CHAPITRE 7

Factorisation unique des idéaux

Nous avons constaté que bien peu d'anneaux de nombres algébriques sont factoriels. Leur défaut de factorialité se mesure notamment par la taille de l'ensemble $\mathrm{Cl}(A)$ des classes d'idéaux non nuls de l'anneau A, dont on a vu qu'il est toujours fini quand A est un ordre d'un corps de nombres. Nous poursuivons cette étude en montrant que si K est un corps de nombres, et si $A = \mathcal{O}_K$, la multiplication des idéaux sur $\mathrm{Cl}(A)$ définit une loi de groupe, ce qui en fait une structure très riche. Cela nous permettra notamment de démontrer le résultat central de la théorie : tout idéal non nul de $\mathcal{O}_K$ se factorise de manière unique comme produit d'idéaux premiers (Dedekind, Kummer).

Nous verrons que cette propriété rend parfois des services analogues à la propriété de factorialité. Son avantage est bien sûr qu'elle vaut pour tout corps de nombres K. C'est par exemple l'un des ingrédients essentiels dans la résolution par Kummer du problème de Fermat $x^n+y^n = z^n$ pour les exposants n qui sont des nombres premiers réguliers. Nous en donnerons des applications à l'étude des solutions entières de l'équation $y^2 = x^3 + k$, ainsi qu'à la détermination de $\mathrm{Cl}(\mathcal{O}_K)$.

Références : Les chapitres III et V du livre de Samuel. Le chapitre 12 du livre de Ireland et Rosen.

1. Le groupe des classes d'ideaux d'un corps de nombres

1.1. Groupe de Picard d'un anneau. Soit A un anneau commutatif unitaire intègre. Nous avons défini au chapitre précédent §1 l'ensemble $\mathrm{Cl}(A)$ des classes d'équivalence d'idéaux non nuls de A. Il est muni d'une loi de composition interne associative et commutative issue de la multiplication des idéaux, et la classe des idéaux principaux en est un élément neutre.

Définition 7.1. *Soit I un idéal non nul A. On dit que I est* inversible *si $[I]$ admet un inverse dans $\mathrm{Cl}(A)$, ou ce qui revient au même, s'il existe un idéal non nul J de A tel que IJ et principal.*

Par exemple, tout idéal principal non nul est inversible. On désigne par

$$\mathrm{Pic}(A) \subset \mathrm{Cl}(A)$$

le sous-ensemble des classes inversibles. Par construction, la multiplication des idéaux définit une structure de groupe abélien sur $\mathrm{Pic}(A)$, appelé *groupe de Picard de A*.

Si I et J sont des idéaux de A on dit que I divise J, et on écrit $I \mid J$, s'il existe un idéal $J' \subset A$ tel que $J = IJ'$. Si $I \mid J$ alors $J \subset I$, mais la réciproque ne vaut pas en général.

Lemme 7.2. *Soient I, J, J' des idéaux de A avec I inversible.*

(i) (Simplification) Si $IJ = IJ'$ alors $J = J'$.

(ii) (Contenir c'est diviser) $J \subset I$ si, et seulement si, I divise J, auquel cas il existe un unique idéal J' tel que $J = IJ'$.

Démonstration — Soit I' est un idéal non nul tel que $II' = (\alpha)$ (et donc $\alpha \neq 0$). Si $IJ = IJ'$ alors en multipliant par I' on a $\alpha J = \alpha J'$ puis $J = J'$ en divisant par α. Cela montre le (i).

Pour le (ii), il est clair que si $J = IJ'$ pour un idéal $J'' \subset A$ alors $J \subset I$. Réciproquement soit $J \subset I$. On constate que

$$J = I(\alpha^{-1} I' J).$$

et que $\alpha^{-1} I' J$ est inclus dans A car $J \subset I$ et donc $JI' \subset II' = (\alpha)$. Ainsi, $J'' = \alpha^{-1} I' J$ est un idéal de A tel que $J = IJ'$. L'assertion d'unicité découle du (i). □

1.2. Cas des anneaux de nombres. Nous avons vu en exercices que

$$\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}]) = \mathrm{Pic}(\mathbb{Z}[\sqrt{-5}]) = \mathbb{Z}/2\mathbb{Z},$$

l'idéal $(2, \sqrt{-5}+1)$ étant un générateur de carré (2). Cela fournit un premier exemple d'idéal inversible non principal. Nous avons vu aussi que $|\mathrm{Cl}(\mathbb{Z}[\sqrt{-3}])| = 2$, la classe non principale étant celle de l'idéal $I = (2, \sqrt{-3}+1)$, qui satisfait $I^2 = 2I$. L'idéal I est donc non inversible, car sinon on aurait $I = (2)$ ce qui est absurde car I n'est pas principal. Ainsi, $\mathrm{Pic}(\mathbb{Z}[\sqrt{-3}])$ est le groupe trivial.

Théorème 7.3. *Si K est un corps de nombres alors tout idéal non nul de $\mathcal{O}_K$ est inversible, autrement dit* $\mathrm{Cl}(\mathcal{O}_K) = \mathrm{Pic}(\mathcal{O}_K)$.

Nous démontré au chapitre précédent que $\mathrm{Cl}(\mathcal{O}_K)$ est fini, il résulte donc de ce théorème que c'est un groupe abélien fini. On note

$$\mathrm{h}_K = |\mathrm{Cl}(\mathcal{O}_K)|$$

son cardinal et on l'appelle le *nombre de classes de K*. L'exemple de $\mathbb{Z}[\sqrt{-3}]$ montre que le théorème ci-dessus est spécifique à $\mathcal{O}_K$ et ne vaut pas pour les ordres généraux de K. On pourrait en fait démontrer que si A est un ordre de K dont tous les idéaux non nuls sont inversibles, alors $A = \mathcal{O}_K$!

Le lemme suivant est une forme faible provisoire du théorème ci-dessus, et sera un point clef de sa démonstration.

