ESERCIZI SU

ANELLI EUCLIDEI E ANELLI A IDEALI PRINCIPALI

N.B.: il simbolo ⛑ *contrassegna gli esercizi (relativamente) più complessi.*

— ∗ —

1 — Sia A un anello commutativo unitario. Dimostrare che

$$A \text{ è un campo } \iff A \text{ ha soltanto gli ideali } \textit{banali}, \text{ ossia } \{0\} \text{ e } A\,.$$

In particolare, ogni campo è un anello a ideali principali.

Suggerimento: *Segue dal fatto che* A *è campo* $\iff A \setminus \{0\} = U(A)$, *insieme al fatto che* $(\varepsilon) = (1) = A$ *per ogni* $\varepsilon \in U(A)$.

2 — Sia A un anello commutativo unitario tale che $A[x]$ sia anello a ideali principali. Dimostrare che ogni $\alpha \in A \setminus \{0\}$ che non sia divisore dello zero è invertibile in A .

Suggerimento: *Si consideri il sottoinsieme* $\mathcal{J}_\alpha$ *di* $A[x]$ *dato da*

$$\mathcal{J}_\alpha := \left\{ f(x) = a_0 + a_1\,x + a_2\,x^2 + \cdots \;\middle|\; a_k \in A \;\forall\, k \geq 0\,,\, a_0 \in (\alpha) := A\,\alpha \right\} .$$

Tale $\mathcal{J}_\alpha$ *è ideale di* $A[x]$, *quindi è principale, diciamo* $\mathcal{J}_\alpha = \big(g(x)\big)$ *per un opportuno* $g(x) \in \mathcal{J}_\alpha$, *dunque* $g(x) = a'_0 + a'_1\,x + a'_2\,x^2 + \cdots$ *con* $a'_0 \in (\alpha)$, *dunque* $a'_0 = \alpha\,z$ *con* $z \in A$. *In particolare scegliamo* $f_\bullet(x) = a_0 + a_1\,x + a_2\,x^2 + \cdots$ *con* $a_0 = \alpha$ *: allora abbiamo* $f_\bullet(x) \in \mathcal{J}_\alpha = \big(g(x)\big)$, *così* $f_\bullet(x) = g(x)\,\ell_\bullet(x)$ *per un opportuno* $\ell_\bullet(x) \in A[x]$, *diciamo* $\ell_\bullet(x) = u_0 + u_1\,x + u_2\,x^2 + \cdots$. *Ne segue che*

$$a_0 + a_1\,x + a_2\,x^2 + \cdots \;=\; f_\bullet(x) \;=\; g(x)\,\ell_\bullet(x)(x) \;=\; a'_0\,u_0 + (a'_0\,u_1 + a'_1\,u_0)\,x + \cdots$$

implica $a'_0\,u_0 = \alpha$, *che insieme a* $a'_0 = \alpha\,z$ *implica* $\alpha\,(1 - z\,u_0) = 0$. *Dato che* α *non è divisore di zero, ne deduciamo che* u_0 *è invertibile con* $u_0^{-1} = z$. *Allora* $g_+(x) := u_0\,g(x)$ *è anch'esso un generatore di* $\mathcal{J}_\alpha$, *cioè* $\mathcal{J}_\alpha = \big(g(x)\big) = \big(g_+(x)\big)$ *; lo scriviamo nella forma* $g_+(x) = a_0^+ + a_1^+\,x + a_2^+\,x^2 + \cdots$ *dove ora è* $a_0^+ = \alpha$. *Consideriamo ora* $f_\times(x) = a_0^\times + a_1^\times\,x + a_2^\times\,x^2 + \cdots$ *con* $a_0^\times = 0$ *e* $a_1^\times := 1$ *: in particolare allora* $f_\times(x) \in \mathcal{J}_\alpha = \big(g_+(x)\big)$, *così* $f_\times(x) = g_+(x)\,\ell_\times(x)$ *per un opportuno* $\ell_\times(x) \in A[x]$, *diciamo* $\ell_\times(x) = u_0^\times + u_1^\times x + u_2^\times x^2 + \cdots$. *Allora*

$$a_0^\times + a_1^\times x + a_2^\times x^2 + \cdots = f_\times(x) = g_+(x)\,\ell_\times(x) = a_0^+ u_0^\times + (a_0^+ u_1^\times + a_1^+ u_0^\times)\,x + \cdots$$

implica $a_0^+\,u_0^\times = a_0^\times$ *e* $a_0^+\,u_1^\times + a_1^+\,u_0^\times = a_1^\times$. *Ora, poiché* $a_0^\times = 0$, $a_1^\times = 1$ *e* $a_0^+ = \alpha$, *da queste identità segue* $\alpha\,u_0^\times = 0$ *e* $\alpha\,u_1^\times + a_1^+ u_0^\times = 1$, *dalle quali si deduce che* $u_0^\times = 0$, *e quindi anche* $\alpha\,u_1^\times = 1$ *; perciò* α *è invertibile, q.e.d.*

3 — Sia D un dominio unitario tale che $D[x]$ sia anello a ideali principali. Dimostrare che D è un campo (e quindi $D[x]$ è anche anello euclideo).

Suggerimento: *Basta applicare l'esercizio 2 qui sopra.*

4 — Sia A un sottoanello di $\mathbb{Q}$ contenente 1. Dimostrare che A è un anello a ideali principali.

