

ESERCIZI SU
DIVISIBILITÀ E FATTORIZZAZIONE

N.B.: il simbolo $\hat{\mathbb{Z}}$ contrassegna gli esercizi (relativamente) più complessi.

— * —

1 — Sia D un dominio a fattorizzazione unica (o “dominio atomico”). Dimostrare che
ogni irriducibile (in D) è primo $\iff D$ è dominio a fattorizzazione unica.

2 — Sia D un dominio a fattorizzazione unica e sia $Q(D)$ il suo campo dei quozienti. Per ogni $p \in D$ irriducibile in D , si consideri il sottoinsieme di $Q(D)$ definito da

$$D_{(p)} := \left\{ a/b \in Q(D) \mid a, b \in D, b \neq 0, b \notin (p) \right\}$$

- (a) Dimostrare che $D_{(p)}$ è un sottoanello di $Q(D)$;
- (b) calcolare il gruppo $U(D_{(p)})$ degli invertibili di $D_{(p)}$.
- (c) dimostrare che $D_{(p)}$ è anello euclideo, con valutazione $v : D_{(p)} \longrightarrow \mathbb{N} \cup \{-\infty\}$ definita da $v(0) := -\infty$ e $v(a/b) := n \iff a \in (p^n) \setminus (p^{n+1})$;
- (d) $\hat{\mathbb{Z}}$ dimostrare che nella divisione con resto in $D_{(p)}$, si ha sempre che o il quoziente è nullo oppure il resto è nullo.

Suggerimento: È la diretta generalizzazione dell’analogo risultato già noto per $D := \mathbb{Z}$.

Si osservi in particolare che ogni elemento $t \in D \setminus \{0\}$ si scrive in modo unico nella forma $t = p^{v(t)} n/d$ con $n/d \in Q(D)$ e $n \in D \setminus (p)$.

Per la parte (d), si dimostri che nella divisione con resto di un elemento $a \in D_{(p)} \setminus \{0\}$ per un elemento $b (\neq 0)$, per il quoziente q e il resto r si ha esattamente

$$q = 0 \iff v(a) \geq v(b) \quad , \quad r = 0 \iff v(a) \leq v(b)$$

Le due implicazioni “ $\Leftarrow$ ” sono le più facili...

3 — Sia D un dominio unitario e sia $p \in D$ un primo in D tale che $\bigcap_{n=0}^{+\infty} (p^n) = \{0\}$. Detto $Q(D)$ il campo dei quozienti di D , definiamo

$$D_{(p)} := \left\{ a/b \in Q(D) \mid a, b \in D, b \neq 0, b \notin (p) \right\}$$

- (a) Dimostrare che $D_{(p)}$ è un sottoanello di $Q(D)$;
- (b) calcolare il gruppo $U(D_{(p)})$ degli invertibili di $D_{(p)}$.
- (c) dimostrare che $D_{(p)}$ è anello euclideo, con valutazione $v : D_{(p)} \longrightarrow \mathbb{N} \cup \{-\infty\}$ definita da $v(0) := -\infty$ e $v(a/b) := n \iff a \in (p^n) \setminus (p^{n+1})$;

(d) $\Leftrightarrow$ dimostrare che nella divisione con resto in $D_{(p)}$, si ha sempre che o il quoziente è nullo oppure il resto è nullo.

Suggerimento: È una diretta estensione del risultato dell'esercizio 3 qui sopra, e si simostra in modo del tutto analogo.

4 — Si consideri il dominio unitario $\mathbb{Z}[\sqrt{-5}]$ — sottoanello unitario di $\mathbb{C}$ generato da $\sqrt{-5}$ — e in esso l'insieme

$$\mathcal{T} := \{ \zeta \in \mathbb{Z}[\sqrt{-5}] \mid N(\zeta) = 9 \}$$

dove N è la norma in $\mathbb{C}$, che per ogni $\zeta = a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ vale ovviamente $N(\zeta) = N(a + b\sqrt{-5}) = a^2 + 5b^2$. Dimostrare che:

- (a) $\mathcal{T} := \{ 3, -3, (2 + \sqrt{-5}), (-2 - \sqrt{-5}), (2 - \sqrt{-5}), (-2 + \sqrt{-5}) \}$;
- (b) ogni elemento di $\mathcal{T}$ è irriducibile ma non è primo;
- (c) $\mathbb{Z}[\sqrt{-5}]$ è un dominio a fattorizzazione (o “dominio atomico”);
- (d) $\mathbb{Z}[\sqrt{-5}]$ non è un dominio a fattorizzazione unica;
- (e) $\mathbb{Z}[\sqrt{-5}]$ non è un anello a ideali principali;
- (f) $\mathbb{Z}[\sqrt{-5}]$ non è un anello euclideo.