Lemme 7.4. *Si J, J' sont des idéaux non nuls de $\mathcal{O}_K$ tels que $JJ' = (\alpha)J'$ avec $\alpha \in \mathcal{O}_K$, alors $J = (\alpha)$.*

Démonstration — Supposons pour commencer que $\alpha = 1$, i.e. $JJ' = J'$. Choisissons $f_1, \ldots, f_n$ une $\mathbb{Z}$-base de J', ce qui est loisible d'après le théorème 6.15. En écrivant $f_j \in JJ'$ on obtient des $m_{i,j} \in J$ avec $1 \leq i, j \leq n$ tels que $\forall j = 1, \ldots, n$, $f_j =$

$\sum_{i=1}^{n} m_{i,j} f_i$. C'est un système linéaire de taille n à coefficients complexes qui s'écrit aussi

$$(\mathrm{I}_n - (m_{i,j})) \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Comme les f_j sont non nuls on obtient que $\det(\mathrm{I}_n - (m_{i,j})) = 0$. Autrement dit $Q(1) = 0$ où Q est le polynôme caractéristique de $(m_{i,j})$. Mais J étant un idéal, on observe par un développement brutal que tous les coefficients non dominants de Q sont dans J, et donc $Q(1) \in 1 + J$. Comme $Q(1) = 0$, on a $1 \in J$, puis $J = A$, ce que l'on voulait démontrer (cet argument s'appelle le "lemme de Nakayama").

Retournons maintenant au cas d'un $\alpha \in \mathcal{O}_K$ général (observons que jusque là nous n'avons pas utilisé de spécificité de $\mathcal{O}_K$, l'argument ci-dessus étant valable dans tout ordre). Pour tout $y \in J$ on a $\frac{y}{\alpha} J' \subset J'$, donc $\frac{y}{\alpha} \in \overline{\mathbb{Z}} \cap K = \mathcal{O}_K$ d'après le critère d'intégralité du chapitre 1 (Proposition 1.16) et le fait que les idéaux de $\mathcal{O}_K$ admettent une $\mathbb{Z}$-base finie (Théorème 6.15). Ainsi, $J'' = \alpha^{-1} J$ est un idéal de $\mathcal{O}_K$, et la relation de l'énoncé s'écrit alors $J''J' = J'$. Le cas $\alpha = 1$ s'applique et donne $J'' = \mathcal{O}_K$, et donc $J = (\alpha)$. □

Démonstration — (du théorème) Soit I un idéal non nul de A. Pour voir qu'il est inversible, il suffit de démontrer qu'il existe un entier $n \geq 1$ tel que I^n est principal, car alors $[I][I^{n-1}] = [A]$. Mais les $\mathrm{h}_K + 1$ idéaux I^i avec $i = 0, \ldots, \mathrm{h}_K$ ne peuvent appartenir à des classes différentes, on peut donc trouver $0 \leq i < j \leq \mathrm{h}_K$ tels que

$$I^i \sim I^j.$$

Soient $x, y \in \mathcal{O}_K$ non nuls tels que $xI^i = yI^j$. On écrit ceci sous la forme $(yI^{j-i})I^i = (x)I^i$ et le lemme précédent conclut donc que $(y)I^{j-i} = (x)$, et donc que I^{j-i} est principal : l'entier $n = j - i$ convient. □

Le théorème 7.3 admet plusieurs corollaires fondamentaux dans l'étude de l'arithmétique de $\mathcal{O}_K$. D'une part, on déduit du lemme 7.2 que :

Corollaire 7.5. *Soient I, J, J' des idéaux non nuls de $\mathcal{O}_K$.*

(i) (Simplification) *Si $IJ = IJ'$ alors $J = J'$.*

(ii) (Contenir c'est diviser) *$I \subset J$ si et seulement J si divise I.*

D'autre part, le théorème de Lagrange appliqué au groupe abélien fini $\mathrm{Cl}(\mathcal{O}_K)$ entraîne que

Corollaire 7.6. *Pour tout idéal non nul I de $\mathcal{O}_K$, l'idéal I^{h_K} est principal où $\mathrm{h}_K = |\mathrm{Cl}(\mathcal{O}_K)|$.*

La détermination de h_K et de la structure de $\mathrm{Cl}(\mathcal{O}_K)$, K étant un corps de nombres donné, est très loin d'être résolue en général, malgrès ses multiples applications. Par exemple, $\mathrm{h}_K = 1$ si, et seulement si, $\mathcal{O}_K$ est factoriel, mais on ne sait toujours pas si une infinité de corps de nombres K ont cette propriété !

2. Idéaux premiers des ordres des corps de nombres

Notre objectif est désormais de démontrer que tout idéal de $\mathcal{O}_K$ admet une décomposition unique comme produit d'idéaux premiers. Cela nous oblige d'une part à quelques rappels et sorites généraux sur les idéaux premiers et maximaux, et d'autre part si possible de les déterminer dans le cas de $\mathcal{O}_K$. À ce stade il sera aussi instructif de travailler avec un ordre général. Fixons pour commencer un anneau commutatif unitaire A quelconque.

Définition 7.7. *Un idéal $P \subset A$ est dit premier si $P \neq A$ et si pour tout $a, b \in P$, la relation $ab \in P$ entraîne $a \in P$ ou $b \in P$. De manière équivalente, un idéal $P \subset A$ est premier si et seulement si l'anneau quotient A/P est intègre.*

Donnons quelques exemples :

(a) L'idéal nul $\{0\}$ est premier si, et seulement si, l'anneau A est intègre.

(b) Si A est intègre et si $\pi \in A$ est non nul, il suit immédiatement des définitions que πA est premier si, et seulement si, l'élément π est premier au sens du Chapitre 4 §1, de sorte que la notion d'idéal premier est la généralisation naturelle de celle d'élément premier dans un anneau.

(c) (suite) En particulier, dans un anneau principal (et donc factoriel) les idéaux premiers non nuls sont exactement ceux engendrés par un élément irréductible. Par exemple, les idéaux premiers non nuls de $\mathbb{Z}$ sont les $p\mathbb{Z}$ avec p premier, et ceux de $k[X]$ avec k un corps sont les (P) avec $P \in k[X]$ irréductible.

(d) Soient $\alpha \in \overline{\mathbb{Z}}$, $A = \mathbb{Z}[\alpha]$ et p un nombre premier. Soit $Q \in (\mathbb{Z}/p\mathbb{Z})[X]$ un diviseur de $\overline{\Pi}_{\alpha,\mathbb{Q}} \in (\mathbb{Z}/p\mathbb{Z})[X]$ et soit $\mathrm{I}(Q)$ l'idéal défini dans la proposition 6.10. Le (iii) de cette proposition affirme que $A/\mathrm{I}(Q) \simeq (\mathbb{Z}/p\mathbb{Z})[X]/(Q)$, ainsi $\mathrm{I}(Q)$ est premier si, et seulement si, Q est irréductible, d'après l'exemple (c).

