Esempio di fattorizzazione in $\mathbb{Z}[\sqrt{-5}]$

1. Premesse

Sia K un campo quadratico, cioè un'estensione di grado 2 del campo razionale. Si può descrivere K come $\mathbb{Q}(\sqrt{d})$ per un opportuno intero d libero da quadrati. Se $d \not\equiv_4 1$, inoltre, l'anello degli interi I_K di K è $\mathbb{Z}[\sqrt{d}]$.

Ogni elemento di K si scrive (in modo unico) come $\alpha+\beta\sqrt{d}$ per opportuni $\alpha, \beta \in \mathbb{Q}$. Poiché il polinomio minimo di $\sqrt{d}$ su $\mathbb{Q}$, cioè $x^2 - d$, ha anche $-\sqrt{d}$ come radice, è una conseguenza del teorema di prolungamento per le estensioni semplici di campi che l'applicazione $\theta\colon \alpha + \beta\sqrt{d} \in K \mapsto \alpha - \beta\sqrt{d} \in K$ è un automorfismo del campo K. Per ogni $k = \alpha+\beta\sqrt{d}$ si chiama *norma* di k (rispetto all'estensione $K/\mathbb{Q}$) l'elemento $N(k) := kk^\theta = \alpha^2-d\beta^2 \in \mathbb{Q}$. L'applicazione norma $k \mapsto N(k)$, da K a $\mathbb{Q}$, è un omomorfismo tra le strutture moltiplicative; vale a dire $N(kl) = N(k)N(l)$ per ogni $k, l \in K$. Questo fatto segue subito dal fatto che θ è un automorfismo, ma si ricava anche facilmente dall'espressione esplicita di $N(k)$ come $\alpha^2-d\beta^2$. Si ha anche che $N(k) \in \mathbb{Z}$ se $k \in I_K$; di nuovo, la verifica si può effettuare direttamente, ma si può anche ricavare, e si tratta di un'osservazione di portata più generale, dal fatto che se $k \in I_K$ allora anche k^θ e quindi $N(k) = kk^\theta$ sono in I_K, ma $I_K \cap \mathbb{Q} = \mathbb{Z}$. Abbiamo così un omomorfismo moltiplicativo $N\colon I_K \to \mathbb{Z}$. Va osservato che gli invertibili di I_K sono precisamente gli elementi di norma 1 o -1 (cioè di norma invertibile in $\mathbb{Z}$): se $r \in I_K$ allora r , divide $rr^\theta = N(r)$, quindi r è invertibile se lo è $N(r)$ (ed il suo inverso è r^θ o $-r^\theta$); viceversa, se r è invertibile allora $1 = N(1) = N(rr^{-1}) = N(r)N(r^{-1})$, quindi $N(r)$ è invertibile in $\mathbb{Z}$. Una conseguenza ulteriore è che se due elementi r e s sono associati in I_K, allora $|N(r)| = |N(s)|$.

L'ultima cosa da ricordare è che, come tutti gli anelli degli interi dei campi che siano estensioni finite di $\mathbb{Q}$, I_K è un anello di Dedekind.

2. Il caso $d = -5$

Concentriamo l'attenzione sul caso in cui $d = -5$. Poiché $-5 \equiv_4 -1$, abbiamo in queso caso $I_K = \mathbb{Z}[\sqrt{-5}]$; chiamiamo R questo anello. Gli elementi di R hanno la forma $r = a + b\sqrt{-5}$, per opportuni $a, b \in \mathbb{Z}$, e si ha $N(r) = a^2 + 5b^2 \geq 0$. Dunque, l'immagine della funzione norma di R è contenuta in $\mathbb{N}$; inoltre $N(r)$ è o un quadrato perfetto, a^2, quando $b = 0$, oppure è maggiore di 4, quando $b \neq 0$.

