-5})$, dont la norme est 36. Il vient que $\mathrm{N}(m)$ diviserait $\mathrm{pgcd}(24,36)=12$, puis $\mathrm{N}(m)=12$. Mais $(1,0,5)$ ne représente pas 12, et donc m n'existe pas.

(iii) Supposons que d est un pgcd des nombres de l'énoncé. Il est donc multiple des irréductibles non associés 3 et $1+\sqrt{-5}$. Écrivons $d=3a$. La relation $d|3(1\pm\sqrt{-5})$ équivaut à $a|(1\pm\sqrt{-5})$, et entraîne que $a=\pm 1$ car $1+\sqrt{-5}$ et $1-\sqrt{-5}$ sont premiers entre eux (irréductibles non associés !). Il reste $d=\pm 3$, également absurde car 3 n'est pas divisible par $1+\sqrt{-5}$.

(vii) Supposons que $(1+\sqrt{-5})a$ est divisible par 2 avec $a\in\mathbb{Z}[\sqrt{-5}]$. Si l'on écrit $a=u+v(1+\sqrt{-5})$ avec $u,v\in\mathbb{Z}$, on constate que $(1+\sqrt{-5})a=-6v+(1+\sqrt{-5})(u+2v)$. Mais ce nombre est multiple de 2 dans $\mathbb{Z}[\sqrt{-5}]$ si et seulement si ses deux coordonnées dans la $\mathbb{Z}$-base 1 et $1+\sqrt{-5}$ le sont (pourquoi ?), i.e. si et seulement si u est pair, i.e. $a\in I$.

Exercice 4.13 L'intégrité de A résulte du lemme des zéros isolés et de la connexité de $\mathbb{C}$. Si $f\in A$ ne s'annule pas, il est bien connu que $1/f$ est holomorphe, i.e. $f\in A^\times$. Le (ii) découle simplement du fait, également bien connu, que si $f\in A$ s'annule en $a\in\mathbb{C}$, alors $z\mapsto f(z)/(z-a)$ se prolonge en une fonction holomorphe sur $\mathbb{C}$, disons $g\in A$, de sorte que $f(z)=(z-a)g(z)$. Le (iii) découle de l'existence de $f\in A$ ayant une infinité de zéros, comme par exemple $z\mapsto\sin(z)$.

5. Exercices du chapitre 5

Exercice 5.1. Si $d\in\mathbb{Z}$ n'est pas un carré, alors X^2-d est irréductible dans $\mathbb{Q}[X]$ est donc $[\mathbb{Q}(\sqrt{d}):\mathbb{Q}]=2$. Si $d=d'u^2$ avec $u\in\mathbb{Z}$ alors $\mathbb{Q}(\sqrt{d})=\mathbb{Q}(\sqrt{d'})$.

Si d,d' sont sans facteur carré et distincts, alors $\mathbb{Q}(\sqrt{d})\cap\mathbb{Q}(\sqrt{d'})=\mathbb{Q}$. En effet, sinon $\mathbb{Q}(\sqrt{d})=\mathbb{Q}(\sqrt{d'})$ pour des raisons de dimension, et donc $\sqrt{d}=a+b\sqrt{d'}$ avec $a,b\in\mathbb{Q}$. Cela entraîne $d=a^2+d'b^2+2ab\sqrt{d'}$, puis $ab=0$ car $1,\sqrt{d'}$ est $\mathbb{Q}$-libre. Si $a=0$ alors $d=d'b^2$, si $b=0$ alors $d=a^2$: les deux cas sont absurdes.

Enfin, si $[K:\mathbb{Q}]=2$ et si $x\in K\backslash\mathbb{Q}$ alors $K=\mathbb{Q}(x)$ avec $\Pi_{x,\mathbb{Q}}=X^2+aX+b$ irréductible dans $\mathbb{Q}[X]$. En particulier, son discriminant $d:=a^2-4b$ n'est pas un carré dans $\mathbb{Q}$. Mais $(2x+a)^2=a^2-4b$ donc $2x+a=\pm\sqrt{d}\in K$, puis $\mathbb{Q}(\sqrt{d})=K$.

Exercice 5.2 D'après l'Exercice 5.1, il faut voir que pour tout entier d sans facteur carré, il existe une racine de l'unité ζ telle que $\sqrt{d}\in\mathbb{Q}(\zeta)$. Se ramener au cas où d est premier, et dans ce cas considérer la somme de Gauss.