Suggerimento: *Data una frazione $n/d \in A$ con $\mathrm{MCD}(n,d)=1$, si ha $1/d \in A$ (dimostrarlo!). In aggiunta, se I è un ideale di A allora se $n/d \in I$ — sempre con $\mathrm{MCD}(n,d)=1$ — si ha anche $n \in I$. Pertanto, per ogni $n/d \in A$ — con $\mathrm{MCD}(n,d)=1$ — si ha $n/d \in I \iff n \in I$. Ne segue che I è l'ideale di A generato dall'insieme $\mathcal{N}_I$ dei numeratori delle frazioni (scritte in forma ridotta) che contiene; ma tale $\mathcal{N}_I$ è anche un ideale di $\mathbb{Z}$, e come tale è principale, diciamo $\mathcal{N}_I = n_0\,\mathbb{Z}$, e questo implica che I a sua volta è generato (come ideale di A) dal solo elemento n_0, cioè $I = A\,n_0$ è principale.*

5 — Sia $\mathbb{Z}\big[\sqrt{-2}\,\big]$ il sottoinsieme di $\mathbb{C}$ definito da

$$\mathbb{Z}\big[\sqrt{-2}\,\big] \;:=\; \big\{\, a+b\,\sqrt{-2} \;\big|\; a,b \in \mathbb{Z} \,\big\}$$

Dimostrare che:

(a) $\mathbb{Z}\big[\sqrt{-2}\,\big]$ è il sottoanello di $\mathbb{C}$ generato dal sottoinsieme $\big\{1\,,\sqrt{-2}\,\big\}$;

(b) la funzione $\mathbb{Z}\big[\sqrt{-2}\,\big] \xrightarrow{\;v\;} \mathbb{N}\cup\{-\infty\}$ data da $v\big(a+b\,\sqrt{-2}\,\big) := a^2+2\,b^2$ $\big($per ogni $\big(a+b\,\sqrt{-2}\,\big) \in \mathbb{Z}\big[\sqrt{-2}\,\big]\big)$ è *moltiplicativa* — cioè è un morfismo dal semigruppo $\big(\mathbb{Z}\big[\sqrt{-2}\,\big]\,;\cdot\big)$ al semigruppo $\big(\mathbb{N}\cup\{-\infty\}\,;\cdot\big)$;

(c) $\mathbb{Z}\big[\sqrt{-2}\,\big]$ è anello euclideo con la funzione v definita in *(b)* come valutazione.

Suggerimento: *Si segue lo stesso procedimento utilizzato per l'anello degli interi di Gauss $\mathbb{Z}[i] = \mathbb{Z}\big[\sqrt{-1}\,\big]$. In particolare, la parte (b) si può dimostrare direttamente (con calcolo esplicito, a mano) ma segue anche immediatamente dal fatto che la funzione v è la restrizione della norma — per numeri complessi — al sottoanello $\mathbb{Z}\big[\sqrt{-2}\,\big]$ di $\mathbb{C}$.*

6 — Sia A un anello euclideo, con valutazione v. Dimostrare che per ogni $a,b \in A\setminus\{0\}$ si ha

$$v(a\,b) \,=\, v(a) \iff b \in U(A) \quad , \qquad v(a\,b) \gneqq v(a) \iff b \notin U(A) \;\;.$$

Suggerimento: *Siccome si ha sempre $v(a\,b) \geq v(a)$, è sufficiente dimostrare una delle due equivalenze. Se consideriamo la prima, si ricordi che per ogni ideale (c) — con $c \in A$ — qualunque suo generatore ha la stessa valutazione di c stesso, e viceversa ogni elemento di (c) che abbia la stessa valutazione di c è generatore dell'ideale (c). Ora, poiché $a\,b \in (a)$, deduciamo che $v(a\,b) = v(a) \iff (a\,b) = (a)$; perciò in conclusione basta dimostrare che $(a\,b) = (a) \iff b \in U(A)$.*

7 — Sia k un campo, e sia $k[x]$ il corrispondente anello dei polinomi in una variabile x a coefficienti in k, che sappiamo essere un anello euclideo (con la valutazione data dal grado). Dimostrare che, nella divisione con resto tra due polinomi (di cui il divisore sia non nullo) il quoziente e il resto sono sempre univocamente determinati.

Suggerimento: *Si tratta di dimostrare che, dati* $a(x), b(x) \in k[x]$ *con* $b(x) \neq 0$, *se*

$$a(x) = b(x)\,q_1(x) + r_1(x) \quad \text{con } r_1(x) = 0 \text{ oppure } r_1(x) \neq 0 \text{ e } \partial\big(r_1(x)\big) \lneqq \partial\big(b(x)\big)$$

e

$$a(x) = b(x)\,q_2(x) + r_2(x) \quad \text{con } r_2(x) = 0 \text{ oppure } r_2(x) \neq 0 \text{ e } \partial\big(r_2(x)\big) \lneqq \partial\big(b(x)\big)$$

allora $q_1(x) = q_2(x)$ *e* $r_1(x) = r_2(x)$. *A tal fine, osserviamo che le due uguaglianze* $b(x)\,q_1(x) + r_1(x) = a(x) = b(x)\,q_2(x) + r_2(x)$ *danno* $b(x)\big(q_1(x) - q_2(x)\big) = r_2(x) - r_1(x)$, *da cui confrontando i gradi si trova* $b(x)\big(q_1(x) - q_2(x)\big) = 0$ *e* $r_2(x) - r_1(x) = 0$, *da cui si conclude.*

8 — Dimostrare che $\mathbb{Z}[\,i\,]$ è isomorfo all'anello quoziente $\mathbb{Z}[x]\Big/\big(x^2+1\big)$.

