ESERCIZI DI ALGEBRA I

ESERCIZI SU ANELLI E POLINOMI

A) Anelli, sottoanelli, caratteristica

A.1. – Sia E un intervallo di **R** e consideriamo l'insieme D_E delle funzioni f:E→**R** derivabili su E.

a) Si dimostri che D_E costituisce un anello commutativo rispetto alle operazioni punto per punto.

b) Si tratta di un dominio d'integrità?

Risposta. a) D_E è un sottoinsieme dell'anello delle funzioni f:E→**R**, perciò occorre dimostrare che D_E è chiuso rispetto all'addizione, agli opposti (o, equivalentemente, alla sottrazione), alla moltiplicazione, alla funzione nulla, alla funzione costante 1. Dall'Analisi Matematica è noto che se due funzioni sono derivabili, anche la loro somma, la loro differenza ed il loro prodotto sono derivabili. Inoltre, le costanti sono derivabili con derivata nulla. Pertanto, anche le costanti 0 ed 1 lo sono, quindi D_E è un anello. Poiché la moltiplicazione è commutativa, è un anello commutativo.

b) No. Sia m un punto interno all'intervallo E. Sia f:E→**R** definita da: $f(x) = \begin{cases} 0 & \text{se } x < m \\ (x-m)^2 & \text{se } x \geq m \end{cases}$. Allora f è derivabile su E, anche nel punto m, in quanto i limiti destro e sinistro del rapporto incrementale in m sono entrambi nulli. Analogamente, sia g:E→**R** definita da: $g(x) = \begin{cases} (x-m)^2 & \text{se } x \leq m \\ 0 & \text{se } x > m \end{cases}$, ed anche g è derivabile. Inoltre, f e g sono non nulle su E, ma risulta $f(x) \cdot g(x) = 0 \ \forall x \in E$.

A.2. – Si consideri l'insieme $R_{[a,b]}$ delle funzioni integrabili secondo Riemann sull'intervallo chiuso $[a, b]$. Si dimostri che $R_{[a,b]}$ costituisce un anello commutativo rispetto alle operazioni punto per punto. È un dominio d'integrità?

A.3. – Sia dato l'insieme delle matrici ad elementi reali, quadrate d'ordine $n > 1$ e triangolari superiori: $T = \left\{ A \in M_n(\mathbf{R}) \,\middle|\, A = [a_{ij}],\ i > j \Rightarrow a_{ij} = 0 \right\}$.

a) Si dimostri che costituisce un anello rispetto alle consuete operazioni di addizione e di moltiplicazione righe per colonne fra matrici.

b) Si tratta di un dominio d'integrità?

Risposta. a) Siano $A, B \in T$, $A = [a_{ij}]$, $i > j \Rightarrow a_{ij} = 0$, $B = [b_{ij}]$, $i > j \Rightarrow b_{ij} = 0$. Allora $A - B = [a_{ij} - b_{ij}]$, $i > j \Rightarrow a_{ij} - b_{ij} = 0 - 0 = 0$. Inoltre, la matrice nulla e la matrice unità sono triangolari superiori. Resta da dimostrare che anche $C = A \times B$ è triangolare superiore. Il suo elemento generico è $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$. Per ogni k, se $i > k$ si ha $a_{ik} = 0$; se $k > j$ si ha $b_{kj} = 0$. Perciò, dato che se $i > j$ si ha sempre $i > k$ oppure $k > j$, allora $c_{ij} = 0$. Pertanto, anche $A \times B \in T$.

b) Non è un anello commutativo, perciò non è un dominio d'integrità.

A.4. – Sia dato l'insieme delle matrici quadrate d'ordine 2 ad elementi della forma: $R = \left\{ A \in M_2(\mathbf{R}) \,\middle|\, A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \right\}$

a) Si dimostri che costituisce un anello commutativo rispetto alle consuete operazioni di addizione e di moltiplicazione righe per colonne fra matrici.

b) È un sottoanello dell'anello $M_2(\mathbf{R})$?

c) Che cos'ha di particolare?

Risposta. a) La verifica della chiusura rispetto alla sottrazione ed alla moltiplicazione è immediata. Inoltre, R contiene lo zero ed ha per unità la matrice $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$. Pertanto, è un anello commutativo.

b) Non è un sottoanello perché la sua unità è diversa da quella di $M_2(\mathbf{R})$.

c) Si tratta di un campo. Infatti, ogni matrice $A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ diversa dalla matrice nulla, ossia con $a \neq 0$, ha per inversa $A' = \begin{bmatrix} 1/a & 0 \\ 0 & 0 \end{bmatrix}$ nell'anello R. Si noti che queste matrici non sono invertibili in $M_2(\mathbf{R})$.

A.4. – Sia dato l'insieme delle matrici quadrate d'ordine 2 ad elementi complessi della forma: $H = \left\{ A \in M_2(\mathbf{C}) \;\middle|\; A = \begin{bmatrix} \alpha & \overline{\beta} \\ -\beta & \overline{\alpha} \end{bmatrix} \right\}$

a) Si dimostri che costituisce un sottoanello di $M_2(\mathbf{C})$ rispetto alle consuete operazioni di addizione e di moltiplicazione righe per colonne fra matrici.

b) È commutativo?

c) Chi è il suo gruppo delle unità?

Risposta. a) Per cominciare, le matrici nulla e unità appartengono ad H, dato che si ottengono con $\beta = 0$ e, rispettivamente, $\alpha = 0$ e $\alpha = 1$. Inoltre, tenendo presenti le proprietà del coniugio, si ha:

$$\begin{bmatrix} \alpha & \overline{\beta} \\ -\beta & \overline{\alpha} \end{bmatrix} - \begin{bmatrix} \gamma & \overline{\delta} \\ -\delta & \overline{\gamma} \end{bmatrix} = \begin{bmatrix} \alpha - \gamma & \overline{\beta - \delta} \\ -(\beta - \delta) & \overline{\alpha - \gamma} \end{bmatrix} \in H$$

$$\begin{bmatrix} \alpha & \overline{\beta} \\ -\beta & \overline{\alpha} \end{bmatrix} \times \begin{bmatrix} \gamma & \overline{\delta} \\ -\delta & \overline{\gamma} \end{bmatrix} = \begin{bmatrix} \alpha\gamma - \overline{\beta}\delta & \alpha\overline{\delta} + \overline{\beta}\overline{\gamma} \\ -\beta\gamma - \overline{\alpha}\delta & -\beta\overline{\delta} + \overline{\alpha}\overline{\gamma} \end{bmatrix} = \begin{bmatrix} \alpha\gamma - \overline{\beta}\delta & \overline{\beta\gamma + \overline{\alpha}\delta} \\ -(\beta\gamma + \overline{\alpha}\delta) & \overline{\alpha\gamma - \overline{\beta}\delta} \end{bmatrix} \in H$$