Remarque 7.8. L'exemple (d) montre que les idéaux premiers de $\mathbb{Z}[\alpha]$ contenant un nombre premier p donné sont en bijection naturelle avec les facteurs irréductibles de $\overline{\Pi}_{\alpha,\mathbb{Q}}$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$. On est donc ramené pour les déterminer à factoriser un polynôme $P \in \mathbb{Z}[X]$ donné dans $(\mathbb{Z}/p\mathbb{Z})[X]$, ce qui est un problème fini. Il existe un algorithme fameux pour cela dû à Berlekamp, qui permet par exemple de factoriser avec un ordinateur en moins d'une seconde un polynôme de degré 100 modulo un nombre premier à 40 chiffres. En revanche, un polynôme $P \in \mathbb{Z}[X]$ étant donné c'est en général un problème très difficile de répondre aux questions du type : "Quels sont les nombres premiers p tels que $P \bmod p$ admet une racine dans $\mathbb{Z}/p\mathbb{Z}$?". Par exemple, si $P = X^2 - a$ c'est essentiellement la loi de réciprocité quadratique ! Ce problème général, de formulation élémentaire, est l'un des problèmes centraux actuellement dans toute la théorie algébrique des nombres, et c'est d'ailleurs l'un des chemins qui mène au fameux "programme de Langlands".

Donnons deux propriétés importantes générales des idéaux premiers.

Proposition 7.9. *Soit A un anneau et soit P un idéal premier de A.*

(i) Si I et J sont des idéaux de A tels que $P \supset IJ$, alors $P \supset I$ ou $P \supset J$.

(ii) Si B est un sous-anneau de A, alors $B \cap P$ est un idéal premier de B.

Démonstration — Si $I \not\subset P$, il existe $x \in I \backslash P$. Si $y \in J$, alors $xy \in P$, et donc $y \in P$: on a $J \subset P$, ce qui prouve le (i). Le (ii) est ... évident ! □

Une source générale d'idéaux premiers est la notion d'idéaux maximaux pour l'inclusion.

Définition 7.10. *Un idéal $I \subset A$ d'un anneau est dit maximal si $I \neq A$ et si les seuls idéaux $J \subset A$ contenant I sont A et I. Il est équivalent de demander que l'anneau A/I est un corps.*

Justifions la dernière assertion. Rappelons que $J \mapsto J/I$ induit une bijection entre idéaux de A contenant I et idéaux de l'anneau quotient A/I. Cette bijection préserve manifestement les inclusions : si $J, J' \supset I$ alors $J \subset J'$ si, et seulement si, $J/I \subset J'/I$. De plus, elle fait correspondre l'idéal trivial A avec l'idéal trivial A/I. Ainsi, $I \neq A$ est maximal pour l'inclusion si, et seulement si, l'anneau quotient A/I a pour seuls idéaux 0 et A/I. Mais les seuls anneaux commutatifs unitaires k qui ont exactement deux idéaux, à savoir 0 et k, sont les corps. En effet, si k est un corps tout élément non nul est inversible, donc engendre l'idéal k. Réciproquement, si les seuls idéaux de k sont 0 et k, tout $x \in k$ non nul engendre l'idéal k et donc il existe $y \in k$ tel que $xy = 1$: k est un corps.

Un corps étant intègre, c'est un fait général que *tout idéal maximal est premier*. La réciproque est toutefois fausse en général : dans un anneau intègre A qui n'est pas un corps, $\{0\}$ est premier mais n'est pas maximal. C'est cependant la seule nuance dans le cas des ordres des corps de nombres.

Proposition 7.11. *Soit A un ordre d'un corps de nombres.*

(i) (Existence) *Tout idéal de A distinct de A est inclus dans un idéal maximal (donc premier).*

(ii) (Maximalité) *Tout idéal premier non nul de A est maximal.*

Démonstration — Vérifions le (i). Soit $I \neq A$ un idéal non nul de A. On a déjà vu que A/I est fini (Thm. 6.15). En particulier, il n'a qu'un nombre fini d'idéaux, et tout idéal strict de A/I dont le cardinal maximal est un idéal maximal de A/I. Son image inverse dans A définit donc un idéal maximal de A contenant I. (En fait l'énoncé du (i) est vrai pour tout anneau A, mais sa démonstration nécessite l'axiome du choix.)

Montrons le (ii). Soit P un idéal premier non nul de A. Alors A/P est un anneau intègre fini : c'est donc un corps ! En effet, soit B un anneau intègre fini, et soit $b \in B$ non nul. La multiplication par b est une injection $B \to B$ par intégrité : c'est donc une bijection pour des raisons de cardinal. On peut donc trouver $b' \in B$ tel que $bb' = 1$. □

Le résultat suivant est une classification grossière des idéaux premiers des ordres des corps de nombres. Il peut être vu comme une généralisation de la détermination rappelée plus haut des idéaux premiers de $\mathbb{Z}$, ou encore de celle de $\mathbb{Z}[i]$ vue en exercices.

Théorème 7.12. *Soit A un ordre d'un corps de nombres K.*

(i) Si P est un idéal premier non nul de A, alors P contient un unique nombre premier $p \in \mathbb{Z}$. On a $P \cap \mathbb{Z} = p\mathbb{Z}$ et A/P est un corps fini à p^n éléments avec $n \leq [K : \mathbb{Q}]$.

(ii) Réciproquement, pour tout nombre premier p l'ensemble des idéaux premiers de A contenant p est fini et non vide.

Démonstration — Soit p un nombre premier. Les idéaux de A contenant p (i.e. pA) sont en bijection avec les idéaux de l'anneau A/pA. Ce dernier a exactement $p^{[K:\mathbb{Q}]}$ éléments d'après le lemme 6.8. Il est donc non nul et fini. Il n'y a donc qu'un nombre fini d'idéaux de A contenant p. L'idéal pA étant strict car $A/pA \neq 0$, il est contenu dans un idéal premier d'après la prop. 7.11 (i), ce qui démontre le (ii). De plus, si P est un idéal premier de A contenant p, l'homomorphisme d'anneaux canonique $A/pA \to A/P$ est surjectif, entre deux anneaux finis, donc $|A/P|$ divise $|A/pA| = p^{[K:\mathbb{Q}]}$ (Lemme 6.8). Il ne reste qu'à démontrer que tout idéal premier non nul de A contient un, et un seul, nombre premier.