Suggerimento: *Si cerchi un isomorfismo* $\phi : \mathbb{Z}[x]\Big/\big(x^2+1\big) \xrightarrow{\ \cong\ } \mathbb{Z}[\,i\,]$, *e quest'ultimo lo si cerchi come isomorfismo* φ_* *indotto dal Teorema Fondamentale di Isomorfismo a partire da un epimorfismo* $\varphi : \mathbb{Z}[x] \twoheadrightarrow \mathbb{Z}[\,i\,]$ *tale che* $Ker(\varphi) = \big(x^2+1\big)$. *In un tale epimorfismo si avrà necessariamente* $\varphi(1) = 1$ *da cui segue* $\varphi(z) = z$ *per ogni* $z \in \mathbb{Z}$; *inoltre, la condizione che* φ *sia un morfismo impone che* $\varphi\big(f(x)\big) = f\big(\varphi(x)\big)$ *per ogni* $f(x) \in \mathbb{Z}[x]$; *infine, la condizione che* $Ker(\varphi) = \big(x^2+1\big)$ *impone che sia* $\varphi(x)^2 + 1 = 0$, *quindi necessariamente* $\varphi(x) \in \{+i\,, -i\,\}$. *Ora, ciascuna delle due scelte per* $\varphi(x)$ *è lecita, e la definendo* $\varphi_+\big(f(x)\big) := f(+i)$ *oppure* $\varphi_-\big(f(x)\big) := f(-i)$ *per ogni* $f(x) \in \mathbb{Z}[x]$ *si ottengono due diversi epimorfismi* $\varphi_\pm : \mathbb{Z}[x] \twoheadrightarrow \mathbb{Z}[\,i\,]$, *ciascuno dei quali va bene come possibile "*φ*" del tipo cercato.*

Per costruzione si ha $\varphi_\pm\big(x^2+1\big) = 0$ *e quindi* $Ker(\varphi_\pm) \supseteq \big(x^2+1\big)$. *Per ottenere l'inclusione inversa, sia* $f(x) \in Ker(\varphi_\pm)$: *facendo la divisione con resto di* $a(x) := f(x)$ *per* $b(x) := x^2 + 1$ *nell'anello* $\mathbb{Z}[x]$ — *il che è possibile (anche se* $\mathbb{Z}$ *non è un campo!) perché il polinomio* $b(x) := x^2 + 1$ *è monico, cioè ha coefficiente direttivo* 1 — *otteniamo*

$$f(x) \;=\; \big(x^2+1\big)\,q(x) \,+\, r(x)$$
$$\text{con } \; r(x) = 0 \;\; \text{oppure} \;\; r(x) \neq 0 \;\; \text{e} \;\; \partial\big(r(x)\big) \lneqq \partial\big(x^2+1\big) = 2$$
$$\text{dunque} \;\; r(x) \,=\, a + b\,x \;\; \text{con } a, b \in \mathbb{Z}\,.$$

Ora, l'uguaglianza in prima linea implica

$$f(\pm i) \;=\; \big((\pm i)^2 + 1\big)\,q(\pm i) \,+\, r(\pm i) \;=\; r(\pm i) \;=\; a \pm i\,b$$

e d'altra parte

$$f(\pm i) \;=\; f\big(\varphi_\pm(x)\big) \;=\; \varphi_\pm\big(f(x)\big) \;=\; 0 \quad \text{perché} \quad f(x) \in Ker(\varphi_\pm)$$

perciò $a \pm i\,b \;=\; 0$, *così* $a = 0 = b$ *e dunque anche* $r(x) = 0$. *Pertanto* $f(x) = \big(x^2+1\big)\,q(x) + r(x) = \big(x^2+1\big)\,q(x) \in \big(x^2+1\big)$ *e quindi* $Ker(\varphi_\pm) \subseteq \big(x^2+1\big)$, *q.e.d.*

9 — Sia $\mathbb{Z}\big[\sqrt{-5}\,\big]$ il sottoanello di $\mathbb{C}$ definito da

$$\mathbb{Z}\big[\sqrt{-5}\,\big] \;:=\; \big\{\, z_0 + z_1\,\sqrt{-5} \;\big|\; z_0, z_1 \in \mathbb{Z} \,\big\}$$

Dimostrare che gli elementi $2\,, 3\,, \big(1+\sqrt{-5}\,\big)\,, \big(1-\sqrt{-5}\,\big) \in \mathbb{Z}\big[\sqrt{-5}\,\big]$ sono tutti *irriducibili* ma *non primi*.

Suggerimento: In perfetta analogia con l'esercizio 5 qui sopra, si consideri la funzione $v : \mathbb{Z}\big[\sqrt{-5}\,\big] \longrightarrow \mathbb{N} \cup \{-\infty\}$ *data da* $v\big(a + b\sqrt{-5}\,\big) := a^2 + 5\,b^2$ *e si verifichi che è moltiplicativa.*

Supponiamo ora che $2 = \alpha\,\beta$ *sia una fattorizzazione di* 2 *in* $\mathbb{Z}\big[\sqrt{-5}\,\big]$ *non banale, dunque con fattori* $\alpha\,, \beta \in \mathbb{Z}\big[\sqrt{-5}\,\big] \setminus U\big(\mathbb{Z}\big[\sqrt{-5}\,\big]\big)$*. Siccome* v *è moltiplicativa, abbiamo* $v(2) = v(\alpha\,\beta) = v(\alpha)\,v(\beta)$*, quindi* $v(2) = 4$ *si fattorizza in* $4 = v(\alpha)\,v(\beta)$*; in tale fattorizzazione non può essere* $v(\alpha) = 2 = v(\beta)$ *perché* $a^2 + 5\,b^2 \neq 2$ *(per ogni* $a, b \in \mathbb{Z}$*), e quindi dev'essere necessariamente* $v(\alpha) = 1$ *e* $v(\beta) = 4$ *oppure* $v(\alpha) = 4$ *e* $v(\beta) = 1$*: ma* $a^2 + 5\,b^2 \neq 1 \iff (a\,, b) = (\pm 1\,, 0) \iff a + b\sqrt{-5} = \pm 1$*, quindi si ha necessariamente* $\alpha = \pm 1 \in U\big(\mathbb{Z}\big[\sqrt{-5}\,\big]\big)$ *oppure* $\beta = \pm 1 \in U\big(\mathbb{Z}\big[\sqrt{-5}\,\big]\big)$*, che è una contraddizione. Quindi* 2 *è irriducibile, q.e.d.*