Pertanto, H è un sottoanello di $M_2(\mathbf{C})$.

b) Non è commutativo: $\begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} \times \begin{bmatrix} i & 1 \\ -1 & -i \end{bmatrix} = \begin{bmatrix} i & -1 \\ 1 & -i \end{bmatrix}, \begin{bmatrix} i & 1 \\ -1 & -i \end{bmatrix} \times \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} = \begin{bmatrix} -i & 1 \\ -1 & i \end{bmatrix}$

c) Si ha: $\det \begin{bmatrix} \alpha & \overline{\beta} \\ -\beta & \overline{\alpha} \end{bmatrix} = \alpha\overline{\alpha} + \beta\overline{\beta} = |\alpha|^2 + |\beta|^2$ è un numero reale ≥ 0, che è nullo se e solo se i due addendi sono entrambi nulli. Ma un numero complesso con modulo nullo è necessariamente nullo, quindi $\alpha = \beta = 0$. Ne segue che la sola matrice singolare è quella nulla, mentre tutte le altre, avendo determinante non nullo, sono invertibili. Pertanto, $H^* = H \setminus \{0\}$ ed H è un corpo (ossia un campo non commutativo). H è il *corpo dei quaternioni di Hamilton*.

A.5. – Sia dato l'anello $\left(\mathbf{Z}_{15},+,\cdot,[1]_{15}\right)$. Sia B l'insieme dei multipli di $[3]_{15}$, ossia $B=\left\{[0]_{15},[3]_{15},[6]_{15},[9]_{15},[12]_{15}\right\}$. Si provi che B è un campo rispetto alle operazioni + e · di $\mathbf{Z}_{15}$, ma non un suo sottoanello. Chi è il suo elemento unità?

Risposta. È immediato verificare che B è chiuso rispetto all'addizione ed alla moltiplicazione mod 15. Ecco le due tavole:

+	0	3	6	9	12
0	0	3	6	9	12
3	3	6	9	12	0
6	6	9	12	0	3
9	9	12	0	3	6
12	12	0	3	6	9

·	0	3	6	9	12
0	0	0	0	0	0
3	0	9	3	12	6
6	0	3	6	9	12
9	0	12	9	6	3
12	0	6	12	3	9

Si vede che la moltiplicazione possiede l'unità, $[6]_{15}$, e che ogni elemento diverso da 0 è invertibile. Pertanto, B è un campo con 5 elementi. Non è un sottoanello di $\mathbf{Z}_{15}$, dato che l'unità è diversa.

A.6. – Vero o falso?

Esiste un campo F con un elemento di periodo 4 in (F, +) [V] [F]

Esiste un campo F con un elemento di periodo 4 in $\left(F^*,\cdot\right)$ [V] [F]

Risposta. Ricordiamo che la caratteristica di un campo è zero oppure è un numero primo. Il periodo di un elemento non nullo nel gruppo additivo di un campo è uguale alla caratteristica, se è un primo, oppure è infinito. Nel nostro caso, 4 non è un numero primo, perciò non è possibile: un tal campo non esiste. Invece, per esempio, nel campo complesso il periodo moltiplicativo dell'unità immaginaria i è proprio 4, dato che $i^2=-1\Rightarrow i^4=\left(-1\right)^2=1$. Un altro esempio è il campo $\mathbf{Z}_5$, nel quale il gruppo moltiplicativo è ciclico, con 5-1 = 4 elementi, ed è generato da $[2]_5$. Infatti, $\left([2]_5\right)^2=[4]_5=[-1]_5\Rightarrow\left([2]_5\right)^4=[1]_5$.

A.7. Nel campo complesso il -1 è un quadrato: $i^2=-1$. Si trovino alcuni primi p tali che nel campo $\mathbf{Z}_p$ la classe $-[1]_p=[p-1]_p$ sia un quadrato.

Risposta. La via più semplice è cercare se tra i numeri del tipo n^2+1 ci sia un qualche numero primo:

n	1	2	3	4	5	6	7	8	…
n^2+1	**2**	**5**	10	**17**	26	**37**	50	65	…

. Per ciascuno dei primi p scritti in grassetto si ha $p-1=n^2 \Rightarrow [p-1]_p = [n]_p{}^2$. La condizione non è però necessaria, infatti si ha

$$[-1]_p = [n]_p{}^2 \Leftrightarrow -1 \equiv n^2 \pmod p \Leftrightarrow \exists k \in \mathbf{Z} \mid n^2+1 = p\cdot k$$

Quindi, per esempio per p = 13 si ha $[5]_{13}{}^2 = [25]_{13} = [12]_{13} = [-1]_{13}$.

A.8. Nel campo complesso si consideri l'insieme $\mathbf{Z}[i] = \{a+bi \mid a,b \in \mathbf{Z}\}$.

a) Si dimostri che è un sottoanello del campo **C**.

b) Si trovi il suo gruppo delle unità.

c) Dati $\alpha = 12+8i$, $\beta = 5+2i$, si trovino due altri elementi $\delta = x+yi$, $\rho = r+si$, appartenenti a **Z**[i], tali che $\alpha = \beta\cdot\delta+\rho$, $|\rho| < |\beta|$.

Risposta. a) Si ha 0 = 0+0i e 1 = 1+0i, quindi appartengono a **Z**[i]. La somma ed il prodotto di due suoi elementi a+bi, c+di appartengono a **Z**[i], infatti:

$$(a+bi)+(c+di) = (a+c)+(b+d)i,\ (a+bi)\cdot(c+di) = (ac-bd)+(ad+bc)i$$

hanno i coefficienti interi. Infine, anche $-(a+bi) = (-a)+(-b)i$ ha i coefficienti interi. Pertanto, **Z**[i] è un sottoanello di **C**.

b) In **C** si ha $(a+bi)^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$, che ha i coefficienti interi se e solo se $a^2+b^2 = 1$. Pertanto, ci sono solo quattro possibilità: ± 1, $\pm i$. Il gruppo che si ottiene ha ordine 4 ed è ciclico, generato da i.

c) In **C** si può considerare la frazione $\frac{12+8i}{5+2i} = \frac{76}{29}+\frac{16}{29}i = \left(2+\frac{18}{29}\right)+\frac{16}{29}i$. Allora il quoziente è δ = 2+0i, mentre il resto è $12+8i-2(5+2i) = 2+4i$, che ha modulo $\sqrt{2^2+4^2} = \sqrt{20} < \sqrt{29} = |5+2i|$. Si osservi che $2+4i = (5+2i)\times\left(\frac{18}{29}+\frac{16}{29}i\right)$.