Observons d'abord que si I est un idéal non nul de A, alors $I \cap \mathbb{Z} \neq \{0\}$. En effet, si $x \in I$ est non nul, il existe un polynôme unitaire $P \in \mathbb{Z}[X]$ tel que $P(x) = 0$ et $P(0) \neq 0$ (sans quoi on peut remplacer P par P/X^d où d est l'ordre d'annulation de P en 0). L'équation $P(x) = 0$ s'écrit alors aussi $P(0) = \sum_{i=1}^{m} a_i x^i$ où les a_i sont dans $\mathbb{Z}$, et donc $P(0) \in I$.

Ainsi, si P est un idéal premier de A, alors $P \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$ d'après le lemme 7.9, non nul d'après l'observation précédente : il est donc de la forme $p\mathbb{Z}$ avec p premier. Cet idéal contient un seul nombre premier : le nombre p. □

3. L'anneau $\mathcal{O}_K$ est de Dedekind.

3.1. Anneaux de Dedekind. On dira qu'un idéal I d'un anneau A est *strict* si $I \neq A$ et $I \neq 0$.

Définition 7.13. *Un anneau de Dedekind est un anneau intègre noethérien tel que pour tout idéal strict $I \subset A$, il existe un unique entier $n \geq 1$ et des idéaux premiers $P_1, \ldots, P_n$ uniques à permutation près tels que $I = P_1 \cdots P_n$.*

Cette propriété de factorisation des idéaux est aussi appelée *propriété de Dedekind*. Les anneaux principaux sont de Dedekind, mais il y en a bien d'autres. Du point de vue des idéaux, un anneau de Dedekind A se comporte de manière très similaire aux anneaux factoriels, les idéaux premiers jouant le rôle des éléments premiers. La situation est même plus simple car il n'y a pas dans le langage des idéaux à s'inquiéter des unités de A.

Théorème 7.14. (Kummer, Dedekind) *Pour tout corps de nombres K, l'anneau $\mathcal{O}_K$ est de Dedekind.*

Démonstration — On a déjà vu que $\mathcal{O}_K$ est noethérien (Théorème 6.15).

Lemme 7.15. *Soient A un ordre d'un corps de nombres, et $I \subset J$ deux idéaux non nuls de A. Alors $\mathrm{N}(J)$ divise $\mathrm{N}(I)$, et $\mathrm{N}(J) = \mathrm{N}(I)$ si, et seulement si, $I = J$.*

Démonstration — En effet, la surjection canonique $A/I \to A/J$, qui est en particulier un morphisme de groupes additifs sous-jacents, a pour noyau J/I. On a donc $\mathrm{N}(I) = \mathrm{N}(J) \cdot |J/I|$, ce qui conclut. □

.

Vérifions tout d'abord l'existence. Supposons qu'il existe un idéal strict I de $\mathcal{O}_K$ qui n'est pas produit fini d'idéaux premiers. On peut alors considérer un tel idéal dont la norme est minimale. En particulier, I n'est pas maximal (car il serait premier). La proposition 7.11 montre qu'il existe un idéal maximal P de $\mathcal{O}_K$ contenant I. L'inversibilité de P montre qu'il existe un idéal Q de $\mathcal{O}_K$ tel que $I = QP$. On a évidemment $I \subset Q$, et même $I \neq Q$ par inversibilité de Q, le lemme ci-dessus assure donc $\mathrm{N}(Q) < \mathrm{N}(I)$. Mais Q n'est pas produit fini d'idéaux premiers car I le serait alors aussi, une contradiction.

Montrons l'unicité. Observons tout d'abord qu'un produit d'un nombre fini d'idéaux premiers est inclus dans chacun d'eux et en particulier toujours distinct de $\mathcal{O}_K$. Supposons donc $P_1 \cdots P_n = Q_1 \cdots Q_m$ où $m, n \geq 1$ sont des entiers et où les P_i et Q_j sont des idéaux premiers de $\mathcal{O}_K$. En particulier, $Q_1 \cdots Q_m \subset P_1$. Le lemme 7.9 entraîne donc qu'il existe $i \in \{1, \ldots, m\}$ tel que $P_1 \supset Q_i$. Mais Q_i est premier non nul donc maximal d'après la proposition 7.11 (ii), puis $P_1 = Q_i$. Mais on peut alors simplifier l'égalité par P_1. On en déduit par induction $m = n$ et qu'il existe $\sigma \in \mathfrak{S}_n$ tel que $Q_i = P_{\sigma(i)}$ pour tout $i = 1, \ldots, n$. □

Comme nous le verrons, ce théorème a de multiples conséquences. De manière similaire à la théorie des anneaux factoriels, il est parfois commode d'introduire la notion de valuation d'un idéal non nul I de $\mathcal{O}_K$ en un idéal premier P : c'est le nombre $v_P(I)$ de fois que l'idéal P intervient dans la décomposition de I. C'est donc 0 si, et seulement si, P ne divise pas I, ou ce qui revient au même, si $I \not\subset P$ (ce qui est le cas de tous les idéaux premiers exceptés un nombre fini par le théorème). On a toujours $I = \prod_P P^{v_P(I)}$ le produit étant fini en un sens évident. L'assertion d'unicité de la décomposition s'écrit alors $v_P(IJ) = v_P(I) + v_P(J)$ si I et J sont des idéaux non nuls. Enfin, I divise J si, et seulement si, $v_P(I) \leq v_P(J)$ pour tout idéal premier P non nul.

Exemple 7.16. (pgcd et ppcm d'idéaux) Ces observations on notamment des conséquences sur les notions de pgcd et ppcm au sens des idéaux. En effet, soit I et J deux idéaux de $\mathcal{O}_K$, on constate que l'idéal $I + J$ est le plus petit idéal contenant (=divisant) I et J, il mérite alors bien son nom de pgcd de I et J. La propriété de Dedekind entraîne

$$I + J = \prod_P P^{\mathrm{Min}(v_P(I), v_P(J))}.$$

De même, $I \cap J$ apparaît comme le ppcm de I et J, et pour lequel on a une formule analogue avec des Max.

3.2. Application à la décomposition ... des nombres premiers ! Au point où nous en sommes, il nous reste à expliquer comment décomposer explicitement un idéal donné en produit d'idéaux premiers. Un cas particulièrement intriguant est de comprendre la décomposition de $p\mathcal{O}_K$ quand $p \in \mathbb{Z}$ est un nombre premier usuel. Nous avons vu dans les exercices que pour décomposer un élément en produit d'irréductibles dans un anneau de nombres, une bonne méthode consiste à déterminer la norme de l'élément, puis de chercher les diviseurs de cette norme qui sont des normes d'éléments de l'anneau. Une stratégie similaire fonctionne pour les idéaux. L'outil clé suivant éclaircit considérablement le problème, car on a vu que tout idéal premier non nul est de norme une puissance d'un nombre premier.

