Algebra 2 - Primo appello - 4 febbraio 2013
Tema B

Nome e Cognome:

Matricola:

Es 1	Es 2	Es 3	Es 4	Es 5	Es 6	Tot

Risolvere ciascun esercizio su una pagina nuova

1. Siano x un elemento ed N un sottogruppo normale del gruppo finito G. Consideriamo l'elemento xN del gruppo quoziente G/N. Dimostrare che l'ordine (= periodo) di xN divide il massimo comun divisore tra l'ordine di x e l'indice $|G : N|$.

   Risoluzione. Sia n l'ordine di xN in G/N. Dobbiamo mostrare che n divide l'ordine di x in G e l'indice $|G : N|$. Che n divida $|G : N| = |G/N|$ segue dal teorema di Lagrange essendo n l'ordine del sottogruppo $\langle xN \rangle$ di G/N. Mostriamo che n divide l'ordine di x in G, sia esso m. Si ha $x^m = 1$, quindi $(xN)^m = N = 1_{G/N}$ in G/N, per cui l'ordine di xN in G/N divide m, cioè n divide m.

2. Sia F un campo con 9 elementi. Consideriamo il sottogruppo T del gruppo $\mathrm{GL}(2, F)$

$$T = \left\{ \begin{bmatrix} a & 0 \\ b & c \end{bmatrix} \mid a, b, c \in F,\ a \neq 0,\ c \neq 0 \right\}.$$

   (a) Determinare l'ordine di T.

   (b) Verificare che i sottoinsiemi H e K di T

$$H = \left\{ \begin{bmatrix} a & 0 \\ b & c \end{bmatrix} \in T \mid b = 0 \right\},\ K = \left\{ \begin{bmatrix} a & 0 \\ b & c \end{bmatrix} \in T \mid a = c = 1 \right\}$$

   sono sottogruppi di T.

   (c) Provare che K è normale in T.

   (d) Determinare il normalizzante $N_T(H)$.

   (e) Dire se H e K sono sottogruppi di Sylow di T.

   (f) Calcolare il numero dei 2-sottogruppi di Sylow e il numero dei 3-sottogruppi di Sylow di T.

   Risoluzione.

(a) Per determinare l'ordine di T dobbiamo contare le scelte per a, b, c. Siccome $a, c \neq 0$ abbiamo $9 - 1 = 8$ scelte per a, c e 9 scelte per b, quindi $|T| = 8^2 \cdot 9 = 2^6 \cdot 3^2$.

(b) Che H e K contengano l'identità di $GL(2, F)$, cioè la matrice identica, è chiaro, basta scegliere $a = c = 1$ per H, e $b = 0$ per K. Dati $a, c, a', c' \neq 0$ e b in F, si ha

$$\begin{bmatrix} a & 0 \\ b & c \end{bmatrix} \cdot \begin{bmatrix} a' & 0 \\ b' & c' \end{bmatrix} = \begin{bmatrix} aa' & 0 \\ ba' + b'c & cc' \end{bmatrix}.$$

Questo implica che H e K sono chiusi rispetto al prodotto, infatti se $b = b' = 0$ allora $ba' + b'c = 0$ e se $a = c = a' = c' = 1$ allora $aa' = cc' = 1$. Implica anche che H e K sono chiusi rispetto agli inversi, basta scegliere $a' = a^{-1}$, $c' = c^{-1}$ per H e $b' = -b$ per K. Inoltre

$$\begin{bmatrix} a & 0 \\ b & c \end{bmatrix}^{-1} = \begin{bmatrix} a^{-1} & 0 \\ -b(ac)^{-1} & c^{-1} \end{bmatrix}.$$

(c) La formula esibita sopra implica che l'applicazione

$$\varphi : T \to T, \qquad \begin{bmatrix} a & 0 \\ b & c \end{bmatrix} \mapsto \begin{bmatrix} a & 0 \\ 0 & c \end{bmatrix}$$

è un omomorfismo di gruppi. Il suo nucleo è K, che quindi è normale in T (è il nucleo di un omomorfismo di gruppi).

(d) Un elemento $\begin{bmatrix} x & 0 \\ y & z \end{bmatrix} \in GL(2, F)$ appartiene al normalizzante $N_T(H)$ se e solo se per ogni $a, c \in F - \{0\}$ l'elemento

$$\begin{bmatrix} x^{-1} & 0 \\ -y(xz)^{-1} & z^{-1} \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & c \end{bmatrix} \begin{bmatrix} x & 0 \\ y & z \end{bmatrix} =$$

$$\begin{bmatrix} x^{-1} & 0 \\ -y(xz)^{-1} & z^{-1} \end{bmatrix} \begin{bmatrix} ax & 0 \\ cy & cz \end{bmatrix} = \begin{bmatrix} a & 0 \\ -yaz^{-1} + cyz^{-1} & c \end{bmatrix}$$

appartiene ad H, cioè $yaz^{-1} = cyz^{-1}$. Questo è ovviamente vero se $y = 0$, quindi supponiamo $y \neq 0$. Dividendo entrambi i membri per yz^{-1} troviamo $a = c$. Questo non può essere vero per ogni $a, c \in F - \{0\}$. Deduciamo che $y = 0$ e quindi $N_T(H) = H$.