Consideriamo queste due fattorizzazioni di 6 in R:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

I fattori 2, 3, $1 + \sqrt{-5}$ e $1 - \sqrt{-5}$ che appaiono in queste due fattorizzazioni hanno norme, rispettivamente, 4, 9, 6, 6. Dunque, nessuno di essi è invertibile in R; mostreremo ora che essi sono tutti irriducibili. Iniziamo da 2. Siano $r, s \in R$ tali che $2 = rs$. Allora $4 = N(2) = N(r)N(s)$. Le osservazioni svolte nel paragrafo precedente mostrano che nessun elemento di R ha norma 2; quindi uno tra r ed s deve avere norma 1 ed essere così invertibile. Ciò mostra che 2 non ha fattorizzazioni non banali, dunque 2 è irriducibile in R. Similmente, poiché nessun divisore non banale (in $\mathbb{N}$) di 9 o di 6 è la norma di un elemento di R, possiamo concludere che 3, $1 + \sqrt{-5}$ e $1 - \sqrt{-5}$ sono irriducibili in R. Dal confronto delle norme sappiamo anche che né 2 né 3 è associato ad uno tra $1 + \sqrt{-5}$ e $1 - \sqrt{-5}$. Abbiamo così trovato in R due fattorizzazioni in irriducibili essenzialmente diverse di 6; sappiamo così che R non è fattoriale.

Poiché R è di Dedekind, possiamo però fattorizzare (in modo unico) l'ideale $6R$ come prodotto di ideali primi in R; vediamo come. Essendo $6R = 2R \cdot 3R$, basterà fattorizzare separatamente $2R$ e $3R$. Né 2 né 3 dividono (in R) $1+\sqrt{-5}$ o $1 - \sqrt{-5}$, il cui prodotto, 6, è in $2R \cap 3R$. È dunque chiaro che $2R$ e $3R$ non sono primi.

Partiamo da $2R$. Gli elementi di $2R$ sono quelli della forma $a + b\sqrt{-5}$ tali che a e b siano entrambi (interi) pari. Da ciò segue che, per ogni $a, b, a', b' \in \mathbb{Z}$, i laterali $(a + b\sqrt{-5}) + 2R$ e $(a' + b'\sqrt{-5}) + 2R$ coincidono se e solo se $a \equiv_2 a'$ e $b \equiv_2 b'$. Ne segue che $|R/2R| = 4$.[1] Sia P un ideale primo divisore di $2R$. Allora, per quanto appena visto, $|R/P| = |P/2R| = 2$, quindi P sarà generato da 2 e da un qualsiasi elemento in $P \setminus 2R$. Ora, $(1+\sqrt{-5})(1-\sqrt{-5}) \in P$, quindi almeno uno tra $1 + \sqrt{-5}$ e $1 - \sqrt{-5}$ è in P. La somma tra questi due elementi è 2, che è in P, quindi entrambi sono in P. Dunque:

$$P = 2R + (1 + \sqrt{-5})R.$$

Troviamo così che $2R$ è contenuto in un solo ideale primo. Poiché R è un anello di Dedekind, ne segue che $2R$ è una potenza di P, diciamo $2R = P^n$. Ora, $n > 1$; se fosse $n > 2$ si avrebbe $2R \subset P^2 \subset P$, impossibile perché $|P : 2R| = 2$. Dunque $2R = P^2$.[2]

[1] questo è un caso particolare di un risultato generale: se R è l'anello degli interi di un campo di numeri e $0 \neq a \in R$, allora $|R : aR| = |N(a)|$.

[2] Ovviamente, anche se non necessario, è possibile verificare in modo diretto questa osservazione descrivendo esplicitamente gli elementi di P^2 e mostrando che essi sono multipli di 2, e osservando poi che $4 = 2 \cdot 2$ e $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ sono entrambi in P^2, quindi $2 = 6 - 4 \in P$.

Passiamo ora alla fattorizzazione di $3R$. In modo analogo a quanto fatto sopra, osserviamo che se $a, b \in \mathbb{Z}$, il laterale $(a + b\sqrt{-5}) + 3R$ è determinato dai resti modulo 3 di a e b, quindi $|R/3R| = 9$. Se Q è un ideale primo divisore di $3R$ abbiamo allora $|R/Q| = |Q/3R| = 3$, e $Q = 3R + rR$ comunque si scelga $r \in Q \setminus 3R$. Dal fatto che $(1 + \sqrt{-5})(1 - \sqrt{-5}) \in 3R \subset Q$ si ha che uno tra $1 + \sqrt{-5}$ e $1 - \sqrt{-5}$ è in Q (e, ovviamente, non in $3R$). Abbiamo così due possibili candidati (e nessun altro!) ad essere divisori primi di $3R$:

$$Q_1 = 3R + (1 + \sqrt{-5})R \qquad \text{e} \qquad Q_2 = 3R + (1 - \sqrt{-5})R.$$