Théorème 7.17. *(i)* (Multiplicativité de la norme) *Si I et J sont des idéaux non nuls de $\mathcal{O}_K$ alors* $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$.

(ii) Si $P \neq 0$ est un idéal premier de $\mathcal{O}_K$ alors $\mathrm{N}(P)$ *est une puissance de l'unique nombre premier $p \in P$.*

(iii) Si $I \neq 0$ est un idéal, alors I divise l'idéal $(\mathrm{N}(I))$.

Démonstration — Le (ii) est le point (iii) du théorème 7.12. Pour le (iii), on observe que le groupe abélien fini A/I est annulé par son cardinal $\mathrm{N}(I)$ (Lagrange), donc $\mathrm{N}(I).1 \in I$, puis I divise $\mathrm{N}(I)$ car I est inversible.

Il reste à vérifier le (i). D'après le théorème précédent, il suffit de démontrer que si les P_i sont des idéaux premiers non nuls (en nombre fini), alors on a $\mathrm{N}(\prod_i P_i) = \prod_i \mathrm{N}(P_i)$. Soient I et P des idéaux non nul de $\mathcal{O}_K$ avec P premier. Nous allons montrer $\mathrm{N}(IP) = \mathrm{N}(I)\mathrm{N}(P)$, ce qui conclura la démonstration.

L'inclusion $IP \subset I$ entraîne $\mathrm{N}(IP) = \mathrm{N}(I)|I/IP|$ d'après le Lemme 7.15, on veut donc montrer $\mathrm{N}(P) = |I/IP|$. Observons que les seuls idéaux Q de $\mathcal{O}_K$ tels que $I \,|\, Q \,|\, IP$, i.e. $IP \subset Q \subset I$, sont I et IP puisque P est premier. Ainsi, si l'on fixe $x \in I \backslash IP$ on a $IP + (x) = I$. On considère l'application

$$\mathcal{O}_K \to I/PI,\ a \mapsto ax + PI.$$

Cette application est additive, surjective, et son noyau est $S = \{a \in \mathcal{O}_K, ax \in PI\}$, qui est même un idéal de $\mathcal{O}_K$. Il contient P, c'est donc P ou $\mathcal{O}_K$ par maximalité de P. Mais $1 \notin S$ car $x \notin PI$, et donc $S = P$. Le morphisme de groupes ci-dessus se factorise donc en un isomorphisme de groupes additifs $\mathcal{O}_K/P \xrightarrow{\sim} I/PI$, d'où $\mathrm{N}(P) = |I/PI|$. □

Théorème 7.18. *Soit $\alpha \in \overline{\mathbb{Z}}$. On suppose que l'anneau des entiers de $\mathbb{Q}(\alpha)$ est l'anneau $A = \mathbb{Z}[\alpha]$. Soient p un nombre premier et $P = \overline{\Pi_{\alpha,\mathbb{Q}}} \in (\mathbb{Z}/p\mathbb{Z})[X]$ la réduction modulo p de $\Pi_{\alpha,\mathbb{Q}}$. Écrivons $P = \prod_i P_i^{e_i}$ où les $P_i \in (\mathbb{Z}/p\mathbb{Z})[X]$ sont irréductibles unitaires deux à deux distincts. Alors les idéaux premiers de A contenant p sont les* $\mathrm{I}(P_i)$ (Prop. 6.10) *et $pA = \prod_i \mathrm{I}(P_i)^{e_i}$.*

Démonstration — Rappelons que d'après la proposition 6.10, on dispose d'une bijection $Q \mapsto \mathrm{I}(Q)$ entre l'ensemble des diviseurs unitaires de P et celui des idéaux contenant, i.e. divisant, l'idéal pA. On a déjà observé que $\mathrm{I}(Q)$ est premier si, et

seulement si, Q est irréductible (exemple (d) §2). Ainsi, il existe des entiers $n_i \geq 1$ tels que

$$pA = \prod_i \mathrm{I}(P_i)^{n_i}$$

et il ne reste qu'à voir que $n_i = e_i$ pour tout i. Considérons l'ensemble X_i des idéaux I divisant pA tels que $I \subsetneq \mathrm{I}(P_j)$ pour $j \neq i$ (i.e. $\mathrm{I}(P_j)$ ne divise pas I si $i \neq j$). La propriété de Dedekind assure que X_i est la famille strictement croissante d'idéaux

$$\mathrm{I}(P_i)^{n_i} \subsetneq \mathrm{I}(P_i)^{n_i-1} \subsetneq \cdots \subsetneq \mathrm{I}(P_i).$$

Mais par construction, la bijection $Q \mapsto \mathrm{I}(Q)$ satisfait $\mathrm{I}(Q) \subset \mathrm{I}(Q')$ si, et seulement si, $Q'|Q$. On en déduit que X_i est également la famille croissante

$$\mathrm{I}(P_i^{e_i}) \subsetneq \mathrm{I}(P_i^{e_i-1}) \subsetneq \cdots \subsetneq \mathrm{I}(P_i),$$

et donc que $n_i = e_i$ et que pour tout $m \leq e_i$ on a $\mathrm{I}(P_i^m) = \mathrm{I}(P_i)^m$. □

Mentionnons que lorsque tous les e_i sont égaux à 1, la conclusion du théorème vaut encore même si A n'est pas supposé égal à l'anneau des entiers de $\mathbb{Q}(\alpha)$: voir le Problème 7.1 (i) et (ii) pour un démonstration très élémentaire de ce résultat.

Le polynôme $X^2 + aX + b \in \mathbb{Z}[X]$, de discriminant $D = a^2 - 4b$, est irréductible modulo p si, et seulement si, D est un carré modulo $4p$, et admet une racine double modulo p si, et seulement si, p divise D (Exercice 1.3). D'après la proposition 5.23, le théorème précédent s'applique donc aux corps quadratiques $\mathbb{Q}(\sqrt{d})$ où $d \in \mathbb{Z}\backslash\{0, 1\}$ est sans facteur carré, et s'écrit :

Corollaire 7.19. *Soit $K = \mathbb{Q}(\sqrt{d})$, $p \in \mathbb{Z}$ un nombre premier, et $D = \mathrm{disc}(\mathcal{O}_K)$, alors :*

(i) (Cas "ramifié") Si $p|D$, il existe un unique idéal premier $P \subset \mathcal{O}_K$ contenant p, et $(p) = P^2$.

