Università degli Studi di Trento

DIPARTIMENTO DI MATEMATICA

Corso di Laurea in Matematica

Tesi triennale

Half-factorial Domain, Other Half-factorial Domain

Laureando:
Luca Girardi

Supervisore:
Prof.ssa Alessandra Bernardi

Anno Accademico 2015-2016

Un'importante proprietà dell'anello degli interi $\mathbb{Z}$ è la fattorizzazione unica, ossia il fatto che ogni elemento si scrive in modo unico come prodotto di irriducibili (a meno di unità). Ma ci sono degli insiemi, come ad esempio $\mathbb{Z}[\sqrt{-5}]$, in cui un elemento può essere scritto in modi diversi come prodotto di irriducibili. In questo lavoro considero due diverse generalizzazioni dei Domini a Fattorizzazione Unica (UFD): gli *Half-Factorial Domains* (HFD) e gli *Other Half-Factorial Domains* (OHFD). Queste due categorie di insiemi si ottengono indebolendo la definizione di UFD; infatti il termine *Half-Factorial Domain* sta ad indicare un dominio che possiede metà degli assiomi che definiscono un UFD (due fattorizzazioni dello stesso elemento hanno la medesima cardinalità). Un insieme che possiede l'altra metà degli assiomi che definiscono un UFD (unicità dei fattori modulo unità) è chiamato, invece, *Other Half-Factorial Domain*.

Questa tesi è divisa in tre capitoli. Nel primo riporto dei concetti preliminari di Teoria dei Numeri di cui non si può fare a meno nelle varie dimostrazioni di questa trattazione.
Nel secondo capitolo tratto gli *Half-Factorial Domains* (HFD) e fornisco un metodo per verificare quali, tra un gruppo ristretto di anelli (gli "ordini di un campo di numeri"), sono degli HFD e quali non lo sono. In particolare, in questo capitolo mostro che $\mathbb{Z}[\sqrt{-3}]$ è proprio un HFD.
Nell'ultimo capitolo descrivo gli *Other Half-Factorial Domains* (OHFD). L'obbiettivo è mostrare che non esistono esempi di OHFD non banali, ossia non esistono OHFD che non siano UFD. Questo significa che le due definizioni sono equivalenti, cioè possiamo indebolire la definizione di dominio a fattorizzazione unica, poiché la metà degli assiomi sono ridondanti.

1 Preliminari

Nella prima parte di questo capitolo riporto alcuni concetti classici della Teoria dei Numeri, che ho studiato nel Corso di Teoria dei Numeri; si possono trovare facilmente in qualsiasi testo di Teoria Algebrica dei Numeri, ad esempio [7] oppure [6]. Nella seconda parte riporto la definizione di ordine in un campo di numeri e alcune sue proprietà, che si possono trovare in molti testi, tra cui in [8].

Definizione 1.1. *Un campo algebrico di numeri K, o più semplicemente un* campo di numeri*, è un sottocampo del campo dei numeri complessi $\mathbb{C}$ che sia un'estensione finita di $\mathbb{Q}$.*

Un caso particolarmente interessante si ha quando il grado dell'estensione da $\mathbb{Q}$ a K, $[K:\mathbb{Q}]$, è uguale a 2, in questo caso K si dice *campo quadratico*. Infatti un campo quadratico K può sempre essere ottenuto estendendo Q con una radice di un intero d libero da quadrati. Se $K = \mathbb{Q}(\sqrt{d_1})$, con $d_1 = k^2 d$ con $k \in \mathbb{Z}$, dato che $d = k^2 d \frac{1}{k^2} \in \mathbb{Q}(\sqrt{k^2 d})$, abbiamo che $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{k^2 d})$.

Definizione 1.2. *Un elemento $\alpha \in \mathbb{C}$ si dice intero algebrico, se esiste un polinomio monico $f \in \mathbb{Z}[x]$ tale che $f(\alpha) = 0$. L'insieme degli elementi di un campo di numeri K che sono interi algebrici è denotato con $\mathcal{O}_K$.*

Si vede che $\mathcal{O}_K$ è un anello e uno $\mathbb{Z}-$modulo libero di grado $[K:\mathbb{Q}]$.

Definizione 1.3. *Siano $x_1, \ldots, x_n$ elementi del campo di numeri K e indichiamo con $\sigma_i : K \hookrightarrow \overline{\mathbb{Q}}$ le n $\mathbb{Q}-$immersioni di K in $\overline{\mathbb{Q}}$. Il discriminante degli n elementi $x_1, \ldots, x_n$ è: $disc(x_1, \ldots, x_n) := (\det A)^2$, dove A è una matrice i cui elementi sono $a_{ij} = \sigma_i(x_j)$.*

Nel caso in cui $K = \mathbb{Q}(\sqrt{d})$ sia un campo quadratico con d un intero libero da quadrati, definiamo il discriminante di $\mathcal{O}_K$ (o di K), indicato con D_K, come il discriminante di una base intera di $\mathcal{O}_K$,

ossia come il discriminante degli elementi di una base di $\mathcal{O}_K$ come $\mathbb{Z}-$modulo. Si può vedere che $(1, \omega_K)$ è una base intera di $\mathcal{O}_K$, dove $\omega_K = \sqrt{d}$ se $d \equiv 2, 3 \pmod 4$, mentre se $d \equiv 1 \pmod 4$, $\omega_K = \frac{1+\sqrt{d}}{2}$. Quindi si ricava che se $d \equiv 2, 3 \pmod 4$, allora $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ e $D_K = 4d$, mentre se $d \equiv 1 \pmod 4$, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ e $D_K = d$.

Definizione 1.4. *Un dominio A si dice* dominio a fattorizzazione unica (UFD) *se ogni elemento ammette un'unica fattorizzazione in elementi irriducibili.*

Ernst Eduard Kummer (1810-1893) nel tentativo di dimostrare l'Ultimo Teorema di Fermat, si accorse che l'anello degli interi di un campo di numeri non è sempre un dominio a fattorizzazione unica (UFD). Per ovviare a questo inconveniente, Kummer introdusse la nozione di *numeri ideali*. Dedekind rivisitò questa intuizione dando vita alla nozione di *ideale di un anello*; dimostrò che per gli ideali di $\mathcal{O}_K$ esiste un'unica decomposizione in ideali primi.

Definizione 1.5. *Un dominio A è di Dedekind, se:*

1. *A è integralmente chiuso;*
2. *A è noetheriano;*
3. *ogni ideale primo non nullo è massimale.*

Teorema 1.6 (Dedekind)**.** *Sia A un anello di Dedekind, allora ogni ideale non banale $I \subset A$ si scrive in modo unico come prodotto di ideali primi.*

$\mathcal{O}_K$ è un dominio di Dedekind e K è il suo campo dei quozienti. Quindi anche se gli elementi $\alpha \in \mathcal{O}_K$ possono presentare fattorizzazioni in primi diverse tra loro, gli ideali di $\mathcal{O}_K$ sono invece a fattorizzazione unica in termini di ideali primi.
Introduciamo ora il concetto di gruppo delle classi, il cui ordine misura in qualche modo quanto $\mathcal{O}_K$ si allontana dall'essere un UFD.

Definizione 1.7. *Sia A un anello integro e sia K il suo campo dei quozienti. Un* ideale frazionario *di A è un sotto A-modulo di K, I, tale che esiste $d \in A$ con $I \subset d^{-1}A$, ovvero dI è un ideale di A.*

Sia J_K il gruppo degli ideali frazionari di $\mathcal{O}_K$ e P_K il suo sottogruppo degli ideali principali, il gruppo delle classi di A è il gruppo quoziente $Cl_K := J_K/P_K$. L'ordine di Cl_K è chiamato numero delle classi (*class number*) ed è indicato con h_K.

Teorema 1.8 (Dirichlet)**.** *Per ogni campo di numeri K, il gruppo delle classi di Cl_K è finito.*

Lemma 1.9. *Sia A un anello. Allora un elemento $p \in A$ è primo se e solo se l'ideale (p) è primo.*

Dimostrazione. Sia p un elemento primo di A e Siano $a, b \in A$ due elementi qualsiasi. Se $ab \in (p)$, allora $p \mid ab$, visto che p è primo abbiamo $p \mid a$, oppure $p \mid b$, cioè $a \in (p)$, o $b \in (p)$ e la prima implicazione è risolta.
Sia (p) un ideale primo di Ae siano $a, b \in A$ due elementi qualsiasi. Se $p \mid ab$, allora $ab \in (p)$, visto che (p) è primo abbiamo $a \in (p)$, oppure $b \in (p)$, cioè $p \mid a$, o $p \mid b$ e abbiamo concluso. □

Questo appena dimostrato è un lemma che utilizzeremo più volte nel corso delle varie dimostrazioni. In particolare ci permette di affermare che se un elemento π appartenente a un dominio di Dedekind è irriducibile, ma non primo, allora l'ideale (π) da esso generato non è primo e dunque può essere scomposto in ideali primi.

Definizione 1.10. *Un dominio A si dice* dominio a ideali principali (PID) *se ogni ideale $I \in A$ è della forma (a) per qualche elemento $a \in A$.*

Per un dominio A qualsiasi vale: se A è un dominio a ideali principali, allora è anche un dominio a fattorizzazione unica (PID $\implies$ UFD). Per i domini di Dedekind vale anche il viceversa:

Lemma 1.11. *Un anello di Dedekind è fattoriale* (UFD) *se e solo se è principale* (PID).

Dimostrazione. Abbiamo appena osservato che un'implicazione vale per tutti i domini. Vediamo l'implicazione opposta.
Sia A un anello di Dedekind fattoriale, basta mostrare che ogni ideale primo $\mathfrak{p}$ è principale. Sia $a \in \mathfrak{p}$ un elemento non nullo e consideriamo la sua fattorizzazione in elementi primi $a = p_1 \cdots p_r$. Allora $p_1 \cdots p_r \in \mathfrak{p}$ e, poiché $\mathfrak{p}$ è primo, esiste i tale che $p_i \in \mathfrak{p}$, cioè $(p_i) \subset \mathfrak{p}$. Per il Lemma 1.9 abbiamo che (p_i) è primo. In un anello di Dedekind ogni ideale primo è massimale, quindi $(p_i) = \mathfrak{p}$ e abbiamo concluso. □

Teorema 1.12. *Sia K un campo di numeri. Allora $h_K = 1$ se e solo $\mathcal{O}_K$ è un* UFD.