OSSERVAZIONE. La situazione esplorata nel punto c) vale per ogni coppia di elementi di $\mathbf{Z}[i]$: per ogni $\alpha,\beta\in\mathbf{Z}[i]$, con $\beta\neq 0$, esistono $\delta,\rho\in\mathbf{Z}[i]$ tali che $\alpha=\beta\cdot\delta+\rho$, $|\rho|<|\beta|$. Ne segue che $\mathbf{Z}[i]$ è un dominio ad ideali principali e fattoriale. È chiamato *anello degli interi di Gauss*.

A.9. Nel campo complesso si consideri l'insieme $\mathbf{Z}\left[i\sqrt{5}\right]=\left\{a+bi\sqrt{5}\mid a,b\in\mathbf{Z}\right\}$.

a) Si dimostri che è un sottoanello del campo $\mathbf{C}$.

b) Si trovi il suo gruppo delle unità.

c) Si provi che 3 è irriducibile in $\mathbf{Z}\left[i\sqrt{5}\right]$

d) Si verifichi che $6=3\cdot 2=\left(1+i\sqrt{5}\right)\cdot\left(1-i\sqrt{5}\right)$, ma 3 non divide quei due fattori.

Risposta. a) Si procede come nel caso precedente.

b) In $\mathbf{C}$ si ha $\left(a+bi\sqrt{5}\right)^{-1}=\frac{a}{a^2+5b^2}-\frac{b}{a^2+5b^2}i\sqrt{5}$, che ha i coefficienti interi se e solo se $a^2+5b^2=1$. Pertanto, ci sono solo due possibilità: $a=\pm1,\ b=0$. Il gruppo che si ottiene ha ordine 2.

c) Poniamo $3=\left(x+yi\sqrt{5}\right)\cdot\left(z+ti\sqrt{5}\right)=\left(xz-5yt\right)+\left(xt+yz\right)i\sqrt{5}\Rightarrow\begin{cases}xz-5yt=3\\xt+yz=0\end{cases}$.

Mediante la formula di Cramer risolviamo il sistema: $\begin{cases}x=\dfrac{3z}{z^2+5t^2}\\ y=\dfrac{-3t}{z^2+5t^2}\end{cases}$. Ora, il denominatore di y è maggiore del valore assoluto del numeratore, perciò si deve avere $t=0$, ma allora $y=0$ e $\begin{cases}z=\pm1\\x=\pm3\end{cases}$ o viceversa, quindi 3 è irriducibile.

d) Cerchiamo $x+yi\sqrt{5}$ tale che $3\cdot\left(x+yi\sqrt{5}\right)=1\pm i\sqrt{5}$. Dovrebbe però essere $\begin{cases}3x=1\\3y=\pm1\end{cases}$, il che è impossibile. Dunque, 3 è irriducibile ma non primo.

A.10. Sia (G,+) un gruppo abeliano. Si definisca tra due funzioni f,g:G→G l'operazione f+g ponendo ∀x∈G, (f+g)(x) = f(x)+g(x). Sia poi End(G) l'insieme degli endomorfismi di G.

a) Si dimostri che ∀f,g∈End(G) si ha f+g ed f∘g∈End(G).

b) Si dimostri che $\left(\mathrm{End}(G), +, \circ, \mathrm{id}_G\right)$ è un anello. Che proprietà possiede?

c) La struttura algebrica $\left(G^G, +, \circ, \mathrm{id}_G\right)$ è un anello?

Risposta. a) Poiché G è commutativo ed f, g sono endomorfismi,∀ x,y∈G, si ha:

$$(f+g)(x+y) = f(x+y) + g(x+y) = f(x) + f(y) + g(x) + g(y) =$$
$$= f(x) + g(x) + f(y) + g(y) = (f+g)(x) + (f+g)(y)$$
$$(f \circ g)(x+y) = f(g(x+y)) = f(g(x) + g(y)) = f(g(x)) + f(g(y)) = f \circ g(x) + f \circ g(y)$$

Pertanto, anche f+g ed $f \circ g \in \mathrm{End}(G)$.

b) La funzione $0 : G \to G$, $0 : x \mapsto 0_G$, che è banalmente un endomorfismo, è l'elemento neutro di +, mentre l'opposto di un endomorfismo f è $-f : x \mapsto -f(x)$. La proprietà associativa e la commutativa si provano come per le funzioni consuete di variabile reale. Pertanto, (End(G), +) è un gruppo abeliano. Sappiamo che la composizione è associativa e che ha l'identità come elemento neutro, la quale è banalmente un endomorfismo. Perciò $\left(\mathrm{End}(G), \circ, \mathrm{id}_G\right)$ è un monoide. Dimostriamo ora le proprietà distributive destra e sinistra. $\forall f, g, h \in \mathrm{End}(G), \forall x \in G$, si ha:

$$(f+g) \circ h(x) = (f+g)(h(x)) = f(h(x)) + g(h(x)) = f \circ h(x) + g \circ h(x) = (f \circ h + g \circ h)(x)$$
$$h \circ (f+g)(x) = h((f+g)(x)) = h(f(x) + g(x)) = h(f(x)) + h(g(x)) =$$
$$= h \circ f(x) + h \circ g(x) = (h \circ f + h \circ g)(x)$$

Pertanto, $(f+g) \circ h = f \circ h + g \circ h$, e $h \circ (f+g) = h \circ f + h \circ g$.

Ne segue che $\left(\mathrm{End}(G), +, \circ, \mathrm{id}_G\right)$ è un anello.

c) Quanto visto nel punto b) vale tutto, tranne la distributività a destra, nella quale si usa il fatto che h sia un endomorfismo, perciò $h \circ (f+g) \neq h \circ f + h \circ g$ in generale. La struttura $\left(G^G, +, \circ, \mathrm{id}_G\right)$ è detta *quasi-anello*.

A.11. – Si determini la caratteristica degli anelli seguenti (dove con × si denota il prodotto diretto di anelli):

a)	$\mathbf{Z}_{12} \times \mathbf{Z}_{18}$	
b)	$\mathbf{Z} \times \mathbf{Z}_2$	
c)	$M_3(\mathbf{Z}_{11})$, anello delle matrici quadrate d'ordine 3 sul campo $\mathbf{Z}_{11}$	
d)	GF(81), ossia un campo (Galois Field) con 81 elementi.	