D'altra parte, 2 *non è primo, perché divide il prodotto* $6 = \big(1+\sqrt{-5}\,\big)\big(1-\sqrt{-5}\,\big)$ *— in quanto* $6 = 2 \cdot 3$ *— ma* 2 *non divide né l'uno né l'altro dei due fattori* $\big(1+\sqrt{-5}\,\big)$ *e* $\big(1-\sqrt{-5}\,\big)$*. Infatti, se fosse* $2 \,\Big|\, \big(1+\sqrt{-5}\,\big)$ *in* $\mathbb{Z}\big[\sqrt{-5}\,\big]$ *allora per la moltiplicatività di* v *avremmo* $2 \,\Big|\, \big(1+\sqrt{-5}\,\big) \implies 4 = v(2) \,\Big|\, v\big(1+\sqrt{-5}\,\big) = 6$*, che è impossibile perché* 4 *non divide* 6 *in* $\mathbb{N}$*. Allo stesso modo si prova che* 2 *non divide l'altro fattore* $\big(1-\sqrt{-5}\,\big)$*.*

In modo del tutto analogo si dimostra che anche $3\,,\ \big(1+\sqrt{-5}\,\big)$ *e* $\big(1-\sqrt{-5}\,\big)$ *sono irriducibili ma non primi.*

10 — Sia $\mathbb{Z}\big[\sqrt{-3}\,\big]$ il sottoanello di $\mathbb{C}$ definito da

$$\mathbb{Z}\big[\sqrt{-3}\,\big] \;:=\; \big\{\, z_0 + z_1\,\sqrt{-3} \;\big|\; z_0, z_1 \in \mathbb{Z} \,\big\}$$

Dimostrare che esistono in $\mathbb{Z}\big[\sqrt{-3}\,\big]$ degli elementi *irriducibili* ma *non primi*.

Suggerimento: È del tutto analogo all'esercizio 9 qui sopra, soltanto con qualche minima difficoltà in più.

11 — Sia $\mathbb{Z}\big[\sqrt{-7}\,\big]$ il sottoanello di $\mathbb{C}$ definito da

$$\mathbb{Z}\big[\sqrt{-7}\,\big] \;:=\; \big\{\, z_0 + z_1\,\sqrt{-7} \;\big|\; z_0, z_1 \in \mathbb{Z} \,\big\}$$

Dimostrare che esistono in $\mathbb{Z}\big[\sqrt{-7}\,\big]$ degli elementi *irriducibili* ma *non primi*.

Suggerimento: È del tutto analogo all'esercizio 10 qui sopra.

12 — Siano $\mathbb{K}$ e $\mathbb{F}$ due campi, con $\mathbb{K} \leq \mathbb{F}$, così che è anche $\mathbb{K}[x] \leq \mathbb{F}[x]$. Dati $h(x)\,,\ \ell(x) \in \mathbb{K}[x]$, dimostrare che il M.C.D. tra $h(x)$ ed $\ell(x)$ esistente in $\mathbb{K}[x]$ coincide — nel senso che sono associati, in $\mathbb{K}[x]$ — con il M.C.D. tra $h(x)$ ed $\ell(x)$ in $\mathbb{F}[x]$.

Suggerimento: *Siccome $\mathbb{K}[x] \leq \mathbb{F}[x]$, a priori $h(x)$ ed $\ell(x)$ possono avere più divisori in $\mathbb{F}[x]$ che in $\mathbb{F}[x]$, quindi la questione non è peregrina... Tuttavia, si ricordi che $\mathbb{K}[x]$ e $\mathbb{F}[x]$ sono entrambi anelli euclidei, quindi in entrambi il MCD$\big(h(x),\ell(x)\big)$ si calcola tramite l'algoritmo euclideo delle divisioni successive. In entrambi i casi, l'algoritmo comincia facendo la divisione di $h(x)$ per $\ell(x)$: ora, dato che $\mathbb{K}[x] \leq \mathbb{F}[x]$ e che quoziente e resto nella divisione in $\mathbb{F}[x]$ sono unici (per l'esercizio 7 qui sopra), la divisione di $h(x)$ per $\ell(x)$ dà lo stesso quoziente e lo stesso resto sia in $\mathbb{K}[x]$ che in $\mathbb{F}[x]$: iterando, i calcoli svolti nell'algoritmo delle divisioni successive risultano essere esattamente gli stessi (con gli stessi passaggi) sia in $\mathbb{K}[x]$ che in $\mathbb{F}[x]$, da cui segue la conclusione.*

13 — Dati $a\,,\ b \in \mathbb{Z}$, dimostrare che il M.C.D. tra a e b esistente in $\mathbb{Z}$ coincide — nel senso che sono associati in $\mathbb{Z}$, dunque uguali a meno (eventualmente) del segno — con il M.C.D. tra a e b nell'anello $\mathbb{Z}[\,i\,]$ degli interi di Gauss.

Suggerimento: *È analogo all'esercizio 12 qui sopra (in particolare, il quesito è sensato perché siccome $\mathbb{Z} \leq \mathbb{Z}[\,i\,]$, a priori a e b possono avere più divisori in $\mathbb{Z}[\,i\,]$ che in $\mathbb{Z}$). Nello specifico, il metodo di calcolo di quoziente e resto per la divisione euclidea in $\mathbb{Z}[\,i\,]$ applicato ad $a, b \in \mathbb{Z}$ ci dà quoziente e resto ancora in $\mathbb{Z}$, cioè ci permette di calcolare la divisione euclidea tra a e b nel sottoanello $\mathbb{Z}$. Ne segue che l'algoritmo euclideo delle divisioni successive per il calcolo di MCD(a,b) inizia con la stessa formula (una divisione) sia effettuandolo in $\mathbb{Z}$ che in $\mathbb{Z}[\,i\,]$, e quindi poi iterativamente anche i passaggi successivi sono tutti uguali, da cui segue la conclusione.*

14 — Dati $a\,,\ b \in \mathbb{Z}$, dimostrare che

$$a \text{ divide } b \text{ nell'anello } \mathbb{Z} \iff a \text{ divide } b \text{ nell'anello } \mathbb{Z}[\,i\,]\ .$$

Suggerimento: *Segue dall'esercizio 13 qui sopra insieme all'osservazione che in ogni anello commutativo unitario si ha $a \,\big|\, b \iff \exists\ MCD(a,b) = a$.*

15 — Nell'anello $\mathbb{Z}[\,i\,]$ si calcoli $\mathrm{MCD}\big(4-3\,i\,,\ 1+2\,i\big)$ e un'identità di Bézout per esso.