Dimostrazione. $h_K = 1$ se e solo se $J_K = P_K$, cioè se e solo se tutti gli ideali sono principali, ovvero $\mathcal{O}_K$ è un PID, che per il Lemma 1.11 è equivalente a dire che $\mathcal{O}_K$ è un UFD. □

Esempio 1.13. Sia $\mathbb{Q}(\sqrt{d})$ un campo quadratico immaginario, ossia $d < 0$. Allora $h_K = 1$ solo per $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$ (cf. [3, Teorema 9.3]). Quindi grazie al Teorema 1.12 gli anelli degli interi di questi campi sono UFD. In particolare noi utilizzeremo il fatto che $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ è un UFD.

Definizione 1.14. *Un* ordine *di un campo quadratico K è un sottoanello $\mathcal{O} \subset \mathcal{O}_K$, che sia anche uno $\mathbb{Z}-$modulo libero di rango 2, contente una base intera per K.*

In particolare, l'anello degli interi algebrici su campo K è chiamato *massimo ordine*, in quanto contiene tutti gli altri ordini di K per definizione. Poiché sia $\mathcal{O}$ che $\mathcal{O}_K$ sono $\mathbb{Z}-$moduli liberi di rango 2, notiamo che l'indice $n = [\mathcal{O}_K : \mathcal{O}]$ è finito.
Si può vedere che una base intera di $\mathcal{O}$ è data da $(1, n\omega_K)$, dove ω_K è così definito:

$$\omega_K = \begin{cases} \sqrt{d} & \text{se } d \equiv 2, 3 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{se } d \equiv 1 \pmod 4. \end{cases}$$

Possiamo definire il discriminante di $\mathcal{O}$, come il discriminante di una base intera di $\mathcal{O}$, ossia come il discriminante degli elementi di una base di $\mathcal{O}$ come $\mathbb{Z}-$modulo. Si mostra che il discriminante di un ordine $\mathcal{O}$ di indice n su K è dato da $D = n^2 D_K$, dove D_K è il discriminante di $\mathcal{O}_K$.
Poiché un ordine $\mathcal{O}$ non è un dominio di Dedekind, non possiamo procedere nello stesso modo fatto per $\mathcal{O}_K$ per definire il class number. In particolare non è sempre vero che ogni ideale frazionario non nullo abbia inverso, e non possiamo usare la fattorizzazione unica in ideale primi. Per ricondurci a queste familiari proprietà caratteristiche del massimo ordine $\mathcal{O}_K$, introduciamo una speciale classe di ideali di $\mathcal{O}$.

Definizione 1.15. *Un ideale $\mathfrak{a} \subset \mathcal{O}$ è detto* proprio *se $\mathcal{O} = \{\beta \in K \mid \beta\mathfrak{a} \subset \mathfrak{a}\}$.*

Notiamo che è sempre vero che $\mathcal{O} \subset \{\beta \in K \,|\, \beta\mathfrak{a} \subset \mathfrak{a}\}$, in quanto $\mathfrak{a}$ è un ideale di $\mathcal{O}$, mentre l'uguaglianza non è sempre vera.
Abbiamo dato la definizione di ideale frazionario chiedendo solo che A sia un anello integro, quindi in $\mathcal{O}$ gli ideali frazionari sono definiti come in $\mathcal{O}_K$. Mentre in $\mathcal{O}_K$ tutti gli ideali frazionari (escluso $\{0\}$) sono invertibili, in un ordine $\mathcal{O}$ di un campo quadratico $K = \mathbb{Q}(\sqrt{d})$, un ideale frazionario $\mathfrak{a}$ è invertibile se e solo se è proprio. In particolare nel massimo ordine $\mathcal{O}_K$ ogni ideale frazionario non nullo è proprio.
Ora che sappiamo che gli ideali frazionari propri sono invertibili, è facile vedere che l'insieme $J(\mathcal{O})$ degli ideali frazionari propri è un gruppo rispetto alla moltiplicazione, come nel caso di $\mathcal{O}_K$, l'insieme degli ideali principali $P(\mathcal{O})$ è un suo sottogruppo, dunque definiamo il gruppo delle classi di $\mathcal{O}$, come il quoziente $Cl(\mathcal{O}) := J(\mathcal{O})/P(\mathcal{O})$. Nel caso in cui $\mathcal{O} = \mathcal{O}_K$ è il massimo ordine, abbiamo che $Cl(\mathcal{O}) = Cl_K$.

Si può vedere che, dato un ideale $\mathfrak{a} \subset \mathcal{O}$ il numero $|\mathcal{O}/\mathfrak{a}|$ (ossia il numero delle classi dell'anello quoziente $\mathcal{O}/\mathfrak{a}$) è finito. Quindi definiamo la norma di un ideale come $N(\mathfrak{a}) := |\mathcal{O}/\mathfrak{a}|$. Notiamo che questa definizione è la stessa che viene usata classicamente nel caso del massimo ordine $\mathcal{O}_K$. Nel caso $I = (\alpha)$ sia un ideale principale abbiamo che $N(I) = N(\alpha) = \alpha\overline{\alpha}$, dove l'ultima uguaglianza indica la norma di un elemento di $\mathcal{O}$.

Diamo ora la definizione di *dominio atomico* e riformuliamo la definizione di dominio a fattorizzazione unica (UFD) utilizzando la nozione di dominio atomico. Questa definizione ci permette di ricavare i concetti di due nuovi tipi di domini che hanno la metà delle proprietà di un UFD, che tratteremo nei due capitoli seguenti.

Definizione 1.16. *Un dominio di integrità R si dice* atomico*, se ogni elemento non nullo e non invertibile di R si scrive come prodotto di elementi irriducibili di R; questi ultimi elementi sono anche detti* atomi*.*

Definizione 1.17. *Un dominio di integrità R è chiamato* dominio a fattorizzazione unica*,* UFD *in breve, se è atomico, e se, data la fattorizzazione in irriducibili*

$$\pi_1\pi_2\cdots\pi_n = \xi_1\xi_2\cdots\xi_m$$

valgono le seguenti proprietà:

(a) $n = m$*;*

(b) esiste una permutazione $\sigma \in S_n$ tale che per ogni $1 \leq i \leq n$, $\pi_i = u_i\xi_{\sigma(i)}$, dove ogni u_i è un'unità di R.

Un *half-factorial domain* (HFD) è un dominio atomico in cui ogni fattorizzazione di un elemento in irriducibili ha la stessa lunghezza, cioè in altre parole un dominio in cui vale la proprietà (a) della Definizione 1.17. Il nome deriva proprio dal fatto che un HFD ha la metà degli assiomi di un UFD. Ci si è poi chiesti se esistono esempi di domini, non UFD, che hanno "l'altra metà degli assiomi", cioè l'assioma (b) della Definizione 1.17, ed è quindi stato introdotto il concetto di *other half-factorial domain* (OHFD). Nel terzo capitolo studieremo questi insiemi e mostreremo che non esistono OHFD che non siano UFD, ciò significa che la definizione di UFD può essere indebolita alla sola proprietà (b).

2 HFD

Gli HFD sono stati studiati implicitamente da L. Carlitz in [1] nel caso degli anelli degli interi di un campo di numeri. Il termine *half-factorial domain* (HFD) è stato successivamente introdotto da Zacks in [10] come generalizzazione del concetto di dominio a fattorizzazione unica (UFD). In questo capitolo riporto il teorema di Carlitz con una rivisitazione della sua dimostrazione in ottica moderna. Questo permette di stabilire quali fra gli anelli di interi algebrici sono degli HFD. Proseguo poi con una caratterizzazione che permette di vedere quali ordini di un campo di numeri sono HFD.

Definizione 2.1. *Un dominio di integrità R è chiamato* half-factorial domain (HFD) *se è atomico, e se, data la fattorizzazione in irriducibili*

$$\pi_1\pi_2\cdots\pi_n = \xi_1\xi_2\cdots\xi_m$$

allora $n = m$.

Per la dimostrazione dei prossimi teoremi utilizzo il seguente risultato (cf. [2, Teorema 4, Capitolo 10]) la cui dimostrazione è al di fuori delle mie conoscenze.

Teorema 2.2 (Weber)**.** *Ogni classe di ideali di un campo quadratico contiene infiniti ideali primi.*

In aggiunta, gli ideali primi che vengono trovati nella dimostrazione di questo teorema sono caratterizzati dal fatto di avere norma un numero primo.

Teorema 2.3 (Carlitz)**.** *Sia K un campo di numeri. Allora $h_K \leq 2$ se e solo se $\mathcal{O}_K$ è un* HFD*.*

Dimostrazione. Vediamo prima il caso $h_K = 1$. Questa condizione è equivalente a dire che tutti gli ideali frazionari sono principali, cioè $\mathcal{O}_K$ è un PID, ma grazie al Lemma 1.11 abbiamo automaticamente che $\mathcal{O}_K$ è anche un UFD.
Supponiamo che $h_K = 2$, assumiamo di avere due fattorizzazioni in irriducibili

$$\pi_1\pi_2\cdots\pi_n = \xi_1\xi_2\cdots\xi_m$$

vogliamo mostrare che $n = m$.
Se un fattore sulla sinistra, π_i è primo, allora divide un fattore sulla destra, ξ_j, il quale è primo, quindi a meno di un'unità ϵ, abbiamo che $\pi_i = \epsilon\xi_j$. Dunque, a meno di unità, possiamo ridurci al caso in cui le fattorizzazioni consistono solo di elementi irriducibili non primi.
Dato che $h_K = 2$ e per il Lemma 1.9, possiamo fattorizzare in ideali primi $(\pi_i) = \mathfrak{p}_{i1}\mathfrak{p}_{i2}$ e $(\xi_i) = \mathfrak{q}_{j1}\mathfrak{q}_{j2}$. Dunque considerando gli ideali delle due fattorizzazioni abbiamo

$$(\pi_1)(\pi_2)\cdots(\pi_n) = (\xi_1)(\xi_2)\cdots(\xi_m) \implies \mathfrak{p}_{11}\mathfrak{p}_{12}\mathfrak{p}_{21}\mathfrak{p}_{22}\cdots\mathfrak{p}_{n1}\mathfrak{p}_{n2} = \mathfrak{q}_{11}\mathfrak{q}_{12}\mathfrak{q}_{21}\mathfrak{q}_{22}\cdots\mathfrak{q}_{m1}\mathfrak{q}_{m2}.$$

