A.A. 2015-2016. CORSO DI ALGEBRA 1.
PROFF. P. PIAZZA, E. SPINELLI.
SOLUZIONE ESERCIZI FOGLIO 9.

Esercizio 9.1. Consideriamo l'anello $\mathbb{Z}[X]$ dei polinomi a coefficienti in $\mathbb{Z}$.

(A) Consideriamo il seguente sottoinsieme di $\mathbb{Z}[X]$:

$$\mathbb{Z}_{\mathscr{P}}[X] = \left\{ P \in \mathbb{Z}[X] \;\middle|\; P(X) = \sum_{i=0}^{n} a_i X^i,\ n \in \mathbb{N},\ a_i \in 2 \cdot \mathbb{Z} \right\}$$

Dimostrare che si tratta di un ideale di $\mathbb{Z}[X]$.
(B) Descrivere l'anello quoziente $\mathbb{Z}[X]/\mathbb{Z}_{\mathscr{P}}(X)$ (determinare un sistema di rappresentanti, descrivere la moltiplicazione tra due classi in $\mathbb{Z}[X]/\mathbb{Z}_{\mathscr{P}}[X]$ sfruttando il sistema di rappresentanti scelto).
(C) Definiamo ora l'insieme $\mathbb{Z}_{\mathscr{P}}^{\geq n}[X] = \mathbb{Z}_{\mathscr{P}}[X] \cap \mathbb{Z}^{\geq n}[X]$, dove denotiamo con $\mathbb{Z}^{\geq n}[X]$ l'insieme dei polinomi di grado $\geq n$ unito all'elemento $0 \in \mathbb{Z}$. Si tratta ancora di un ideale? Dimostrare che $\lim_{n\to\infty} \mathbb{Z}_{\mathscr{P}}^{\geq n}[X] = \{0\}$. [*Suggerimento. Si osservi che* $\mathbb{Z}_{\mathscr{P}}^{\geq n}[X] = \bigcap_{i=1}^{n} \mathbb{Z}_{\mathscr{P}}^{\geq i}[X]$]

Soluzione. Cominciamo dal punto (A). Dimostriamo che $\mathbb{Z}_{\mathscr{P}}[X]$ è un sottogruppo rispetto alla somma in $\mathbb{Z}[X]$. Siano dunque $P, Q \in \mathbb{Z}_{\mathscr{P}}[X]$, $P(X) = \sum_{i=0}^{m} a_i X^i$, $Q(X) = \sum_{i=0}^{n} b_i X^i$ dove $a_i, b_i \in 2\,\mathbb{Z}$; supponiamo $n > m$ allora:

$$(P+Q)(X) = P(X) + Q(X) = \sum_{i=0}^{m} a_i X^i + \sum_{i=0}^{n} b_i X = \sum_{i=0}^{m} (a_i + b_i) X^i + \sum_{i=m+1}^{n} b_i X^i$$

È chiaro che il polinomio $(P+Q)$ è un polinomio a coefficienti pari: segue dal fatto che $2\,\mathbb{Z}$ è un sottogruppo additivo di $\mathbb{Z}$.
È altrettanto chiaro che se $P \in \mathbb{Z}_{\mathscr{P}}[X]$ allora anche il polinomio $(-P) \in \mathbb{Z}_{\mathscr{P}}[X]$ (infatti se $a_i \in 2\,\mathbb{Z}$ allora $-a_i \in 2\,\mathbb{Z}$); infine $0 \in 2\,\mathbb{Z}$ e quindi $0 \in \mathbb{Z}_{\mathscr{P}}[X]$ e dunque $\mathbb{Z}_{\mathscr{P}}[X]$ è un sottogruppo additivo di $\mathbb{Z}[X]$. Dimostriamo ora che, dato un qualunque polinomio $P \in \mathbb{Z}[X]$ ed un qualsiasi polinomio $Q \in \mathbb{Z}_{\mathscr{P}}[X]$ allora $(P \cdot Q) = \mathbb{Z}_{\mathscr{P}}[X]$. Scriviamo $\mathbb{Z}[X] \ni P(X) = \sum_{i=0}^{m} b_i X^i$, $\mathbb{Z}_{\mathscr{P}}[X] \ni Q(X) = \sum_{i=0}^{m} a_i X^i$ e scriviamo il prodotto dei due:

$$\sum_{j=0}^{n+m} \left(\sum_{i_1+i_2=j\,;\, i_1,i_2=0}^{j} (a_{i_1} \cdot b_{i_2}) \right) X^j$$

Poiché ciascun a_i è pari ne segue che per ogni $j = 0, ..., n+m$ risulta che la somma che definisce il coefficiente del monomio di grado j à ancora un intero pari, perché somma di interi pari. Ne segue che $P \cdot Q \in \mathbb{Z}_{\mathscr{P}}[X]$ e dunque, poiché P, Q sono stati scelti in modo arbitrario, ne deduciamo che $\mathbb{Z}_{\mathscr{P}}[X]$ è un ideale di $\mathbb{Z}[X]$.

