Corso di Algebra 1 - a.a. 2017-2018

Prova scritta del 22/02/2018

1. Trovare gli interi positivi x che verificano la congruenza

$$x^x \equiv 2 \mod n$$

per $n = 3$, $n = 4$ e $n = 5$.

2. Siano $f\colon G \to G'$ un omomorfismo di gruppi e

$$H := \{(a, b) \in G \times G \,:\, f(a) = f(b)\}.$$

   (a) Dimostrare che H è un sottogruppo di $G \times G$.

   (b) Dimostrare che H è abeliano se e solo se G è abeliano.

   (c) È vero che H è normale in $G \times G$ se G' è abeliano?

3. Dato un anello commutativo A, siano T un suo sottogruppo additivo e

$$B := \{b \in A \,:\, bt \in T \text{ per ogni } t \in T\}.$$

   (a) Dimostrare che B è un sottoanello di A.

   (b) Dimostrare che $B \cap T$ è un ideale di B.

   (c) Assumendo $A = \mathbb{Z}[X]$, trovare T tale che $B = \mathbb{Z}$ e $B \cap T = \{0\}$.

4. Siano p un numero primo e $f := 6X^4 + 5X^3 - X^2 + 6X - 1 \in \mathbb{Z}/p\mathbb{Z}[X]$.

   (a) Fattorizzare f per $p = 2, 3, 5$.

   (b) Esiste $p > 5$ tale che f sia irriducibile?

Soluzioni

1. Per $n = 4$ non ci sono soluzioni. Infatti, se x è dispari, anche ogni sua potenza lo è, e quindi $x^x \equiv 1, 3 \mod 4$; se invece $x = 2y$ (con y intero positivo) è pari, $x^x = 2^x y^x \equiv 0 \mod 4$, dato che $x \geq 2$.

   Per trattare i casi $n = 3$ e $n = 5$, osserviamo in generale che, se n è un primo dispari, risulta $\overline{2} \in \mathbb{Z}/n\mathbb{Z}^*$. Ciò chiaramente implica che, se x è una soluzione, allora $\overline{x} \in \mathbb{Z}/n\mathbb{Z}^*$ e $\overline{2} \in \langle \overline{x} \rangle$. D'altra parte, se quest'ultima condizione è verificata, per definizione esiste $k \in \mathbb{Z}$ tale che $\overline{x}^k = \overline{2}$, e si ha $\overline{x}^l = \overline{2}$ se e solo se $l \equiv k \mod m$ con $m := \mathrm{ord}(\overline{x}) = \#\langle \overline{x} \rangle$. Fissato dunque $\overline{x} \in \mathbb{Z}/n\mathbb{Z}^*$ tale che $\overline{2} \in \langle \overline{x} \rangle$, l'intero positivo x è una soluzione se verifica anche $x \equiv k \mod m$. Per trovare tutte le soluzioni si tratta quindi di risolvere, per ogni scelta di $\overline{a} \in \mathbb{Z}/n\mathbb{Z}^*$ tale che $\overline{2} \in \langle \overline{a} \rangle$, un sistema di congruenze della forma

$$\begin{cases} x \equiv a \mod n \\ x \equiv k \mod m. \end{cases}$$

   Tenendo conto che $\mathrm{mcd}(n, m) = 1$ (essendo n primo e $m \leq n - 1$), per il teorema cinese del resto tale sistema ha un'unica soluzione modulo nm.

   Se $n = 3$, l'unico valore di $\overline{a} \in \mathbb{Z}/3\mathbb{Z}^*$ tale che $\overline{2} \in \langle \overline{a} \rangle$ è $\overline{a} = \overline{2}$, e $\overline{2}^l = \overline{2}$ se e solo se $l \equiv 1 \mod 2$. Quindi le soluzioni sono gli interi positivi x che verificano il sistema

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 1 \mod 2, \end{cases}$$

   cioè $x \equiv 5 \mod 6$.

   Se $n = 5$, si ha $\overline{2} \in \langle \overline{a} \rangle$ se e solo se $\overline{a} = \overline{2}$ o $\overline{a} = \overline{3}$. Poiché $\overline{2}^l = \overline{2}$ se e solo se $l \equiv 1 \mod 4$ e $\overline{3}^l = \overline{2}$ se e solo se $l \equiv 3 \mod 4$, le soluzioni sono gli interi positivi x che verificano uno dei due sistemi

$$\begin{cases} x \equiv 2 \mod 5 \\ x \equiv 1 \mod 4 \end{cases} \qquad \begin{cases} x \equiv 3 \mod 5 \\ x \equiv 3 \mod 4, \end{cases}$$

   cioè $x \equiv 17, 3 \mod 20$.