Grazie al teorema di Dedekind sappiamo che la fattorizzazione in ideali primi è unica, quindi $2n = 2m$ e concludiamo che $n = m$.
Consideriamo ora il caso in cui $h_K > 2$. Per il teorema di Dirichlet h_K è finito, quindi ogni classe di Cl_K ha ordine finito che divide h_K. Abbiamo quindi due casi:

1. l'esponente (il massimo ordine delle classi) di Cl_K è maggiore di 2, quindi esiste una classe con ordine maggiore di 2;

2. l'esponente di Cl_K è 2. Visto che $h_K > 2$, Cl_K deve contenere un sottogruppo isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

1. Supponiamo l'esistenza di una classe di ordine $n > 2$ e prendiamo un ideale primo $\mathfrak{p}$ in questa classe (sappiamo che esiste grazie al Teorema 2.2). Dato che l'ordine della classe è n, abbiamo che $\mathfrak{p}^n$ è un ideale principale, cioè $\mathfrak{p}^n = (\alpha)$. Affermiamo che α è irriducibile, infatti se non lo fosse avremmo $\alpha = ab$, con a, b non unità, dunque $\mathfrak{p}^n = (a)(b)$ e per il teorema di Dedekind abbiamo che $(a) = \mathfrak{p}^m$ con $m < n$, ma ciò contraddice l'ipotesi che la classe di $\mathfrak{p}$ ha ordine n. Ora prendiamo un ideale primo $\mathfrak{q}$ nella classe di $\mathfrak{p}^{-1}$, che ha sempre ordine n, quindi come per $\mathfrak{p}$, si vede che $\mathfrak{q}^n = (\beta)$ con β irriducibile. Notiamo che $\mathfrak{pq}$ è un ideale principale, quindi possiamo scrivere $\mathfrak{pq} = (\pi)$. Affermiamo che π è irriducibile, infatti se non lo fosse avremmo $\pi = cd$, con c, d non unità, dunque $\mathfrak{pq} = (c)(d)$, ma poiché la scomposizione in ideali primi è unica e (c) e (d) sono diversi da (1) deve essere $\mathfrak{p} = (c)$ oppure $\mathfrak{p} = (d)$, ma ciò contraddice l'ipotesi che l'ordine della classe di $\mathfrak{p}$ sia $n > 2$. Consideriamo ora la fattorizzazione $(\mathfrak{pq})^n = \mathfrak{p}^n\mathfrak{q}^n$, o, equivalentemente, $(\pi)^n = (\alpha)(\beta)$, allora abbiamo $\pi^n = u\alpha\beta$, dove u è un'unità. Abbiamo assunto $n > 2$, dunque concludiamo che $\mathcal{O}_K$ non è un HFD.

2. L'ultimo caso da considerare è quello in cui Cl_K contiene un sottogruppo isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Assumiamo che le classi corrispondenti a $(0,1)$, $(1,0)$ e $(1,1)$ siano diverse dalle classe degli ideali principali. Prendiamo un ideale primo $\mathfrak{p}$ nella classe corrispondente a $(0,1)$, un ideale primo $\mathfrak{q}$ nella classe corrispondente a $(1,0)$ e un ideale primo $\mathfrak{r}$ nella classe corrispondente a $(1,1)$. Poiché l'esponente è 2, abbiamo che tutte e 3 le classi considerate hanno ordine 2, quindi, come abbiamo fatto sopra, possiamo trovare elementi irriducibili $\alpha, \beta, \gamma, \xi$, tali che $\mathfrak{p}^2 = (\alpha)$, $\mathfrak{q}^2 = (\beta)$, $\mathfrak{r}^2 = (\gamma)^2$, $\mathfrak{pqr} = (\xi)$. Dunque

$$(\mathfrak{pqr})^2 = \mathfrak{p}^2\mathfrak{q}^2\mathfrak{r}^2 \implies \xi^2 = u\alpha\beta\gamma$$

dove u è un'unità. Dunque concludiamo che anche in questo caso $\mathcal{O}_K$ non è un HFD e abbiamo concluso. □

Esempio 2.4. Sia $\mathbb{Q}(\sqrt{d})$ un campo quadratico immaginario, ossia $d < 0$. Allora $h_K = 1$ solo per $d = -5, -6, -10, -13, -15, -22, -35, -37, -51, -58, -91, -115, -123, -187, -235, -267, -403, -427$ ([3, Teorema 9.4]). Quindi, per il Teorema 2.3 gli anelli degli interi associati a questi campi, insieme a quelli visti nell'Esempio 1.13, sono HFD.

Introduciamo un paio di lemmi che ci permetteranno di dimostrare il prossimo risultato.

Lemma 2.5. *Sia K un campo di numeri con numero delle classi $h_K > 2$, allora esistono primi distinti $p, q, r \in \mathbb{Z}$ e un elemento irriducibile $\pi \in \mathcal{O}_K$ tale che $N(\pi) = pqr$.*

Dimostrazione. Questa dimostrazione si rifà alla seconda parte della dimostrazione del Teorema di Carlitz.
Per il teorema di Dirichlet h_K è finito, quindi ogni classe di Cl_K ha ordine finito che divide h_K. Abbiamo quindi due casi:

1. l'esponente (il massimo ordine delle classi) di Cl_K è maggiore di 2, quindi esiste una classe con ordine maggiore di 2;

2. l'esponente di Cl_K è 2. Visto che $h_K > 2$, Cl_K deve contenere un sottogruppo isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

1. Supponiamo l'esistenza di una classe di ordine $n > 2$ e prendiamo due ideali primi $\mathfrak{p}$ e $\mathfrak{q}$ in questa classe, con norma rispettivamente, due numeri primi p e q. Consideriamo la classe di $\mathfrak{p}^{-2}$, questa è diversa della classe dell'unità, perché l'ordine è maggiore di 2. Prendiamo un ideale $\mathfrak{r}$ in questa classe con norma un primo r. Per costruzione l'ideale $\mathfrak{pqr}$ è principale, quindi possiamo scrivere $\mathfrak{pqr} = (\pi)$. Notiamo che π è irriducibile, infatti se non lo fosse avremmo $\pi = cd$, con c, d non unità, dunque $\mathfrak{pqr} = (c)(d)$, ma poiché la scomposizione in ideali primi è unica e (c) e (d) sono diversi da (1) deve essere uno tra (c) e (d) è primo, mentre l'altro si scompone in due ideali primi. Quindi uno tra $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$ è un ideale principale, ma questo è assurdo, perché sono stati presi in classi non banali.

2. Facciamo ora il caso in cui Cl_K contiene un sottogruppo isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Assumiamo che le classi corrispondenti a $(0,1)$, $(1,0)$ e $(1,1)$ siano diverse dalle classe degli ideali principali. Prendiamo un ideale primo $\mathfrak{p}$ nella classe corrispondente a $(0,1)$, un ideale primo $\mathfrak{q}$ nella classe corrispondente a $(1,0)$ e un ideale primo $\mathfrak{r}$ nella classe corrispondente a $(1,1)$, con norma rispettivamente un numero primo p, q, r. Come abbiamo fatto sopra troviamo che $\mathfrak{pqr} = (\pi)$, con π irriducibile.

In entrambi i casi abbiamo trovato un ideale principale, generato da un elemento irriducibile con norma pqr, e dato che la norma di un ideale principale è uguale alla norma di un elemento che genera l'ideale stesso, abbiamo anche trovato un elemento irriducibile in $\mathcal{O}_K$ con norma pqr. □

Notiamo che p, q ed r, dato che rappresentano la norma di ideali non principali, sono elementi irriducibili di $\mathcal{O}_K$. Proviamolo per la norma p dell'ideale primo $\mathfrak{p}$. Se p non fosse irriducibile avremmo che $p = ab$ con $a, b \in \mathcal{O}_K$ non unità. Quindi abbiamo che $(p) = (a)(b)$, la norma dell'ideale generato da p è p^2 e dunque $N(a) = N(b) = p$, cioè gli ideali $(a), (b)$ sono primi. Sappiamo che l'ideale $\mathfrak{p}$ divide l'ideale generato dalla sua norma cioè $\mathfrak{p}$, questo significa che esiste un ideale $\mathfrak{q}$ di norma p, quindi primo, tale che $(a)(b) = (p) = \mathfrak{pq}$. Per il teorema di Dedekind la scomposizione in ideali primi è unica, dunque avremmo $\mathfrak{p} = (a)$, oppure $\mathfrak{p} = (b)$, ma ciò è una contraddizione perché l'ideale $\mathfrak{p}$ non è principale. Quindi possiamo scomporre la norma dell'elemento π in due fattorizzazioni in irriducibili di lunghezza differente: $\pi\overline{\pi} = pqr$.