Nel punto (B) ci viene chiesto di descrivere l'anello quoziente $\mathbb{Z}[X]/\mathbb{Z}_{\mathscr{P}}[X]$. Cominciamo determinando le classi di equivalenza. Sia $P \in \mathbb{Z}[X]$, scriviamo $P(X) = \sum_{i=0}^{m} a_i X^i$. Sia $r : \mathbb{Z} \to \{0,1\}$ la funzione che associa ad ogni numero intero il rappresentante in $\{0,1\}$ della sua classe resto modulo 2 allora $P(X) = \sum_{i=0}^{m} r(a_i) X^i + \sum_{i=0}^{m} (a_i - r(a_i)) X^i$. In altre parole: $P \in \sum_{i=0}^{m} r(a_i) X^i + \mathbb{Z}_{\mathscr{P}}[X]$. Mostreremo ora che $\mathcal{R} = \{\sum_{i=0}^{n} a_i X^i \mid n \in \mathbb{N}, a_i \in \{0,1\}\}$ è un sistema di rappresentanti per le classi di $\mathbb{Z}[X]/\mathbb{Z}_{\mathscr{P}}[X]$. Abbiamo appena mostrato che ogni polinomio $P(X)$ ammette un rappresentante in $\mathcal{R}$. Mostriamo ora che due elementi distinti di $\mathcal{R}$ non sono nella stessa classe di $\mathbb{Z}[X]/\mathbb{Z}_{\mathscr{P}}[X]$. Siano infatti $P(X) = \sum_{i=0}^{m} a_i X^i$ e $Q(X) = \sum_{i=0}^{n} b_i X^i$ due polinomi in $\mathcal{R}$; se appartenessero alla stessa classe allora innanzitutto dovrebbe valere $n = m$, infatti il coefficiente del termine di grado m ed n di P e Q, rispettivamente, è non nullo. Se dunque fosse $n > m$ (risp. $m > n$) avremmo che il polinomio $Q - P$ o(risp. $P - Q$) avrebbe il termine di grado massimo uguale a 1, dunque dispari, pertanto non potrebbe essere $Q - P \in \mathbb{Z}_{\mathscr{P}}[X]$; dunque deve risultare $n = m$, mostriamo ora che per ogni $i = 0, ..., m$

si deve avere $a_i = b_i$; supponiamo che non sia così e sia i_0 il primo indice per cui $a_{i_0} \neq b_{i_0}$ allora deve essere $a_{i_0} = 1$ e $b_{i_0} = 0$ oppure $a_{i_0} = 0$ e $b_{i_0} = 1$; nel primo caso si ha che $P - Q$ ha coefficiente del termine di grado i_0 uguale ad 1, dunque dispari, nel secondo $Q - P$ ha coefficiente del termine di grado i_0 uguale ad 1, dispari; in ogni caso risulta che $P - Q \notin \mathbb{Z}_{\mathscr{P}}[X]$. Pertanto due elementi in $\mathcal{R}$ provengono dalla stessa classe modulo $\mathbb{Z}_{\mathscr{P}}[X]$ se e soltanto se sono lo stesso elemento.
Questo conclude la prova del fatto che $\mathcal{R}$ è un sistema di rappresentanti.
Descriviamo quindi la somma ed il prodotto tra due classi . Per comodità di scrittura identifichiamo i polinomi in $\mathcal{R}$ con delle successioni infinite a valori in $\{0, 1\}$ definitivamente nulle. Prendiamo quindi $P = (i_0, ..., i_m, 0, 0, ..., 0, ...)$, $Q = (j_0, ..., j_n, 0, 0, ..., 0, ...)$ e supponiamo $m < n$. $[P] \pm [Q]$ ammette il seguente rappresentante in $\mathcal{R}$,

$$(P \pm Q)_{\mathcal{R}} = (\delta_{ij,0}, ..., \delta_{ij,\,m}, j_{m+1}, ..., j_n, 0, 0, ..., 0, ...)$$

dove $\delta_{ij,k} = 0$ se $i_k = j_k = 1, 0$ e 1 se $i_k = 1, j_k = 0$ o $i_k = 0$, $j_k = 1$. Mentre per quanto riguarda il prodotto $[P] \cdot [Q]$ risulta:

$$(P \cdot Q)_{\mathcal{R}} = (\delta_{ij,0}, \delta_{ij,1}, ..., \delta_{ij,(n+m)}, 0, ..., 0, ...)$$

dove $\delta_{ij,k} = 0$ se $\#\{(i_{k_1}, j_{k_2}) \mid k_1 + k_2 = k,\ 0 \leq k_1, k_2 \leq k,\ (i_{k_1}, j_{k_2}) = (1, 1)\}$ è pari, $\delta_{ij,k} = 1$ se tale numero è dispari.

