A.A. 2015-2016. CORSO DI ALGEBRA 1.
PROFF. P. PIAZZA, E. SPINELLI.
SOLUZIONE ESERCIZI FOGLIO 12.

Esercizio 12. 1. Sia A un anello unitario. Consideriamo $\mathcal{F}(A,A)$, l'insieme delle applicazioni da A in A. Notare che esse formano un anello unitario rispetto alle operazioni:

$$(f+g)(a) = f(a)+g(a)\,; \quad (f\cdot g)(a) = f(a)\cdot g(a)\,.$$

Denotiamo con $\mathcal{U}(A)$ l'insieme degli invertibili dell'anello A.
Definiamo infine per ogni $u \in \mathcal{U}(A)$ ed ogni $f \in \mathcal{F}(A,A)$ l'applicazione:

$$(u \bullet f) : A \to A\,; \quad (u \bullet f)(a) = u \cdot f(a \cdot u^{-1})$$

(A) Mostrare che se $\mathcal{U}(A)$ è commutativo allora valgono le seguenti proprietà:

$$(u\cdot u') \bullet f = u \bullet (u' \bullet f)\,; \quad 1_A \bullet f = f\,.$$

(B) Diremo che f è $\mathcal{U}(A)$-invariante se vale $(u \bullet f)(a) = f(a)$ per ogni $a \in A$. Mostrare che le funzioni $\mathcal{U}(A)$ invarianti formano un sottogruppo additivo di $(\mathcal{F}(A,A),+,\cdot)$ ma non sono un sottoanello.
(C) Mostrare che se f è $\mathcal{U}(A)$-invariante allora $f(1_A) = 1_A$ se e soltanto se $f(u) = u$ per ogni $u \in \mathcal{U}(A)$.
(D) Supponiamo adesso che f sia un omomorfismo di A e che sia $\mathcal{U}(A)$-invariante; dimostrare che vale: $f(u\,a\,u^{-1}) = u\,f(a)\,u^{-1}$ per ogni $u \in \mathcal{U}(A)$, per ogni $a \in A$.
(E) Determinare le funzioni $\mathcal{U}(\mathbb{Z})$-invarianti in $\mathcal{F}(\mathbb{Z},\mathbb{Z})$. Determinare gli $\mathcal{U}(\mathbb{Z})$-invarianti in $\mathbb{Z}[X]$.

Soluzione. Punto (A). Abbiamo $((u\cdot u')\bullet f)(a) = u\cdot u'\cdot f(a\,u'^{-1}\cdot u^{-1}) = (u \bullet (u'\cdot f(au'^{-1}))) = (u\bullet(u'\bullet f))(a)$. Per quanto riguarda l'identità dell'anello A invece: $(1_A \bullet f)(a) = 1_A \cdot f(a\cdot 1_a) = f(a)$.

Punto (B). Consideriamo due funzioni $\mathcal{U}(A)$-invarianti, f e g. Mostriamo che $f-g$ è anche lei $\mathcal{U}(A)$-invariante: sia $u \in \mathcal{U}(A)$ allora

$$(u\bullet(f-g))(a) = u\cdot(f-g)(au^{-1}) = u\,f(au^{-1}) - u\,g(au^{-1}) = (u\bullet f)(a) + (u\bullet g)(a) = f(a)-g(a) = (f-g)(a)$$

Anche la funzione m_{0_A}, $m_{0_A}(a) = 0_A$ per ogni $a \in A$ è chiaramente $\mathcal{U}(A)$-invariante, ne deduciamo che l'insieme delle funzioni $\mathcal{U}(A)$-invarianti forma un sottogruppo additivo dell'anello $(\mathcal{F}(A,A),+,\cdot)$. Non si tratta a priori di un sottoanello per la ragione seguente:

$$(u\bullet(f\cdot g))(a) = u\cdot(f\cdot g)(a\,u^{-1}) = u\cdot f(a\,u^{-1})\cdot g(a\,u^{-1}) = u^{-1}\cdot u\cdot f(a\,u^{-1})\cdot u\cdot g(a\,u^{-1}) =$$

$$= u^{-1}\cdot f(a)\cdot g(a) = u^{-1}\cdot(f\cdot g)(a) \neq (f\cdot g)(a)$$

Punto (C). Supponiamo che f sia $\mathcal{U}(A)$-invariante e supponiamo che valga $f(1_A) = 1_A$. Allora per ogni $u \in \mathcal{U}(A)$ vale $1_A = f(1_A) = (u\bullet f)(1_a) = u\cdot f(u^{-1})$ da cui ricaviamo che $f(u^{-1}) = u^{-1}$ per ogni $u \in \mathcal{U}(A)$.