Lemma 2.6. *Sia $K = \mathbb{Q}(\sqrt{d})$ un campo quadratico con anello degli interi $\mathcal{O}_K$ e sia $\mathcal{O}$ un ordine di indice n su $\mathcal{O}_K$. Ogni elemento di $\mathcal{O}$ che divide n è della forma uk, dove $k \in \mathbb{Z}$, mentre u è un'unità di $\mathcal{O}_K$.*

Dimostrazione. Innanzitutto mostriamo che ogni elemento $\alpha \in \mathcal{O}$ che divide n ha norma un quadrato in $\mathbb{Z}$. Per fare ciò, supponiamo per assurdo che la norma di α sia della forma $p^{2m+1}b$ con p primo in $\mathbb{Z}$ e b coprimo con p.
Se $d \equiv 2, 3 \pmod 4$, possiamo scrivere α nella forma $x + yn\sqrt{d}$ con $x, y \in \mathbb{Z}$; dalla norma ricaviamo la seguente equazione

$$\alpha\overline{\alpha} = p^{2m+1}b \implies (x + yn\sqrt{d})(x - yn\sqrt{d}) = p^{2m+1}b \implies x^2 - y^2n^2d = p^{2m+1}b$$

α divide n, quindi $N(\alpha) \mid N(n)$, cioè $p^{2m+1}b$ divide n^2, in particolare p^{2m+1} deve dividere n^2 e quindi anche x^2. Ora x^2 e n^2 sono quadrati, quindi devono essere divisi anche da p^{2m+2}, dunque p^{2m+2} divide $p^{2m+1}b$, cioè $p \mid b$, ma questa è una contraddizione, in quanto avevamo assunto b coprimo con p.
Invece, se $d \equiv 1 \pmod 4$, α è della forma $x + ny\frac{1+\sqrt{d}}{2}$, con $x, y \in \mathbb{Z}$. Dalla norma ricaviamo la

seguente equazione

$$\alpha\overline{\alpha} = p^{2m+1}b \implies (x + yn\frac{1+\sqrt{d}}{2})(x + yn\frac{1-\sqrt{d}}{2}) = p^{2m+1}b$$
$$\implies x^2 + xny - n^2y^2\frac{1-d}{4} = p^{2m+1}b.$$

Come abbiamo già visto sopra, p^{2m+1} divide n^2, quindi deve dividere anche $x^2 + xny = x(x + ny)$; come prima, anche p^{2m+2} divide n^2, quindi p^{m+1} divide n.
Se fosse $p^k \,||\, x$ con $k \leq m$, avremmo $p^{2k} \,||\, x^2$ e visto che $p^k \,|\, p^{m+1} \,|\, n$ troveremmo $p^{2k} \,||\, x^2 + xny$, ma questo è assurdo. Dunque $p^{m+1} \,|\, x$, e usando il fatto che $p^{m+1} \,|\, n$, troviamo che $p^{2m+2} \,|\, x^2$, $p^{2m+2} \,|\, xn$, $p^2m + 2 \,|\, n^2$. Utilizzando l'uguaglianza trovata sopra ricaviamo che $p^{2m+2} \,|\, p^{2m+1}$, cioè $p \,|\, b$, ma questa è una contraddizione, in quanto avevamo assunto b coprimo con p.
Ora sappiamo che la norma di α vale $\pm k^2$ con $k \in \mathbb{Z}$.
Se $d \equiv 2, 3 \pmod 4$ scriviamo $\alpha = x + ny\sqrt{d}$ con $x, y \in \mathbb{Z}$. Consideriamo l'equazione della norma

$$x^2 - y^2n^2d = \pm k^2$$

$\alpha \,|\, n$ implica che $k^2 \,|\, n^2$, quindi k^2 deve dividere anche x^2, cioè $k \,|\, x$. Ora scriviamo $x = ka$ e $n = kb$, da cui ricaviamo che $\alpha = ka + kby\sqrt{d} = k(a + by\sqrt{d})$. Sappiamo che k è un intero, quindi la sua norma è k^2; la norma di α è $\pm k^2$, perciò abbiamo che la norma di $u := a + by\sqrt{d}$ è ± 1, cioè u è un'unità di $\mathcal{O}_K$ e abbiamo scritto α come prodotto di un intero per un'unità di $\mathcal{O}_K$, come nell'enunciato.
Se $d \equiv 1 \pmod 4$ scriviamo α nella forma $x + ny\frac{1+\sqrt{d}}{2}$ con $x, y \in \mathbb{Z}$. Consideriamo l'equazione della norma

$$x^2 + xny - n^2y^2\frac{1-d}{4} = \pm k^2.$$

Per ogni primo $p \in \mathbb{Z}$ sia m tale che $p^m \,||\, k$. Allora $p^{2m} \,||\, k^2 \,|\, n^2$, cioè $p^m \,|\, n$ e ricaviamo che $p^{2m} \,|\, x^2 + xny = x(x + ny)$. Sia r il minimo esponente con cui p divide x. Se per assurdo $r < m$, avremmo che $p^m \,|\, p^{2m-r} \,|\, x + ny$, sappiamo che $p^m \,|\, n$, dunque p^m dividerebbe anche x, ma ciò sarebbe in contraddizione con il fatto che $r < m$. Dunque $r > m$, cioè $p^m \,|\, x$. Questo vale per ogni primo in $\mathbb{Z}$, quindi ricaviamo che k è un divisore di x, come lo è di n. Come abbiamo fatto sopra scriviamo $x = ka$ e $n = kb$, sostituiamo per trovare

$$\alpha = ka + kby\frac{1+\sqrt{d}}{2} = k\left(a + by\frac{1+\sqrt{d}}{2}\right).$$

Poniamo $u := a + by\frac{1+\sqrt{d}}{2}$ e vediamo che come prima la sua norma è ± 1, quindi anche in questo caso abbiamo scritto $\alpha = uk$ con $k \in \mathbb{Z}$ e u un'unità di $\mathcal{O}_K$. □

Teorema 2.7. *Sia $K = \mathbb{Q}(\sqrt{d})$ un campo quadratico e sia $\mathcal{O}$ un ordine di indice n sull'anello degli interi $\mathcal{O}_K$. Allora $\mathcal{O}$ è un* HFD *se e solo se $\mathcal{O}_K$ è un* HFD *e ogni irriducibile di $\mathcal{O}$ è anche irriducibile in $\mathcal{O}_K$.*

Dimostrazione. $\Longleftarrow$ Questa è l'implicazione più semplice. Assumiamo che $\mathcal{O}_K$ sia un HFD e che ogni irriducibile in $\mathcal{O}$ rimane irriducibile in $\mathcal{O}_K$. Prendiamo un elemento $a \in \mathcal{O}$ e consideriamo le seguenti fattorizzazioni in irriducibili (di $\mathcal{O}$)

$$a = \pi_1\pi_2 \cdots \pi_k = \xi_1\xi_2 \cdots \xi_m.$$

Queste sono fattorizzazioni in irriducibili anche in $\mathcal{O}_K$; dato che $\mathcal{O}_K$ è HFD per ipotesi, abbiamo $k = m$. Questo vale per ogni fattorizzazione in irriducibili, quindi anche $\mathcal{O}$ è un HFD.

$\Longrightarrow$ Innanzitutto mostriamo che se $\mathcal{O}$ è un HFD, allora anche il massimo ordine $\mathcal{O}_K$ è un HFD. Sia $\mathcal{O}$ un HFD e supponiamo per assurdo che, invece, $\mathcal{O}_K$ non lo sia. Grazie al Lemma 2.6, sappiamo che esiste un elemento irriducibile $\alpha \in \mathcal{O}_K$ tale che $N(\alpha) = pqr$ con p, q, r primi in $\mathbb{Z}$ (e irriducibili in $\mathcal{O}_K$).
Come sempre consideriamo due casi:

1. Se $d \equiv 2, 3 \pmod 4$ scriviamo $\alpha = x + y\sqrt{d}$, con $x, y \in \mathbb{Z}$. Consideriamo l'equazione della norma in $\mathcal{O}_K$

$$x^2 - dy^2 = pqr.$$

Moltiplicando entrambi i membri dell'equazione per n^2 otteniamo la seguente equazione in $\mathcal{O}$

$$(nx)^2 - dn^2y^2 = pqrn^2$$

dove la fattorizzazione in irriducibili della parte destra dell'equazione è data da 3 primi in $\mathbb{Z}$, che sono irriducibili in $\mathcal{O}_K$ e quindi anche in $\mathcal{O}$, e da un numero pari di fattori irriducibili, dato dal doppio del numero di fattori irriducibili di n, quindi ha lunghezza dispari. La parte sinistra dell'equazione ha, invece, una fattorizzazione in irriducibili di lunghezza pari, poiché è una norma. Quindi $\mathcal{O}$ non è un HFD.

2. Se $d \equiv 1 \pmod 4$ scriviamo $\alpha = x + y\frac{1+\sqrt{d}}{2}$, con $x, y \in \mathbb{Z}$. Consideriamo l'equazione della norma in $\mathcal{O}_K$

$$x^2 + xy + y^2\frac{1-d}{4} = pqr.$$

Moltiplicando entrambi i lati per n^2 otteniamo la seguente equazione in $\mathcal{O}$

$$(xn)^2 + (xn)yn + n^2y^2\frac{1-d}{4} = pqrn^2.$$

Come prima, la parte destra ha una fattorizzazione in irriducibili di lunghezza dispari, mentre la parte sinistra, essendo una norma, ha un numero pari di fattori irriducibili, dunque concludiamo che $\mathcal{O}$ non è un HFD.
Abbiamo quindi dimostrato che, in generale, se $\mathcal{O}_K$ non è un HFD nessuno dei suoi ordini è un HFD. Equivalentemente se $\mathcal{O}$ è un HFD allora anche $\mathcal{O}_K$ lo è.

Ora vogliamo invece mostrare che se esiste un irriducibile di $\mathcal{O}$ che si può scomporre in $\mathcal{O}_K$, allora $\mathcal{O}$ non può essere un HFD.
Assumiamo che $\mathcal{O}$ sia un HFD e prendiamo un elemento irriducibile $\pi \in \mathcal{O}$, tale che esistano $\alpha, \beta \in \mathcal{O}_K \setminus \mathcal{O}$ non unità, tali che $\pi = \alpha\beta$. Notiamo che

$$N(\pi) = \pi\overline{\pi} = \alpha\beta\overline{\alpha}\overline{\beta} = (\alpha\overline{\alpha})(\beta\overline{\beta}) = N(\alpha)N(\beta).$$

La norma di π ha numero di fattori irriducibili in $\mathcal{O}$ maggiore o uguale al numero di fattori primi in $\mathbb{Z}$. Dunque se $N(\pi)$ avesse più di due fattori primi in $\mathbb{Z}$, avremmo che $\mathcal{O}$ non sarebbe un HFD. Possiamo, quindi, assumere che $N(\alpha) = p$ e $N(\beta) = q$, con p, q primi in $\mathbb{Z}$, cioè (α) e (β) sono ideali primi o, equivalentemente, α e β sono primi in $\mathcal{O}_K$.