(ii) (Cas "inerte") Si D n'est pas un carré modulo $4p$, l'idéal (p) est premier.

(iii) (Cas "décomposé") Si $(p, D) = 1$ et D est un carré modulo $4p$, alors $(p) = PP'$ où P et P' sont deux idéaux premiers distincts.

Ce dernier corollaire peut également se vérifier par calcul direct à partir de la proposition 6.10.

4. De l'utilité de la décomposition des idéaux

Il se trouve que cette décomposition des idéaux en produit d'idéaux premiers rend en pratique des services comparables à la propriété sensiblement plus forte de factorialité. Une illustration fameuse de ceci est le théorème suivant dû à Kummer :

Théorème 7.20. *(Kummer, 1850) Si le nombre premier impair p ne divise pas le nombre de classes de $\mathbb{Q}(e^{\frac{2i\pi}{p}})$ alors l'équation de Fermat $x^p + y^p = z^p$ n'admet pas de solution $x, y, z \in \mathbb{Z}$ avec $xyz \neq 0$.*

Nous ne démontrerons pas ce résultat qui est difficile. Une variante faible, dite aussi "premier cas de l'équation de Fermat", qui exclut seulement les solutions telles que $xyz \neq 0 \bmod p$ est cependant tout à fait accessible à ce stade du cours (voir le chapitre 17 du livre de Ireland et Rosen).

Définition 7.21. *Un nombre premier p tel que p divise $\mathrm{h}_{\mathbb{Q}(e^{\frac{2i\pi}{p}})}$ est appelé irrégulier.*

Une seconde découverte majeure de Kummer est d'avoir démontré le critère surprenant suivant d'irrégularité : le nombre premier $p > 3$ est irrégulier si et seulement s'il divise le numérateur de l'un au moins des nombres de Bernoulli $\mathrm{B}_2, \mathrm{B}_4, \ldots, \mathrm{B}_{p-3}$. On rappelle que ces nombres B_k peuvent être définis par la série génératrice

$$\frac{t}{e^t - 1} = \sum_{k \geq 0} \mathrm{B}_k \frac{t^k}{k!}.$$

Les B_k s'annulent si k est impair > 1, et sont intimement liés à la fonction ζ de Riemann par la formule d'Euler $\zeta(k) = (-1)^{k/2+1} \frac{\mathrm{B}_k (2\pi)^k}{2\, k!}$ pour tout entier $k \geq 2$ pair.

Je renvoie à la table qui suit pour les premières valeurs. Le premier nombre premier irrégulier qui apparaît est donc 691, qui divise B_{12}. Ce n'est pas le plus petit... qui est d'après cette table le nombre 37, divisant B_{32}. Il est aisé de vérifier que les nombres premiers irréguliers plus petits que 200 sont exactement $37, 59, 67, 101, 103, 131, 149$ et 157. On voit alors que le théorème de Kummer entraîne celui de Fermat pour de nombreux exposants p ! On peut montrer en revanche que $\mathrm{h}_{\mathbb{Q}(e^{\frac{2i\pi}{p}})} = 1$ si, et seulement si, $p < 23$ (voir les exercices pour les cas $p \leq 7$ et $p = 23$) : on voit bien l'intêret des résultats de Kummer. Les nombres premiers irréguliers sont encore l'objet de nombreuses recherches. On sait par exemple qu'il y en a une infinité mais on ne sait pas s'il y a un nombre infini de nombre premiers qui ne sont pas irréguliers. On ne sait pas non plus s'il existe des nombres premiers p tels que p^2 divise le numérateur de B_k pour $2 \leq k \leq p-3$.

k	B_k	k	B_k	k	B_k	k	B_k
2	$\frac{1}{6}$	10	$\frac{5}{66}$	18	$\frac{43867}{798}$	26	$\frac{13 \cdot 657931}{6}$
4	$-\frac{1}{30}$	12	$-\frac{691}{2730}$	20	$-\frac{283 \cdot 617}{330}$	28	$-\frac{7 \cdot 9349 \cdot 362903}{870}$
6	$\frac{1}{42}$	14	$\frac{7}{6}$	22	$\frac{11 \cdot 131 \cdot 593}{138}$	30	$\frac{5 \cdot 1721 \cdot 1001259881}{14322}$
8	$-\frac{1}{30}$	16	$-\frac{3617}{510}$	24	$-\frac{103 \cdot 2294797}{2730}$	32	$-\frac{37 \cdot 683 \cdot 305065927}{510}$

TABLE 1. Les nombres B_k pour $k \leq 32$, avec leurs numérateurs factorisés.

Plutôt que d'étudier l'équation de Fermat et le théorème de Kummer, ce qui nous conduirait à l'étude des corps cyclotomiques que nous n'avons guère approchée, nous allons nous pencher sur l'équation diophantienne $y^2 = x^3 + k$ chère à Fermat et Mordell, ayant des liens avec l'arithmétique des corps quadratiques. Mordell a démontré que cette équation n'a qu'un nombre fini de solutions $x, y \in \mathbb{Z}$ si $k \in \mathbb{Z}$ est non nul. Nous l'avons déjà vérifié dans le cas $k = -2$.

Théorème 7.22. *On suppose $k < 0$ sans facteur carré, $k \equiv 2, 3 \bmod 4$, et que $\mathrm{h}_{\mathbb{Q}(\sqrt{k})}$ n'est pas multiple de 3. Alors l'équation $y^2 = x^3 + k$ a au plus deux solutions.*

Nous allons voir qu'en fait il n'y a pas de solution si $-k$ n'est pas de la forme $3m^2 \pm 1$, et que s'il est de cette forme les solutions sont $(x, y) = (m^2 - k, \pm(m^3 +$

$3km$)). Par exemple, si $k = -13 = -(3 \cdot 2^2 + 1)$, cela s'applique car $\mathrm{h}_{\mathbb{Q}(\sqrt{-13})} = 2$ (voir l'exercice 7.4) et les solutions entières sont $(17, \pm 70)$ (solution qui ne sautait d'ailleurs pas aux yeux a priori).

La similarité avec l'énoncé du théorème de Kummer est grosso-modo que "si un certain nombre de classes a une certaine propriété alors une certaine équation diophantienne n'a pas de solution entière". À l'aide des résultats du chapitre suivant, il serait facile de vérifier au cas par cas que les premiers $k < 0$ sans facteur carré tels que $3 \mid \mathrm{h}_{\mathbb{Q}(\sqrt{k})}$ sont ceux de la table suivantes.