Risposta. Ricordiamo che la caratteristica è il periodo dell'unità nel gruppo additivo dell'anello, con la sola convenzione che se il periodo è infinito, si dice che la caratteristica è zero. Ciò posto, nel primo caso l'unità è la coppia $\left([1]_{12},[1]_{18}\right)$ e, per quanto sappiamo sul prodotto diretto di gruppi, ha periodo mcm(12, 18) = 36. Nel secondo caso, l'unità è $\left(1,[1]_2\right)$, e poiché per ogni $n \in \mathbf{N}$, $n \neq 0$, si ha $n\left(1,[1]_2\right) = \left(n,[n]_2\right) \neq \left(0,[0]_2\right)$, il periodo è infinito e la caratteristica è 0. Nel terzo anello, sia $A = [a_{ij}]$, $1 \leq i, j \leq 3$, $a_{ij} \in \mathbf{Z}_{11}$ una di queste matrici, allora $nA = [na_{ij}] \Rightarrow 11A = 0_3$ (matrice nulla d'ordine 3). In particolare, $11I_3 = 0_3$, mentre ovviamente per $1 \leq n < 11$ si ha $nI_3 \neq 0_3$. Dunque, la caratteristica è 11.

Infine, un campo di ordine 81 ha per caratteristica un numero primo, che deve essere 3, dato che il periodo dell'unità nel gruppo additivo deve avere ordine divisore di 81 per il teorema di Lagrange.

B) Ideali, omomorfismi, quozienti.

B.1. – Sia E un sottoinsieme non vuoto di **R**, sia x_0 un suo punto di accumulazione e consideriamo l'insieme L delle funzioni f:E→**R** aventi limite finito in x_0.

a) Si dimostri che L costituisce un anello commutativo rispetto alle operazioni punto per punto.

b) Il limite è un'applicazione dall'anello L al campo **R**, che associa ad ogni f∈L il numero reale $\lim_{x\to x_0} f(x)$. È un omomorfismo di anelli? Se sì, chi è il suo nucleo? Chi è l'immagine? Che cosa si può concludere a proposito del nucleo?

Risposta. a) Occorre dimostrare che L è chiuso rispetto alla sottrazione, alla moltiplicazione, alla funzione nulla, alla funzione costante 1. Dall'Analisi Matematica è noto che se due funzioni hanno limite finito in x_0, anche la loro somma, la loro differenza ed il loro prodotto hanno limite finito. Inoltre, ogni funzione costante ha per limite la costante stessa. Pertanto, anche le costanti 0 ed 1 hanno limite finito in x_0, quindi L è un anello, ed è commutativo perché la moltiplicazione punto per punto lo è.

b) È noto che in x_0 il limite della somma è la somma dei limiti, il limite del prodotto è il prodotto dei limiti il limite della costante 1 è 1, perciò il limite è un omomorfismo di anelli. Il suo nucleo I è costituito dalle funzioni f tali che $\lim_{x\to x_0} f(x) = 0$. L'immagine è tutto **R**, infatti per ogni c∈**R** si ha $\lim_{x\to x_0} c = c$. Allora, poiché il quoziente L/I è un campo, I è un ideale massimale di L.

B.2. – Sia $(A,+,\cdot,1_A)$ un anello commutativo con unità e sia 0_A il suo elemento neutro additivo. Per ogni a∈A definiamo $\mathrm{Ann}(a) = \{x\in A \mid a\cdot x = 0_A\}$.

(a) Provare che Ann(a) è un ideale di A.

(b) Può contenere a? Si esamini il caso degli anelli $\mathbf{Z}_m$.

Risposta. (a) Dobbiamo dimostrare che Ann(a) è un sottogruppo del gruppo additivo e che assorbe il prodotto. Intanto, $0_A \in \mathrm{Ann}(a)$ dato che $a\cdot 0_A = 0_A$.

Inoltre, per la proprietà distribuitiva si ha:

$$\forall x, y \in \mathrm{Ann}(a), a \cdot (x + y) = a \cdot x + a \cdot y = 0_A + 0_A = 0_A$$

Infine, ovviamente $a \cdot (-x) = -a \cdot x = -0_A = 0_A$. Dunque (Ann(a),+) è un sottogruppo di (A, +). Sia ora sempre $x \in \mathrm{Ann}(a)$ e sia $y \in A$. Allora, $a \cdot (x \cdot y) = (a \cdot x) \cdot y = 0_A \cdot y = 0_A$. Pertanto, essendo A commutativo, Ann(a) è un ideale bilatero.

(b) Ann(a) contiene a se $a^2 = 0_A$. Per esempio, nell'anello $\mathbf{Z}_4$ si ha $[2]_4^{\,2} = [0]_4$.

Negli anelli $\mathbf{Z}_m$ si ha $[a]_m^{\,2} = [a^2]_m = [0]_m$ se e solo se esiste $k \in \mathbf{Z}$, tale che $a^2 = m \cdot k$. Ciò accade se m è un quadrato ed a è la sua radice quadrata, ma non solo: $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_r^{\alpha_r}$, $m = p_1^{\mu_1} \cdot p_2^{\mu_2} \dots p_r^{\mu_r}$, con la condizione che per ogni i, $1 \le i \le r$, $2\alpha_i \ge 2\mu_i$. In tal caso, $k = p_1^{2\alpha_1 - \mu_1} \cdot p_2^{2\alpha_2 - \mu_2} \dots p_r^{2\alpha_r - \mu_r}$.

Se m è "libero da quadrati", ossia se gli esponenti μ_i sono tutti = 1, allora nessun $[a]_m$ appartiene ad Ann($[a]_m$). Inversamente, un numero positivo a è tale che $[a]_m$ appartiene ad Ann($[a]_m$) nell'anello $\mathbf{Z}_m$ se e solo se m > a ed m divide a^2.

Un esempio: sia $m = 12 = 2^2 \cdot 3$ allora a = 6 = 2·3 è l'unica possibilità. Dualmente, per a = 6 si ha m = 9, 12, 18, 36.

OSSERVAZIONE. In un anello non commutativo esistono sottogruppi che possiedono la proprietà di assorbire il prodotto o solo a destra o solo a sinistra. Essi sono detti ideali destri o rispettivamente ideali sinistri. Formalmente, un ideale destro I di un anello A è un sottogruppo additivo di A, tale che per ogni $i \in I$, per ogni $a \in A$, $i \cdot a \in I$. Un esempio è *l'annullatore destro* di un elemento, ossia $\mathrm{Ann}_d(a) = \{x \in A \mid a \cdot x = 0_A\}$: $\forall x \in \mathrm{Ann}_d(a)$, $\forall y \in A$, $x \cdot y \in \mathrm{Ann}_d(a)$. Dualmente si può definire l'annullatore sinistro di a.