Mostriamo che se u è un'unità di $\mathcal{O}_K$ allora $u\alpha$ e $u\beta$ non stanno in $\mathcal{O}$. Se $u\alpha \in \mathcal{O}$ per qualche unità u di $\mathcal{O}_K$ otteniamo l'equazione

$$N(\pi) = N(\alpha)N(\beta) = \pm\, N(u)N(\alpha)N(\beta) = \pm N(u\alpha)N(\beta) = \pm(u\alpha)(\overline{u\alpha})(\beta\overline{\beta})$$
$$\implies \pi\overline{\pi} = \pm(u\alpha)(\overline{u\alpha})(\beta\overline{\beta})$$

dove la parte destra può essere fattorizzata con più di due irriducibili, cioè $\mathcal{O}$ non è un HFD.
Scegliamo $x \in \mathcal{O}$ tale che $N(x) = k_1^2 p$ con k_1 il minimo intero positivo che divide n e tale che x stia in $\mathcal{O}$. Notiamo che un tale elemento esiste, infatti, consideriamo l'insieme $S := \{k \in \mathbb{N} \,|\, k \text{ divide } n,\ \exists\ x \in \mathcal{O} \text{ t.c. } N(x) = k^2 p\} \subset \mathbb{N}$; l'insieme non è vuoto, perché $n^2 \in S$, dato che $n\alpha \in \mathcal{O}$, dunque, per il principio del minimo, l'insieme ha un minimo. Allo stesso modo scegliamo $y \in \mathcal{O}$ tale che $N(y) = k_2^2 q$, con k_2 il minimo intero positivo che divide n.
Affermiamo che gli elementi così scelti x e y sono irriducibili in $\mathcal{O}$. Se $x = ab$ con $a, b \in \mathcal{O}$, non unità, allora $p \,|\, N(x) = N(a)N(b)$, cioè $p \,|\, N(a)$ o $p \,|\, N(b)$. Senza perdita di generalità assumiamo $N(a) = pm$, dove m deve dividere k_1^2 e quindi n^2. Con un ragionamento molto simile a quello fatto nel Lemma 2.6 si trova che m deve essere un quadrato e ciò contraddice la minimalità di k_1.
Poiché α è primo in $\mathcal{O}_K$ possiamo scrivere $x = \alpha_1\gamma_1$ con $\alpha_1 = \alpha$ o $\alpha_1 = \overline{\alpha}$ e $\gamma_1 \in \mathcal{O}_K$. Infatti $\alpha\overline{\alpha} = N(\alpha) \,|\, N(x) = x\overline{x}$, in particolare $\alpha \,|\, x\overline{x}$, cioè $\alpha \,|\, x$, oppure $\alpha \,|\, \overline{x}$; nel secondo caso coniugando entrambi i membri troviamo $\overline{\alpha} \,|\, x$. Poiché la norma del coniugato è la stessa abbiamo $N(\alpha_1) = p$, quindi $N(\gamma_1) = k_1^2$. Allo stesso modo possiamo scrivere $y = \beta_2\gamma_2$ con $\beta_2 = \beta$ o $\beta_2 = \overline{\beta}$ e $\gamma_2 \in \mathcal{O}_K$ con $N(\gamma_2) = k_2^2$. Nè k_1 nè k_2 possono avere norma ± 1, altrimenti avremo che $u\alpha$ o $u\beta$ sta in $\mathcal{O}_K$ con u unità.
Consideriamo ora la fattorizzazione

$$N(\pi)N(\gamma_1)N(\gamma_2) = N(\alpha\beta)N(\gamma_1)N(\gamma_2) = N(\alpha_1\gamma_1)N(\beta_2\gamma_2) = N(x)N(y)$$
$$(\pi)(\overline{\pi})k_1^2k_2^2 = x\overline{x}y\overline{y}.$$

La parte destra è una fattorizzazione in irriducibili di $\mathcal{O}$, mentre la parte sinistra ha almeno 6 fattori irriducibili, dunque si vede che $\mathcal{O}$ non è un HFD e abbiamo concluso la dimostrazione. □

Esempio 2.8. Consideriamo l'ordine non massimale $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$, l'ordine di indice 2 su $\mathcal{O}_K = \mathbb{Z}[\omega]$, dove $\omega = \frac{1+\sqrt{-3}}{2}$. Abbiamo visto nell'Esempio 1.13 che $\mathcal{O}_K$ è un UFD e quindi anche un HFD. Mostriamo che ogni elemento irriducibile in $\mathcal{O}$ è anche irriducibile in $\mathcal{O}_K$. Innanzitutto notiamo che la norma che abbiamo utilizzato per $\mathcal{O}$ e per $\mathcal{O}_K$ è la norma degli elementi di $\mathbb{C}$ ristretta ai rispettivi insiemi, quindi abbiamo la stessa funzione per entrambi gli anelli. In più la norma di un elemento è ± 1 se e solo se l'elemento è un'unità.
Sia $a \in \mathcal{O}_K$ un'elemento qualsiasi, allora almeno uno fra $a, a\omega, a\overline{\omega}$ sta in $\mathcal{O}$. Infatti, scriviamo $a = x + \omega y$:

- $a = \left(x + \frac{y}{2}\right) + \frac{y}{2}\sqrt{-3}$, allora $a \in \mathcal{O}$ se $y \equiv 0 \pmod 2$;
- $a\overline{\omega} = \left(\frac{x}{2}\right) - x\sqrt{-3}$, allora $a\overline{\omega} \in \mathcal{O}$, se $x \equiv 0 \pmod 2$;
- $a\omega = \left(\frac{x-y}{2}\right) + \left(\frac{x+y}{2}\right)\sqrt{-3}$, allora $a\omega \in \mathcal{O}$ se $x + y \equiv x - y \equiv 0 \pmod 2$, ossia se $x \equiv y \equiv 0 \pmod 2$ oppure $x \equiv y \equiv 1 \pmod 2$.

Sia r un elemento irriducibile in $\mathcal{O}$, con norma $N(r)$. Allora in $\mathcal{O}$ non esiste nessun elemento ξ, con norma $N(\xi)$ che divida la norma di r. Supponiamo che in $\mathcal{O}_K$ esista un elemento π tale che $\pi \,|\, \alpha$.

Allora $N(\pi) \mid N(\alpha)$, ma uno tra $\pi, \omega\pi, \overline{\omega}\pi$ sta in $\mathcal{O}$, tutti e tre questi elementi hanno norma $N(\pi)$, perché ω e $\overline{\omega}$ sono unità. Dunque in $\mathcal{O}$ c'è un divisore di α, una contraddizione.
Concludiamo che ogni irriducibile in $\mathcal{O}$ resta irriducibile in $\mathcal{O}_K$ e grazie al Teorema 2.7 otteniamo che $\mathbb{Z}[\sqrt{-3}]$ è un HFD.

Teorema 2.9. *L'anello $\mathbb{Z}[\sqrt{-3}]$ è l'unico ordine non integralmente chiuso, ossia non massimale, in un campo quadratico immaginario che sia un* HFD*.*

Dimostrazione. Sia $K = \mathbb{Q}(\sqrt{d})$, con $d < 0$, un campo immaginario. Consideriamo tutti gli ordini non massimali, cioè gli ordini $\mathcal{O}$ con indice $n > 1$ su $\mathcal{O}_K$ e vediamo quali tra questi sono HFD. Ci dividiamo in due casi:

1. Se $d \equiv 2, 3 \pmod 4$, allora un ordine $\mathcal{O}$ non massimale sul campo K è della forma $\mathbb{Z}[n\sqrt{d}]$, con $n > 1$. Un qualsiasi elemento $\xi \in \mathcal{O}$ lo possiamo scrivere nella forma $\xi = x + ny\sqrt{d}$, con $x, y \in \mathbb{Z}$. La norma $N(\xi) = x^2 - dn^2y^2$ è non negativa, visto che per ipotesi d è sempre negativo.
Sia $p \in \mathbb{Z}$ un primo che divide n e scriviamo $n = pk$. Consideriamo l'elemento $\alpha = n\sqrt{d} \in \mathcal{O}$, ossia l'elemento corrispondente a $x = 0$ e $y = 1$, di norma $N(\alpha) = -dn^2 = -dp^2k^2$. Affermiamo che α è irriducibili in $\mathcal{O}$. Infatti un qualsiasi divisore proprio $\beta \in \mathcal{O}$ ha norma $N(\beta) < -dn^2$. Consideriamo l'insieme $S = \{N(\xi) \mid \xi = x + ny\sqrt{d} \in \mathcal{O},\ y \neq 0\}$ degli elementi con componente immaginaria non nulla. Non è difficile vedere che $-dn^2$ è il minimo di questo insieme. Allora β ha parte immaginaria nulla, cioè $\beta \in \mathbb{Z}$, ma non possiamo scrivere un elemento non intero come prodotto di elementi in $\mathbb{Z}$. Dalla norma otteniamo la seguente equazione

$$(n\sqrt{d})(-n\sqrt{d}) = (p)(p)(k)(k)(d).$$

Siccome la parte sinistra dell'equazione è una fattorizzazione in irriducibili di $\mathcal{O}$, si ha che $\mathcal{O}$ non è un HFD, a meno che $k = 1$ e $d = -1$. In questo caso gli unici ordini possibili sono quelli di indice un numero primo nel campo $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$.
Sia $p \in \mathbb{N}$ un numero primo e sia $\mathcal{O}$ un ordine di indice p in $\mathbb{Z}[i]$. Un qualsiasi elemento $\xi \in \mathcal{O}$ lo possiamo scrivere nella forma $\xi = x + py$, con $x, y \in \mathbb{Z}$. La norma è $N(\xi) = x^2 + p^2y^2 \geq 0$. Per $x = p,\ y = 1$ otteniamo l'elemento $\alpha = p + pi \in \mathcal{O}$, che ha norma $N(\alpha) = 2p^2$. Affermiamo che α è irriducibili in $\mathcal{O}$. La minima norma di un elemento con parte immaginaria non nulla in $\mathcal{O}$ è p^2 e si ha nel caso $x = 0,\ y = \pm 1$, cioè per $\pm pi$. Ma in $\mathcal{O}$ non c'è nessun elemento non invertibile, di norma minore o uguale a due. Quindi ci rimane solo il caso in cui tutti i divisori di α sono interi, ma $p + pi \notin \mathbb{Z}$, e dunque siamo giunti a una contraddizione. Dalla norma troviamo l'equazione

$$(p + pi)(p - pi) = (2)(p)(p)$$

dove a sinistra ci sono solo due elementi irriducibili, mentre a destra ce ne sono almeno tre, quindi in questo caso $\mathcal{O}$ non è un HFD.

