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

Esercizio 11.1. 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 valgono le seguenti proprietà:

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

(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 $\mathbb{Z}[X]$.

Esercizio 11.2. Mostrare che il polinomio $P(X) = X^4 - 3X^2 + X + 5$ è irriducibile in $\mathbb{Q}[X]$.

Esercizio 11.3. 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.

Esercizio 11.4. 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) $d \,|\, m \cdot n$;
(3) $d = m \cdot n$ se e soltanto se $G = \langle H, K \rangle$.

Esercizio 11.5. 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.

Esercizio 11.6. 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 $|Im(\varphi^n)| = |Im(\varphi^N)|$.

ESERCIZI PER CASA

Esercizio 11.7. 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 $\mathscr{E} = \{a + b\,\omega \mid a, b \in \mathbb{Z}\}$.

(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 valutazione 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: $-\omega - 2 = \omega \cdot (2 + 2\omega) - \omega$*]

Esercizio 11.8. 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).

Esercizio 11.9. 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 $Im(\pi) = \ker(m_{\overline{2}}) \cap \mathbb{Z}_8^{\mathcal{U}(\mathbb{Z}_8)}[X]$.