Punto (D). Segue dalla definizione di omomorfismo di anelli e dalla definizione di funzione $\mathcal{U}(A)$-invariante sfruttando il punto (C): sappiamo infatti che un omomorfismo di anelli unitari manda l'unità in sé; segue quindi per (C), che un tale omomorfismo $f : A \to A$ deve mandare ogni $u \in \mathcal{U}(A)$ in sé stesso. Pertanto risulta per ogni $a \in A$ ed ogni $u \in \mathcal{U}(A)$:

$$(u\bullet f)(a) = u\cdot f(a\,u^{-1}) = u\cdot f(a)\cdot f(u^{-1}) = u\cdot f(a)\cdot u^{-1}$$

Punto (E). Ricordiamo che $\mathcal{U}(\mathbb{Z}) = \{\pm 1\}$. Ne deduciamo che le funzioni $\mathcal{U}(\mathbb{Z})$-invarianti sono quelle per cui vale $f(k) = (-1\bullet f)(k) = -f(-k)$ per ogni $k \in \mathbb{Z}$, ovvero le funzioni dispari da $\mathbb{Z}$ in $\mathbb{Z}$. In restrizione a $\mathbb{Z}[X]$ questo ci fornisce i polinomi dispari, ovvero i polinomi che non hanno monomi di grado pari. □

Esercizio 12. 2. Mostrare che il polinomio $P(X) = X^4 - 3X^2 + X + 5$ è irriducibile in $\mathbb{Q}[X]$.

Soluzione. Osserviamo innanzitutto che un tale polinomio non ammette zeri razionali, e che dunque non può essere fattorizzato come un prodotto di un polinomio di grado 1 per un polinomio di grado 3. Per vedere questo fatto ci è sufficiente applicare il criterio di Cartesio: $\frac{a}{b}$, frazione ridotta, è una radice razionale di P (che è un polinomio a coefficienti interi) se e soltanto se $b \mid 1$ ed $a \mid 5$ dunque i possibili zeri razionali sono ± 5 e ± 1. Valutando il polinomio in tali numeri si verifica che P non ha zeri razionali. Supponiamo quindi che si possa fattorizzare come prodotto di due polinomi irriducibili di grado 2 in $\mathbb{Q}[X]$. Per il Teorema di Gauss allora dovrebbe essere possibile scrivere P come prodotto di due polinomi di grado 2 in $\mathbb{Z}[X]$ (associati ai polinomi della fattorizzazione in $\mathbb{Q}[X]$). Essendo il polinomio P monico tali polinomi dovrebbero essere monici anch'essi. Dovrebbe quindi risultare:

$$(X^4 - 3X^2 + X + 5) = (X^2 + aX + b) \cdot (X^2 + cX + d)$$

Uguagliando i coefficienti dei monomi dello stesso grado troviamo quindi:

$$\begin{aligned} a + c &= 0 \\ ac + b + d &= -3 \\ bc + ad &= 1 \\ b \cdot d &= 5 \end{aligned}$$

L'ultima equazione ha come soluzioni intere $b = \pm 1, d = \pm 5$ e $b = \pm 5, d = \pm 1$; inoltre, dalla prima equazione si ottiene $a = -c$, e sostituendo nella terza equazione di ha $1 = a(d - b)$. Quest'ultima equazione implica che $d - b = \pm 1$, dunque in particolare sia b che d devono essere diversi da ± 1. In sistema perciò non ammette soluzioni, e dunque ne concludiamo che una tale fattorizzazione non esiste, contraddicendo dunque l'ipotesi che il polinomio P fosse fattorizzabile in $\mathbb{Q}[X]$ come prodotto di polinomi irriducibili di grado 2. □

Esercizio 12. 3. Consideriamo l'anello di polinomi $\mathbb{Z}[X]$. Siano $P(X) = X^{n+1} - 1$, $Q(X) = X^n - 1$; dimostrare che l'ideale generato da P, Q in $\mathbb{Z}[X]$ è principale.

