SOLUZIONI DELL'APPELLO C DEL CORSO AL210 – ALGEBRA 2
11 GIUGNO 2019

(1) Si consideri il gruppo

$$G = \langle x, y | x^4 = 1, y^4 = 1, yxy^{-1} = x^3 \rangle.$$

(A) (3 punti) Dimostrare che ogni elemento di G si scrive in maniera unica nella forma (chiamata in seguito forma canonica)

$$x^h y^i \text{ con } h, i \in \mathbb{Z}_4,$$

con la solita convenzione che $a^0 x^0 = 1$ è l'identità di G.

Soluzione:

Ogni elemento di G si scrive come una parola con lettere x, x^{-1}, y e y^{-1}, e dunque si scriverà nella forma

$$g = x^{i_1} y^{j_1} x^{i_2} y^{j_2} \dots x^{i_k} y^{j_k},$$

per un certo $k \in \mathbb{N}$ e certi elementi $i_1, j_1, \dots, i_k, j_k \in \mathbb{Z}$.

Le prime due relazioni implicano che posso considerare gli indici $i_1, \dots, i_k$ e $j_1, \dots, j_k$ come elementi di $\mathbb{Z}_4$. L'ultima relazione implica che

$$y^j x^k = x^{3^j \cdot k} y^j \quad \text{per ogni } j, k \in \mathbb{Z}_4, \tag{0.1}$$

e questo consente di semplificare l'espressione di g fino a ridursi all'espressione in forma canonica $g = x^h y^i$ con $h, i \in \mathbb{Z}_4$.

Osserviamo anche che l'espressione in forma canonica non si può ulteriormente semplificare perché non contiene sottoparole della forma x^4 oppure y^4 oppure yxy^{-1}.

(B) (3 punti) Determinare la formula di moltiplicazione del gruppo G, cioè scrivere $(x^h y^i) \cdot (x^k y^j)$ (per $h, k, i, j \in \mathbb{Z}_4$) in forma canonica.

Soluzione:

Usando la formula (0.1), calcoliamo

$$(x^h y^i) \cdot (x^k y^j) = x^h x^{3^i \cdot k} y^i y^j = x^{h+3^i k} y^{i+j}. \tag{0.2}$$

(C) (4 punti) Calcolare l'ordine degli elementi di G e scrivere l'inverso di ogni elemento in forma canonica.

Soluzione:

Usando la formula (0.2), calcoliamo

$$\begin{cases} (x^k y^i)^2 = x^{k(3^i+1)} y^{2i}, \\ (x^k y^i)^4 = (x^{k(3^i+1)} y^{2i})^2 = x^{k(3^i+1)+3^{2i}k(3^i+1)} y^{4i} = x^{2k(3^i+1)} y^{4i} = 1, \end{cases} \tag{0.3}$$

dove si è usato il fatto che $3^2 \equiv 1 \mod 4$ e $(3^i + 1) \equiv 0$ o $2 \mod 4$ per ogni i. Dunque l'ordine degli elementi di G è dato da

$$o(x^k y^i) = \begin{cases} 1 & \text{se } (k, i) = (0, 0), \\ 2 & \text{se } (k, i) = (2, 0), (0, 2), (2, 2), \\ 4 & \text{altrimenti.} \end{cases} \tag{0.4}$$

Usando (0.4) e le formule (0.2), insieme al fatto che $3^2 \equiv 1 \mod 4$, calcoliamo che

$$(0.5) \qquad (x^k y^i)^{-1} = \begin{cases} 1 & \text{se } (k,i) = (0,0), \\ x^k y^i & \text{se } (k,i) = (2,0), (0,2), (2,2), \\ (x^k y^i)^3 = x^{k(3^i+2)} y^{3i} & \text{altrimenti.} \end{cases}$$