16 — Per ciascuno dei possibili campi $\mathbb{K} \in \big\{\mathbb{Q}\,,\mathbb{Z}_5\,,\mathbb{Z}_7\big\}$, si calcolino $\mathrm{MCD}\big(h(x)\,,\ \ell(x)\big)$ e un'identità di Bézout per esso nei due casi

(a) $\quad h(x) := x^3 - 6\,x^2 + x + 4\ ,\quad \ell(x) := x^5 - 6\,x + 1\ ;$

(b) $\quad h(x) := x^2 + 1\ ,\quad \ell(x) := x^6 + x^3 + x + 1\ .$

17 — Nell'anello $\mathbb{Z}[\,i\,]$ degli interi di Gauss si calcoli — se esiste... — una soluzione dell'equazione diofantea $(5-i)\,x+(1-4\,i)\,y\,=-2+3\,i$.

18 — Nell'anello $\mathbb{Q}[x]$ si calcoli — se esiste... — una soluzione dell'equazione diofantea $\big(x^3-2\,x+1\big)\,h(x)+\big(x^4-3\big)\,k(x)\,=x$ nelle incognite (polinomiali) $h(x)$ e $k(x)$.

19 — Nell'anello quoziente $\mathbb{Z}_7[x]\Big/\big(\,3\,x^2-x+1\,\big)$ si risolvano le seguenti equazioni (modulari) nell'incognita $\overline{p(x)}$:

(a) $\overline{\big(4\,x+3\big)}\cdot\overline{p(x)}\,=\,\overline{3\,x-2}$;

(b) $\overline{\big(2\,x^3+5\,x^2-11\big)}\cdot\overline{p(x)}\,=\,\overline{-2\,x+1}$;

(c) $\overline{\big(x^4-5\,x^2-2\,x+1\big)}\cdot\overline{p(x)}\,=\,\overline{12\,x^3-2\,x+5}$.

Suggerimento : *Nelle equazioni in esame, ogni polinomio (rappresentante di una classe) può essere sostituito — dividendolo per* $\big(\,3\,x^2-x+1\,\big)$ *e prendendo il resto — con un altro polinomio ad esso congruente modulo* $\big(\,3\,x^2-x+1\,\big)$ *ma di grado minore di 2 (o eventualmente nullo).*

20 — Nell'anello $\mathbb{Q}[x]$ si calcoli un generatore dell'ideale

$$I\,:=\,\big(\,x^3+x^2-x-1\,,\;x^4-2\,x^2+1\,,\;x^5-x^3\,\big)\ .$$

Suggerimento: *Si ricordi che in un anello euclideo A un ideale $I=(a_1,a_2):=\big(\{a_1,a_2\}\big)$ generato da due elementi a_1 e a_2 è anche generato dal singolo elemento* $\mathrm{MCD}(a_1,a_2)$ *; iterando, si ha anche $I=(a_1,a_2,\ldots,a_k):=\big(\{a_1,a_2,\ldots,a_k\}\big)$ per un ideale generato da k elementi $a_1,a_2,\ldots,a_k$.*

21 — Nell'anello quoziente $\mathbb{Z}[\,i\,]\Big/\big(1-4\,i\,\big)$ si determini se la classe $\alpha:=\overline{(5+i\,)}$ sia invertibile oppure no. In caso negativo, si spieghi perché tale classe non sia invertibile; in caso affermativo, si calcoli esplicitamente la classe inversa $\alpha^{-1}=\overline{(5+i\,)}^{\,-1}$.

Suggerimento: *Il problema posto equivale alla discussione e risoluzione dell'equazione modulare* $\overline{(5+i\,)}\cdot\overline{x}=\overline{1}$ *in* $\mathbb{Z}[\,i\,]\Big/\big(1-4\,i\,\big)$, *che equivale all'equazione congruenziale* $(5+i\,)\,x\equiv_{(1-4\,i\,)}1$ *in* $\mathbb{Z}[\,i\,]$, *la quale a sua volta equivale all'equazione diofantea — ancora in* $\mathbb{Z}[\,i\,]$ — $(5+i\,)\,x+(1-4\,i\,)\,y\,=\,1$. *Quest'ultima avrà soluzioni se e soltanto se* $MCD\big(\,5+i\,,\,1-4\,i\,\big)\sim 1$, *e in tal caso un'identità di Bézout per* $MCD\big(\,5+i\,,\,1-4\,i\,\big)$ *ci darà una coppia (x_0,y_0) soluzione dell'equazione diofantea: sia il* $MCD\big(\,5+i\,,\,1-4\,i\,\big)$ *che un'identità di Bézout per esso si trovano mediante l'algoritmo euclideo delle divisioni successive. Se dunque* $MCD\big(\,5+i\,,\,1-4\,i\,\big)\sim 1$, *dalla coppia (x_0,y_0) otteniamo che x_0*

è soluzione dell'equazione congruenziale $(5+i)\,x \equiv_{(1-4\,i)} 1$ *in* $\mathbb{Z}[\,i\,]$ *e quindi poi* $\overline{x_0}$ *è soluzione dell'equazione modulare* $\overline{(5+i)}\cdot\overline{x} = \overline{1}$ *in* $\mathbb{Z}[\,i\,]\Big/\big(1-4\,i\big)$ *di partenza, così che in conclusione* $\overline{(5+i)}^{\,-1} = \overline{x_0}$ *.*

22 — Dimostrare che l'anello quoziente $\mathbb{Q}[x]\Big/\big(x^2-3\big)$ è un campo.