Soluzione. Cominciamo osservando che possiamo fattorizzare come segue i due polinomi P e Q:

$$P(X) = (X-1)(X^n + X^{n-1} + \cdots + 1)\,; \quad Q(X) = (X-1) \cdot (X^{n-1} + X^{n-2} + \cdots + 1)$$

Mostriamo adesso che il polinomio $(X-1)$ genera l'ideale (P, Q). Osserviamo che dalla fattorizzazione precedente segue che $(X-1) \supseteq (P, Q)$. Mostriamo ora che possiamo scrivere $(X-1)$ come combinazione lineare a coefficienti in $\mathbb{Z}[X]$ di P e Q:

$$P(X) - XQ(X) = (X-1)[(X^n + \cdots + X + 1) - (X^n + \cdots + X)] = (X-1) \cdot 1 = (X-1)$$

Questo dimostra che $(X-1) \subseteq (P, Q)$, dimostrando così che l'ideale (P, Q) è principale. □

Esercizio 12. 4. Sia G un gruppo abeliano e siano H, K due sottogruppi di G. Siano $m = [G : H]$, $n = [G : K]$, $d := [G : H \cap K]$. Dimostrare che:

(1) $d \leq m \cdot n$; [*Suggerimento. Sfruttare le classi laterali di G/H e G/K*]
(2) $d \mid m \cdot n$;
(3) $d = m \cdot n$ se e soltanto se $G = \langle H, K \rangle$.

Soluzione. Osserviamo preliminarmente che il secondo punto implica il primo; tuttavia troviamo istruttivo dare una dimostrazione indipendente.

Punto (A). Siano $H\,x_1, \ldots, H\,x_m$ le classi laterali di H e siano $K\,y_1, \ldots, K\,y_n$ le classi laterali di K. Chiaramente risulta

$$G = \bigcup_{i=1}^{m} (H\,x_i) = \bigcup_{j=1}^{n} (K\,y_j) = \bigcup_{i,j} (Hx_i) \cap (Ky_j).$$

L'ultima espressione è l'unione di mn sottoinsiemi. Per dimostrare la tesi è dunque sufficiente dimostrare che ciascuno di questi mn sottoinsiemi è contenuto in un'unica classe laterale di $H \cap K$. Proviamo che per ogni scelta di (i, j) con $i \in \{1, \ldots m\}$ e $j \in \{1 \ldots n\}$, comunque scelti due elementi $a, b \in (Hx_i) \cap (Ky_j)$ vale la relazione $(H \cap K)a = (H \cap K)b$. Se scegliamo due tali elementi, le ipotesi implicano che $a \cdot b^{-1} \in H$ e $a \cdot b^{-1} \in K$, dunque $a \cdot b^{-1} \in H \cup K$ e quindi le classi $(H \cap K)a$ e $(H \cap K)b$

sono uguali.

Punto (B). Sia f l'omomorfismo dato da

$$f : G \longrightarrow G/H \times G/K$$

definito come $f(x) = (H\,x, K\,x)$. Osserviamo che f è un omomorfismo in quanto entrambe le sue componenti lo sono, essendo le proiezioni canoniche di G sui quozienti G/K e G/H (ricordiamo a tal proposito che essendo G abeliano in particolare ogni sottogruppo è normale).
Si ha che

$$\ker(f) = \{x \in G | x \in H, x \in K\} = H \cap K.$$

Quindi per il Primo Teorema di Omomorfismo f induce al quoziente un omomorfismo iniettivo $\varphi : G/(H \cap K) \longrightarrow G/H \times G/K$. L'esistenza di tale omomorfismo iniettivo ci consente di dedurre la seguente disuguaglianza sulle cardinalità dei gruppi coinvolti:

$$|G/(H \cap K)| \leq |G/H| \cdot |G/K| = mn,$$

da cui la tesi.