Siamo ora nelle condizioni di verificare che $\mathbb{Z}[X]/\mathbb{Z}_{\mathscr{P}}[X]$ è isomorfo a $\mathbb{Z}_2[X]$: è sufficiente infatti verificare che la mappa:

$$\varphi : \mathbb{Z}_2[X] \to \mathbb{Z}[X]/\mathbb{Z}_{\mathscr{P}}[X]\ , \quad \varphi\left(\sum_{i=0}^{n} \overline{\varepsilon}_i\, X^i\right) = \sum_{i=0}^{n} \varepsilon_i\, X^i + \mathbb{Z}_{\mathscr{P}}[X]$$

dove $\varepsilon_i \in \{0, 1\}$, è un isomorfismo di anelli; questo può essere fatto ad esempio sfruttando la descrizione precedentemente fornita dell'anello quoziente in termini della famiglia di rappresentanti $\mathcal{R}$.

Passiamo al punto (C) dell'esercizio. Si osservi che $\mathbb{Z}^{\geq n}[X]$ non è un ideale, ad esempio non si tratta di un sottogruppo additivo di $\mathbb{Z}[X]$; basta infatti prendere la differenza dei polinomi $P(X) = X^n + X$ e $Q(X) = X^n + X^2$; lo stesso si può dire dell'intersezione $\mathbb{Z}^{\geq n}[X] \cap \mathbb{Z}_{\mathscr{P}}[X]$: si consideri la differenza tra i polinomi $2\,P$ e $2\,Q$, ambedue appartenenti a $\mathbb{Z}^{\geq n}_{\mathscr{P}}[X]$ essa chiaramente non è nell'insieme $\mathbb{Z}^{\geq n}_{\mathscr{P}}[X]$ perché non è in $\mathbb{Z}^{\geq n}[X]$.
Verifichiamo infine che risulta $\lim_{n\to+\infty} \mathbb{Z}^{\geq n}_{\mathscr{P}}[X] = \{0\}$. Osserviamo che se $\deg P = m$ allora $P \notin \mathbb{Z}^{\geq n}_{\mathscr{P}}[X]$, per ogni $n > m$. Dunque se P è un polinomio differente da 0 (che per ipotesi è contenuto in $\mathbb{Z}^{\geq n}[X]$ per ogni $n \in \mathbb{N}$) allora $P \notin \lim_{n\to+\infty} \mathbb{Z}^{\geq n}_{\mathscr{P}}[X] = \lim_{n\to+\infty} \bigcap_{i=0}^{n} \mathbb{Z}^{\geq i}_{\mathscr{P}}[X]$. Ne deduciamo che $\lim_{n\to+\infty} \mathbb{Z}^{\geq n}_{\mathscr{P}}[X] = \{0\}$. □

Esercizio 9. 2. Sia A un anello unitario. Supponiamo che $a \in A$ sia un elemento invertibile di ordine finito (dunque tale che $a^n = 1_A$ per un opportuno n) e supponiamo che non sia zero di nessun polinomio $\sum_{i=0}^{j} (-1_A)^{\delta_i} X^i$ per $j < n$ con $\delta_i \in \{0, 1\}$. Mostrare che $(1_A - a)$ è un divisore di 0_A. Mostrare che se $o(a)$ è pari allora $(1_A + a)$ è un divisore di 0_A. Cosa possiamo dire di $(1_A + a)$ nel caso in cui $o(a)$ sia dispari? Si tratta anche in questo caso di un divisore di 0_A? [*Suggerimento. Sfruttare la formula per scrivere la somma/differenza di due potenze n-sime. Per l'ultima domanda si osservi che se a ha ordine dispari a^2 ha lo stesso ordine*]

Soluzione. Cominciamo dalla prima parte dell'esercizio. Vogliamo far vedere che $(1_A - a)$ è un divisore di 0_A. Stiamo qui dando per assunto che $a \neq 1_A$, altrimenti l'affermazione è banale. Si osservi quindi che:

$$(1_A - a) \cdot (1_A + a + a^2 + \cdots + a^{n-1}) = 1_A - a + a - a^2 + a^2 + \cdots - a^{n-1} + a^{n-1} - a^n = 1_A - a^n = 1_A - 1_A = 0_A$$

Poiché a per ipotesi non può essere zero di un polinomio del tipo $\sum_{i=0}^{j} (-1_A)^{\delta_i} X^i$ con $j \leq n - 1$ ne deduciamo che l'elemento $(1_A + a + a^2 + \cdots + a^{n-1}) \neq 0_A$ e dunque $(1_A - a)$ è uno zero-divisore.