B.3. – Sia $M_2(\mathbf{R})$ l'anello delle matrici quadrate d'ordine 2 ad elementi in $\mathbf{R}$. Si trovi l'annullatore destro per ciascuna delle matrici seguenti: $A = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$.

Risposta. Poiché det(A) = 3 ≠ 0, allora A è invertibile, quindi cancellabile, ed

allora $\mathrm{Ann_d}(A) = \{\mathbf{0}_2\}$. Invece, $\det(B) = 0$, quindi cerchiamo quali matrici $X = \begin{bmatrix} x & y \\ z & t \end{bmatrix}$ siano tali che $B \times X = \mathbf{0}_2$. Si ha:

$$B \times X = \mathbf{0}_2 \Rightarrow \begin{bmatrix} x+2z & y+2t \\ 2x+4z & 2y+4t \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \Rightarrow \begin{cases} x+2z=0 \\ 2x+4z=0 \\ y+2t=0 \\ 2y+4t=0 \end{cases}$$

La seconda e la quarta equazione sono conseguenza della prima e della terza rispettivamente, quindi resta il sistema $\begin{cases} x+2z=0 \\ y+2t=0 \end{cases} \Rightarrow X = \begin{bmatrix} -2z & -2t \\ z & t \end{bmatrix}$.

Pertanto, $\mathrm{Ann_d}(B) = \left\{ X \in M_2(\mathbf{R}) \;\middle|\; X = \begin{bmatrix} -2z & -2t \\ z & t \end{bmatrix},\ t,z \in \mathbf{R} \right\}$ è un ideale destro non banale di $M_2(\mathbf{R})$.

OSSERVAZIONE. Si è visto che gli unici anelli commutativi che hanno solo gli ideali (bilateri) banali sono i campi. Esistono però anelli non commutativi con la stessa proprietà. Vediamo un esempio nel prossimo esercizio B.4.

B.4. – Sia $M_2(\mathbf{R})$ l'anello delle matrici quadrate d'ordine 2 ad elementi in $\mathbf{R}$. Siano $S = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $T_{12}(x) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$, $T_{21}(x) = \begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix}$. Sia poi $\Im$ un ideale (bilatero) non nullo ed $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Im$, non nulla. Si dimostri che $\Im = M_2(\mathbf{R})$, mediante i passi seguenti.

a) Si esamini la situazione se si ha $\det(A) \neq 0$.

b) Supposto nel seguito $\det(A) = 0$, dopo avere calcolato $S \times A$, $A \times S$, $S \times A \times S$, si concluda che si può scegliere A in $\Im$ in modo che sia $a \neq 0$.

c) Dopo avere calcolato $A \times \left(\frac{1}{a} I_2\right)$, si concluda che si può scegliere A in $\Im$ in modo che sia $a = 1$.

d) Dopo avere calcolato $T_{21}(-c) \times A$ e $A \times T_{12}(-b)$, tenuto conto che $\det(A) = 0$ si concluda che la matrice $E_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in \Im$.

e) Si dimostri che $\Im$ contiene anche la matrice $E_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$.

f) Si deduca infine che $\Im$ contiene anche la matrice $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ e quindi $\Im = M_2(\mathbf{R})$.

Risposta. a) Se $\det(A) \neq 0$, allora A è invertibile, quindi $\Im = M_2(\mathbf{R})$.

b) $S \times A = \begin{bmatrix} c & d \\ a & b \end{bmatrix} \in \Im$, $A \times S = \begin{bmatrix} b & a \\ d & c \end{bmatrix} \in \Im$, $S \times A \times S = \begin{bmatrix} d & c \\ b & a \end{bmatrix} \in \Im$. Poiché almeno un elemento di A è non nullo, se $a = 0$, in almeno uno di questi prodotti nel posto 11 c'è un elemento non nullo. Dunque, si può supporre $a \neq 0$.

c) $A \times \left(\frac{1}{a} I_2\right) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \times \begin{bmatrix} 1/a & 0 \\ 0 & 1/a \end{bmatrix} = \begin{bmatrix} 1 & b/a \\ c/a & d/a \end{bmatrix} \in \Im$. Allora supponiamo senz'altro $A = \begin{bmatrix} 1 & b \\ c & d \end{bmatrix} \in \Im$.

d) $T_{21}(-c) \times A \times T_{12}(-b) = \begin{bmatrix} 1 & 0 \\ -c & 1 \end{bmatrix} \times \begin{bmatrix} 1 & b \\ c & d \end{bmatrix} \times \begin{bmatrix} 1 & -b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b \\ 0 & -cb+d \end{bmatrix} \times \begin{bmatrix} 1 & -b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -cb+d \end{bmatrix}$.

Quest'ultima matrice appartiene ad $\Im$ ed ha determinante $-cb+d$. Se non fosse nullo, saremmo nel caso a). Se lo è, si ha la matrice $E_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $\Rightarrow E_{11} \in \Im$.

e) Come visto al punto b), si ha $S \times E_{11} \times S = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = E_{22} \Rightarrow E_{22} \in \Im$.

f) Ora usiamo la chiusura di $\Im$ rispetto alla somma per concludere che $I_2 = E_{11} + E_{22} \in \Im$, e quindi $\Im = M_2(\mathbf{R})$.

B.5. Nel campo $\mathbf{C}$ dei numeri complessi sia definita la seguente relazione: $\forall z_1, z_2 \in \mathbf{C}$, $z_1 \sim z_2$ se la parte reale di $z_1 - z_2$ è nulla.

A) Si dimostri che $\sim$ è una relazione d'equivalenza.

B) Si descriva la classe d'equivalenza del numero $z_1 = \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i\right)^2$.

C) Si dimostri che la relazione $\sim$ è compatibile con l'addizione in $\mathbf{C}$.

D) La classe d'equivalenza di 0 è un ideale di $\mathbf{C}$? Se la risposta è affermativa, si descriva l'anello quoziente rispetto a tale ideale.

Risposta. A) La relazione è esprimibile anche dicendo che $z_1 \sim z_2$ se $\mathrm{Re}(z_1) = \mathrm{Re}(z_2)$. Pertanto, $\sim$ è la relazione associata alla funzione Re:**C**→**R**, che ad ogni z∈**C** associa la sua parte reale. È quindi una relazione d'equivalenza.

B) Si ha $z_1 = \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\mathrm{i}\right)^2 = \mathrm{i}$, la cui parte reale è nulla, quindi la sua classe contiene tutti e soli i numeri complessi bi, b∈**R**. In particolare, essa contiene lo zero.