2. (a) $H \neq \emptyset$ perché $(a, a) \in H$ per ogni $a \in G$. Se $(a, b), (c, d) \in H$ (cioè $f(a) = f(b)$ e $f(c) = f(d)$), allora $(a, b)(c, d)^{-1} = (ac^{-1}, bd^{-1}) \in H$ perché $f(ac^{-1}) = f(a)f(c)^{-1} = f(b)f(d)^{-1} = f(bd^{-1})$.

(b) È ovvio che, se G è abeliano, lo stesso vale per $G \times G$ e quindi per il suo sottogruppo H. Viceversa, se H è abeliano, per ogni $a, b \in G$ si ha (considerando che $(a,a), (b,b) \in H$)

$$(ab, ab) = (a,a)(b,b) = (b,b)(a,a) = (ba, ba),$$

per cui $ab = ba$.

(c) Se G' è abeliano H è normale in $G \times G$ perché per ogni $(a,b) \in H$ e per ogni $(c,d) \in G \times G$ si ha $(c,d)(a,b)(c,d)^{-1} = (cac^{-1}, dbd^{-1}) \in H$, dato che

$$\begin{aligned} f(cac^{-1}) &= f(c)f(a)f(c)^{-1} = f(a)f(c)f(c)^{-1} = f(a) \\ &= f(b) = f(b)f(d)f(d)^{-1} = f(d)f(b)f(d)^{-1} = f(dbd^{-1}). \end{aligned}$$

3. (a) $1 \in B$ perché $1t = t \in T$ per ogni $t \in T$. Se $b, b' \in B$, allora $b - b', bb' \in B$ perché per ogni $t \in T$ si ha $(b - b')t = bt - b't \in T$ (dato che $bt, b't \in T$ e T è un sottogruppo di A) e $(bb')t = b(b't) \in T$ (dato che $b't \in T$).

(b) Essendo intersezione di sottogruppi, $B \cap T$ è un sottogruppo di A, e dunque anche di B. Resta da dimostrare che, se $b \in B$ e $a \in B \cap T$, allora $ba \in B \cap T$. In effetti $ba \in B$ perché B è un sottoanello di A e $ba \in T$ per definizione di B.

(c) Sia per esempio $T := \{nX : n \in \mathbb{Z}\}$ (è un sottogruppo di $\mathbb{Z}[X]$ perché $0 = 0X \in T$ e $nX - mX = (n-m)X \in T$ per ogni $n, m \in \mathbb{Z}$). È allora chiaro che $\mathbb{Z} \subseteq B$, e se, viceversa, $f = \sum_{i \geq 0} a_i X^i \in B$, in particolare $fX = \sum_{i \geq 0} a_i X^{i+1} \in T$, per cui deve essere $a_i = 0$ per ogni $i > 0$, cioè $f = a_0 \in \mathbb{Z}$. Dunque $B = \mathbb{Z}$ e ovviamente anche $B \cap T = \{0\}$.

4. (a) Se $p = 2$, $f = X^3 + X^2 + 1$ è irriducibile (essendo di terzo grado e senza radici). Se $p = 3$, $f = -(X^3 + X^2 + 1)$ ha solo la radice 1 (con molteplicità 1) e la fattorizzazione è $f = -(X-1)(X^2 - X - 1)$. Se $p = 5$, $f = X^4 - X^2 + X - 1$ ha solo la radice 1 (con molteplicità 1) e la fattorizzazione è $f = (X-1)(X^3 + X^2 + 1)$.

(b) Non esiste $p > 5$ tale che f sia irriducibile. Se infatti esistesse un tale p, f sarebbe irriducibile anche in $\mathbb{Z}[X]$ (poiché p non divide il coefficiente di grado massimo di f, cioè 6), ma f ha la radice $\frac{1}{6}$ in $\mathbb{Q}$ e la sua fattorizzazione in $\mathbb{Z}[X]$ è $f = (6X-1)(X^3 + X^2 + 1)$.