$-k$	23	26	29	31	38	53	59	61	83	87	89	106	107	109	110
$\mathrm{h}_{\mathbb{Q}(\sqrt{k})}$	3	6	6	3	6	6	3	6	3	6	12	6	3	6	12

TABLE 2. Les $-111 < k < 0$ sans facteur carré tels que 3 divise $\mathrm{h}_{\mathbb{Q}(\sqrt{k})}$.

DÉMONSTRATION — Soit $A = \mathbb{Z}[\sqrt{k}]$, c'est l'anneau des entiers de $\mathbb{Q}(\sqrt{k})$ car $k \not\equiv 1 \bmod 4$. L'équation se factorise dans A sous la forme $(y + \sqrt{k})(y - \sqrt{k}) = x^3$, que l'on peut aussi voir sous la forme d'un produit d'idéaux principaux

$$II' = (x)^3$$

où $I = (y + \sqrt{k})$ et $I' = (y - \sqrt{k})$.

Vérifions d'abord que I et I' sont premiers entre eux. Soit $D = I + I'$ leur pgcd. Il contient $y \pm \sqrt{k} \in D$ ainsi donc que $2y$ et $2k$. Comme k est sans facteur carré, on constate que x, y et k sont deux à deux premiers entre eux. En particulier le pgcd de $2y$ et $2k$ est 2, puis $2 \in D$ par Bézout. Les idéaux de A contenant 2 sont $2A$, A et un idéal premier $P = 2A + \sqrt{k}A$ ou $2A + (\sqrt{k} + 1)A$ selon que k est pair ou non, avec de plus $P^2 = (2)$. Le cas $D = 2A$ est absurde car $y + \sqrt{k} \notin 2A$, donc $D = P$. Comme $P^2 = (2)$, et $y \pm \sqrt{k} \notin 2A$, on a dans ce cas $v_P(I) = v_P(I') = 1$. Mais alors $v_P(II') = 3v_P(x) = v_P(I) + v_P(I') = 2$ est contradictoire. La seule possibilité est donc $D = A$.

Ainsi I et I' sont premiers entre eux. Comme II' est le cube d'un idéal de A, on en déduit que I est aussi le cube d'un idéal de A par factorisation unique des idéaux en produit d'idéaux premiers (par exemple, on constate que $v_P(I)$ est multiple de 3 pour tout idéal premier P de A). Ainsi, $I = J^3$ pour un certain idéal $J \subset A$. Mais $I = J^3$ est principal, donc l'ordre de $[J]$ dans $\mathrm{Cl}(A)$ divise 3. Comme il divise aussi $\mathrm{h}_{\mathbb{Q}(\sqrt{k})}$ qui est premier à 3, cet ordre est 1 : l'idéal J est principal.

On conclut alors comme dans l'étude du cas $k = 2$: soient $a, b \in \mathbb{Z}$ tels que $J = (a + b\sqrt{k})$. L'identité $I = J^3$ entraîne que $y + \sqrt{k}$ et le cube de l'élément $a + b\sqrt{k}$ diffèrent multiplicativement d'une unité de A. Mais tout unité de A est un cube car $k \neq 3$. Quitte à remplacer $a + b\sqrt{k}$ par un multiple par une unité, on a donc une identité dans A :

$$y + \sqrt{k} = (a + b\sqrt{k})^3 = a^3 + 3kab^2 + (3a^2b + kb^3)\sqrt{k}.$$

En particulier, $1 = b(3a^2 + kb^2)$ puis $b = \pm 1$ et $-k = 3a^2 - b$. Il n'y a donc pas de solution si $-k$ n'est pas de cette forme. S'il est de cette forme, il l'est pour exactement

une valeur de b et deux valeurs de a car $b \equiv k \bmod 3$. La relation $y = a^3+3ka$ donne deux valeurs possibles opposées pour y, et donc une seule pour $y^2 - k = x^3$, ainsi que pour $x = (a + b\sqrt{k})(a - b\sqrt{k}) = a^2 - k$. Les deux solutions obtenues au final sont

$$(x, y) = (a^2 - k, \pm(a^3 + 3ka)),$$

qui sont bien solutions.

□

5. Application à la détermination de $\mathrm{Cl}(\mathcal{O}_K)$ sur un exemple

On se propose dans ce paragraphe de voir sur un exemple comment ces résultats fournissent des méthodes pour déterminer le groupe $\mathrm{Cl}(\mathcal{O}_K)$. Précisément, on se propose de démontrer

$$\mathrm{Cl}(\mathbb{Z}[\frac{1+\sqrt{-47}}{2}]) \simeq \mathbb{Z}/5\mathbb{Z}.$$

Tout d'abord, comme -47 est sans facteur carré et $\equiv 1 \bmod 4$, l'anneau $A := \mathbb{Z}[\frac{1+\sqrt{-47}}{2}]$ est l'anneau des entiers du corps de nombres $K = \mathbb{Q}(\sqrt{-47})$, de sorte que A est de Dedekind et $\mathrm{Cl}(A)$ est bien un groupe.

On a $A = A_{-47}$, donc $\mathrm{disc}(A) = -47$, et le théorème de Minkowski assure que toute classe d'idéaux non nuls de A contient un idéal contenant un entier $1 \leq N \leq C(1, 2)\sqrt{47} < 5$ (table 5).

Considérons le problème de trouver tous les idéaux I contenant $1, 2, 3$ ou 4. Comme $A = \mathcal{O}_K$, "contenir c'est diviser", et il suffit donc de déterminer les idéaux divisant 3 ou $4 = 2^2$. On détermine d'abord les idéaux premiers de A contenant 2 ou 3 (ceux contenant 4 contiennent 2). Soient $\alpha = \frac{1+\sqrt{-47}}{2}$ et $P = \Pi_{\alpha,\mathbb{Q}} = X^2 - X + 12$. Les congruences

$$P \equiv X(X - 1) \bmod 2, 3$$

montrent qu'il y a deux idéaux premiers contenant 2 (resp. 3), qui sont $D = (2, \alpha)$ et $D' = (2, \alpha - 1)$ (resp. $T = (3, \alpha)$ et $T' = (3, \alpha - 1)$). On a alors $(2) = DD'$ et $(3) = TT'$. Ainsi les idéaux contenant $(4) = D^2D'^2$ sont $4A$, A, D^2, D'^2, $D^2D' = 2D'$ et $2D$. Les idéaux contenant 3 sont $3A$, A, T et T'. Au final, on voit en particulier que $\mathrm{Cl}(A)$ est engendré par les classes de D, D', T et T'.