Exercice 5.3 Si d n'est pas un cube dans $\mathbb{Q}$, et si $\alpha=\sqrt[3]{d}$, alors $[\mathbb{Q}(\alpha):\mathbb{Q}]=3$. Un calcul dans la base $1,\alpha,\alpha^2$ montre que $\mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(a+b\alpha+c\alpha^2)=a^3+db^3+d^2c^3-3abcd$. Conclure dans ce cas par multiplicativité de la norme. Dans le cas général, fixer $a,b,c,a',b',c'\in\mathbb{Z}$ et observer que l'identité cherchée équivaut à l'annulation d'un certain polynôme en d à coefficients dans $\mathbb{Z}$, qui s'annule sur l'infinité des non cubes.

Exercice 5.4 Observer que $\mathrm{disc}(P)\neq 0$ puis que $\frac{\mathrm{disc}(Q)}{\mathrm{disc}(P)}\in\mathbb{Q}\cap\overline{\mathbb{Z}}=\mathbb{Z}$.

Exercice 5.5 C'est un calcul direct dans la $\mathbb{Z}$-base $1,\sqrt{d}$ si $d\not\equiv 1 \bmod 4$, dans $1,\frac{1+\sqrt{d}}{2}$ sinon.

Exercice 5.6 Pour le (i), d'après le cours le carré de l'indice de $\sum_i\mathbb{Z}e_i$ dans $\mathcal{O}_K$ divise l'entier $\mathrm{disc}_{K/\mathbb{Q}}(e_1,\cdots,e_n)$. Cet indice est donc 1 par hypothèse. Pour le (ii), X^3-X+1 est irréductible dans $\mathbb{Q}[X]$ car sans racine rationnelle, donc $[K:\mathbb{Q}]=3$. Son discriminant est ± 23, sans facteur carré, d'où le (ii).

Exercice 5.7 Le (i) est immédiat en considérant la $\mathbb{Q}$-base $1,x,x^2$ de K. Le (ii) se déduit de $\mathrm{Tr}_{K/\mathbb{Q}}(x)=\mathrm{Tr}_{K/\mathbb{Q}}(x^2)=0$.Pour le (iii), l'indication montre d'abord que $4(3b)^3\in\mathbb{Z}$, ce qui entraîne $3b\in\mathbb{Z}$ car $3b\in\frac{1}{2}\mathbb{Z}$, puis on voit que $3c\in\mathbb{Z}$ de la même manière. Pour le (v), observer que la norme de l'élément $\pm\frac{1}{3}(1-x+x^2)$ vaut $\pm\frac{1}{27}(1-2+4-6)\notin\mathbb{Z}$.

Exercice 5.8 Comme m et n sont distincts et sans facteurs carré, on a $\mathbb{Q}(\sqrt{m})\cap\mathbb{Q}(\sqrt{n})=\mathbb{Q}$ (Exercice 5.1). On en déduit que $[K:\mathbb{Q}(\sqrt{n})]=2$ puis que $[K:\mathbb{Q}]=4$ par la base télescopique, ainsi que le fait que $1,\alpha,\beta,\alpha\beta$ est une $\mathbb{Q}$-base de K. Observons qu'un $\sigma\in\Sigma(K)$ est uniquement déterminé par ses valeurs $\sigma(\sqrt{n})$ et $\sigma(\sqrt{m})$. Mais $\sigma(\sqrt{n})=\pm\sqrt{n}$ et $\sigma(\sqrt{m})=\pm\sqrt{m}$, donc les 4 possibilités de signes sont atteintes car $|\Sigma(K)|=[K:\mathbb{Q}]=4$.

Soit $z = a + b\sqrt{n} + c\sqrt{m} + d\sqrt{mn} \in \mathcal{O}_K$ avec $a, b, c, d \in \mathbb{Q}$. Considérons l'unique $\sigma \in \Sigma(K)$ vérifiant $\sigma(\sqrt{n}) = -\sqrt{n}$ et $\sigma(\sqrt{m}) = \sqrt{m}$). On a alors $\sigma(z) \in \mathcal{O}_K$ et $\sigma(z) = a - b\sqrt{n} + c\sqrt{m} - d\sqrt{mn}$. On en déduit

$$z + \sigma(z) = 2a + 2c\sqrt{m} \in \mathcal{O}_{\mathbb{Q}(\sqrt{m})} = \mathbb{Z} + \mathbb{Z}\beta.$$

En particulier, on a $4a, 4c \in \mathbb{Z}$. On conclut le (ii) en considérant de même les deux autres plongements non triviaux.