Punto (C). La tesi equivale a dimostrare che l'omomorfismo f introdotto al punto precedente è suriettivo se e solo se $\langle H, K\rangle = G$.
Se $G = \langle H, K\rangle$, sia $(Ha, Kb) \in G/H \times G/K$ un generico elemento nel codominio. Allora per ipotesi l'elemento $ab^{-1} \in G$ può essere scritto come $ab^{-1} = h \cdot k$ con $h \in H$ e $k \in K$. Allora, scegliamo come elemento $g = ah^{-1} = bk$; si ha che

$$f(g) = (Hg, Kg) = (Ha, Kb),$$

dunque la coppia (Ha, Kb) appartiene all'immagine di f. Dall'arbitrarietà di a, b segue che f è suriettivo.
Viceversa, supponiamo che f sia suriettivo. Allora per ogni $x \in G$ esiste $g \in G$ tale che $f((H \cap K)g) = (Hx, K)$. Dalla definizione di f, ciò significa che $Hg = Hx$, da cui $xg^{-1} \in H$, e $Kg = K$, cioè $g \in K$. Ne segue che $x = hg = hk \in \langle H, K\rangle$, da cui si ha l'inclusione $G \subseteq \langle H, K\rangle$; l'altra inclusione è ovvia. □

Esercizio 12.5. Un sottogruppo proprio M di un gruppo G è detto massimale se per ogni sottogruppo $H \leq G$ di G tale che $M \leq H$ vale la seguente dicotomia: o $H = M$ altrimenti $H = G$.

(A) Dimostrare che se $K \trianglelefteq G$ e $K < M$ allora M è massimale in G se e soltanto se M/K è massimale in G/K.
(B) Dimostrare che se G è un gruppo finito ogni sottogruppo di G è contenuto in un sottogruppo massimale di G.
(C) Mostrare che se G è un gruppo abeliano finito non banale i suoi sottogruppi massimali sono tutti e soli i sottogruppi il cui indice in G è primo.

Soluzione. Notazione: Dato un sottogruppo A di G, diremo che B un sottogruppo intermedio tra A e G se $A \subsetneq B \subsetneq G$.
Punto (A). Dalla teoria sappiamo che la proiezione canonica al quoziente $\pi : G \longrightarrow G/K$ induce una corrispondenza biunivoca tra i sottogruppi di G che contengono K e i sottogruppi di G/K; inoltre chiaramente tale corrispondenza preserva le inclusioni. Poiché i sottogruppi di G che contengono M contengono anche K, esiste un sottogruppo intermedio tra M e G se e solo se esiste un sottogruppo intermedio tra M/K e G/K. Ciò prova la tesi.

Punto (B). Procediamo per assurdo. Supponiamo che la tesi sia falsa; allora esisterebbero dei sottogruppi di G che non sono contenuti in nessun sottogruppo massimale. Sia H un sottogruppo di G non contenuto in nessun sottogruppo massimale, tale che H abbia il massimo ordine possibile tra tutti i sottogruppi che godono della proprietà di non massimalità (un tale H esiste perché G è finito). Allora H stesso non è massimale, quindi esiste un sottogruppo intermedio L tra H e G. Ma allora $|L| > |H|$, quindi poiché H ha la massima cardinalità tra i gruppi che godono della proprietà di non massimalità si ha che L è contenuto in un sottogruppo massimale M. Ma allora si avrebbe che $H \subseteq L \subseteq M$, contro

l'ipotesi su H.