Consideriamo ora l'elemento $(1_A + a)$, ed assumiamo che $n \in 2\,\mathbb{Z}$; allora:

$$(1_A + a) \cdot (1_A - a + a^2 + \cdots - a^{n-1}) = 1_A - a + a - a^2 + a^2 - \cdots - a^{n-1} + a^{n-1} - a^n = 1_A - 1_A = 0_A$$

Come nel caso precedente anche qui usiamo l'ipotesi che a non sia zero di alcun polinomio del tipo $\sum_{i=0}^{j}(-1_A)^{\delta_i}X^i$ con $j \leq n-1$; anche in questo caso ne deduciamo che l'elemento $1_A - a + a^2 - \cdots - a^{n-1}$ è differente da 0_A e dunque $(1_A + a)$ è un divisore di 0_A.

Arriviamo quindi ad analizzare il caso in cui a abbia ordine n dispari. Si osservi che in tal caso l'argomento duro e puro utilizzato in precedenza non può essere utilizzato, in tal caso infatti:

$$(1_A + a) \cdot (1_A - a + a^2 + \cdots + a^{n-1}) = (1_A + a^n) = (1_A + 1_A)$$

e l'ultimo termine a priori è differente da 0_A (a meno che $(A, +)$ non sia composto esclusivamente da elementi $a \in A$ tali che $a + a = 0_A$). In tal caso non possiamo concludere senza ulteriori ipotesi sull'anello A. □

Esercizio 9.3. Sia A un anello unitario e sia $a \in A$. Diremo che a è idempotente se $a^2 = a$.

(A) Dimostrare che un idempotente non banale (quindi $\neq 0_A, 1_A$) di A è un divisore di 0_A.
(B) Determinare due elementi idempotenti non banali in $\mathfrak{M}_{2\times 2}(\mathbb{R})$ (matrici 2×2 a coefficienti reali).

Soluzione. Diamo la soluzione del punto (A). Supponiamo che a sia un idempotente non banale (quindi $a \neq 0_A, 1_A$); esso verifica l'equazione $a^2 = a$ ovvero $a - a^2 = 0_A \Leftrightarrow a \cdot (1_A - a) = 0_A$. Poiché $a \neq 1_A, 0_A$ ne segue che $(1_A - a) \neq 0_A$, dunque a (e $(1_A - a)$) sono due divisori di 0_A.

Si osservi che se a è un idempotente non banale, allora $1_A - a$ è un idempotente non banale: $(1_A - a)^2 = a^2 - a - a + 1_A = 1_A - a$.

Rispondiamo ora al punto (B). Sono di banale verifica i due conti seguenti:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \; ; \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Osservate che $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ e dunque la coppia di idempotenti presentata è della forma a, $1_A - a$. □

Esercizio 9.4. Sia A un anello commutativo unitario. Dato un insieme $S \subseteq A$ definiamo l'annullatore dell'insieme S come segue:

$$\mathscr{A}(S) = \{a \in A \mid a \cdot s = 0_A, \forall s \in S\}$$

(A) Dimostrare che $\mathscr{A}(S)$ è un ideale di A. Dimostrare che se $J \subseteq A$ è un ideale allora $\mathscr{A}(J) \cap J = \{0_A\}$. [*Suggerimento. Sfruttare il fatto che in un anello lo zero è unico.*]
(B) Sia $J \subseteq A$ un ideale. Dimostrare che se I è un ideale e $I \cap J = \{0_A\}$, allora $I \subseteq \mathscr{A}(J)$.
(C) Dimostrare che se I e J sono due ideali propri di A tali che $I \cap J = \{0_A\}$ ed I (o J) non contiene elementi idempotenti non banali (ovvero $\neq 0_A, 1_A$) allora $I + J$ è un ideale proprio di A. [*Suggerimento. Supponete per assurdo che* $1_A \in I + J$.]