Le (i) montre que $\mathrm{disc}(K)$ est un diviseur de m^2n^2. Le (ii) montre que

$$\mathrm{disc}(1, \sqrt{n}, \sqrt{m}, \sqrt{mn}) = 4^4 n^2 m^2$$

divise $16^4\mathrm{disc}(\mathcal{O}_K)$, il vient que $\mathrm{disc}(K) = m^2n^2$ car m et n sont impairs, et donc que $1, \alpha, \beta, \alpha\beta$ est une $\mathbb{Z}$-base de $\mathcal{O}_K$ par le (i).

Exercice 5.9 On considère le morphisme d'anneaux $\varphi : (\mathbb{Z}/2\mathbb{Z})[X, Y] \to \mathcal{O}_K/2\mathcal{O}_K$ envoyant X sur la classe de α et Y sur celle de β. Il est surjectif par l'exercice précédent. De plus $X^2 - X \in \mathrm{Ker}(\varphi)$. En effet, $\alpha^2 - \alpha = \frac{n-1}{4} \in 2\mathbb{Z}$ car $n \equiv 1 \bmod 8$. De même, $Y^2 - Y \in \mathrm{Ker}(\varphi)$, de sorte que φ induit par passage au quotient un morphisme surjectif d'anneaux $\varphi^* : A \to \mathcal{O}_K/2\mathcal{O}_K$. Mais $|\mathcal{O}_K/2\mathcal{O}_K| = 2^4$. De plus, on voit que A est engendré comme $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel par les classes de 1, X, Y et XY, il a donc au plus 2^4 éléments. Pour des raisons de cardinal il s'ensuit que φ^* est bijective.

Pour le (ii), observer que se donner un morphisme d'anneaux $\psi : A \to \mathbb{Z}/2\mathbb{Z}$ est équivalent par la propriété universelle d'un quotient à se donner deux éléments $x = \psi(X), y \in \psi(Y) \in \mathbb{Z}/2\mathbb{Z}$ tels que $x^2 = x$ et $y^2 = y$. Cette dernière condition est automatiquement satisfaite dans $\mathbb{Z}/2\mathbb{Z}$. Il y a donc exactement deux choix pour x et deux pour y. La seconde assertion du (iii) est la propriété universelle du quotient. La première s'en déduit car tout polynôme a évidemment au plus deux racines dans $\mathbb{Z}/2\mathbb{Z}$.

Enfin, si $\mathcal{O}_K$ est monogène, alors il existe un polynôme $P \in \mathbb{Z}[X]$ unitaire de degré 4 tel que $\mathcal{O}_K \simeq \mathbb{Z}[X]/(P)$, et donc $\mathcal{O}_K/2\mathcal{O}_K \simeq (\mathbb{Z}/2\mathbb{Z})[X]/(P \bmod 2)$, ce qui est absurde par (i) et (ii).

Exercice 5.10 Si $x \in \mathcal{O}_K$, il existe $y \in \mathcal{O}_K$ tel que $xy = 1$. La multiplicativité de $\mathrm{N} = \mathrm{N}_{K/\mathbb{Q}}$ entraîne $\mathrm{N}(xy) = 1 = \mathrm{N}(x)\mathrm{N}(y)$, puis $\mathrm{N}(x) = \pm 1$ car $\mathrm{N}(\mathcal{O}_K) \subset \mathbb{Z}$. Réciproquement, si $\mathrm{N}(x) = \pm 1$ et $x \in \mathcal{O}_K$, alors $\chi_{x,K/\mathbb{Q}}(X) \in \mathbb{Z}[X]$ et son coefficient constant vaut ± 1. Ainsi, $x^n + \sum_{i=1}^{n-1} a_i x^i \pm 1 = 0$ avec des $a_i \in \mathbb{Z}$. On conclut par l'identité $1 = \pm x(x^{n-1} + \sum_{i=1}^{n-1} a_i x^{i-1})$.