(D) (4 punti) Dimostrare che il centro di G è dato da $Z(G) = \{1, x^2, y^2, x^2y^2\}$.
Soluzione:
Un elemento $x^h y^i$ appartiene al centro di G se e solo se commuta con i due generatori x e y di G. Dalla formula (0.2) deduciamo che

$$\begin{cases} (x^h y^i)x = x^{h+3^i} y^i \quad \text{e} \quad x(x^h y^i) = x^{1+h} y^i, \\ (x^h y^i)y = x^h y^{i+1} \quad \text{e} \quad y(x^h y^i) = x^{3h} y^{i+1}. \end{cases}$$

Dunque $x^h y^i$ commuta con x se e solo se $i = 0, 2$ e $x^h y^i$ commuta con y se e solo se $h = 0, 2$. Dunque $Z(G) = \{1, x^2, y^2, x^2y^2\}$.
Siccome x^2 e y^2 commutano e hanno ordine 2 per il punto (C), segue che il sottogruppo generato da x^2 e y^2 è uguale a $\{1, x^2, y^2, x^2y^2\}$ ed è contenuto in $Z(G)$.

(E) (4 punti) Dimostrare che $Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ e che $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
Soluzione:
Siccome x^2 e y^2 commutano e hanno ordine 2 per il punto (C), segue che $\{1, x^2, y^2, x^2y^2\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Dalla presentazione di G deduciamo che il quoziente $G/Z(G)$ ha la seguente presentazione

$$G/Z(G) = \langle x, y | x^2 = 1, y^2 = 1, yxy^{-1} = x^3 = x \rangle,$$

o in altre parole, è generato da due elementi di ordine 2 che commutano. Questa è la stessa presentazione di $\mathbb{Z}_2 \times \mathbb{Z}_2$, da cui la conclusione segue.

(F) (4 punti) Dimostrare che gli unici sottogruppi di ordine 2 di G sono $\langle x^2 \rangle$, $\langle y^2 \rangle$ e $\langle x^2y^2 \rangle$ e che essi sono tutti normali.
Soluzione:
I sottogruppi di ordine due sono esattamente i sottogruppi ciclici generati dagli elementi di ordine due di G. Per il punto (C), deduciamo che tali sottogruppi sono $\langle x^2 \rangle$, $\langle y^2 \rangle$ e $\langle x^2y^2 \rangle$. Siccome ogni tale sottogruppo è contenuto nel centro per il punto (D), allora ogni tale sottogruppo è normale.

(G) (4 punti) Per ciascuno dei sottogruppi del punto precedente, si calcoli una presentazione del quoziente e si identifichi il quoziente con dei gruppi noti (cioè già visti a lezione).
Soluzione:
Dalla presentazione di G deduciamo che i quozienti in questione hanno la seguente presentazione

$$\begin{cases} G/\langle x^2 \rangle = \langle x, y | x^2 = 1, y^4 = 1, yxy^{-1} = x^3 = x \rangle, \\ G/\langle y^2 \rangle = \langle x, y | x^4 = 1, y^2 = 1, yxy^{-1} = x^3 \rangle, \\ G/\langle x^2y^2 \rangle = \langle x, y | x^4 = 1, y^4 = 1, x^2y^2 = 1, yxy^{-1} = x^3 \rangle = \\ \qquad = \langle x, y | x^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1} \rangle, \end{cases}$$

Dalle presentazioni di sopra, deduciamo che

$$G/\langle x^2 \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2, \quad G/\langle x^2 \rangle \cong D_4, \quad G/\langle x^2y^2 \rangle \cong Q.$$

(H) (4 punti) Dimostrare che il sottogruppo derivato $[G, G]$ di G è uguale a $\langle x^2 \rangle$. [Suggerimento: si usi la struttura di $G/\langle x^2 \rangle$ determinata in (G).]
Soluzione:
Siccome sappiamo che $G/\langle x^2 \rangle$ è abeliano per il punto (G) e $[G, G]$ è il più piccolo sottogruppo normale di G tale che il quoziente è abeliano, allora deduciamo che $G \subseteq \langle x^2 \rangle$. Tuttavia, siccome G non è abeliano, allora $G \neq \{1\}$. Dunque necessariamente deve essere che $[G, G] = \langle x^2 \rangle$.