(e) Determiniamo gli ordini $|H|$, $|K|$. Per quanto riguarda H, abbiamo 8 scelte per a e per c e quindi $|H| = 8^2 = 2^6$. Per quanto riguarda K, abbiamo 9 scelte per b e quindi $|K| = 9 = 3^2$. Si ha $|T| = 2^6 \cdot 3^2$, quindi effettivamente H è un 2-Sylow di T e K è un 3-Sylow di T.

(f) Siccome K è normale in T, K è l'unico 3-Sylow di T, cioè $N_3 = 1$. Come visto sopra $N_T(H) = H$, quindi il numero di 2-Sylow di T è uguale a $N_2 = |T : N_T(H)| = |T : H| = 2^6 \cdot 3^2 / 2^6 = 9$.

3. Siano $H = \langle a \rangle$ un gruppo ciclico infinito e $K = \langle b \rangle$ un gruppo ciclico finito di ordine $n > 1$.

   Dimostrare che il prodotto diretto $H \times K$ non è ciclico.

   Risoluzione. Per assurdo, $H \times K$ sia ciclico, e sia (x, y) un suo generatore, con $x \in H$ e $y \in K$. Allora esiste un intero $m \geq 0$ tale che $(x, y)^m = (1, b)$, cioè $x^m = 1$ e $y^m = b$. Siccome K è un gruppo ciclico infinito, da $x^m = 1$ segue che $x = 1$ oppure $m = 0$. Non può essere $x = 1$ perché le potenze di $(1, y)$ sono della forma $(1, y^k)$, quindi non esauriscono tutti gli elementi di $H \times K$, essendo $H \neq \{1\}$. Ne segue che $m = 0$. Ma allora $b = y^m = 1$ e quindi $n = |K| = 1$, assurdo.

4. Sia $f = x^4 - x^2 + 4 \in \mathbb{Q}[x]$.

   (a) Verificare che f non ha zeri reali.

   (b) Verificare che f è irriducibile in $\mathbb{Q}[x]$.

   (c) Sia $u \in \mathbb{C}$ uno zero di f. Verificare che anche $v = \frac{2}{u}$ è uno zero di f.

   (d) Controllare se $\mathbb{Q}(u)$ è campo di spezzamento di f su $\mathbb{Q}$.

   Risoluzione.

   (a) Per dimostrare che f non ha zeri reali basta dimostrare che $f(x) > 0$ per ogni $x \in \mathbb{R}$. Studiando la derivata f' troviamo che f ha due minimi, $x = \pm\sqrt{2}/2$, e per tali valori di x si ha $x^2 = 1/2$ e quindi $f(x) = 1/4 - 1/2 + 4 > 0$. Ne segue che $f(x) > 0$ per ogni $x \in \mathbb{R}$, quindi f non ha zeri reali.

   (b) Per il punto precedente, rimane da controllare che non si abbiano fattorizzazioni in due fattori di grado 2. Per il lemma di Gauss, possiamo supporre che l'eventuale fattorizzazione avvenga in $\mathbb{Z}[x]$. Scriviamo quindi

   $$(x^2 + ax + b)(x^2 + cx + d) = x^4 - x^2 + 4$$

   con $a, b, c, d \in \mathbb{Z}$ e svolgendo il prodotto troviamo

   $$a + c = 0,\ d + ac + b = -1,\ ad + bc = 0,\ bd = 4.$$

   Sostituendo la prima nella terza troviamo $a(d - b) = 0$. Se $a = 0$ allora $c = 0$, $d + b = -1$ e $bd = 4$, quindi $b(-1 - b) = 4$, cioè $b^2 + b + 4 = 0$, e questa equazione non ha soluzioni reali. Deduciamo che $a \neq 0$ e quindi da $a(d - b) = 0$ segue $b = d$, per cui $b = d = \pm 2$ e $a + c = 0$, $2b - a^2 = -1$. Se $b = 2$ allora $a^2 = 5$, assurdo. Se $b = -2$ allora $a^2 = -3$, assurdo.