Exercice 5.11 Pour le (ii), observer que si $x \in U(K)$, et si $\chi_{x,K/\mathbb{Q}} = X^n + \sum_{i=0} a_i X^i$ alors $a_i \in \mathbb{Z}$ et $|a_i| \leq \binom{n}{i}$. Il n'y a donc qu'un nombre fini de polynômes caractéristiques possibles. Ces polynômes ont au total un nombre fini de racines, donc $U(K)$ est fini. Soient $n = |U(K)|$ et $\mu_n = \{\zeta \in \mathbb{C}, \zeta^n = 1\}$. Si $x \in U(K)$ alors $x^n = 1$ (Lagrange) donc $U(K) \subset \mu(K) \subset \mu_n$. Mais $|U(K)| = |\mu_n| = n$ donc $U(K) = \mu(K) = \mu_n$. Le (iv) se déduit du (iii) en considérant $K = \mathbb{Q}(x)$. Pour le (iv), on écrit $U(K) = \mu_n$, donc $\zeta = e^{2i\pi/n} \in K$, puis $\mathbb{Q}(\zeta) \subset K$. La base téléscopique entraîne que $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ divise $[K : \mathbb{Q}]$, mais $\varphi(n) = [\mathbb{Q}(\zeta) : \mathbb{Q}]$ (irréductibilité du polynôme cyclotomique).

Exercice 5.12 Soit $K = \mathbb{Q}(\alpha)$, c'est le corps de fractions de $\mathbb{Z}[\alpha]$. On sait que $\mathcal{O}_K$ est intégralement clos. Si $\mathbb{Z}[\alpha]$ l'est aussi, alors par définition il contient $\mathcal{O}_K$. Il est donc égal à $\mathcal{O}_K$ car $\alpha \in \mathcal{O}_K$ par hypothèse.

Exercice 5.13 Si $P = QR = \prod_i (X - x_i)$ alors $x_i \in \overline{\mathbb{Z}}$ car $P \in \mathbb{Z}[X]$ est unitaire. Les racines de Q et R dans $\mathbb{C}$ sont parmi les x_i, donc $P, Q \in \overline{\mathbb{Z}}[X]$ car ils sont unitaires à un signe près. On conclut car $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$. Le (i) s'ensuit et le (ii) en est une conséquence immédiate.

Exercice 5.15 Écrivons $K = \mathbb{Q}(x)$ avec $x \in \overline{\mathbb{Z}}$. Si $P = \Pi_{x,\mathbb{Q}}$ alors $\mathrm{disc}(K)$ est le carré d'un entier non nul fois $\mathrm{disc}(P)$. Par définition, $\mathrm{disc}(P)$ est un produit de termes de la forme $(a-b)^2 = (b-a)^2$ où $\{a, b\}$ parcourt les parties à deux éléments de l'ensemble R des racines de P dans $\mathbb{C}$. La conjugaison complexe induit une involution de R, et donc de l'ensemble de ses parties, disons $I \mapsto \overline{I} = \{\overline{x}, x \in I\}$. Obervons que si $a \neq b$, alors $(a-b)^2(\overline{a} - \overline{b})^2 = |a-b|^4$ est réel strictement positif. De plus, $I = \overline{I}$ et $|I| = 2$ si et seulement si $I = \{a, \overline{a}\}$ avec $a \in R$ non réel, auquel cas $(a - \overline{a})^2 = -4\mathrm{Im}(a)^2$. On conclut car le nombre d'éléments non réels de R est $2s$ par définition.

Exercice 5.16 Pour le (i), observer que l'élément $S = \prod_{1 \leq i < j \leq n}(x_i + x_j)$ est un polynôme symétrique à coefficients entiers en les x_i. C'est donc un polynôme à coefficients entiers en les coefficients de P (qui est unitaire), donc $S \in \mathbb{Z}$. Pour le (ii), on remarque que si $a, b \in \overline{\mathbb{Z}}$ alors $(a-b)^2 = (a+b-2b)^2 \equiv (a+b)^2 \bmod 4$. On en déduit $\mathrm{disc}(P) \equiv S^2 \bmod 4$ et on conclut car $S \in \mathbb{Z}$ par le (i). Le (iii) s'en déduit car $\mathrm{disc}(K)$ est le carré d'un entier non nul fois $\mathrm{disc}(\Pi_{x,\mathbb{Q}})$ où $x \in \overline{\mathbb{Z}}$ est un élément primitif de K.