Suggerimento: Si osservi che le diverse richieste sono tra loro collegate, e così possono esserlo le risposte...

5 — Nel dominio unitario $\mathbb{Z}[\sqrt{8}]$ — sottoanello unitario di $\mathbb{R}$ generato da $\sqrt{8}$ — determinare quali tra gli elementi $(1 + 3\sqrt{8})$, $(4 - \sqrt{8})$, $(-21 + 8\sqrt{8})$ siano (eventualmente) tra loro associati.

Suggerimento: Si ricordi che in un dominio unitario D la condizione perché due elementi a e b siano associati è la seguente: $a \sim b \iff \exists \varepsilon \in U(D) : a = \varepsilon b$.

Pertanto, basta calcolare il rapporto (come numero in $\mathbb{R}$, o semplicemente in $\mathbb{Q}[\sqrt{2}]$...) tra due dei numeri assegnati, e verificare se appartiene a $U(\mathbb{Z}[\sqrt{8}])$, cioè se sta in $\mathbb{Z}[\sqrt{8}]$ ed è invertibile; a tal scopo, si ricordi la formula

$$\frac{a + b\sqrt{8}}{c + d\sqrt{8}} = \frac{a + b\sqrt{8}}{c + d\sqrt{8}} \cdot \frac{c - d\sqrt{8}}{c - d\sqrt{8}} = \frac{(a + b\sqrt{8})(c - d\sqrt{8})}{c^2 - d^2 8}$$

Così facendo, alla fine si trova il solo caso $(1 + 3\sqrt{8}) \sim (-21 + 8\sqrt{8})$.

6 — Si consideri il dominio unitario $\mathbb{Z}[\sqrt{-11}]$ — sottoanello unitario del campo $\mathbb{C}$ dei numeri complessi generato da $\sqrt{-11}$.

- (a) Dimostrare che $\mathbb{Z}[\sqrt{-11}]$ è un dominio a fattorizzazione (o “dominio atomico”);
 (b) dimostrare che $\mathbb{Z}[\sqrt{-11}]$ non è un dominio a fattorizzazione unica;
 (c) determinare — se esiste... — un elemento di $\mathbb{Z}[\sqrt{-11}]$ che sia *irriducibile* ma non sia primo;
 (d) determinare due fattorizzazioni in irriducibili — o “atomi” — in $\mathbb{Z}[\sqrt{-11}]$ tra loro *non equivalenti* per ciascuno dei due elementi 15 e 45.

Suggerimento: Le diverse richieste sono tra loro collegate, quindi possono esserlo anche le risposte...

7 — Dato un numero dispari $d \in (2\mathbb{N}_+ + 1)$ maggiore o uguale di 3, si consideri il dominio unitario $\mathbb{Z}[\sqrt{-d}]$ — sottoanello unitario del campo $\mathbb{C}$ dei numeri complessi generato da $\sqrt{-d}$.

- (a) Dimostrare che $\mathbb{Z}[\sqrt{-d}]$ è un dominio a fattorizzazione (o “dominio atomico”);
 (b) dimostrare che $\mathbb{Z}[\sqrt{-d}]$ non è un dominio a fattorizzazione unica;
 (c) dimostrare che esistono elementi di $\mathbb{Z}[\sqrt{-d}]$ che sono *irriducibili* ma non primi;
 (d) determinare un elemento non nullo e non invertibile in $\mathbb{Z}[\sqrt{-d}]$ per il quale esistano due fattorizzazioni in irriducibili — o “atomi” — tra loro *non equivalenti*.

Suggerimento: Si tratta di generalizzare gli analoghi risultati già considerati negli esercizi 4 e 6 qui sopra. In particolare, si consideri l'elemento $(1+d) \in \mathbb{Z}[\sqrt{-d}]$. Abbiamo $(1+d) \in \mathbb{Z}$ e quindi esiste una fattorizzazione in interi irriducibili della forma $(1+d) = p_1 \cdots p_h$, con $p_1, \dots, p_h \in \mathbb{Z}$; considerando la norma di tali numeri, si trova che ciascun p_i è irriducibile anche nell'anello $\mathbb{Z}[\sqrt{-d}]$. Inoltre si ha $(1+d) = (1+\sqrt{d})(1-\sqrt{d})$, e chiaramente ciascun p_i non divide nè il fattore $(1+\sqrt{d})$ né il fattore $(1-\sqrt{d})$; ne segue che ogni p_i non è primo in $\mathbb{Z}[\sqrt{-d}]$, sebbene sia irriducibile: ciò risponde al quesito (c), che a sua volta implica il punto (b) in forza dell'esercizio 1. Se poi fattorizziamo in prodotto di irriducibili — nell'anello $\mathbb{Z}[\sqrt{-d}]$, una volta che sia provato il punto (a) — ciascuno dei due fattori $(1+\sqrt{d})$ e $(1-\sqrt{d})$, otteniamo una seconda fattorizzazione di $(1+d)$ in irriducibili che, per quanto già visto, non può essere equivalente a $(1+d) = p_1 \cdots p_h$.