(c) Si ha $u^4 - u^2 + 4 = u^2(u^2-1) + 4 = f(u) = 0$, per cui $(1/u)^2 = (1-u^2)/4$.

$$\begin{aligned} f(2/u) &= (2/u)^4 - (2/u)^2 + 4 \\ &= 16((1-u^2)/4)^2 - 4(1-u^2)/4 + 4 \\ &= (1-u^2)^2 - (1-u^2) + 4 \\ &= u^4 - 2u^2 + 1 - 1 + u^2 + 4 \\ &= u^4 - u^2 + 4 = f(u) = 0. \end{aligned}$$

(d) Siccome $f(x)$ è un polinomio biquadratico e $u \neq 2/u$ sono due suoi zeri e $-u \neq 2/u$, i quattro zeri di $f(x)$ in $\mathbb{C}$ sono $u, -u, 2/u, -2/u \in \mathbb{Q}(u)$. Ne segue che $\mathbb{Q}(u)$ è effettivamente un campo di spezzamento per $f(x)$ su $\mathbb{Q}$.

5. (a) Sia n un intero positivo. Definire il polinomio ciclotomico n-esimo $\Phi_n(x)$.
   (b) Dimostrare che se $n > 1$ è dispari allora $\Phi_{2n}(x) = \Phi_n(-x)$.

Risoluzione.

(a) Il polinomio ciclotomico n-esimo $\Phi_n(x)$ è l'unico polinomio monico di $\mathbb{C}[X]$ che ha come zeri semplici le radici primitive n-esime di 1, in altre parole $\Phi_n(x) = \prod_{i=1,\ (i,n)=1}^{n}(x - \mu^i)$ dove μ è una radice primitiva n-esima di 1.

(b) Ricordiamo che si ha $x^n - 1 = \prod_{d|n} \Phi_d(x)$ e che il grado di $\Phi_n(x)$ è uguale al numero delle radici primitive n-esime di 1, cioè al numero di generatori del gruppo ciclico di ordine n generato da una delle radici primitive, cioè $\varphi(n)$, dove φ è la funzione di Eulero. Siccome $\Phi_2(x) = x+1 = -\Phi_1(-x)$ e $\Phi_6(x) = x^2 - x + 1 = \Phi_3(-x)$, argomentando per induzione su n abbiamo, per ogni $n \geq 3$ dispari,

$$\begin{aligned} \Phi_{2n}(x) &= \frac{x^{2n}-1}{\prod_{d|2n, d<2n} \Phi_d(x)} = \frac{x^n - 1}{\prod_{d|n} \Phi_d(x)} \cdot \frac{x^n+1}{\prod_{d|n, d<n} \Phi_{2d}(x)} \\ &= \frac{x^n+1}{\prod_{d|n,d<n} \Phi_d(-x)} = -\frac{x^n+1}{(-x)^n - 1}\Phi_n(-x) = \Phi_n(-x). \end{aligned}$$

6. Sia A un anello commutativo (con unità 1).
   (a) Completare la definizione: "Un ideale M di A è un ideale massimale se..."
   (b) Dimostrare che ogni ideale proprio I di A è contenuto in un ideale massimale.

Risoluzione.

(a) Un ideale M di A è un ideale massimale se $M \neq A$ e ogni volta che I è un ideale di A tale che $M \subseteq I$ si ha $I = M$ oppure $I = A$. In altre parole, M è un elemento massimale nella famiglia degli ideali propri di A parzialmente ordinato dall'inclusione.

(b) Sia $\mathcal{F}$ la famiglia degli ideali propri di A contenenti I, ordinata per inclusione. Per dimostrare l'asserto basta dimostrare che $\mathcal{F}$ ammette un elemento massimale. Per il lemma di Zorn, per fare questo basta mostrare che ogni catena in $\mathcal{F}$ ammette un maggiorante in $\mathcal{F}$. Sia $(I_k)_k$ una catena in $\mathcal{F}$. Senz'altro $J = \bigcup_k I_k$ contiene tutti gli ideali della catena $(I_k)_k$, e per concludere bisogna mostrare che $J \in \mathcal{F}$, cioè che J è un ideale proprio di A contenente I. Che J contenga I è chiaro, dato che J è unione di ideali contenenti I. Mostriamo che J è un ideale. Siano quindi $i, j \in J$ e $a \in A$. Dobbiamo mostrare che $ai, i + j \in J$. Per definizione di J, esistono due indici h, k tali che $i \in I_h$ e $j \in I_k$. Siccome $(I_k)_k$ è una catena, l'ordine indotto in essa è totale e quindi $I_h \subseteq I_k$ oppure $I_k \subseteq I_h$. Supponiamo senza perdita in generalità che $I_h \subseteq I_k$. Ne segue che $i \in I_h \subseteq I_k$ e quindi $i, j \in I_k$. Siccome I_k è un ideale di A, $ai, i + j \in I_k$. Siccome $I_k \subseteq J$, segue che $ai, i + j \in J$. Infine $1 \notin J$ (altrimenti $1 \in I_k$ per qualche I_k, e sarebbe $I_k = A$), quindi J è un ideale proprio.