Suggerimento: Si tratta di dimostrare che, per ogni $p(x) \in \mathbb{Q}[x]$ *, la classe* $\overline{p(x)} \in \mathbb{Q}[x]\Big/\big(x^2-3\big)$ *se è diversa dalla classe nulla è invertibile. Questo corrisponde a dire che se* $p(x) \notin \big(x^2-3\big) = \mathbb{Q}[x]\cdot\big(x^2-3\big)$ *, cioè se* $p(x)$ *non è divisibile per* $\big(x^2-3\big)$ *, allora* $\overline{p(x)}$ *è invertibile in* $\mathbb{Q}[x]\Big/\big(x^2-3\big)$ *. Quest'ultima affermazione corrisponde a dire che esiste soluzione dell'equazione modulare* $\overline{p(x)}\cdot\overline{X} = \overline{1}$ *in* $\mathbb{Q}[x]\Big/\big(x^2-3\big)$ *nell'incognita* $\overline{X}$ *, il che a sua volta equivale a dire che esistono soluzioni dell'equazione congruenziale* $p(x)\cdot X \equiv_{(x^2-3)} 1$ *in* $\mathbb{Q}[x]$ *, la quale infine equivale all'equazione diofantea — ancora in* $\mathbb{Q}[x]$ *, nelle due variabili* X *e* Y *—* $p(x)\,X + \big(x^2-3\big)\,Y = 1$ *. Quest'ultima avrà soluzioni se e soltanto se* $MCD\big(\,p(x)\,,\,x^2-3\,\big) \sim 1$ *, e in tal caso un'identità di Bézout per* $MCD\big(\,p(x)\,,\,x^2-3\,\big) \sim 1$ *ci darà una coppia* (X_0, Y_0) *soluzione dell'equazione diofantea, da cui poi alla fine si otterrà* $\overline{X_0} = \overline{p(x)}^{\,-1}$ *.*

Per calcolare $MCD\big(\,p(x)\,,\,x^2-3\,\big)$ *e un'identità di Bézout per esso usiamo l'algoritmo euclideo delle divisioni successive. Dividendo* $p(x)$ *per* x^2-3 *troviamo*

$$p(x) \;=\; \big(x^2-3\big)\,q_1(x) \,+\, r_1(x) \tag{1}$$

per certi $q_1(x), r_1(x) \in \mathbb{Q}[x]$ *con* $r_1(x) = 0$ *oppure* $r_1(x) \neq 0$ *e* $\partial\big(r_1(x)\big) \lneqq \partial\big(x^2-3\big) = 2$ *: dunque in ogni caso sarà* $r_1(x) = a + b\,x$ *per opportuni* $a, b \in \mathbb{Q}$ *. Ora,* $r_1(x) = 0$ *se e soltanto se* $p(x)$ *è multiplo di* $\big(x^2-3\big)$ *, cioè* $\overline{p(x)} = \overline{0}$ *in* $\mathbb{Q}[x]\Big/\big(x^2-3\big)$ *. Il caso invece di* $\overline{p(x)} \neq \overline{0}$ *corrisponde a* $r_1(x) = a + b\,x \neq 0$ *, cioè* $(a,b) \neq (0,0)$ *.*

A questo punto, se $b = 0$ *abbiamo* $r_1(x) = a \neq 0$ *, che è invertibile (in* $\mathbb{Q}$ *e quindi in* $\mathbb{Q}[x]$ *) perciò tale* a *è* $\mathrm{MCD}\big(\,p(x)\,,\,x^2-3\,\big)$ *e abbiamo* $\mathrm{MCD}\big(\,p(x)\,,\,x^2-3\,\big) \sim a \sim 1$ *, q.e.d.*

Se invece è $b \neq 0$ *, allora l'algoritmo euclideo prosegue, e il passo successivo è fare la divisione di* $\big(x^2-3\big)$ *per* $r_1(x) = a + b\,x$ *: questo ci dà*

$$\big(x^2-3\big) \;=\; (a+b\,x)\,q_2(x) \,+\, r_2(x) \tag{2}$$

con $q_2(x), r_2(x) \in \mathbb{Q}[x]$ *e* $r_2(x) = 0$ *oppure* $r_2(x) \neq 0$ *e* $\partial\big(r_2(x)\big) \lneqq \partial(a+b\,x) = 1$ *, e quindi* $r_2(x) = c \in \mathbb{Q}$ *è uno scalare. Sostituendo* $x := -b^{-1}a$ *in quest'ultima identità otteniamo che* $c = r_2\big(b^{-1}a\big) = \big(b^{-2}a^2-3\big)$ *, e quest'ultimo valore è diverso da zero perché* 3 *non è un quadrato in* $\mathbb{Q}$ *— in altre parole, non esiste in* $\mathbb{Q}$ *una radice quadrata di* 3*... Adesso il passo successivo a (2) nell'algoritmo sarà una divisione esatta (cioè con resto zero) e l'algoritmo si arresterà, con* $r_2(x) = c \in \mathbb{Q}$ *come ultimo resto non nullo: dunque questo è proprio il* $\mathrm{MCD}\big(\,p(x)\,,\,x^2-3\,\big)$ *cercato, con* $\mathrm{MCD}\big(\,p(x)\,,\,x^2-3\,\big) \sim c \sim 1$ *, q.e.d.*

23 — Si consideri l'anello quoziente $A := \mathbb{Z}\big[\sqrt{-2}\,\big]\Big/\big(3-\sqrt{-2}\,\big)$. Dimostrare che:

(a) A è un campo.

(b) A è isomorfo all'anello di interi modulari $Z_{11} := \mathbb{Z}\Big/(11) = \mathbb{Z}\Big/\equiv_{11}$.