C) Siano $z_k = a_k + \mathrm{i}b_k$, $k = 1,2,3,4$ tali che $z_1 \sim z_3$, $z_2 \sim z_4$. Allora $\mathrm{Re}(z_1) = \mathrm{Re}(z_3)$, $\mathrm{Re}(z_2) = \mathrm{Re}(z_4)$. Ora, nella somma si ha:

$$\mathrm{Re}(z_1 + z_2) = \mathrm{Re}(z_1) + \mathrm{Re}(z_2) = \mathrm{Re}(z_3) + \mathrm{Re}(z_4) = \mathrm{Re}(z_3 + z_4)$$

Pertanto, $z_1 + z_2 \sim z_3 + z_4$.

Osservazione. La funzione Re:**C**→**R** è un omomorfismo dei gruppi additivi, perciò la compatibilità con la somma è un fatto generale.

D) La classe d'equivalenza di 0 non si riduce al solo zero, perché contiene tutti gli immaginari puri. Non coincide con tutto **C** perché non contiene 1. Ne segue che non è un ideale, perché i soli ideali di un campo come **C** sono {0} e **C** stesso.

C) Anelli di polinomi

C.1. Sia **R** il campo reale. Si considerino i due polinomi f, g∈**R**[x], definiti da:

$$f(x) = 4x^4 + x^2 - 3x + 1,\ \ g(x) = 2x^4 - x^3 - 2x + 1.$$

Siano poi I e J gli ideali generati rispettivamente da f e da g.

A) Si scompongano f e g in **R**[x].

B) Si trovino quoziente e resto della divisione di f per g.

C) Si trovino un generatore per l'ideale I+J ed uno per l'ideale I∩J.

D) L'ideale I è massimale in **R**[x]? Sì No.

Risposta. a) Poiché i due polinomi hanno i coefficienti interi e coprimi, cerchiamone le eventuali radici razionali.

Per quanto riguarda f, esse hanno la forma $\frac{\pm 1}{q},\ q = 1,2,4$. Si ha

$f(1) = 3,\ f(-1) = 9,\ f\left(\frac{1}{2}\right) = 0$. Allora dividiamo f per $x - \frac{1}{2}$, per esempio con il metodo di Ruffini-Horner,

	4	0	1	−3	1
1/2		2	1	1	−1
	4	2	2	−2	0

, quindi otteniamo:

$$f(x) = 2\left(x - \frac{1}{2}\right)\cdot\left(2x^3 + x^2 + x - 1\right) = (2x - 1)\cdot\left(2x^3 + x^2 + x - 1\right).$$

Il quoziente $\left(2x^3 + x^2 + x - 1\right)$ potrebbe avere ancora $\frac{1}{2}$ per radice, ed infatti è così. Allora dividiamolo per $x - \frac{1}{2}$:

	2	1	1	−1
1/2		1	1	1
	2	2	2	0

. Allora otteniamo:

$$f(x) = (2x - 1)\cdot\left(x - \frac{1}{2}\right)\cdot\left(2x^2 + 2x + 2\right) = (2x - 1)^2\cdot\left(x^2 + x + 1\right)$$

Il trinomio $x^2 + x + 1$ ha il discriminante = -3, quindi non ha ulteriori radici; essendo di II grado, ciò equivale ad essere irriducibile. La scomposizione indicata è anche valida in **Z**[x], perché i fattori hanno i coefficienti interi.

In modo analogo, scomponiamo il polinomio g, cercandone le eventuali radici razionali, che stavolta hanno la forma $\frac{\pm 1}{q},\ q = 1,2$. Si ha subito g(1) = 0, quindi:

$$\begin{array}{c|cccc|c} & 2 & -1 & 0 & -2 & 1 \\ 1 & & 2 & 1 & 1 & -1 \\ \hline & 2 & 1 & 1 & -1 & 0 \end{array} \Rightarrow g(x) = (x-1)\cdot(2x^3+x^2+x-1).$$ Il quoziente $2x^3+x^2+x-1$ non ha per radice né 1 né -1, ma ha $\frac{1}{2}$, quindi:

$$\begin{array}{c|ccc|c} & 2 & 1 & 1 & -1 \\ 1/2 & & 1 & 1 & 1 \\ \hline & 2 & 2 & 2 & 0 \end{array} \Rightarrow g(x) = (x-1)\cdot(2x-1)\cdot(x^2+x+1)$$

e questa è la scomposizione in **R**[x] ed anche in **Z**[x].

b) La divisione col resto di f per g si esegue con lo schema consueto:

$$\begin{array}{l|l} 4x^4+x^2-3x+1 & \frac{2x^4-x^3-2x+1}{2} \\ \underline{-4x^4+2x^3+4x-2} & \\ 2x^3+x^2+x-1 & \end{array},$$

ed ha termine qui perché il resto ha grado 3 minore del grado 4 del divisore.

c) L'ideale I+J è generato dal MCD(f,g), quindi da $(2x-1)\cdot(x^2+x+1)$. L'ideale I∩J è generato dal mcm(f,g) = $(x-1)\cdot(2x-1)^2\cdot(x^2+x+1)$.

d) L'ideale I non è massimale, poiché f non è irriducibile. Un ideale che lo contiene è per esempio quello generato da 2x-1.

C.2. Sia **R** il campo reale. Si consideri il polinomio f∈**R**[x], definito da: $f(x) = x^4+9x^3+30x^2+44x+24$. Siano poi g la derivata di f ed I l'ideale generato da f.

A) Si scompongano f e g in **R**[x].

B) Si calcolino quoziente e resto della divisione di f per g.

C) Il quoziente **R**[x]/I è un campo? Sì No

Risposta. a) Si può procedere come nell'esercizio precedente. Intanto, $g(x) = f'(x) = 4x^3+27x^2+60x+44$. Le radici razionali possibili di f sono i divisori interi di 24. Si verifica subito che due radici sono -2 e -3, e si ottiene $f(x) = (x+2)^3\cdot(x+3)$. Poiché -2 è radice tripla di f, allora è radice doppia della derivata, ossia di g(x). Si ha subito $g(x) = (x+2)^2\cdot(4x+11)$.

b) Dividiamo f per g:

$$\begin{array}{l|l} x^4+9x^3+30x^2+44x+24 & \underline{4x^3+27x^2+60x+44} \\ \quad -x^4-\frac{27}{4}x^3-15x^2+11x & \frac{1}{4}x+\frac{9}{16} \\ \hline \quad \frac{9}{4}x^3+15x^2+33x+24 & \\ \quad -\frac{9}{4}x^3-\frac{243}{16}x^2-\frac{135}{4}x-\frac{99}{4} & \\ \hline \quad -\frac{3}{16}x^2-\frac{3}{4}x-\frac{3}{4} & \end{array}$$

Il resto è $-\frac{3}{16}\left(x^2+4x+4\right)=-\frac{3}{16}\left(x+2\right)^2$.

c) Il quoziente $\mathbf{R}[x]/I$ non è un campo, dato che, essendo f non irriducibile, allora I non è un ideale massimale.