Punto (C). Osserviamo che in un gruppo abeliano tutti i sottogruppi sono normali, ed utilizziamo il punto (A). Se $[G : K] = p$ è un numero primo, allora $K/K \cong \{0\}$ è un sottogruppo massimale di $G/K \cong \mathbb{Z}/p\mathbb{Z}$, in quanto sappiamo che un gruppo di ordine p primo ha solo sottogruppi banali.
Se invece $[G : K] = |G/K| = m$ non è un numero primo, allora esiste un primo p che divide m. Per il Teorema di Cauchy esiste un sottogruppo di G/K di ordine p, che un sottogruppo intermedio tra K/K e G/K. Ma allora esiste un sottogruppo intermedio tra K e G, dunque K non è massimale. □

Esercizio 12. 6. Sia G un gruppo finito e sia $\varphi \in Hom(G, G)$. Mostrare che esiste $N \in \mathbb{N}$ tale che per ogni $n \geq N$ risulta $|Im(\varphi^n)| = |Im(\varphi^N)|$.

Soluzione. Osserviamo preliminarmente che se φ è un automorfismo non c'è niente da dimostrare. Supponiamo quindi $\ker(\varphi)$ sia diverso da 1_G. Supponiamo che $\ker(\varphi) \cap Im(\varphi) = 1_G$ allora $\varphi|_{Im(\varphi)}$ è iniettiva ed inoltre $\varphi(Im(\varphi)) \subseteq \varphi(G) = Im(\varphi)$. Poiché φ è iniettiva in restrizione a $Im(\varphi)$ abbiamo allora che $|\varphi(Im(\varphi))| = |Im(\varphi)|$ ne concludiamo che $\varphi(Im(\varphi)) = Im(\varphi)$. Supponiamo dunque che $\ker(\varphi) \cap Im(\varphi) \neq 1_G$, ne deduciamo quindi che $|Im(\varphi^2)| < |Im(\varphi)|$. Proseguendo in questa maniera, essendo G un gruppo finito, arriviamo a dire che esiste un $N \in \mathbb{N}$ tale che $\ker(\varphi) \cap Im(\varphi^n) = 1_G$ per ogni $n \geq N$, ovvero che $|Im(\varphi^n)| = |Im(\varphi^N)|$ per ogni $n \geq N$. Se così non fosse infatti avremmo che per un numero infinito di $n_k \in \mathbb{N}$ vale $|Im(\varphi^{n_k})| < |Im(\varphi^{n_{k-1}})|$. Ma questo è impossibile perché G ha cardinalità finita. □

Esercizio 12. 7. Sia $\omega = \frac{1}{2} \cdot \left(-1 + i\sqrt{3}\right) = e^{\frac{i2\pi}{3}} \in \mathbb{C}$. Gli interi di Eisenstein sono l'insieme di numeri complessi del tipo $\mathscr{E} = \{a + b\,\omega \,|\, a, b \in \mathbb{Z}\}$.

(A) Dimostrare che $a + b\omega$ è una radice del polinomio monico a coefficienti in $\mathbb{Z}$

$$P_{a,b}(X) = X^2 - (2a - b)\,X + (a^2 - ab + b^2)$$

(B) Dedurre dal punto (A) che gli interi di Eisenstein, $\mathscr{E}$, sono il sottoanello di $\mathbb{C}$ denotato $\mathbb{Z}[\omega]$.
(C) Dimostrare che la funzione d che associa all'intero di Eisenstein $a + b\,\omega$ il modulo del termine noto del polinomio $P_{a,b}$ è ben definita ed è una funzione Euclidea su $\mathbb{Z}[\omega]$. [*Suggerimento. Come si relaziona tale funzione con la norma su* $\mathbb{C}$*? L'algoritmo di divisione è definito nel modo seguente: sia* $(a+b\,\omega)$ *il divisore e* $(c+d\,\omega)$ *il dividendo. Si consideri il reticolo di* $\mathbb{C}$ *dato dall'ideale* $\mathbb{Z}[\omega] \cdot (a+b\,\omega)$*. Tale reticolo fornisce una tassellazione di* $\mathbb{C}$ *in triangoli equilateri il cui lato ha lunghezza uguale alla norma complessa di* $a + b\omega$*. Poiché il reticolo dà luogo ad una tassellazione di* $\mathbb{C}$ *l'elemento* $c + d\,\omega$ *dovrà cadere in uno dei triangoli di tale tassellazione; il quoziente sarà allora l'elemento di* $\mathbb{Z}[\omega]$ *che moltiplicato per* $a+b\,\omega$ *fornisce l'elemento del reticolo più vicino (rispetto alla distanza della norma su* $\mathbb{C}$*)* $a\,c+d\,\omega$ *ed il resto sarà la differenza tra* $c+d\,\omega$ *e tale elemento. Esempio: allo scopo di sincerarvi di aver capito l'algoritmo di divisione verificate che una possibile divisione con resto di* $(-2-\omega)$ *per* $2 + 2\omega$ *è la seguente:* $-\omega - 2 = \omega \cdot (2 + 2\omega) - \omega$]