2. Se $d \equiv 1 \pmod 4$, allora un ordine $\mathcal{O}$ non massimale sul campo K è della forma $\mathbb{Z}\left[n\frac{1+\sqrt{d}}{2}\right]$, con $n > 1$. Un qualsiasi elementi $\xi \in \mathcal{O}$ lo possiamo scrivere nella forma $\xi = x + ny\frac{1+\sqrt{d}}{2}$, con $x, y \in \mathbb{Z}$. La norma $N(\xi) = x^2 + nxy + n^2y^2\frac{1-d}{4} = \left(x + \frac{n}{2}y\right)^2 - \frac{dn}{4}y^2$ è non negativa, visto che per ipotesi d è sempre negativo. Scegliamo l'elemento $\alpha = n\frac{1+\sqrt{d}}{2}$, corrispondente a $x = 0,\ y = 1$, che ha norma $N(\alpha) = \frac{1-d}{4}n^2$. Affermiamo che α è irriducibile. Infatti un divisore proprio $\beta = x_1 + ny_1\frac{1+\sqrt{d}}{2}$, ha norma che divide non banalmente $\frac{1-d}{4}n^2$, cioè $N(\beta) \leq \frac{1-d}{8}n^2$. Se

fosse $|y_1| \geq 2$, allora $N(\beta) \geq -dn^2 > \frac{1-d}{8}n^2$ (ricordiamo che $d \leq -3$). Se $|y_1| = \pm 1$, allora la norma di β è $x_1^2 \pm nx_1 + \frac{1-d}{4}n^2$, ma nemmeno in questo caso la disequazione

$$x_1^2 \pm nx_1 + \frac{1-d}{4}n^2 \leq \frac{1-d}{8}n^2$$

ha soluzioni accettabili. Rimane quindi il caso in cui $y_1 = 0$, cioè quando $\beta \in \mathbb{Z}$, ma non possiamo scrivere α come prodotto di soli numeri interi, dunque α è irriducibile.
Dalla norma troviamo la seguente equazione

$$\left(\frac{1+\sqrt{d}}{2}n\right)\left(\frac{1-\sqrt{d}}{2}n\right) = \left(\frac{1-d}{4}\right)(n)(n).$$

L'unica possibilità che ha $\mathcal{O}$ di essere un HFD è nel caso in cui $\frac{1-d}{4}$ è un'unità ed n è primo, cioè solo se $d = -3$. Dunque gli unici ordini non massimali che possono aspirare ad essere degli HFD sono quelli di indice un numero primo p nell'anello $\mathcal{O}_K = \mathbb{Z}[\omega]$, dove $\omega = \omega_K = \frac{1+\sqrt{-3}}{2}$.
Sia $\mathcal{O}$ un ordine di indice un primo $p > 2$ nell'anello $\mathcal{O}_K = \mathbb{Z}[\omega]$. Un qualsiasi elemento $\xi \in \mathcal{O}$ lo possiamo scrivere nella forma $\xi = x + py\omega$, con $x, y \in \mathbb{Z}$ e la sua norma è $N(\xi) = x^2 + pxy + p^2y^2$.
Per $x = p,\ y = 1$ otteniamo l'elemento $\alpha = p + p\omega \in \mathcal{O}$, la cui norma è $N(\alpha) = 3p^2$.
Dalla forma della norma si vede che non esiste nessun elemento in $\mathcal{O}$ di norma p. Infatti se esistesse $\xi \in \mathcal{O}$ con $N(\xi) = p$, la sua norma sarebbe $x^2 + pxy + p^2y^2 = p$, cioè $p \mid x^2$, in particolare $p \mid x$, ossia $x = pa$, con $a \in \mathbb{Z}$ e troveremmo $p^2a^2 + p^2ay + p^2y^2 = p$ con $a, y \in \mathbb{Z}$, ma quest'equazione non ha soluzioni intere.
Gli elementi di norma 3 in $\mathcal{O}_K$ sono della forma $u\sqrt{-3}$ dove $u \in \{\pm 1,\ \pm\omega\ \pm\omega^2\}$ è un'unità, ma nessuno di questi sta in $\mathcal{O}$, tranne nel caso $p = 2$, che non abbiamo ancora considerato. Quindi, visto che in $\mathcal{O}$ non ci sono elementi di norma p, o 3 abbiamo che α è irriducibile e dalla norma ricaviamo la seguente equazione

$$(p + p\omega)(p + p\overline{\omega}) = (3)(p)(p)$$

dove $\overline{\omega} = \frac{1-\sqrt{-3}}{2}$ è il coniugato di ω. A sinistra ci sono due irriducibili, mentre a destra ce ne sono almeno tre; questo mostra che $\mathcal{O}$ non è un HFD.
L'unico caso che rimane da vedere è il caso in cui $p = 2$, cioè $\mathbb{Z}[\sqrt{-3}]$ e nell'Esempio 2.8 abbiamo visto che è un HFD. □

3 OHFD

Definizione 3.1. *Un dominio di integrità R è chiamato* other half-factorial domain (OHFD) *se è atomico, e se, data la fattorizzazione in irriducibili*

$$\pi_1\pi_2\cdots\pi_m = \xi_1\xi_2\cdots\xi_n$$

esiste una permutazione $\sigma \in S_n$ tale che per ogni $1 \leq i \leq n$, $\pi_i = u_i\xi_{\sigma(i)}$, dove ogni u_i è un'unità di R.

Intuitivamente un OHFD è un dominio atomico in cui un dato elemento può avere più fattorizzazioni in irriducibili di differenti lunghezze, ma dato un qualsiasi intero n, un elemento ha al più una fattorizzazione in irriducibili di lunghezza n. L'obbiettivo di questo capitolo è quello di mostrare che ogni OHFD è anche un HFD, cioè ogni OHFD è un UFD. Come immediata conseguenza ricaviamo che possiamo indebolire la Definizione 1.17, eliminando sostanzialmente la proprietà (a). Introduciamo alcune nuove definizioni che ci aiuteranno nello studio di questi domini.

Definizione 3.2. *Diciamo che due fattorizzazioni in irriducibili $\pi_1\pi_2\cdots\pi_n = \xi_1\xi_2\cdots\xi_m$ sono una* coppia non degenere *se gli irriducibili π_i, ξ_j sono a due a due non associati.*

Due fattorizzazioni in irriducibili con diversa lunghezza possono essere ricondotte a una coppia non degenere cancellando (a meno di unità) le coppie di elementi associati. Notiamo che, se due fattorizzazioni in irriducibili hanno la stessa lunghezza, allora, per definizione di OHFD, ogni elemento della prima fattorizzazione sarà associato con un elemento della seconda fattorizzazione, cioè cancellando gli elementi associati, troviamo un'uguaglianza tra unità.

Definizione 3.3. *Sia R un dominio atomico e sia $\pi_1 \in R$ un elemento irriducibile. Diciamo che π_1 è un atomo* lungo *se esiste una coppia non degenere $\pi_1\pi_2\cdots\pi_n = \xi_1\xi_2\cdots\xi_m$ tale che $n > m$.*

Definizione 3.4. *Sia R un dominio atomico e sia $\pi_1 \in R$ un elemento irriducibile. Diciamo che π_1 è un atomo* corto *se esiste una coppia non degenere $\pi_1\pi_2\cdots\pi_n = \xi_1\xi_2\cdots\xi_m$ tale che $n < m$.*

Da queste definizioni si ricava facilmente che se $\pi \in R$ è primo, allora non può essere nè lungo nè corto, poiché non può far parte di una coppia non degenere, in quanto deve dividere un elemento irriducibile dall'altro lato dell'uguaglianza. Le prossime proposizioni ci assicurano che ogni irriducibile non primo è un atomo lungo oppure un atomo corto, quindi la scelta di questi nomi ha senso.

Proposizione 3.5. *Sia R un $OHFD$ e siano*

$$\alpha_1\alpha_2\cdots\alpha_m = \beta_1\beta_2\cdots\beta_n$$
$$\gamma_1\gamma_2\cdots\gamma_r = \delta_1\delta_2\cdots\delta_s$$

due coppie di fattorizzazioni in irriducibili non degeneri con $m > n$ e $r > s$. Allora ogni α_i è associato a un qualche γ_j e viceversa. Allo stesso modo ogni β_i è associato a un qualche δ_j e viceversa.

Dimostrazione. Sia $a := r - s$, $b := m - n$, $am + bs = an + br$. Allora possiamo costruire due fattorizzazioni delle stessa lunghezza:

$$\alpha_1^a\alpha_2^a\cdots\alpha_m^a\delta_1^b\delta_2^b\cdots\delta_s^b = \beta_1^a\beta_2^a\cdots\beta_n^a\gamma_1^b\gamma_2^b\cdots\gamma_r^b.$$

Poiché R è un $OHFD$ ogni α_i deve essere associato a un qualche fattore all'altro lato dell'uguaglianza, ma per ipotesi α_i non è associato a nessun β_j e quindi deve essere che α_i è associato a qualche γ_j. Viceversa ogni γ_j non è associato a nessun δ_i, quindi deve essere associato a qualche α_i. Nello stesso modo si vede che β_i e δ_j sono associati. □

Proposizione 3.6. *Sia R un $OHFD$ che non è un HFD. Allora un elemento irriducibile non primo di R non può essere sia lungo che corto.*

Dimostrazione. Assumiamo per assurdo esista un elemento α, irriducibile, non primo, sia lungo che corto. Allora esistono due coppie di fattorizzazioni in irriducibili non degeneri

$$\alpha\alpha_2 \cdots \alpha_m = \beta_1\beta_2 \cdots \beta_n,$$
$$\gamma_1\gamma_2 \cdots \gamma_r = \alpha\delta_2 \cdots \delta_s$$

con $m > n$ e $r > s$. Per la Proposizione 3.5 α è associato a qualche β_j, ma questa è una contraddizione, perché $\alpha\alpha_2 \cdots \alpha_m = \beta_1\beta_2 \cdots \beta_n$ è una coppia non degenere e α non è associato a nessun β_j. □