Soluzione. Risolviamo (A). Dobbiamo dimostrare che $\mathscr{A}(S)$ è un ideale di A; mentre, in restrizione al caso in cui J è un ideale, dobbiamo mostrare che $\mathscr{A}(J) \cap J = \{0_A\}$. Notiamo che se $a_1, a_2 \in \mathscr{A}(S)$ allora $(a_1 + a_2) \cdot s = a_1 \cdot s + a_2 \cdot s = 0_A + 0_A = 0_A$, mentre $a \in \mathscr{A}(S)$ implica $-a \in \mathscr{A}(S)$ infatti $-a \cdot s = -(a \cdot s) = -0_A = 0_A$. Poiché evidentemente $0_A \in \mathscr{A}(S)$ ne deduciamo che $\mathscr{A}(S)$ è un sottogruppo additivo di A, inoltre dato $a \in A$ e dato $a' \in \mathscr{A}(S)$ si ha che $a\,a' \cdot s = a \cdot 0_A = 0_A$, per ogni $s \in S$ e dunque abbiamo $a\,a' \in \mathscr{A}(S)$, per ogni $a \in A$ ed ogni $a' \in \mathscr{A}(S)$ e dunque possiamo concludere che $\mathscr{A}(S)$ è un ideale. Ora abbiamo due modi di procedere per dimostrare la seconda parte di (A); una è osservare che se vi fosse $a \in \mathscr{A}(J) \cap J$ allora a svolgerebbe nell'anello J (pensato come anello a sé stante) lo stesso ruolo di $0_A \in J$; ma poiché in un anello lo zero è unico ne deduciamo $a = 0_A$. Un secondo metodo per risolvere questa parte è osservare che $\mathscr{A}(J) \cap J = \mathscr{A}(J) \cdot J = \{0_A\}$ per definizione di $\mathscr{A}(J)$.

Nel punto (B) si chiedeva di dimostrare che se J è un ideale e $I \cap J = \{0_A\}$ allora $I \subseteq \mathscr{A}(J)$. A tal scopo si osservi che $i \cdot j \in I \cap J$ (infatti I e J sono entrambi ideali) ma tale intersezione è $\{0_A\}$ allora

$i \in \mathscr{A}(J)$, poiché j è un arbitrario elemento in J; dunque siccome i era un arbitrario elemento in I ne deduciamo che $I \subseteq \mathscr{A}(J)$.

Per quanto riguarda (C) sappiamo che, siccome I e J sono ideali, $I + J$ è un ideale. Per dimostrare che è un ideale proprio è sufficiente far vedere che $1_A \notin I + J$. Supponiamo per assurdo che $1_A = i + j$. Allora $(i + j) = 1_A\,(i + j) = i^2 + j^2$ dove abbiamo usato il fatto che $I \cap J = \{0_A\}$. Ora, si osservi che $i + j = i^2 + j^2 \Leftrightarrow i^2 - i = j - j^2$; dunque $(i^2 - i)$ e $(j^2 - j)$ sono entrambi in $I \cap J = \{0_A\}$ pertanto i e j sono due elementi idempotenti entrambi non banali (poiché gli ideali I e J sono entrambi propri), il che è assurdo perché per ipotesi I e J non contengono idempotenti non banali. □

Esercizio 9. 5. Consideriamo $C^0([-1, 1], \mathbb{R})$, l'insieme delle funzioni continue $f : \mathbb{R} \to \mathbb{R}$. Mostrare che si tratta di un anello rispetto alle operazioni:

$$(f + g)(x) = f(x) + g(x), \qquad (f \bullet g)(x) = \frac{f(x) \cdot g(-x) + f(-x) \cdot g(x)}{2}\,.$$

(A) È un anello unitario? È commutativo?
(B) In restrizione all'insieme delle funzioni pari determinare l'insieme degli elementi invertibili.
(C) Dimostrare che il sottoanello delle funzioni pari è un ideale. Dimostrare che la funzione c_1 data da $c_1(x) \equiv 1$ è un'unità in restrizione a tale ideale.
(D) Sia $f \in C^0([-1, 1], \mathbb{R})$ mostrare che $f \bullet f = 0$ se e solo se

$$([-1, 1] \setminus \operatorname{supp}(f)) \cup ([-1, 1] \setminus \{x \in [-1, 1] \mid -x \in \operatorname{supp}(f)\}) = [-1, 1]$$

(E) Dimostrare che l'insieme $\mathcal{C}_0 = \{f \in C^0([-1, 1], \mathbb{R}) \mid f(0) = 0\}$ è un ideale (bilatero) di $C^0([-1, 1], \mathbb{R})$.