C.3. Sia $\mathbf{R}$ il campo reale. Si consideri il polinomio $f(x)\in\mathbf{R}[x]$, definito da: $f(x)=x^4-x^3-3x^2+5x-2$. Siano poi g(x) la derivata di f(x) ed I l'ideale generato da f(x).

a) Si determinino il quoziente ed il resto della divisione di f(x) per g(x).

b) Si calcolino MCD(f(x), g(x)) e mcm(f(x), g(x)).

c) Si trovino due polinomi non costanti u(x) e v(x), di grado < 4, tali che $\left(I+u(x)\right)\cdot\left(I+v(x)\right)=0_{\mathbf{R}[x]/I}$.

Risposta. a) Si ha $g(x)=f'(x)=4x^3-3x^2-6x+5$. La divisione di f per g fornisce quoziente $\frac{x}{4}-\frac{1}{16}$ e resto $-\frac{27}{16}\left(x-1\right)^2$.

b) Se dividiamo g(x) per $\left(x-1\right)^2$ otteniamo quoziente 4x+5 e resto = 0, quindi MCD(f,g) = $\left(x-1\right)^2$ (il fattore -27/16 è una costante moltiplicativa non nulla, quindi invertibile e pertanto si può eliminare).

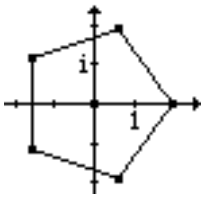
Ne segue $\mathrm{mcm}(f,g)=\frac{f(x)\cdot g(x)}{\left(x-1\right)^2}=f(x)\cdot\left(4x+5\right)=4x^4+x^4-17x^3+5x^2+17x-10$.

c) Dividiamo f per il MCD(f, g) = $\left(x-1\right)^2$, ed otteniamo $f(x)=\left(x-1\right)^2\cdot\left(x^2+x-2\right)$.

Denotiamo con u(x) e v(x) i due fattori, ed allora si ha:

$$\left(I+u(x)\right)\cdot\left(I+v(x)\right)=I+f(x)=I=0_{\mathbf{R}[x]/I}.$$

C.4. Sia dato il polinomio $f(z)=z^5-32$ a coefficienti interi.



A) Si scomponga il polinomio nel campo complesso.

B) Si scomponga il polinomio nel campo reale.

C) Si scomponga il polinomio nel campo razionale.

Risposta. A) La formula di De Moivre consente di trovare le cinque radici in forma trigonometrica. Il numero complesso 32 ha modulo 32 e argomento nullo, perciò le sue radici quinte hanno modulo $\sqrt[5]{32}=2$ ed argomento $\frac{2\pi k}{5}$, $0\le k\le 4$. Per k = 0 si ottiene 2. Le altre radici sono complesse coniugate, dato che i coefficienti sono reali; in particolare lo sono quelle per k = 1 e 4, e per k = 2 e 3, come mostrato dalla figura. Ossia,

$$\left(\cos\frac{8\pi}{5}+i\cdot\sin\frac{8\pi}{5}\right)=\left(\cos\frac{2\pi}{5}-i\cdot\sin\frac{2\pi}{5}\right),\ \left(\cos\frac{6\pi}{5}+i\cdot\sin\frac{6\pi}{5}\right)=\left(\cos\frac{4\pi}{5}-i\cdot\sin\frac{4\pi}{5}\right)$$

Ne segue:

$$f(z)=(z-2)\cdot\left(z-\left(\cos\frac{2\pi}{5}+i\cdot\sin\frac{2\pi}{5}\right)\right)\cdot\left(z-\left(\cos\frac{2\pi}{5}-i\cdot\sin\frac{2\pi}{5}\right)\right)\cdot$$
$$\cdot\left(z-\left(\cos\frac{4\pi}{5}+i\cdot\sin\frac{4\pi}{5}\right)\right)\cdot\left(z-\left(\cos\frac{4\pi}{5}-i\cdot\sin\frac{4\pi}{5}\right)\right)$$

Ora, nel campo reale possiamo ottenere la scomposizione moltiplicando i fattori II - III, e IV – V. È ben noto che $(z-\alpha)\cdot(z-\overline{\alpha})=z^2-2\,\mathrm{Re}(\alpha)+|\alpha|^2$, dunque:

$$\left(z-\left(\cos\frac{2\pi}{5}+i\cdot\sin\frac{2\pi}{5}\right)\right)\cdot\left(z-\left(\cos\frac{2\pi}{5}-i\cdot\sin\frac{2\pi}{5}\right)\right)=z^2-2z\cdot\cos\frac{2\pi}{5}+1$$

Analogamente,

$$\left(z-\left(\cos\frac{4\pi}{5}+i\cdot\sin\frac{4\pi}{5}\right)\right)\cdot\left(z-\left(\cos\frac{4\pi}{5}-i\cdot\sin\frac{4\pi}{5}\right)\right)=z^2-2z\cdot\cos\frac{4\pi}{5}+1$$

Pertanto, posto x in luogo di z, nel campo reale si ha:

$$f(x)=(x-2)\cdot\left(x^2-2x\cdot\cos\frac{2\pi}{5}+1\right)\cdot\left(x^2-2x\cdot\cos\frac{4\pi}{5}+1\right).$$

Con l'aiuto di tavole o di software si possono calcolare quei coseni, ottenendo:

$$f(x)=(x-2)\cdot\left(x^2-\frac{\sqrt{5}-1}{2}x+1\right)\cdot\left(x^2+\frac{\sqrt{5}+1}{2}x+1\right)$$

Questa scomposizione non vale nel campo razionale, per la presenza di $\sqrt{5}$. D'altra parte, con la divisione di polinomi o con la regola di Ruffini si ricava:

$$\begin{array}{c|ccccc|c} & 1 & 0 & 0 & 0 & 0 & -32 \\ 2 & & 2 & 4 & 8 & 16 & 32 \\ \hline & 1 & 2 & 4 & 8 & 16 & 0 \end{array} \Rightarrow f(x) = (x-2)\cdot\left(x^4+2x^3+4x^2+8x+16\right),$$

quindi questa è la scomposizione nel campo razionale, dato che per l'unicità della fattorizzazione, si ha necessariamente:

$$\left(x^4+2x^3+4x^2+8x+16\right) = \left(x^2-\frac{\sqrt{5}-1}{2}x+1\right)\cdot\left(x^2+\frac{\sqrt{5}+1}{2}x+1\right)$$

C.5. Sia dato il polinomio $f(x) = 3x^4+6x^3+5x^2+4x+2$ a coefficienti interi.