(I) (4 punti) Dimostrare che $\langle x \rangle$ è un sottogruppo normale di G tale che $\langle x \rangle \cong \mathbb{Z}_4$ e $G/\langle x \rangle \cong \mathbb{Z}_4$.
Soluzione:
Il sottogruppo $\langle x \rangle$ è isomorfo a $\mathbb{Z}_4$ perché x ha ordine 4, come determinato nel punto (C). Inoltre il sottogruppo $\langle x \rangle$ è normale visto che $yxy^{-1} = x^3$. Infine, il quoziente $G/\langle x \rangle$ ha la seguente presentazione

$$G/\langle x \rangle = \langle x, y | x = 1, y^4 = 1, yxy^{-1} = x^3 \rangle = \langle y | y^4 = 1 \rangle$$

e dunque chiaramente $G/\langle x \rangle \cong \mathbb{Z}_4$.

(J) (4 punti) Dire se esiste un sottogruppo S di G tale che $G \cong \langle x \rangle \rtimes S$.
Soluzione:
Un tale sottogruppo è uguale a $\langle y \rangle$, visto che

$$G = \langle x \rangle \cdot \langle y \rangle \quad \text{e} \quad \langle x \rangle \cap \langle y \rangle = \{1\}.$$

(K) (5 punti) Dimostrare che le classi di coniugio di G sono

$$\{1\}, \{x^2\}, \{y^2\}, \{x^2y^2\}, \{x, x^3\}, \{y, x^2y\}, \{xy, x^3y\}, \{xy^2, x^3y^2\}, \{y^3, x^2y^3\}, \{xy^3, x^3y^3\}.$$

[Suggerimento: in alternativa ai conti, si possono usare le informazioni su $Z(G)$ (vedere punto (D)) e su alcuni quozienti abeliani di G (vedere i punti (G) e (I)).]
Soluzione:
Siccome $Z(G) = \{1, x^2, y^2, x^2y^2\}$ per il punto (D), segue che $\{1\}, \{x^2\}, \{y^2\}, \{x^2y^2\}$ sono classi di coniugio. Per determinare le altre classi, osserviamo che per ogni quoziente abeliano $G \twoheadrightarrow G/K$ le classi di coniugio di G sono contenute nella classi laterali di K. Usando il quoziente abeliano $G/\langle x^2 \rangle$ del punto (G), otteniamo che le altre classi di coniugio sono contenute nei seguenti sottoinsiemi

$$\{x, x^3\}, \{y, x^2y\}, \{xy, x^3y\}, \{xy^2, x^3y^2\}, \{y^3, x^2y^3\}, \{xy^3, x^3y^3\}.$$

Per concludere che le classi di coniugio sono uguali agli insiemi di sopra, bastare calcolare

$$\begin{cases} yxy^{-1} = yxy^3 = x^3yy^3 = x^3, \\ xyx^{-1} = xyx^3 = xx^{3\cdot 3}y = x^2y, \\ xxyx^{-1} = xxyx^3 = x^2x^{3\cdot 3}y = x^3y, \end{cases}$$

e usare che y^2 è nel centro di G.