Soluzione. Cominciamo con la verifica del fatto che $(C^0([-1, 1], \mathbb{R}), +, \bullet)$ è un anello. Chiaramente si tratta di un gruppo additivo rispetto alla somma (tale verifica è stata fatta altre volte e non verrà ripetuta in questa sede). Verifichiamo invece le proprietà distributiva del prodotto rispetto alla somma:

$$\begin{aligned} f \bullet (g_1 + g_2) &= \frac{f(x)(g_1(-x) + g_2(-x)) + f(-x)\,(g_1(x) + g_2(x))}{2} = \\ &= \frac{f(x)\,g_1(-x) + f(-x)\,g_1(x)}{2} + \frac{f(x)\,g_2(-x) + f(-x)\,g_2(x)}{2} = f \bullet g_1 + f \bullet g_2 \\ (g_1 + g_2) \bullet f &= \frac{(g_1(x) + g_2(x))\,f(-x) + (g_1(-x) + g_2(-x))\,f(x)}{2} = \\ &= \frac{f(-x)\,g_1(x) + f(x)\,g_1(-x)}{2} + \frac{f(-x)\,g_2(x) + f(x)\,g_2(-x)}{2} = g_1 \bullet f + g_2 \bullet f \end{aligned}$$

e la proprietà associativa del prodotto:

$$\begin{aligned} ((f \bullet g) \bullet h)(x) &= \frac{(f(x)\,g(-x) + f(-x)\,g(x))\,h(-x) + (f(-x)\,g(x) + f(x)\,g(-x))\,h(x)}{4} = \\ &= \frac{f(x)(g(x)\,h(-x) + g(-x)\,h(x)) + f(-x)\,(g(-x)\,h(x) + g(x)\,h(-x))}{4} = (f \bullet (g \bullet h))(x) \end{aligned}$$

Si tratta dunque di un anello.

Rispondiamo al punto (A). Ci viene chiesto se si tratta di un anello unitario e se l'anello è commutativo. Cominciamo dalla seconda domanda. La risposta è che il prodotto è commutativo:

$$(f \bullet g)(x) = \frac{f(x)\,g(-x) + f(-x)\,g(x)}{2} = \frac{g(x)\,f(-x) + g(-x)\,f(x)}{2} = (g \bullet f)(x)$$

Per quanto riguarda l'esistenza di un'unità si consideri una funzione f dispari (dunque tale che $f(-x) = -f(x)$) e sia g una eventuale identità; allora si dovrebbe avere $f \bullet g = f$; ma per definizione $f \bullet g$ è una funzione pari e dunque deve essere $f \bullet g = 0$ (poiché la funzione costante uguale a zero è l'unica funzione sia pari che dispari).

Passiamo al punto (B). Osserviamo che in restrizione all'insieme delle funzioni pari in $C^0([-1, 1], \mathbb{R})$ (chiameremo per comodità tale insieme $\mathscr{P}^0([-1, 1], \mathbb{R})$), c_1, la funzione costante uguale ad 1, è un'unità:

$$(f \bullet c_1) = \frac{f(x) \cdot c_1(-x) + f(-x) \cdot c_1(x)}{1} = \frac{f(x) + f(-x)}{2} = \frac{f(x) + f(x)}{2} = f(x)$$

Vale la pena osservare che $(\mathscr{P}^0([-1,1],\mathbb{R}),+,\bullet)$ è un sottoanello di $(C^0([-1,1],\mathbb{R}),+,\bullet)$ (verificate tale affermazione); inoltre è bene notare che se $f,g\in\mathscr{P}^0([-1,1],\mathbb{R})$, allora $f\bullet g=f\cdot g$. In particolare, in restrizione a $\mathscr{P}^0([-1,1],\mathbb{R})$ gli invertibili rispetto a $\bullet$ sono gli stessi rispetto a $\cdot$. Dunque sono le funzioni iniettive in $\mathscr{P}^0([-1,1],\mathbb{R})$. Ma per definzione di funzione pari se $f\in\mathscr{P}^0([-1,1],\mathbb{R})$ essa non può essere iniettiva (vale infatti $f(x)=f(-x)$), pertanto nessun elemento è invertibile.

Per quanto riguarda (C) abbiamo già verificato al passo precedente che c_1 è un'unità per il sottoanello $(\mathscr{P}^0([-1,1],\mathbb{R}),+,\bullet)$. Rimane soltanto da verificare che $(\mathscr{P}^0([-1,1],\mathbb{R}),+,\bullet)$. Data $f\in C^0([-1,1],\mathbb{R})$ e $g\in\mathscr{P}^0([-1,1],\mathbb{R})$, risulta infatti che:

$$(f\bullet g)(x)=\frac{f(x)\,g(-x)+f(-x)\,g(x)}{2}=\frac{(f(x)+f(-x))\,g(x)}{2}=g(x)\cdot\frac{f(x)+f(-x)}{2}$$

che è prodotto di funzioni pari e dunque necessariamente una funzione pari.