Proposizione 3.7. *Data una qualsiasi coppia non degenere $\alpha_1\alpha_2 \cdots \alpha_m = \beta_1\beta_2 \cdots \beta_n$, con $m > n$ e un qualsiasi atomo lungo γ, si vede che γ è associato a qualche α_i. Dunque, esistono solo un numero finito di atomi lunghi.*

Dimostrazione. Sia $\alpha_1\alpha_2 \cdots \alpha_m = \beta_1\beta_2 \cdots \beta_n$, con $m > n$, una qualsiasi coppia non degenere. Supponiamo che γ sia un generico atomo lungo. Allora esiste una coppia non degenere $\gamma\gamma_2 \cdots \gamma_r = \delta_1\delta_2 \cdots \delta_s$ con $r > s$. Per la Proposizione 3.5 γ è associato a qualche α_i. Questo implica che, ogni atomo lungo appartiene all'insieme finito $\{\alpha_1, \ldots, \alpha_m\}$ degli atomi lunghi della prima coppia non degenere. □

In modo del tutto analogo si dimostra lo stesso risultato per gli atomi corti:

Proposizione 3.8. *Data una qualsiasi coppia non degenere $\alpha_1\alpha_2 \cdots \alpha_m = \beta_1\beta_2 \cdots \beta_n$, con $m > n$ e un qualsiasi atomo corto δ, si vede che δ è associato a qualche β_i. Dunque, esistono solo un numero finito di atomi corti.*

Notiamo che, grazie a queste ultime proposizioni, possiamo affermare che ogni coppia non degenere contiene almeno una volta ciascun atomo corto da una parte e ciascun atomo lungo dall'altra (a meno di unità). Infatti se così non fosse, supponiamo che esista un atomo corto δ che non fa parte della coppia non degenere $\alpha_1\alpha_2 \cdots \alpha_m = \beta_1\beta_2 \cdots \beta_n$, con $m > n$. Questo vorrebbe dire che δ non è associato a nessun β_j, ma questo contraddice ciò che abbiamo appena affermato nella proposizione 3.8.

Lemma 3.9. *Se $x \in R$ è un elemento irriducibile che non è né lungo né corto, allora x è primo in R.*

Dimostrazione. Supponiamo che $x \mid ab$ con $a, b \in R$. Allora esiste un elemento $c \in R$, tale che $cx = ab$. Scriviamo a, b, c come prodotto di irriducibili: $a = a_1a_2 \cdots a_r$, $b = b_1b_2 \cdots b_s$, $c = c_1c_2 \cdots c_t$. Possiamo quindi scrivere

$$c_1c_2 \cdots c_tx = a_1a_2 \cdots a_rb_1b_2 \cdots b_s.$$

Distinguiamo due casi: le fattorizzazioni hanno la stessa lunghezza, oppure lunghezza diversa.

1. Se le due fattorizzazioni hanno la stessa lunghezza, poiché R è un $OHFD$ abbiamo che x è associato a qualche a_i o a qualche b_j.

2. Se le due fattorizzazioni non hanno la stessa lunghezza, visto che x non è né lungo né corto, questa non è una coppia non degenere e x è associato a qualche a_i o a qualche b_j. Infatti se x non fosse associato a nessun a_i o b_j, se semplifichiamo tutti i c_i che sono associati a qualche a_i, b_j dall'altro lato dell'uguaglianza, otteniamo una coppia non degenere che contiene x, ma questa è una contraddizione.

Quindi in entrambi i casi concludiamo che $x \mid a$ o $x \mid b$, cioè x è primo. □

Fino ad ora non abbiamo mai chiesto che, data una coppia non degenere

$$\alpha_1\alpha_2\cdots\alpha_m = \beta_1\beta_2\cdots\beta_n,$$

con $m > n$, ogni α_i non sia associato a nessun altro α_j per $i \neq j$. Ora raccogliamo tutti gli elementi associati sotto un'unica potenza (raccogliendo opportunamente le unità), in modo da scrivere la coppia non degenere nella forma

$$\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_m^{a_m} = \xi_1^{b_1}\xi_2^{b_2}\cdots\xi_n^{b_n}$$

con $\sum_{i=1}^m a_i > \sum_{j=1}^n b_j$, e dove ogni π_i non è associato a nessun π_j per $i \neq j$ e ogni ξ_i non è associato a nessun ξ_j per $i \neq j$.
Gli insiemi $\{\pi_1, \pi_2, \ldots, \pi_m\}$ e $\{\xi_1, \xi_2, \ldots, \xi_n\}$ sono rispettivamente gli insiemi degli atomi lunghi e degli atomi corti in R, nel senso che un qualsiasi atomo lungo di R, per la Proposizione 3.7, è associato a un π_i, mentre un qualsiasi atomo corto di R, per la Proposizione 3.8, è associato a un ξ_j.
Notiamo che per le Proposizioni 3.7 e 3.8, gli esponenti della coppia non degenere sono tutti non negativi, ossia ogni $a_i, b_j > 0$.

Definizione 3.10. *Siano $\{\pi_1, \pi_2, \ldots, \pi_m\}$ e $\{\xi_1, \xi_2, \ldots, \xi_n\}$ rispettivamente gli insiemi degli atomi lunghi e degli atomi corti in R. Tra tutte le coppie non degeneri ne scegliamo una*

$$\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_m^{a_m} = \xi_1^{b_1}\xi_2^{b_2}\cdots\xi_n^{b_n}$$

tale che a_1 sia minimo e la chiamiamo master factorization (MF).

Lemma 3.11. *Sia $\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_m^{a_m} = \xi_1^{b_1}\xi_2^{b_2}\cdots\xi_n^{b_n}$ la* master factorization (MF). *Allora ogni coppia non degenere è una potenza della MF. In altre parole, ogni coppia non degenere è della forma*

$$\pi_1^{a_1 t}\pi_2^{a_2 t}\cdots\pi_m^{a_m t} = \xi_1^{b_1 t}\xi_2^{b_2 t}\cdots\xi_n^{b_n t}$$

per qualche $t \geq 1$.

Dimostrazione. Abbiamo già notato che una qualsiasi coppia non degenere contiene tutti gli atomi lunghi e corti di R, quindi può essere scritta nella forma

$$\pi_1^{c_1}\pi_2^{c_2}\cdots\pi_m^{c_m} = \xi_1^{d_1}\xi_2^{d_2}\cdots\xi_n^{d_n}$$

con ogni $c_i, d_j > 0$. Poniamo $a := \sum_{i=1}^m a_i$, $b := \sum_{i=1}^m b_i$, $c := \sum_{i=1}^m c_i$, $d := \sum_{i=1}^m d_i$; abbiamo che $a > b$ e $c > d$, infatti la parte sinistra di ciascuna coppia non degenere contiene gli atomi lunghi,

mentre la parte destra contiene quelli corti. Applichiamo lo stesso metodo che abbiamo utilizzato nella dimostrazione della Proposizione 3.5, chiamiamo $r := a - b$, $s := c - d$ e possiamo costruire la seguente equazione:

$$\pi_1^{a_1 s}\pi_2^{a_2 s}\cdots\pi_m^{a_m s}\xi_1^{d_1 r}\xi_2^{d_2 r}\cdots\xi_n^{d_n r} = \pi_1^{c_1 r}\pi_2^{c_2 r}\cdots\pi_m^{c_m r}\xi_1^{b_1 s}\xi_2^{b_2 s}\cdots\xi_n^{b_n s}.$$

Facili calcoli mostrano che $sa+dr = cr+bs$ e quindi le due fattorizzazioni hanno la stessa lunghezza, cioè la fattorizzazione è unica e abbiamo che $a_i s = c_i r$ e $d_j r = b_j s$ per ogni i, j. Ricaviamo che $c_i = \frac{s}{r}a_i$ e $d_j = \frac{s}{r}b_j$. In particolare $c_1 = \frac{s}{r}a_1$, e per minimalità di a_1 deduciamo che $\frac{s}{r} \geq 1$. Da ciò segue naturalmente che $a_i \leq c_i$ per ogni $1 \leq i \leq m$ e $b_j \leq d_j$ per ogni $1 \leq j \leq n$.

Ora vogliamo mostrare che $\frac{s}{r}$ è un numero intero, o, equivalentemente, che per ogni indice i, j, i quozienti $\frac{c_i}{a_i}$ e $\frac{d_j}{b_j}$ sono interi e sono tutti equivalenti. Applichiamo l'algoritmo della divisione Euclidea a tutti gli esponenti e otteniamo un sistema di equazioni in cui per ogni $0 \leq i \leq m$, $c_i = q_i a_i + r_i$, con $0 \leq r_i < a_i$, e per ogni $0 \leq j \leq n$, $d_j = Q_j b_j + R_j$, con $0 \leq R_j < b_j$.
Consideriamo nuovamente la coppia non degenere

$$\pi_1^{c_1}\pi_2^{c_2}\cdots\pi_m^{c_m} = \xi_1^{d_1}\xi_2^{d_2}\cdots\xi_n^{d_n}.$$

Abbiamo visto che per ogni i, j, $a_i \leq c_i$ e $b_j \leq d_j$, possiamo quindi dividere la parte sinistra dell'equazione per $\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_m^{a_m}$ e la parte destra per $\xi_1^{b_1}\xi_2^{b_2}\cdots\xi_n^{b_n}$. Ripetiamo questa divisione fino a quando non troviamo che uno degli esponenti è uno dei resti r_i o R_j. Possiamo quindi riscrivere l'equazione come

$$\pi_1^{v_1}\pi_2^{v_2}\cdots\pi_m^{v_m} = \xi_1^{w_1}\xi_2^{w_2}\cdots\xi_n^{w_n}$$

dove almeno uno dei v_i è r_i, oppure uno dei w_j è R_j. Se questa fosse una coppia non degenere, per quanto visto sopra, esisterebbero interi s_1, r_1, tali che $v_i = \frac{s_1}{r_1}a_i$, $w_j = \frac{s_1}{r_1}b_j$ con $\frac{s}{r} \geq 1$, cioè $v_i \geq a_i > r_i$ e $w_j \geq b_j > R_j$, una contraddizione. L'unica possibilità è che tutti gli esponenti siano nulli, cioè per ogni i, j, $r_i = R_j = 0$, cioè $a_i \mid c_i$ e $b_j \mid d_j$. Dunque il quoziente $\frac{s}{r}$ è intero, e posto $t := \frac{s}{r}$, possiamo scrivere

$$\pi_1^{a_1 t}\pi_2^{a_2 t}\cdots\pi_m^{a_m t} = \xi_1^{b_1 t}\xi_2^{b_2 t}\cdots\xi_n^{b_n t}$$

e la dimostrazione è conclusa. □

Abbiamo ora gli strumenti per dimostrare il teorema più importante di questa sezione.