(L) (4 punti) Dimostrare che gli unici sottogruppi di indice 2 sono $U_1 := \langle x, y^2 \rangle$, $U_2 := \langle x^2, y \rangle$ e $U_3 := \langle x^2, xy \rangle$.
[Suggerimento: ci si può ridurre (perché?) a classificare tutti gli omomorfismi suriettivi $G \twoheadrightarrow \mathbb{Z}_2$.]
Soluzione:

Tutti i sottogruppi di indice sono normali con quoziente isomorfo a $\mathbb{Z}_2$. E viceversa, dato un omomorfismo suriettivo $G \twoheadrightarrow \mathbb{Z}_2$ il suo nucleo è un sottogruppo di indice due di G.
Dunque, per trovare tutti i sottogruppi di G di indice 2, basta trovare tutti gli omomorfismi suriettivi $G \twoheadrightarrow \mathbb{Z}_2$ e poi prendere i loro nuclei. Dalla presentazione di G e dalla proprietà universale delle presentazioni dei gruppi, deduciamo che gli omomorfismi suriettivi $G \twoheadrightarrow \mathbb{Z}_2$ sono i seguenti

$$\begin{array}{lll} \phi_1 : G \longrightarrow \mathbb{Z}_2, & \phi_2 : G \longrightarrow \mathbb{Z}_2, & \phi_3 : G \longrightarrow \mathbb{Z}_2, \\ x \mapsto 0 & x \mapsto 1 & x \mapsto 1 \\ y \mapsto 1, & y \mapsto 0, & y \mapsto 1, \end{array}$$

I nuclei degli omomorfismi di sopra sono

$$\begin{cases} \ker(\phi_1) = \langle x, y^2 \rangle = U_1, \\ \ker(\phi_2) = \langle x^2, y \rangle = U_2, \\ \ker(\phi_3) = \langle x^2, xy, y^2 \rangle = U_2, \end{cases}$$

dove nell'ultima relazione abbiamo usato che $(xy)(xy) = x^{1+3}yy = y^2$.

(M) (4 punti) Per ciascuno dei sottogruppi U_i del punto precedente, si dica se esiste un sottogruppo L_i di G tale che $G \cong U_i \rtimes L_i$.

Soluzione:

Siccome il quoziente G/U_i è isomorfo a $\mathbb{Z}_2$, allora un sottogruppo L_i come quello cercato sarà necessariamente ciclico generato da un elemento di ordine 2. Dunque per il punto (C), dovrà essere che $L_i = \langle x^2 \rangle$, $\langle y^2 \rangle$ oppure $\langle x^2y^2 \rangle$. Da un'ispezione diretta, si vede che gli elementi $\{x^2, y^2, x^2y^2\}$ sono tutti contenuti in ciascun U_i, e dunque non esiste un tale sottogruppo L_i per ciascun gruppo U_i.

(N) (3 punti) Dimostrare che gli unici sottogruppi ciclici di ordine 4 sono

$$C_1 := \langle x \rangle, C_2 := \langle xy^2 \rangle, C_3 := \langle y \rangle, C_4 := \langle xy \rangle, C_5 := \langle x^2y \rangle, C_6 := \langle x^3y \rangle.$$

Soluzione:

Ogni sottogruppo ciclico di ordine 4 è generato da un elemento di ordine 4. Usando il punto (C), calcoliamo che i possibili tali gruppi sono

$$\begin{aligned} C_1 = \langle x \rangle = \langle x^3 \rangle &= \{1, x, x^2, x^3\}, \\ C_2 = \langle xy^2 \rangle = \langle x^3y^2 \rangle &= \{1, xy^2, x^2, x^3y^2\}, \\ C_3 = \langle y \rangle = \langle y^3 \rangle &= \{1, y, y^2, y^3\}, \\ C_4 = \langle x^2y \rangle = \langle x^2y^3 \rangle &= \{1, x^2y, y^2, x^2y^3\}, \\ C_5 = \langle xy \rangle = \langle xy^3 \rangle &= \{1, xy, y^2, xy^3\}, \\ C_6 = \langle x^3y \rangle = \langle x^3y^3 \rangle &= \{1, x^3y, y^2, x^3y^3\}. \end{aligned}$$

(O) (5 punti) Si dica quali dei sottogruppi C_i del punto precedente sono normali, e per ciascuno di essi si calcoli il quoziente G/C_i e si dica se l'estensione

$$0 \to C_i \to G \to G/C_i \to 0$$

spezza.
[Suggerimento: usare i punti (K) e (C).]