Dimostriamo ora quanto affermato nel punto (D). Definiamo $\mathrm{supp}(f)=\{x\in[-1,1]\,|\,f(x)\neq 0\}$. Supponiamo che valga $(f\bullet f)=0$; questo è possibile $\Leftrightarrow 0=\frac{f(x)\,f(-x)+f(-x)\,f(x)}{2}=f(x)\,f(-x)$, per ogni $x\in[-1,1]\Leftrightarrow$ per ogni $x\in[-1,1]$ tale che $f(\pm x)\neq 0$ vale $f(\mp x)=0\Leftrightarrow$ risulta che per ogni $x\in[-1,1]$ vale $x\in[-1,1]\setminus\mathrm{supp}(f)$ oppure $-x\in[-1,1]\setminus\mathrm{supp}(f)$.

Per quanto riguarda (E); omettiamo la dimostrazione del fatto che $\mathcal{C}_0$ è un sottogruppo additivo dell'anello $(C^0([-1,1],\mathbb{R}),+,\bullet)$. Ci limitiamo invece ad osservare che per ogni $f\in C^0([-1,1],\mathbb{R})$ ed ogni $g\in\mathcal{C}_0$ risulta:

$$(f\bullet g)(0)=\frac{f(0)\,g(0)+f(0)\,g(0)}{2}=f(0)\,g(0)=0$$

Il che conclude la dimostrazione del punto (D). □

Esercizio 9.6. Calcolare l'MCD delle seguenti coppie di polinomi in $\mathbb{Z}[X]$:

(a) $P(X)=X^3+X^2-2X-2$ e $Q(X)=X^3+X^2-4X-4$.
(b) $P(X)=X^4-4$ e $Q(X)=3X^{10}-6X^8$
(c) $P(X)=X^{14}+X^{13}-X^{12}-X^{11}$ e $Q(X)=2X^4-X^3-3X^2+X+1$

Soluzione. Ricordiamo che l'MCD di due polinomi in $\mathbb{Z}[X]$ è per definizione il polinomio monico che divide ambedue i polinomi di grado massimale.

Cominciamo da (a). Si osservi che $P(-1)=0=Q(-1)$. Possiamo dunque dividere ambedue i polinomi per $(X+1)$. In particolare risulta $P(X)=(X+1)\cdot(X^2-2)$, $Q(X)=(X+1)\,(X^2-4)$. Osserviamo che entrambi i polinomi che appaiono nella scomposizione di P sono irriducibili mentre per quanto riguarda il fattore (X^2-4) nella scomposizione di Q esso può essere ulteriormente scomposto: $Q(X)=(X+1)\,(X-2)\,(X+2)$. Dunque $\mathrm{MCD}(P,Q)=(X+1)$.

Passiamo alla coppia (b). Scomponiamo in fattori irriducibili il polinomio $P(X)=X^4-4$. Osserviamo che $P(X)=(X^2+2)\cdot(X^2-2)$. La scomposizione non può essere portata più avanti poiché entrambi i polinomi sono irriducibili in $\mathbb{Z}[X]$. Per quanto riguarda $Q(X)$ possiamo innnanzitutto mettere in evidenza un $3\,X^8$: $Q(X)=3\,X^8\cdot(X^4-2)$. Il polinomio (X^4-2) non può essere ulteriormente scomposto in $\mathbb{Z}[X]$. Ne deduciamo che $\mathrm{MCD}(P,Q)=1$.

Coppia (c). Fattorizziamo il polinomio P. Innanzitutto $P(X)=X^{11}\cdot(X^3+X^2-X-1)$. Il secondo polinomio di tale fattorizzazione si annulla in 1 ed in -1; dividendo (X^3+X^2-X-1) per il polinomio (X^2-1) ci si accorge che -1 ha molteplicità algebrica 2. Dunque la fattorizzazzione di P è la seguente: $P(X)=X^{11}\cdot(X+1)^2\cdot(X-1)$.
Andiamo a fattorizzare il polinomio Q. Anche in questo caso Q ha uno zero in $X=1$ ed in $X=-1$. Pertanto Q è divisibile per (X^2-1). Otteniamo così: $Q(X)=(X+1)\cdot(X-1)\cdot(2\,X^2-X-1)$. Ora, il polinomio $(2\,X^2-X-1)$ si annulla ancora in 1, pertanto $(2\,X^2-X-1)=(2X+1)\,(X-1)$. Possiamo quindi scrivere la fattorizzazione di Q: $Q(X)=(X-1)^2\cdot(X+1)\cdot(2X+1)$. Scriviamo

quindi l'MCD: $\mathrm{MCD}(P,Q) = (X+1)(X-1)$. □

Esercizio 9. 7. Sia $K[X_1,..,X_n]$ l'anello dei polinomi in n-variabili sul campo K. Denoteremo con K^n lo spazio vettoriale n-dimensionale sul campo K e denoteremo con $S \subseteq K^n$ un suo sottoinsieme. Sia $J \subseteq K[X_1,..,X_n]$ un ideale di $K[X_1,...,X_n]$. Definiamo:

$$\mathcal{I}(S) = \{P \in K[X_1,...,X_n] \mid P(y_1,..,y_n) = 0_K \text{ per ogni } (y_1,..,y_n) \in S\}$$
$$\mathcal{V}(J) = \{(y_1,..,y_n) \mid P(y_1,..,y_n) = 0_K \text{ per ogni } P \in J\}$$