Soluzione. Punto (A). Calcoliamo esplicitamente $P_{a,b}(a + b\omega)$:

$$\left(a + \frac{b}{2}(-1 + i\sqrt{3})\right)^2 - (2a - b)\left(a + \frac{b}{2}(-1 + i\sqrt{3})\right) + (a^2 - ab + b^2) =$$

$$= a^2 - ab + \frac{b^2}{4} - \frac{3b^2}{4} + i \cdot \left(a - \frac{b}{2}\right) \cdot b\sqrt{3} - 2a^2 + 2ab - \frac{b^2}{2} - (2a - b) \cdot \frac{b\sqrt{3}}{2} + a^2 - ab + b^2 = 0$$

Punto (B). Osserviamo che $P_{0,1}(X) = X^2 + X + 1$, e dunque che ω verifica la relazione $\omega^2 = -\omega - 1$. Pertanto $\mathbb{Z}[\omega] = \mathscr{E}$: sfruttando infatti l'esercizio 10. 5 possiamo infatti dedurre che gli elementi del sottoanello di $\mathbb{C}$ definito come $\mathbb{Z}[\omega]$ possono essere scritti in modo unico come combinazioni lineari a coefficienti interi di $\{1, \omega\}$.

Punto (C). Allo scopo di verificare che la funzione $v : (a+b\omega) \mapsto a^2-ab+b^2$ definisce una valutazione su $\mathbb{Z}[\omega]$, cominciamo osservando che

$$|(a+b\omega)|^2 = \Big|\left(a-\frac{b}{2}\right)+\frac{b\sqrt{3}}{2}\Big|^2 = \left(a-\frac{b}{2}\right)^2+\left(\frac{b\sqrt{3}}{2}\right)^2 = a^2-ab+\frac{b^2}{4}+\frac{3b^2}{4} = a^2-ab+b^2$$

Pertanto la funzione proposta come valutazione è la restrizione al sottoanello $\mathbb{Z}[\omega]$ del quadrato dell'usuale norma di un numero complesso. Questo implica automaticamente il fatto che $v : \mathbb{Z}[\omega] \to \mathbb{N}$ è moltiplicativa: $v((a+b\omega)\cdot(c+d\omega)) = v(a+b\omega)\cdot v(c+d\omega)$. Per verificare che la funzione v così definita determina una valutazione sull'anello $\mathbb{Z}[\omega]$ non ci resta quindi che verificare che assegnati due interi di Eisenstein $(a+b\omega)$ e $(c+d\omega)$, volendo dividere $c+d\omega$ per $a+b\omega$ attraverso l'algoritmo definito nel Suggerimento, il resto $r+s\omega$ che si ottiene sia tale che $v(r+s\omega) < v(a+b\omega)$. Questo si verifica geometricamente, sfruttando il fatto che v coincide con il quadrato della norma usuale su $\mathbb{C}$. Siete invitati a verificare tale fatto. □

Esercizio 12. 8. Dimostrare in modo diretto che la funzione:

$$\gamma : \mathbb{Z}[X] \to \mathbb{N}\cup\{-\infty\},\ \gamma(P) := \deg(P) + \mathtt{t}(P)$$

non definisce una valutazione su $\mathbb{Z}[X]$ (denotiamo con $\mathtt{t}(P)$ il modulo del coefficiente direttore di P).