Soluzione:

Un sottogruppo è normale se e solo se è unione di classi di coniugio. Dalla lista delle classi di coniugio contenute in (K), si vede facilmente che solo C_1 e C_2 sono normali.
Per il sottogruppo $C_1 = \langle x \rangle$, la risposta è già stata calcolata nei punti (I) e (J): il quoziente G/C_1 è isomorfo a $\mathbb{Z}_4$ e vale che $G = C_1 \rtimes \langle y \rangle$. Dunque l'estensione in questione spezza.
Consideriamo ora il sottogruppo C_2. Il quoziente G/C_2 ha la seguente presentazione

$$G/C_2 = \langle x, y | x^4 = 1, y^4 = 1, yxy^{-1} = y^2, xy^2 = 1 \rangle = \langle x, y | y^4 = 1, x = y^{-2} = y^2 \rangle = \langle y | y^4 = 1 \rangle$$

e dunque è isomorfo a $\mathbb{Z}_4$. Da un'ispezione diretta si vede che

$$G = C_2 \cdot \langle y \rangle \quad \text{e} \quad C_2 \cap \langle y \rangle = \{1\}.$$

Quindi deduciamo che $G = C_2 \rtimes \langle y \rangle$ e dunque l'estensione in questione spezza.

(2) Sia p un primo e sia F un campo finito di caratteristica p.

(A) (4 punti) Dimostrare che se $f(x) \in \mathbb{Z}_p[x]$ è irriducibile di grado $n \geq 1$ allora $\mathbb{Z}_p[x]/(f(x))$ è un campo finito di cardinalità p^n.
Soluzione:
Siccome $\mathbb{Z}_p[x]$ è un PID, allora gli ideali massimali di $\mathbb{Z}_p[x]$ sono tutti e soli gli ideali della forma $(f(x))$ con $f(x)$ irriducibile (vedi Esercizio (2) dell'Appello B). Dunque, per ogni polinomio irriducibile $f(x)$ abbiamo che $\mathbb{Z}_p[x]/(f(x))$ è un campo. Se inoltre $f(x)$ ha grado n, allora gli elementi del quoziente $\mathbb{Z}_p[x]/(f(x))$ si possono scrivere univocamente nella forma

$$\mathbb{Z}_p[x]/(f(x)) = \{a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} \ : a_i \in \mathbb{Z}_p\},$$

da cui si evince che la cardinalità di $\mathbb{Z}_p[x]/(f(x))$ è p^n.

(B) (4 punti) Dimostrare che F contiene $\mathbb{Z}_p$ e la sua cardinalità è uguale a p^n per qualche $n \geq 1$.
Soluzione:
Dalla teoria sappiamo che F ha caratteristica p se e solo se F contiene (canonicamente) il campo $\mathbb{Z}_p$. Questo munisce F di una struttura di spazio vettoriale su $\mathbb{Z}_p$. Siccome F ha cardinalità finita, allora la dimensione di F come $\mathbb{Z}_p$-spazio vettoriale è finita, uguale ad un certo $n \geq 1$. Questo implica che la cardinalità di F è uguale a p^n.

(C) (4 punti) Dimostrare che F^* è un gruppo ciclico.
[Suggerimento: si può usare il seguente criterio di ciclicità: un gruppo abeliano finito G è ciclico se e solo se, per ogni $m \geq 1$, il gruppo G contiene al più m elementi di ordine che divide m].
Soluzione:
Usando il criterio di ciclicità ricordato nel suggerimento, basta controllare che, per ogni $m \geq 1$, F^* ha al più m elementi di ordine che divide m. Ma gli elementi di F^* di ordine che divide m sono esattamente le radici del polinomio $x^m - 1$. Dalla teoria sappiamo che $x^m - 1$ ha al più m radici su F, il che conclude la dimostrazione.