8 — Nell'anello $\mathbb{Z}[i]$ degli interi di Gauss, si fattorizzino 168 e 3150 come prodotto di irriducibili (=“atomi”).

Suggerimento: Una possibile soluzione è $168 = (1+i)^3 \cdot (1-i)^3 \cdot 3 \cdot 7$ per il primo e $3150 = 3^2 \cdot 7 \cdot (1+i) \cdot (1-i) \cdot (1+2i)^2 \cdot (1-2i)^2$ per il secondo, ma sono ovviamente possibili delle varianti...

In ogni caso, visto che i numeri in esame sono degli interi, la strategia standard per

ottenerne una fattorizzazione è questa: prima si fattorizza il numero dato in $\mathbb{Z}$ — cioè come prodotto di interi irriducibili (in $\mathbb{Z}$) — e poi ciascuno degli interi irriducibili in tale fattorizzazione deve essere a sua volta fattorizzato in interi di Gauss irriducibili. Ad esempio, si ha $6 = 2 \cdot 3$, e poi $2 = (1+i) \cdot (1-i)$ mentre 3 è irriducibile (anche) in $\mathbb{Z}[i]$.

9 — Sia D un dominio a fattorizzazione unica, sia $Q(D)$ il suo campo dei quozienti, e sia $p \in D$ un elemento irriducibile in D . Dimostrare che:

(a) non esiste un elemento $\pi \in Q(D)$ tale che $\pi^2 = p$ (in parole, non esiste in $Q(D)$ una “radice quadrata” di p);

(b) il polinomio $(x^2 - p)$ è irriducibile in $Q(D)[x]$.

Suggerimento: Per la parte (a), si scriva π come frazione $\pi = a/b$ e poi da $\pi^2 = p$ si scriva la relazione corrispondente $a^2 = pb^2$; infine, si fattorizzino in irriducibili sia a^2 che pb^2 , e si analizzi il risultato... Per la parte (b), si osservi che $(x^2 - p)$ è riducibile in $Q(D)[x]$ se e soltanto ha una radice in $Q(D)$, ovvero se e soltanto se esiste $\pi \in Q(D)$ tale che $\pi^2 = p$; quindi la conclusione egue dalla parte (a).

10 — Sia $\{p_1, \dots, p_k\}$ un insieme finito di irriducibili in $\mathbb{Z}$, e sia $\mathbb{Z}_{\{p_1, \dots, p_k\}}$ il corrispondente sottoinsieme di $\mathbb{Q}$ definito da

$$\mathbb{Z}_{\{p_1, \dots, p_k\}} := \left\{ p_1^{e_1} \cdots p_k^{e_k} z \mid e_1 \in \mathbb{Z}, \dots, e_k \in \mathbb{Z}, z \in \mathbb{Z} \right\} \quad (\subseteq \mathbb{Q})$$

(a) Dimostrare che $\mathbb{Z}_{\{p_1, \dots, p_k\}}$ è un sottoanello di $\mathbb{Q}$ contenente $\mathbb{Z}$.

(b) Calcolare il gruppo degli invertibili $U(\mathbb{Z}_{\{p_1, \dots, p_k\}})$.

(c) $\diamond_{\mathbb{Z}}$ Dimostrare che $\mathbb{Z}_{\{p_1, \dots, p_k\}}$ è un dominio a fattorizzazione unica.

11 $\diamond_{\mathbb{Z}}$ — Sia D un dominio a fattorizzazione unica e sia $Q(D)$ il suo campo dei quozienti. Fissiamo un sottoinsieme Π di elementi irriducibili in D , e consideriamo

$$D_{\Pi} := \left\{ q_1^{e_1} \cdots q_n^{e_n} d \mid n \in \mathbb{N}, q_1, \dots, q_n \in \Pi, e_1, \dots, e_n \in \mathbb{Z}, d \in D \right\} \quad (\subseteq Q(D))$$

(a) Dimostrare che D_{Π} è un sottoanello di $Q(D)$ contenente D .

(b) Calcolare il gruppo degli invertibili $U(D_{\Pi})$.

(c) $\diamond_{\mathbb{Z}}$ Dimostrare che D_{Π} è un dominio a fattorizzazione unica.

Suggerimento: Si tratta di una diretta generalizzazione dell’esercizio 10 qui sopra — che corrisponde a $D := \mathbb{Z}$ e $\Pi := \{p_1, \dots, p_k\}$ — e si può dimostrare allo stesso modo.