Corso di Algebra 1 - a.a. 2009-2010

Prova scritta del 25.1.2011

1. Trovare tutte le soluzioni intere nell'intervallo $[20, 80]$ del sistema di congruenze
$$\begin{cases} 2x \equiv 5 \mod 9 \\ x \equiv 10 \mod 12 \end{cases}$$

2. Sia G l'insieme dei numeri complessi z tali che $z^n = 1$ per qualche intero positivo n.
   (a) Dimostrare che G è un sottogruppo di $\mathbb{C}^*$.
   (b) Dimostrare che, per ogni intero positivo n, G contiene un unico sottogruppo di ordine n.

3. Sia $f\colon G \to G'$ un omomorfismo suriettivo di gruppi tale che il nucleo K di f sia contenuto nel centro di G.
   (a) Mostrare che la seguente applicazione è ben definita:
$$\begin{aligned} \alpha\colon G' \times G' &\to G \\ (g'_1, g'_2) &\mapsto g_1 g_2 g_1^{-1} g_2^{-1} \end{aligned}$$
   dove $g_i \in f^{-1}(g'_i)$ per $i = 1, 2$.
   (b) Mostrare che se G' è abeliano, allora l'immagine di α è contenuta in K.

4. Sia A un anello e I un ideale sinistro di A. Dimostrare che l'insieme $\tilde{A} = A \times I$ con le operazioni
$$\begin{aligned} (a, i) + (a', i') &= (a + a', i + i') \\ (a, i)(a', i') &= (aa', ai' + a'i) \end{aligned}$$
   è un anello. Dimostrare inoltre che $\tilde{I} = \{0\} \times I$ è un ideale (bilatero) di $\tilde{A}$ e che l'anello quoziente $\tilde{A}/\tilde{I}$ è isomorfo a A.

5. Dire se i seguenti anelli sono domini e/o campi:
   (a) $(\mathbb{Z}/3\mathbb{Z})[X]/(X^2 + 1)$;
   (b) $\mathbb{Z}[X]/(2, X^2 + 1)$.

Soluzioni

1. La prima congruenza è equivalente a $x \equiv 7 \mod 9$, mentre la seconda è equivalente (per il teorema cinese del resto, essendo $12 = 3 \cdot 4$ e $\mathrm{mcd}(3,4) = 1$) al sistema
$$\begin{cases} x \equiv 10 \mod 3 \\ x \equiv 10 \mod 4 \end{cases}$$
Poiché la prima di tali congruenze è automaticamente soddisfatta quando $x \equiv 7 \mod 9$, il sistema di partenza è equivalente al sistema
$$\begin{cases} x \equiv 7 \mod 9 \\ x \equiv 10 \mod 4 \end{cases}$$
Di nuovo per il teorema cinese del resto, questo sistema ha un'unica soluzione modulo $9 \cdot 4 = 36$, che si vede facilmente essere $x \equiv 34 \mod 36$. Dunque le soluzioni nell'intervallo $[20, 80]$ sono 34 e 70.

2. (a) Chiaramente $G \subseteq \mathbb{C}^*$ perché $0 \notin G$. Inoltre $G \neq \emptyset$ perché $1 \in G$. Resta dunque da dimostrare che, se $x, y \in G$, anche $xy^{-1} \in G$. Infatti per ipotesi esistono interi positivi m, n tali che $x^m = y^n = 1$, quindi
$$(xy^{-1})^{mn} = x^{mn}y^{-mn} = (x^m)^n(y^n)^{-m} = 1^n1^{-m} = 1,$$
cioè $xy^{-1} \in G$.

   (b) Per ogni intero positivo n sia $\epsilon_n := e^{2\pi i/n} \in \mathbb{C}$. Chiaramente $\epsilon_n \in G$ e $\mathrm{ord}(\epsilon_n) = n$, dunque il sottogruppo H_n di G generato da ϵ_n ha ordine n. Se H è un altro sottogruppo di G di ordine n e $z \in H$, allora (per il teorema di Lagrange) $z^n = 1$, per cui $z = \epsilon_n^k$ per qualche $k \in \mathbb{Z}$, cioè $z \in H_n$. Questo dimostra che $H \subseteq H_n$, e, poiché $\#H = \#H_n = n$, $H = H_n$.