(A) Dimostrare che $\mathcal{I}(S)$ è un ideale di $K[X_1,...,X_n]$.
(B) Dimostrare che dati due ideali $J_1, J_2 \subseteq K[X_1,..,X_n]$ si ha $\mathcal{V}(J_1 \cap J_2) = \mathcal{V}(J_1) \cup \mathcal{V}(J_2)$.
[*Suggerimento. Un'inclusione è facile. La seconda si ottiene ragionando per assurdo*]
(C) Dimostrare che dati due ideali $J_1, J_2 \subseteq K[X_1,..,X_n]$ si ha $\mathcal{V}(J_1 + J_2) = \mathcal{V}(J_1) \cap \mathcal{V}(J_2)$.

Soluzione. Cominciamo dal punto (A). Siano $P, Q \in \mathcal{I}(S)$ allora chiaramente $P(s) - Q(s) = 0_K - 0_K = 0_K$, per ogni $s \in S$; questo dimostra che $\mathcal{I}(S)$ è un sottogruppo additivo. Sia ora $Q \in K[X_1, \ldots, X_n]$ e $P \in \mathcal{I}(S)$, allora $Q(s)\,P(s) = Q(s) \cdot 0_K = 0_K$ per ogni $s \in S$ e dunque $\mathcal{I}(S)$ è un ideale.

Risolviamo il punto (B). Un'inclusione è semplice: $J_1 \cap J_2$ infatti è contenuto sia in J_1 che in J_2. In particolare se $\underline{y} \in \mathcal{V}(J_1)$ oppure $\underline{y} \in \mathcal{V}(J_2)$ allora deve valere $P(\underline{y}) = 0_K$ per ogni $P \in \mathcal{V}(J_1 \cap J_2)$, da cui segue l'inclusione $\mathcal{V}(J_1) \cup \mathcal{V}(J_2) \subseteq \mathcal{V}(J_1 \cap J_2)$. Lavoriamo ora all'altra inclusione. Sia $\underline{y} \in \mathcal{V}(J_1 \cap J_2)$ e supponiamo che $\underline{y}$ non sia né in $\mathcal{V}(J_1)$ né in $\mathcal{V}(J_2)$. Allora esisterebbero due polinomi, uno $P \in \mathcal{V}(J_1)$ e l'altro $Q \in \mathcal{V}(J_2)$ tali che $P(\underline{y}) \neq 0_K$ e $Q(\underline{y}) \neq 0_K$. Ma allora dovrebbe risultare $(P \cdot Q)(\underline{y}) \neq 0_K$ (perché K è un campo) e questo non è possibile perché il polinomio $(P \cdot Q) \in \mathcal{V}(J_1 \cap J_2)$. Dunque $\underline{y} \in \mathcal{V}(J_1) \cup \mathcal{V}(J_2)$. Abbiamo così dimostrato l'inclusione $\mathcal{V}(J_1 \cap J_2) \subseteq \mathcal{V}(J_1) \cup \mathcal{V}(J_2)$.

Per quanto riguarda (C). Entrambe le inclusioni sono semplici da dimostrare: $\underline{y} \in \mathcal{V}(J_1) \cap \mathcal{V}(J_2) \Leftrightarrow P(\underline{y}) = Q(\underline{y}) = 0_K$ per ogni $P \in J_1$, $Q \in J_2$; quindi risulta $(P+Q)(\underline{y}) = 0_K$, per ogni $P \in J_1$, $Q \in J_2$ e dunque $\underline{y} \in \mathcal{V}(J_1 + J_2)$. Questo dimostra l'inclusione $\mathcal{V}(J_1) \cap \mathcal{V}(J_2) \subseteq \mathcal{V}(J_1 + J_2)$.
Per quanto riguarda l'inclusione opposta osserviamo che $J_1, J_2 \subseteq J_1 + J_2$, pertanto se $\underline{y} \in \mathcal{V}(J_1 + J_2)$ in particolare $P(\underline{y}) = 0_K = Q(\underline{y})$ per ogni $P \in J_1$, $Q \in J_2$ e dunque $\underline{y} \in \mathcal{V}(J_1) \cap \mathcal{V}(J_2)$. □