Sia Q_1 che Q_2 sono ideali primi. Lo si può dimostrare o verificando in modo diretto (facendo calcoli sugli elementi di questi ideali) che $1 \notin Q_1 \cup Q_2$, quindi ciascuno dei due ideali è proprio e dunque necessariamente di indice 3 in R, quindi massimale, oppure, meglio, ragionando come segue. Almeno uno dei due deve essere primo, perché $3R$ ha almeno un divisore primo. L'automorfismo $\theta\colon \alpha + \beta\sqrt{-5} \mapsto \alpha - \beta\sqrt{-5}$ di $K = \mathbb{Q}(\sqrt{-5})$, menzionato tra le premesse, fissa R (l'anello degli interi di K) e scambia tra loro Q_1 e Q_2. Dunque, se uno tra Q_1 e Q_2 è primo in R (cosa che sappiamo vera) anche l'altro deve esserlo; pertanto sia Q_1 che Q_2 sono primi. È ancora importante notare che $Q_1 \neq Q_2$: se così non fosse Q_1 dovrebbe contenere $2 = (1 + \sqrt{-5}) + (1 - \sqrt{-5})$, ma ciò è impossibile perché $3R + 2R = R$. Ora, $3R \subseteq Q_1 \cap Q_2 \subset Q_1$; poiché come visto sopra $|Q_1/3R| = 3$, deduciamo $3R = Q_1 \cap Q_2$. Ma Q_1 e Q_2 sono massimali, quindi coprimi, e si ha dunque $Q_1 \cap Q_2 = Q_1Q_2$. Abbiamo così trovato la fattorizzazione cercata: $3R = Q_1Q_2$.

In conclusione, la fattorizzazione di $6R$ in prodotto di ideali primi di R è

$$6R = P^2Q_1Q_2.$$

Possiamo notare che le due fattorizzazioni di 6 in irriducibili di R da cui eravamo partiti si ricavano da questa fattorizzazione di $6R$. Infatti, come visto, $P^2 = 2R$ e $Q_1Q_2 = 3R$ (che ci mostrerebbe, se ce ne fosse bisogno, che $6R = 2R \cdot 3R$ e quindi $2 \cdot 3$ è associato a 6) ma abbinando diversamente i fattori, possiamo scrivere $6R$ come $(PQ_1)(PQ_2)$. Come non è difficile verificare, direttamente o con argomentazioni simili a quelle svolte sopra, $PQ_1 = (1 + \sqrt{-5})R$ e $PQ_2 = (1 - \sqrt{-5})R$, che da sole avrebbero già mostrato che 6 è associato al prodotto $(1 + \sqrt{-5})(1 - \sqrt{-5})$.

Esercizio. Così come osservato in una nota per l'ideale P, anche gli ideali Q_1 e Q_2 si possono ottenere come nuclei di omomorfismi di anelli unitari, che si possono definire, in modo generale, per tutti gli anelli della forma $\mathbb{Z}[\sqrt{d}]$, per un intero d.

Siano n e k interi tali che $n \neq 0$ e $k^2 \equiv_n d$. Allora l'applicazione $\varphi\colon a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}] \mapsto [a + kb]_n \in \mathbb{Z}_n$ è un omomorfismo di anelli unitari. Verificarlo, e verificare anche che, per $d = -5$ si ha: se $n = 2$ e $k = 1$, φ coincide con l'omomorfismo $r \in \mathbb{Z}[\sqrt{-5}] \mapsto [N(r)]_2 \in \mathbb{Z}_2$ già descritto, il cui nucleo è P, mentre se $n = 3$ il nucleo di φ è Q_1 se $k = -1$ ed è Q_2 se $k = 1$.

Un'altra osservazione (inutile) è che P è costituito precisamente dagli elementi $a + b\sqrt{-5} \in R$ tali che $a \equiv_2 b$; in effetti si può verificare che l'applicazione $r \in R \mapsto [N(r)]_2 \in \mathbb{Z}_2$ è un omomorfismo di anelli unitari, il cui nucleo è P.