Suggerimento: *Siccome* 11 *è numero primo sappiamo che* $\mathbb{Z}_{11}$ *è un campo; perciò la parte (b) implica anche la parte (a).*

L'enunciato in (a) è analogo a quello dell'esercizio 21 qui sopra, poiché anche $\mathbb{Z}\big[\sqrt{-2}\,\big]$ *è un anello euclideo (come spiegato nell'esercizio 5) e si può trattare nello stesso modo, salvo un diverso approccio nella parte finale. Per questa, osserviamo che — detta "*v*" la valutazione in* $\mathbb{Z}\big[\sqrt{-2}\,\big]$ *data da* $v\big(a+b\sqrt{-2}\,\big) := a^2+2\,b^2$ *— si ha* $v\big(3-\sqrt{-2}\,\big) = 11$ *, che è irriducibile in* $\mathbb{Z}$*: come nell'esercizio 9, ne deduciamo che* $\big(3-\sqrt{-2}\,\big)$ *è irriducibile in* $\mathbb{Z}\big[\sqrt{-2}\,\big]$ *— ha soltanto i divisori banali — quindi è coprimo con ogni* $\alpha \in \mathbb{Z}\big[\sqrt{-2}\,\big]$ *che non sia suo multiplo, cioè tale che* $\overline{\alpha} \neq \overline{0} \in \mathbb{Z}\big[\sqrt{-2}\,\big]\Big/\big(3-\sqrt{-2}\,\big) =: A$ *. Perciò ogni tale* $\overline{\alpha}$ *è invertibile in* A *, e dunque tale anello è un campo, q.e.d.*

Per la parte (b), si consideri il morfismo $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}\big[\sqrt{-2}\,\big]$, $z \mapsto z$, *l'epimorfismo canonico* $\psi : \mathbb{Z}\big[\sqrt{-2}\,\big] \twoheadrightarrow \mathbb{Z}\big[\sqrt{-2}\,\big]\Big/\big(3-\sqrt{-2}\,\big)$, $\big(a+b\sqrt{-2}\,\big) \mapsto \overline{\big(a+b\sqrt{-2}\,\big)}$, *e la composizione* $\psi\circ\phi : \mathbb{Z} \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}\big[\sqrt{-2}\,\big]\Big/\big(3-\sqrt{-2}\,\big)$ *. Allora* $Im(\psi\circ\phi) \ni \overline{1} = (\psi\circ\phi)(1)$ *ma anche* $Im(\psi\circ\phi) \ni (\psi\circ\phi)(3) = \overline{3} = \overline{\sqrt{-2}}$ *perché in* $\mathbb{Z}\big[\sqrt{-2}\,\big]\Big/\big(3-\sqrt{-2}\,\big)$ *vale l'identità* $\overline{3} - \overline{\sqrt{-2}} = \overline{\big(3-\sqrt{-2}\,\big)} = \overline{0}$ *. Siccome* $\overline{1}$ *e* $\overline{\sqrt{-2}}$ *generano tutto l'anello* $\mathbb{Z}\big[\sqrt{-2}\,\big]\Big/\big(3-\sqrt{-2}\,\big)$ *, da questo segue che* $Im(\psi\circ\phi) = \mathbb{Z}\big[\sqrt{-2}\,\big]\Big/\big(3-\sqrt{-2}\,\big)$ *, dunque il morfismo* $\psi\circ\phi$ *è suriettivo: allora per il Teorema Fondamentale di Omomorfismo (per anelli) l'epimorfismo* $\psi\circ\phi$ *induce un isomorfismo*

$$(\psi\circ\phi)_* : \mathbb{Z}\Big/Ker(\psi\circ\phi) \xrightarrow{\ \cong\ } Im(\psi\circ\phi) = \mathbb{Z}\big[\sqrt{-2}\,\big]\Big/\big(3-\sqrt{-2}\,\big)$$

definito da $(\psi\circ\phi)_*\big(\overline{z}\big) := (\psi\circ\phi)(z)$ $\big(=\overline{z}\big)$ *. Infine, osserviamo che*

$$11 = \big(3-\sqrt{-2}\,\big)\big(3+\sqrt{-2}\,\big) \qquad \Longrightarrow \qquad (\psi\circ\phi)(11) := \overline{11} = \overline{0}$$

quindi $11\cdot\mathbb{Z} = (11) \subseteq Ker(\psi\circ\phi)$ *. Inoltre, se* $k \in Ker(\psi\circ\phi) \setminus \{0\}$ *allora significa che* $\overline{k} \in \big(3-\sqrt{-2}\,\big) \setminus \big\{\,\overline{0}\,\big\}$ *cioè* k *è multiplo non nullo di* $\big(3-\sqrt{-2}\,\big)$ *in* $\mathbb{Z}\big[\sqrt{-2}\,\big]$ *, e quindi* $v(k) = k^2$ *è multiplo non nullo di* $v\big(3-\sqrt{-2}\,\big) = 11$ *in* $\mathbb{N}$ *, cioè* 11 *divide* k^2 *in* $\mathbb{N}$ *, perciò necessariamente* 11 *divide* k *in* $\mathbb{Z}$ *, così che* $k \in 11\cdot\mathbb{Z} = (11)$ *. Quindi abbiamo anche* $Ker(\psi\circ\phi) \subseteq 11\cdot\mathbb{Z} = (11)$ *, per cui* $Ker(\psi\circ\phi) \subseteq 11\cdot\mathbb{Z} = (11)$ *. Perciò abbiamo* $\mathbb{Z}\Big/Ker(\psi\circ\phi) = \mathbb{Z}\Big/(11) = \mathbb{Z}\Big/\equiv_{11} =: \mathbb{Z}_{11}$ *e l'isomorfismo di cui sopra* $(\psi\circ\phi)_* : \mathbb{Z}\Big/Ker(\psi\circ\phi) \xrightarrow{\ \cong\ } \mathbb{Z}\big[\sqrt{-2}\,\big]\Big/\big(3-\sqrt{-2}\,\big)$ *è in effetti un isomorfismo* $(\psi\circ\phi)_* : \mathbb{Z}_{11} \xrightarrow{\ \cong\ } \mathbb{Z}\big[\sqrt{-2}\,\big]\Big/\big(3-\sqrt{-2}\,\big)$ *come richiesto.*

24 — *Criterio per i Domini Euclidei:* Dato un dominio unitario D, si definiscano iterativamente i seguenti sottoinsiemi di D:

$$V_{-1} := \{0\} \ , \qquad V_n := \left\{ b \in D \,\middle|\, V_{n-1} \longrightarrow D/(b) \text{ è suriettiva} \right\} \bigcup \{0\} \quad \forall\ n \in \mathbb{N} \ .$$

Dimostrare che:

(a) $V_0 \setminus V_{-1} = U(D)$;

(b) $V_\ell \subseteq V_t \qquad \forall\ \ell \leq t \text{ in } \mathbb{N}$;

(c) D è anello euclideo $\iff \bigcup_{n=-1}^{+\infty} V_n = D$.