A) Si scomponga il polinomio nel campo razionale, reale e complesso.

B) Si trovi un polinomio g(x) che abbia le stesse radici complesse di f(x), ma tutte con molteplicità 1.

C) Si calcolino quoziente e resto della divisione di f(x) per g(x).

Risposta. A) Si può procedere cercandone le radici razionali, ma si può fare anche così:

$$f(x) = 3x^4+6x^3+\left(3x^2+2x^2\right)+4x+2 = 3x^2\cdot\left(x^2+2x+1\right)+2\cdot\left(x^2+2x+1\right) =$$
$$= \left(x^2+2x+1\right)\cdot\left(3x^2+2\right) = (x+1)^2\cdot\left(3x^2+2\right)$$

Questa è la scomposizione sia in **Q**[x] sia in **R**[x], dato che $3x^2+2 \geq 2 > 0$. In **C**[x], invece, questo fattore si annulla per $x = \; x = \pm\sqrt{-\frac{2}{3}} = \pm\frac{i\sqrt{6}}{3}$. Pertanto, in **C**[x] si ha:

$$f(x) = (x+1)^2\cdot\left(x-\frac{i\sqrt{6}}{3}\right)\cdot\left(x+\frac{i\sqrt{6}}{3}\right).$$

b) Il polinomio f ha una radice doppia, -1, e due semplici, dunque per trovare g basta riscrivere la scomposizione con gli esponenti tutti = 1:

$$g(x) = (x+1)\cdot\left(x-\frac{i\sqrt{6}}{3}\right)\cdot\left(x+\frac{i\sqrt{6}}{3}\right) = (x+1)\cdot\left(3x^2+2\right) = 3x^3+3x^2+2x+2$$

c) Ovviamente il quoziente è x+1 ed il resto è zero.

C.6. Consideriamo l'anello $\mathbf{Z}[x]$ dei polinomi a coefficienti interi. Sia I l'ideale generato dai polinomi x e 2, ossia $I = (x) + (2)$.

A) Come sono gli elementi di I?

B) I è principale?.

C) L'ideale (x) è massimale?.

Risposta. A) $I = \{x \cdot p(x) + 2 \cdot q(x) \mid p(x), q(x) \in \mathbf{Z}[x]\}$, perciò ogni elemento di I è somma di un polinomio a termine noto nullo con uno a coefficienti pari. Ne segue che per ogni polinomio f si ha $f \in I$ se e solo se il suo termine noto è pari.

B) Sia I principale, generato da un polinomio d. Allora x e 2 sono multipli di d, pertanto, d è un divisore comune di x e 2, quindi d = 1. Ma $1 = 1 + 0x + 0x^2 + \ldots$ ha il termine noto dispari, quindi non appartiene ad I. Dunque, I non è principale.

C) Si ha $(x) \subset I \subset \mathbf{Z}[x]$. Infatti, $2 \in I \setminus (x)$, $1 \in \mathbf{Z}[x] \setminus I$. Pertanto, pur essendo generato da un elemento irriducibile, (x) non è un ideale massimale.

C.6. Consideriamo l'anello $\mathbf{Q}[x]$ dei polinomi a coefficienti razionali. Sia I l'ideale generato dal polinomio $x^2 + 1$.

A) L'ideale I è massimale?

B) Come sono gli elementi del quoziente $\mathbf{Q}[x]/I$?

C) Si ottiene il campo complesso?

Risposta. A) Poiché i numeri razionali costituiscono un campo, l'anello dei polinomi ha gli ideali principali e, poiché $x^2 + 1$ è irriducibile, l'ideale I è di conseguenza massimale.

B) Il quoziente ha per elementi i laterali I+f(x) di I. Si può procedere come visto nel caso di $\mathbf{R}[x]$: si divide f per $x^2 + 1$ ottenendo resto a+bx, quindi I+f = I+a+bx. Per ogni $a \in \mathbf{Q}$ si può identificare il laterale I+a con a (questi laterali costituiscono un sottocampo isomorfo a $\mathbf{Q}$). Posto i = I+x, ne segue $\mathbf{Q}[x]/I = \{a+bi \mid a,b \in \mathbf{Q}\}$.

C) Il campo ottenuto è numerabile e non è perciò il campo complesso.

C.7. Sia K un campo. Sia I l'insieme dei polinomi di K[x] che hanno per radici tutti gli elementi di K.

A) Si dimostri che I è un ideale di K[x]

B) Che cosa accade se K è il campo reale?

C) Che cosa accade se K è il campo $\mathbf{Z}_p$, p primo?

Risposta. A) Il polinomio nullo appartiene ad I. Se f, g appartengono ad I, per ogni $x\in K$ si ha $f(x) = g(x) = 0$, ed allora anche $(f-g)(x) = f(x) - g(x) = 0$ per ogni $x\in K$, quindi $f-g\in I$. Se poi h(x) è un altro polinomio qualsiasi, allora

$$(f\cdot h)(x) = f(x)\cdot h(x) = 0\cdot h(x) = 0 \text{ per ogni } x\in K,$$

quindi $h\cdot f = f\cdot h\in I$. Pertanto, I è un ideale.

B) Sappiamo che se un polinomio ha grado n, esso ha al massimo n radici. Poiché i numeri reali sono infiniti, solo il polinomio nullo ha per radici tutti i numeri reali, ossia $I = \{0\}$.

B) Il teorema di Fermat (o di Eulero) dice che ogni elemento $a\in\mathbf{Z}_p$, non nullo, soddisfa la condizione $a^{p-1} = 1$. Allora ogni elemento, zero compreso, soddisfa la condizione $a^p = a$, ossia è uno zero del polinomio $x^p - x$. Pertanto, $x^p - x \in I$. D'altra parte, essendo $\mathbf{Z}_p$ un campo, $\mathbf{Z}_p[x]$ ha gli ideali principali, ed anche I lo è, quindi I è generato da un polinomio di cui $x^p - x$ è un multiplo. Ma un polinomio di grado $< p$ non può avere p radici, quindi $x^p - x$ è il polinomio monico di grado minimo in I e lo genera.

OSSERVAZIONE. Da B) segue che tutti i polinomi di grado < p danno funzioni distinte da $\mathbf{Z}_p$ a se stesso. Poiché ci sono p^p polinomi di grado < p e anche p^p funzioni da $\mathbf{Z}_p$ in sé, ecco che ogni funzione da $\mathbf{Z}_p$ in sé è ottenuta da un polinomio di grado < p.