(D) (4 punti) Fissato un generatore g di F^*, si mostri che la mappa

$$\begin{aligned} \Psi : \mathbb{Z}_p[x] &\longrightarrow F \\ p(x) &\mapsto p(g), \end{aligned}$$

è un omomorfismo unitario e suriettivo di anelli. Dedurre che

$$F \cong \frac{\mathbb{Z}_p[x]}{(f(x))}$$

per un certo polinomio $f(x) \in \mathbb{Z}_p[x]$ irriducibile di grado n.

Soluzione:

La mappa Ψ è un omomorfismo unitario di anelli in quanto

$$\begin{cases} \Psi(p(x)+q(x)) = p(g)+q(g) = \Psi(p(x))+\Psi(q(x)), \\ \Psi(p(x)\cdot q(x)) = p(g)\cdot q(g) = \Psi(p(x))\cdot\Psi(q(x)), \\ \Psi(0) = 0(g) = 0, \\ \Psi(1) = 1(g) = 1. \end{cases}$$

Inoltre Ψ è suriettivo perché la sua immagine contiene $g \in F^*$ che è un generatore di $(F^*, \cdot)$.

Dunque per il teorema di fattorizzazione dei morfismi, abbiamo che Ψ induce un isomorfismo di anelli commutativi unitari

$$F \cong \frac{\mathbb{Z}_p[x]}{\ker(\Psi)}.$$

Siccome F è un campo per ipotesi, allora $\ker(\Psi)$ è un ideale massimale che, come ricordato nel punto (A), deve essere della forma $(f(x))$ con $f(x) \in \mathbb{Z}_p[x]$ polinomio irriducibile.

(3) Sia D un dominio a fattorizzazione unica e sia $F := Q(D)$ il suo campo dei quozienti.

(A) (5 punti) Sia $f(x) \in D[x] \subseteq F[x]$ un polinomio non constante monico (cioè con coefficiente direttore uguale a 1). Dimostrare che ogni fattore irriducibile monico di $f(x)$ in $F[x]$ è contenuto in $D[x]$.

Soluzione:

Consideriamo la fattorizzazione di $f(x)$ in irriducibili di $F[x]$:

$$f(x) = q_1(x)\dots q_n(x),$$

con $q_i(x) \in F[x]$ irriducibile e monico. Da un Lemma visto a lezione, sappiamo che ogni $q_i(x)$ si scrive come

$$q_i(x) = \gamma_i \cdot p_i(x),$$

con $\gamma_i \in F^*$ e $p_i[x] \in D[x]$ primitivo. Tuttavia, siccome $q_i(x)$ è monico e $p_i(x)$ ha coefficienti in D, allora γ deve essere necessariamente un'unità di D. Questo implica che $q_i(x)$ ha coefficienti in D come voluto.

(B) (5 punti) Dimostrare che gli elementi irriducibili di $D[x]$ sono gli elementi irriducibili di D (visti come polinomi costanti) e i polinomi non costanti $f(x) \in D[x]$ tali che $C(f) \sim 1$ e $f(x)$ è irriducibile in $F[x]$.

Soluzione:

Dalla teoria sappiamo che ogni polinomio $f(x) \in D[x]$ si scrive come

$$f(x) = C(f)p(x),$$

con $p(x) \in D[x]$ primitivo. Dunque se $f(x)$ è irriducibile, allora o $f(x) = C(f) \in D$ (e allora deve essere necessariamente un elemento irriducibile di D) oppure $f(x) \sim p(x)$ deve essere primitivo non costante. Da un Lemma visto a lezione, sappiamo che un polinomio primitivo non costante è irriducibile in $D[x]$ se e solo se è irriducibile in $F[x]$ e questo conclude la dimostrazione.