3. (a) $f^{-1}(g'_i) \neq \emptyset$ perché f è suriettivo. Se inoltre $g_i, h_i \in f^{-1}(g'_i)$ (per $i = 1, 2$), cioè $f(g_i) = f(h_i) = g'_i$, allora $f(g_ih_i^{-1}) = f(g_i)f(h_i)^{-1} = g'_ig_i'^{-1} = 1$. Questo significa che $g_ih_i^{-1} \in K$, e quindi esiste $k_i \in K$ tale che $g_i = k_ih_i$. Poiché k_i e k_i^{-1} appartengono al centro di G, otteniamo
$$\begin{aligned} g_1g_2g_1^{-1}g_2^{-1} &= k_1h_1k_2h_2(k_1h_1)^{-1}(k_2h_2)^{-1} \\ &= k_1h_1k_2h_2h_1^{-1}k_1^{-1}h_2^{-1}k_2^{-1} = h_1h_2h_1^{-1}h_2^{-1}, \end{aligned}$$
il che dimostra che α è ben definita.

(b) Bisogna dimostrare che $f(\alpha(g_1', g_2')) = 1$ per ogni $g_1', g_2' \in G'$. Infatti, scelti $g_i \in G$ (per $i = 1, 2$) tali che $f(g_i) = g_i'$, per definizione $\alpha(g_1', g_2') = g_1 g_2 g_1^{-1} g_2^{-1}$, e

$$f(g_1 g_2 g_1^{-1} g_2^{-1}) = f(g_1)f(g_2)f(g_1)^{-1}f(g_2)^{-1} = g_1' g_2' {g_1'}^{-1} {g_2'}^{-1} = 1$$

perché G' è abeliano.

4. $(\tilde{A}, +)$ è un gruppo abeliano perché prodotto dei due gruppi abeliani $(A, +)$ e $(I, +)$. L'elemento neutro moltiplicativo di A è $(1, 0)$, in quanto $(1, 0)(a, i) = (a, i) = (a, i)(1, 0)$ per ogni $(a, i) \in \tilde{A}$. Inoltre per ogni (a, i), (a', i') e (a'', i'') in $\tilde{A}$ si ha

$$\begin{aligned}(a, i)[(a', i')(a'', i'')] &= (a, i)(a'a'', a'i'' + a''i') \\ &= (aa'a'', aa'i'' + aa''i' + a'a''i) \\ &= (aa', ai' + a'i)(a'', i'') = [(a, i)(a', i')](a'', i'')\end{aligned}$$

(associatività del prodotto) e

$$\begin{aligned}(a, i)[(a', i') + (a'', i'')] &= (a, i)(a' + a'', i' + i'') \\ &= (aa' + aa'', ai' + ai'' + a'i + a''i) \\ &= (aa', ai' + a'i) + (aa'', ai'' + a''i) = (a, i)(a', i') + (a, i)(a'', i'')\end{aligned}$$

e analogamente $[(a', i') + (a'', i'')](a, i) = (a', i')(a, i) + (a'', i'')(a, i)$ (proprietà distributive).

$\tilde{I}$ è un ideale di $\tilde{A}$ perché $(0, 0) \in \tilde{I}$ e, dati $(0, i), (0, i') \in \tilde{I}$ e $(a, j) \in \tilde{A}$, si ha $(0, i) + (0, i') = (0, i + i') \in \tilde{I}$ e $(a, j)(0, i) = (0, ai) = (0, i)(a, j) \in \tilde{I}$.

La proiezione $\tilde{A} \to A$, $(a, i) \mapsto a$ è chiaramente un omorfismo suriettivo di anelli con nucleo $\tilde{I}$, dunque $\tilde{A}/\tilde{I} \cong A$ per il primo teorema di isomorfismo.

5. (a) L'anello dato è un dominio e/o un campo se e solo se l'ideale $(X^2 + 1)$ è primo e/o massimale in $(\mathbb{Z}/3\mathbb{Z})[X]$. Poiché quest'ultimo anello è un dominio a ideali principali (essendo $\mathbb{Z}/3\mathbb{Z}$ un campo), tali condizioni sono equivalenti e sono verificate perché $X^2 + 1$ è irriducibile in $(\mathbb{Z}/3\mathbb{Z})[X]$ (dato che è un polinomio di secondo grado senza radici in $\mathbb{Z}/3\mathbb{Z}$).

   (b) Per il terzo teorema di isomorfismo (applicato agli ideali $(2) \subseteq (2, X^2 + 1)$ nell'anello $\mathbb{Z}[X]$) e tenendo conto che $\mathbb{Z}[X]/(2) \cong (\mathbb{Z}/2\mathbb{Z})[X]$, l'anello dato è isomorfo a $(\mathbb{Z}/2\mathbb{Z})[X]/(X^2 + 1)$. Ragionando come nel punto precedente, concludiamo che esso non è né un dominio né un campo perché $X^2 + 1 = (X + 1)^2$ non è irriducibile in $(\mathbb{Z}/2\mathbb{Z})[X]$.