Teorema 3.12. *Se R è un* OHFD*, allora R è un* HFD*.*

Dimostrazione. Supponiamo R sia un OHFD, che non sia un HFD. Usando la stessa notazione della Definizione 3.10 sia

$$\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_m^{a_m} = \xi_1^{b_1}\xi_2^{b_2}\cdots\xi_n^{b_n}$$

con $\sum_{i=1}^{m} a_i > \sum_{j=1}^{n} b_j$, la master factorization (MF). Dividiamo la dimostrazione in tre casi, dipendenti da m e da n.

Caso 1. $m \geq 2$ e $n \geq 2$.
Consideriamo il prodotto

$$(\pi_1^{a_1} - \xi_1^{b_1})(\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_m^{a_m} - \xi_2^{b_2}\xi_3^{b_3}\cdots\xi_n^{b_n}).$$

Ovviamente π_1 divide il prodotto, ma π_1 non divide nè $\xi_1^{b_1}$, nè $\xi_2^{b_2}\xi_3^{b_3}\cdots\xi_n^{b_n}$. Infatti se π_1 divide $\xi_2^{b_2}\xi_3^{b_3}\cdots\xi_n^{b_n}$, allora esiste un $c \in R$ tale che

$$c\pi_1 = \xi_2^{b_2}\xi_3^{b_3}\cdots\xi_n^{b_n}$$

e visto che π_1 non è associato con nessuno degli ξ_j, fattorizzando c in irriducibili si trova una coppia di fattorizzazioni in irriducibili di diseguale lunghezza. Dopo aver semplificato i fattori associati si trova una coppia non degenere, dove a sinistra stanno gli atomi lunghi, mentre a destra stanno quelli corti. L'elemento ξ_1 è un atomo corto e la Proposizione 3.8 afferma che è associato a uno degli ξ_j con $2 \leq j \leq n$, ma questa è una contraddizione. Allo stesso modo si mostra che π_1 non divide $\xi_1^{b_1}$.
Abbiamo detto sopra che π_1 divide il prodotto, cioè esiste $k \in R$ tale che

$$(\pi_1^{a_1} - \xi_1^{b_1})(\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_m^{a_m} - \xi_2^{b_2}\xi_3^{b_3}\cdots\xi_n^{b_n}) = k\pi_1.$$

Fattorizzando $(\pi_1^{a_1} - \xi_1^{b_1}) = \alpha_1\alpha_2\cdots\alpha_s$ e $(\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_m^{a_m} - \xi_2^{b_2}\xi_3^{b_3}\cdots\xi_n^{b_n}) = \beta_1\beta_2\cdots\beta_t$ otteniamo

$$\alpha_1\alpha_2\cdots\alpha_s\beta_1\beta_2\cdots\beta_t = k\pi_1$$

con α_i e β_j irriducibili in R. Per quanto mostrato sopra, π_1 non è associato a nessun α_i o β_j, quindi, dopo aver fattorizzato k, troviamo una coppia di fattorizzazioni in irriducibili di diseguale lunghezza. Dopo aver semplificato gli elementi associati, troviamo una coppia non degenere, dove a sinistra ci sono gli atomi corti, mentre a destra ci sono quelli lunghi. Ora la Proposizione 3.8 afferma che ξ_1 è associato a una degli irriducibili nella parte sinistra dell'equazione, cioè ξ_1 divide $(\pi_1^{a_1} - \xi_1^{b_1})$, oppure ξ_1 divide $(\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_m^{a_m} - \xi_2^{b_2}\xi_3^{b_3}\cdots\xi_n^{b_n})$. Questo implica che ξ_1 divide $\pi_1^{a_1}$ oppure ξ_1 divide $\xi_2^{b_2}\xi_3^{b_3}\cdots\xi_n^{b_n}$.
Se $\xi \,|\, \pi_1^{a_1}$, allora esiste $c \in R$ tale che $\pi_1^{a_1} = c\xi_1$ e queste sono due fattorizzazioni di diseguale lunghezza (dopo aver fattorizzato c). Semplificando gli elementi associati troviamo una coppia non degenere e per la Proposizione 3.7 π_i è associato a π_1, ma questa è una contraddizione.
Se $\xi_1 \,|\, \xi_2^{b_2}\xi_3^{b_3}\cdots\xi_n^{b_n}$, allora esiste $d \in R$ tale che $d\xi_1 = \xi_2^{b_2}\xi_3^{b_3}\cdots\xi_n^{b_n}$, ma dopo aver fattorizzato troviamo che queste sono fattorizzazioni di diseguale lunghezza con atomi corti non associati sia a destra che a sinistra e ciò è assurdo.
Tutto ciò mostra che, in questo caso, non può esistere una MF.

Caso 2. $m \geq 2$ e $n = 1$ oppure $m = 1$ e $n \geq 2$.
Questi due casi sono simmetrici, quindi studiamo solo quello in cui $m \geq 2$ e $n = 1$. La MF diventa

$$\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_m^{a_m} = \xi_1^{b_1}.$$

Visto che ξ_1 è irriducibile, deve essere $b_1 \geq 2$, altrimenti avremmo scritto ξ_1 come prodotto non banale di più elementi di R. Consideriamo il prodotto

$$(\pi_1^{a_1} - \xi_1)(\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_m^{a_m} - \xi_1^{b_1-1}).$$

Come prima π_1 divide il prodotto, ma non divide nessuno dei due fattori. Se fattorizziamo $(\pi_1^{a_1} - \xi_1) = \alpha_1\alpha_2\cdots\alpha_s$ e $(\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_m^{a_m} - \xi_1^{b_1-1}) = \beta_1\beta_2\cdots\beta_t$, allora esiste $k \in R$, tale che

$$\alpha_1\alpha_2\cdots\alpha_s\beta_1\beta_2\cdots\beta_t = k\pi_1$$

con $\alpha_i,\ \beta_j$ elementi irriducibili di R. Dato che π_1 non divide i fattori del prodotto, allora π_1 non è associato a nessun $\alpha_i,\ \beta_j$. Fattorizzando k e semplificando gli elementi associati troviamo una coppia non degenere con a sinistra gli atomi corti. L'irriducibile ξ_1 non è associato con π_1, quindi non può dividere $(\pi_1^{a_1} - \xi_1)$, cioè non è associato con nessuno degli α_i. Per il Lemma 3.11, abbiamo che $\xi_1^{b_1}$ divide la parte sinistra della fattorizzazione non degenere, quindi deve dividere $(\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_m^{a_m} - \xi_1^{b_1-1})$, ma questo vorrebbe dire che $\xi_1^{b_1} \mid \xi_1^{b_1-1}$ e questa è una contraddizione.
Dunque anche in questo caso non esiste una MF.

Caso 3. $m = n = 1$
In quest'ultimo caso la MF ha la forma

$$\pi^a = \xi^b$$

con $a > b \geq 2$. Consideriamo il prodotto

$$(\pi - \xi)(\pi^{a-1} - \xi^{b-1}).$$

Come prima π divide il prodotto, ma non divide i singoli fattori, quindi fattorizzando $(\pi - \xi) = \alpha_1\alpha_2\cdots\alpha_s$ e $(\pi^{a-1} - \xi^{b-1}) = \beta_1\beta_2\cdots\beta_t$, esiste $k \in R$, tale che

$$\alpha_1\alpha_2\cdots\alpha_s\beta_1\beta_2\cdots\beta_t = k\pi.$$

Come abbiamo già detto sopra π non può dividere nessuno degli α_i, β_j. Dopo aver fattorizzato k e semplificato gli elementi associati, troviamo un coppia non degenere dove a sinistra troviamo solo atomi corti. Il Lemma 3.11 ci garantisce che ogni $\alpha_i,\ \beta_j$ è divisibile per ξ, in particolare $\xi \mid (\pi - \xi)$, cioè ξ e π sono associati, assurdo.
In tutti i casi abbiamo mostrato che non esiste una master factorization(MF), dunque ciò dimostra che non esistono OHFD che non siano anche HFD e abbiamo concluso la dimostrazione. □

Il teorema appena dimostrato ci permette di affermare che un dominio atomico è un OHFD se e solo se è un UFD, quindi la Definizione 1.17 e la Definizione 3.1 sono equivalenti.
Un dominio atomico che non è un UFD ha almeno un elemento con due fattorizzazioni in irriducibili della stessa lunghezza.

Riferimenti bibliografici

[1] L. Carlitz, "A characterization of algebraic number fields with class number two, Proc. Amer. Math. Soc. **11** (1960), 391–392.

[2] H. Cohn, "Advanced Number Theory", Dover Publications, New York, 1980.

[3] J. Coykendall, "Extensions of half-factorial domains: a survey", Lecture Notes in Pure and Appl. Math., **241** (2005), 46–70.

[4] J. Coykendall, "Half-factorial domains in quadratic fields", J. Algebra **235** (2001), 417–430.

[5] J. Coykendall, W. W. Smith, "On unique factorization domains", J. Algebra **332** (2011), 62–70.

[6] P. Ellia, "Teoria dei numeri", 2013, http://dm.unife.it/philippe.ellia/Docs/TeoriaNumeri2013-14-OnLine.pdf.

[7] K. Ireland, M. Rosen, "A classical introduction to modern number theory", Springer, New York, 1990.

[8] J. Klaise, "Orders in quadratic imaginary fields of small class number", undergraduate degree, University of Warwick (2012), disponibilità http://www2.warwick.ac.uk/fac/cross_fac/complexity/people/students/dtc/students2013/klaise/janis_klaise_ug_report.pdf.

[9] A. Russo, "Proprietà di fattorizzazione per anelli di interi algebrici e gruppo delle classi", 2006, sintesi di Tesi di laurea in Matematica, Università degli Studi Roma Tre.

[10] A. Zaks, "Half factorial domains", Bull. Amer. Math. Soc. **82** (1976), 721–723.