Suggerimento: Le parti (a) e (b) seguono direttamente dalle definizioni.

Per la "$\Longrightarrow$" in (c), supponendo che D sia un anello euclideo, siano

$$v_{-1} < v_0 < v_1 < \cdots < v_{n-1} < v_n < v_{n+1} < \cdots$$

i valori, in ordine strettamente crescente, assunti dalla valutazione $v : D \longrightarrow \mathbb{N} \cup \{-\infty\}$ di D. Definendo i sottoinsiemi $W_n := \left\{ r \in D \,\middle|\, v(r) \leq v_n \right\}$ per ogni $n \in \mathbb{N} \cup \{-1\}$, si dimostri che $V_n = W_n$ per ogni $n \in \mathbb{N} \cup \{-1\}$, e da questo si ricavi che $\bigcup_{n=-1}^{+\infty} V_n = D$.

Viceversa, per l'implicazione "$\Longleftarrow$" — ancora in (c) — a partire dall'identità insiemistica $\bigcup_{n=-1}^{+\infty} V_n = D$ si definisca la funzione $v : D \longrightarrow \mathbb{N} \cup \{-\infty\}$ come segue:

$$v(0) := -\infty \ , \qquad v(a) := n \iff a \in V_n \setminus V_{n-1} \ , \quad \forall\ a \in A \setminus \{0\} \ .$$

Si dimostri allora che, rispetto a tale funzione v come valutazione, D è anello euclideo.

25 — Dimostrare che per ogni $n \in \mathbb{N}$ con $n > 2$ i domini unitari $D := \mathbb{Z}\big[\sqrt{-n}\,\big]$ *non* sono anelli euclidei.

Suggerimento: Si utilizzi il Criterio dato nell'esercizio 24 qui sopra. Cominciando col calcolare V_0 si trova $V_0 = U\big(\mathbb{Z}\big[\sqrt{-n}\,\big]\big) \cup \{0\} = \{+1, -1, 0\}$. Da questo, calcoliamo

$$V_1 := \left\{ b \in D \,\middle|\, V_0 \longrightarrow D/(b) \text{ è suriettiva} \right\} \bigcup \{0\} \quad .$$

che con $V_0 = \{+1, -1, 0\}$ dà $V_1 = \{+1, -1, 0\} = V_0$. Infatti, sappiamo già che vale l'inclusione "$\supseteq$", e per l'inversa abbiamo $b \in V_1 \setminus \{0\} \iff$ ogni elemento di $a \in D$ è congruente modulo b a $+1$, 0 o -1: in formule, per le classi (di congruenza modulo b) in $D/(b)$ dobbiamo avere $[a]_{\equiv_b} \in \big\{[+1]_{\equiv_b}, [0]_{\equiv_b}, [-1]_{\equiv_b}\big\}$. In particolare per $a := 2$ avremo $[2]_{\equiv_b} \in \big\{[+1]_{\equiv_b}, [0]_{\equiv_b}, [-1]_{\equiv_b}\big\}$ cioè $2 \equiv_b +1$ oppure $2 \equiv_b 0$ oppure $2 \equiv_b -1$, che significano rispettivamente $b \,\Big|\, (2-1) = 1$, oppure $b \,\Big|\, (2-0) = 2$, oppure $b \,\Big|\, (2+1) = 3$, dove "$\Big|$" è la relazione di divisibilità in $D := \mathbb{Z}\big[\sqrt{-n}\,\big]$. Ora, il caso $b \,\Big|\, 1$ significa che b divide 1, dunque b è invertibile in D, cioè $b \in U\big(D\big) = \{+1, -1\}$, q.e.d. Nei casi $b \,\Big|\, 2$ e $b \,\Big|\, 3$ invece, passando alla norma (dei numeri complessi) troviamo rispettivamente la relazione di divisibilità — in $\mathbb{N}$ — $N(b) \,\Big|\, N(2) = 2^2 = 4$ oppure $N(b) \,\Big|\, N(3) = 3^2 = 9$.

Siccome $N(b) = b_0^2 + nb_1^2$ *con* $b = b_0 + b_1\sqrt{-n} \in \mathbb{Z}\big[\sqrt{-n}\,\big]$, *in entrambi i casi si trova* $b_1 = 0$ *e quindi poi* $b \in \{+1, -1, +2, -2\}$ *nel primo caso e* $b \in \{+1, -1, +3, -3\}$ *nel secondo. Infine, se* $b = \pm 2$ *(nel primo caso) oppure* $b = \pm 3$ *(nel secondo caso) succede che per* $a := \sqrt{-n}$ *si ha* $[a]_{\equiv_b} \notin \big\{[+1]_{\equiv_b}, [0]_{\equiv_b}, [-1]_{\equiv_b}\big\}$, *che è un assurdo.*

Avendo trovato che $V_1 = \{+1, -1, 0\} = V_0$, *a partire da questo per induzione si trova subito che* $V_n = V_0$ *per ogni* $n \in \mathbb{N}$. *Così abbiamo* $\bigcup_{n=-1}^{+\infty} V_n = V_0 = \{+1, 0, -1\} \neq D$, *e quindi, per il criterio dell'esercizio 24 qui sopra, l'anello* $D := \mathbb{Z}\big[\sqrt{-n}\,\big]$ *non è euclideo.*