Soluzione. Siamo naturalmente a conoscenza del fatto che, non essendo $\mathbb{Z}[X]$ un PID esso in particolare non è un anello euclideo, pertanto non esistono su di esso funzioni di valutazione. Vogliamo però fornire un argomento diretto. A tal scopo si considerino i due polinomi seguenti: $P(X) = 15X^6$ e $Q(X) = 10X$. Risulta $\gamma(P) = 21, \gamma(Q) = 11$ ciò nonostante ogni possibile scrittura $P = S\,Q + R$ prevede un resto che verifica $\gamma(R) \geq \gamma(Q)$. Infatti o $S = 0$ nel qual caso $R = P$ e $\gamma(R) > \gamma(Q)$ altrimenti o $\deg(P-SQ) > \deg(P) > \deg(Q)$ nel qual caso $\mathtt{t}(P-SQ) = \mathtt{t}(SQ) \geq \mathtt{t}(Q)$ e dunque $\gamma(R) > \gamma(Q)$, altrimenti $\deg(P-SQ) = \deg(P)$ (non è infatti possibile cancellare il termine di grado 6) nel qual caso risulta sempre $\mathtt{t}(P-SQ) \geq 5$ ne segue anche in questo caso che $\gamma(R) \geq \deg(P)+5 = 6+5 = 11 = \gamma(Q)$. □

Esercizio 12. 9. Consideriamo $\mathbb{Z}_8[X]$ Definiamo per ogni $\overline{x} \in \mathcal{U}(\mathbb{Z}_8)$

$$(\overline{x} \bullet P)(X) = \overline{x}\cdot P(\overline{x}^{-1}\,X)$$

(A) Dimostrare le proprietà: $((\overline{xy}) \bullet P) = (\overline{x} \bullet (\overline{y} \bullet P))$, $\overline{1} \bullet P = P$.
(B) Diremo che P è $\mathcal{U}(\mathbb{Z}_8)$-invariante se $\overline{x} \bullet P = P$ per ogni $\overline{x} \in \mathcal{U}(\mathbb{Z}_8)$. Determinare l'insieme dei polinomi $\mathcal{U}(\mathbb{Z}_8)$-invarianti (denoteremo in seguito $\mathbb{Z}_8^{\mathcal{U}(\mathbb{Z}_8)}[X]$ tale insieme).
(C) Dimostrare che ogni polinomio P si scrive come $P = P' + P''$ dove P'' è $\mathcal{U}(\mathbb{Z}_8)$-invariante mentre P' non contiene alcun monomio $\mathcal{U}(\mathbb{Z}_8)$-invariante.
(D) Consideriamo la seguente applicazione:

$$\pi : \mathbb{Z}_8[X] \to \mathbb{Z}_8[X]\,, \qquad \pi(P) = \sum_{\overline{x}\in\mathcal{U}(\mathbb{Z}_8)} (\overline{x} \bullet P)$$

Mostrare che si tratta di un omomorfismo di gruppi. Sia $m_{\overline{2}}$ l'omomorfismo di anelli da $\mathbb{Z}_8[X]$ in sé dato dalla moltiplicazione per $\overline{2}$. Mostrare che $Im(\pi) = \ker(m_{\overline{2}}) \cap \mathbb{Z}_8^{\mathcal{U}(\mathbb{Z}_8)}[X]$.

Soluzione. La verifica di (A) è simile alla verifica fatta nell'esercizio 12.1 e pertanto non verrà replicata.

Per quanto riguarda (B) osserviamo preliminarmente che $\mathcal{U}(\mathbb{Z}_8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$. Si osserva quindi che per ogni elemento $\overline{x} \in \mathcal{U}(\mathbb{Z}_8)$ vale $\overline{x}^2 = \overline{1}$, o in altre parole $\overline{x}^{-1} = \overline{x}$. Un polinomio $P(X) = \overline{a}_0 + \overline{a}_1 X + \overline{a}_2 X^2 + \cdots + \overline{a}_n X^n$ è pertanto $\mathcal{U}(\mathbb{Z}_8)$-invariante se vale la seguente:

$$\overline{a}_0 + \overline{a}_1 X + \overline{a}_2 X^2 + \cdots + \overline{a}_n X^n = P(X) = (\overline{x} \bullet P)(X) = \overline{x}\cdot\overline{a}_0 + \overline{x}^2\overline{a}_1\,X + \overline{x}^3\overline{a}_2\,X^2 + \cdots + \overline{x}^{n+1}\overline{a}_n X^n =$$
$$= \overline{x}\overline{a}_0 + \overline{a}_1\,X + \overline{x}\overline{a}_2\,X^2 + \cdots + \overline{x}^{\delta_n}\overline{a}_n X^n$$

dove $\delta_n = 0$ se n è dispari e $\delta_n = 1$ per n pari; tale relazione inoltre deve valere per ogni $\overline{x} \in \mathcal{U}(\mathbb{Z}_8)$. Questo è possibile se e soltanto se i coefficienti dei monomi di grado pari sono tutti nulli (sapete spiegare il motivo?). Abbiamo quindi scoperto che i polinomi $\mathcal{U}(\mathbb{Z}_8)$-invarianti sono tutti e soli i polinomi

che non hanno monomi di grado pari.

Punto (C). Data quindi la precedente caratterizzazione è chiaro che ogni polinomio P in $\mathbb{Z}_8[X]$ può essere spezzato come somma del polinomio P' formato dai monomi di P di grado pari e P'' formato dai monomi di P di grado dispari.

Punto (D). Osserviamo che la trasformazione π agisce sui polinomi $\mathcal{U}(\mathbb{Z}_8)$-invarianti come la moltiplicazione per $\overline{4}$, infatti se $P \in \mathbb{Z}_8^{\mathcal{U}(\mathbb{Z}_8)}[X]$ è

$$\pi(P) = \sum_{\overline{x} \in \mathcal{U}(\mathbb{Z}_8)} (\overline{x} \bullet P)(X) = P(X) + P(X) + P(X) + P(X) = \overline{4} \cdot P(X)$$

Se invece P è un polinomio contenente esclusivamente monomi di grado pari per ciascun $\overline{x} \in \mathcal{U}(\mathbb{Z}_8)$ risulta: $(\overline{x} \bullet P)(X) = \overline{x} \cdot P(X)$ pertanto:

$$\pi(P) = \sum_{\overline{x} \in \mathcal{U}(\mathbb{Z}_8)} (\overline{x} \bullet P)(X) = \sum_{\overline{x} \in \mathcal{U}(\mathbb{Z}_8)} \overline{x} \cdot P(X) = \left(\sum_{\overline{x} \in \mathcal{U}(\mathbb{Z}_8)} \overline{x} \right) \cdot P = \overline{0}$$

Si osservi infine che dato P polinomio in $\mathbb{Z}_8[X]$, scritto $P = P' + P''$ come somma del polinomio ottenuto come somma dei suoi monomi di grado pari e della sua parte $\mathcal{U}(\mathbb{Z}_8)$-invariante risulta $\pi(P) = \pi(P' + P'') = \pi(P') + \pi(P'') = \pi(P'')$. Poiché $P \in \mathbb{Z}_8^{\mathcal{U}(\mathbb{Z}_8)}[X]$ implica $\pi(P) \in \mathbb{Z}_8^{\mathcal{U}(\mathbb{Z}_8)}[X]$ e poiché per ogni $P \in \mathbb{Z}_8[X]$ risulta $\pi(P) = \overline{4}\, P''$ è chiaro che $Im(\pi) \subseteq \ker(m_{\overline{2}}) \cap \mathbb{Z}_8^{\mathcal{U}(\mathbb{Z}_8)}[X]$. Il viceversa segue osservando che tale intersezione consiste esattamente dei polinomi i cui monomi sono tutti di grado dispari e i cui coefficienti sono tutti uguali a $\overline{4}$. Tali polinomi sono immagine tramite π dei polinomi in $\mathbb{Z}_8^{\mathcal{U}(\mathbb{Z}_8)}[X]$ i cui coefficienti sono tutti uguali ad $\overline{1}$. Ne segue l'uguaglianza $Im(\pi) = \ker(m_{\overline{2}}) \cap \mathbb{Z}_8^{\mathcal{U}(\mathbb{Z}_8)}[X]$. □