Mais on a $(2) = II'$ et $(3) = JJ'$, de sorte que $[I']$ est l'inverse de $[I]$ et $[J']$ est l'inverse de $[J]$: le groupe $\mathrm{Cl}(A)$ est donc engendré par les classes de I et J.

Une manière de trouver des relations multiplicatives entre ces classes, c'est-à-dire des idéaux principaux de la forme I^aJ^b, est de trouver d'abord des éléments de A de norme 2^a3^b puis de décomposer les idéaux principaux qu'ils engendrent : ce sont des monômes en D, D', T et T'. Cette méthode s'appelle la "méthode des éléments de petite norme". On rappelle que

$$\mathrm{N}(x + y\alpha) = x^2 + xy + 12y^2 = \frac{1}{4}(2x + y)^2 + \frac{47}{4}y^2$$

(forme principale de discriminant -47) et constate notamment que $\mathrm{N}(\alpha) = 12$ et $\mathrm{N}(4 + \alpha) = 32$ (plus petite puissance de 2 qui est une norme). Observons que l'on a $\alpha \in I, \alpha \in J$ mais $\alpha \notin I'$ (car sinon on aurait $I = I'$), d'où l'égalité $(\alpha) = I^2J$.

Ainsi, $[J] = [I]^{-2}$ dans $\mathrm{Cl}(A)$, qui est donc engendré comme groupe par la classe de I. De même, $(4+\alpha) = I^5$, donc $[I]$ est d'ordre divisant 5 ! Il est donc d'ordre 1 ou 5, mais il n'est pas principal car 2 n'est pas une norme. On a donc démontré donc que

$$\mathrm{Cl}(\mathbb{Z}[\frac{1+\sqrt{-47}}{2}]) \simeq \mathbb{Z}/5\mathbb{Z},$$

et qu'il est par exemple engendré par $[I]$ (et donc aussi par $[J] = [I]^{-2}$...).

6. Exercices

Exercice 7.1. *(i) Trouver tous les idéaux de $\mathbb{Z}[\sqrt{6}]$ contenant 15.*

(ii) Factoriser en produit d'idéaux premiers l'idéal $(1+2\sqrt{-5})$ de $\mathbb{Z}[\sqrt{-5}]$.

Exercice 7.2. *On se place dans l'anneau $A = \mathbb{Z}[\sqrt{-5}]$.*

(i) Factoriser en produit d'idéaux premiers les idéaux principaux (2), (3), $(1+\sqrt{-5})$ et $(1-\sqrt{-5})$.

(ii) Expliquer pourquoi la relation $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ n'est pas en contradiction avec la propriété de Dedekind, bien qu'elle entraîne comme on l'a vu au chapitre 5 que A n'est pas factoriel.

Exercice 7.3. *On se propose de déterminer $\mathrm{Cl}(\mathbb{Z}[\sqrt{-14}])$.*

(i) Montrer que tout idéal non nul de $A = \mathbb{Z}[\sqrt{-14}]$ est équivalent à un idéal contenant un entier $1 \leq N \leq 4$.

(ii) Déterminer tout les idéaux de A contenant $1, 2, 3$ et 4.

(iii) En considérant des petits nombres bien choisis représentés par la forme $x^2 + 14y^2$, montrer que $\mathrm{Cl}(A)$ est cyclique d'ordre 4.

Exercice 7.4. *Montrer de même que $\mathrm{Cl}(\mathbb{Z}[\sqrt{-13}]) \simeq \mathbb{Z}/2\mathbb{Z}$ et que $\mathrm{Cl}(\mathbb{Z}[\sqrt{-26}]) \simeq \mathbb{Z}/6\mathbb{Z}$.*

Exercice 7.5. (Principal équivaut à factoriel pour les ordres d'un corps de nombres) *Soit K un corps de nombres.*

(i) Montrer qu'un idéal premier non nul de $\mathcal{O}_K$ est principal si et seulement si il contient un élément premier de $\mathcal{O}_K$.

(ii) En déduire que $\mathcal{O}_K$ est factoriel si, et seulement si, il est principal.

(iii) Montrer que si un ordre A de K est factoriel, alors $A = \mathcal{O}_K$, puis que A est principal.

Problème 7.1. (Arithmétique de[1] $\mathbb{Z}[\alpha]$) *Soit $A = \mathbb{Z}[\alpha]$ où $\alpha \in \overline{\mathbb{Z}}$. Si $p \in \mathbb{Z}$ est un nombre premier, et si $Q \in (\mathbb{Z}/p\mathbb{Z})[X]$ est un facteur de $\Pi_{\alpha,\mathbb{Q}}$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$, on notera $I(Q)$ l'idéal $pA + \widetilde{Q}(\alpha)$ défini dans la proposition 6.10.*

(i) Montrer que si Q et Q' sont premiers entre eux dans $(\mathbb{Z}/p\mathbb{Z})[X]$ alors $\mathrm{I}(Q)\mathrm{I}(Q') = \mathrm{I}(QQ')$. On pourra partir d'une relation de Bézout dans $(\mathbb{Z}/p\mathbb{Z})[X]$ entre Q et Q'.

(ii) En déduire que si $\overline{\Pi}_{\alpha,\mathbb{Q}} = Q_1 \cdots Q_g$ où les Q_i sont irréductibles unitaires deux à deux distincts, alors on a la décomposition $pA = \prod_{i=1}^{g}(pA + \widetilde{Q}_i(\alpha)A)$.

(iii) En déduire que si p ne divise pas l'entier $D = \mathrm{disc}(\Pi_{\alpha,\mathbb{Q}}) = \mathrm{disc}(A)$, tous les idéaux premiers de A contenant p sont inversibles.

(iv) (Factorisation conditionnelle) *Montrer que tout idéal de A de norme première à $\mathrm{disc}(A)$ se factorise de manière unique comme produit d'idéaux premiers de A.*

(v) Montrer que si I et J sont des idéaux non nuls de A de norme première à $\mathrm{disc}(A)$, alors $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$.

1. On prendra garde que l'on ne suppose pas dans cet exercice que $\mathbb{Z}[\alpha]$ est l'anneau des entiers de $\mathbb{Q}(\alpha)$.