Algebra 2 - 15 settembre 2014

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. Provare che i sottogruppi di un gruppo ciclico finito di ordine n sono in corrispondenza biunivoca con i divisori di n.

   Svolgimento. Sia D l'insieme dei divisori di n e sia S l'insieme dei sottogruppi del gruppo ciclico C_n. Dobbiamo costruire una biiezione $f : D \to S$. Scegliamo un generatore x di C_n cosicché $C_n = \langle x \rangle$ e definiamo

   $$f : D \to S, \qquad f(d) := \langle x^{n/d} \rangle.$$

   Mostriamo che f è biiettiva.

   - Iniettività. Supponiamo che $\langle x^{n/d_1} \rangle = \langle x^{n/d_2} \rangle$ per due divisori d_1, d_2 di n. Dobbiamo mostrare che $d_1 = d_2$. Osserviamo che per ogni divisore d di n si ha $o(x^{n/d}) = n/(n, n/d) = n/(n/d) = d$. Abbiamo quindi

     $$d_1 = o(x^{n/d_1}) = |\langle x^{n/d_1} \rangle| = |\langle x^{n/d_2} \rangle| = o(x^{n/d_2}) = d_2.$$

   - Suriettività. Sia H un sottogruppo di C_n, cioè $H \in S$. Sia $d := |H|$ il suo ordine. Per il teorema di Lagrange d divide n, cioè $d \in D$. Per concludere basta mostrare che $f(d) = H$, cioè che H è ciclico generato da $x^{n/d}$. Osserviamo che tutti gli elementi di C_n sono potenze di x, ed è così che le indicheremo d'ora in poi. Sia k il più piccolo intero positivo tale che $x^k \in H$. Dato un qualunque elemento $x^l \in H$ effettuando la divisione con resto tra l e k abbiamo $l = qk + r$ con q, r interi e $0 \leq r < k$. Ma allora $x^r = x^{l-qk} = x^l (x^k)^{-q} \in H$ perciò essendo $r < k$ segue $r = 0$ per minimalità di k. Ne segue che $x^l = (x^k)^q$ e quindi abbiamo dimostrato che ogni elemento di H è una potenza di x^k da cui $H = \langle x^k \rangle$. Ora si ha $d = |H| = o(x^k) = n/(n, k)$ da cui $(n, k) = n/d$ e resta da mostrare che $\langle x^k \rangle = \langle x^{(n,k)} \rangle$. Siccome (n, k) divide k è chiaro che x^k è una potenza di $x^{(n,k)}$ quindi resta da mostrare che $x^{(n,k)}$ è una potenza di x^k. Applicando l'algoritmo di Euclide troviamo a, b interi con $an + bk = (n, k)$ da cui $x^{(n,k)} = x^{an+bk} = (x^n)^a (x^k)^b = (x^k)^b$ essendo $x^n = 1$.

2. Sia $F = \mathbb{Z}/p\mathbb{Z}$ e sia $f(x) \in F[x]$ un polinomio irriducibile di grado n. Provare che $f(x)$ divide $x^{p^n} - x$.

   Svolgimento. Possiamo assumere che $f(x)$ sia monico dato che moltiplicare per uno scalare non nullo non cambia la relazione di divisibilità tra polinomi. Sia a una radice di $f(x)$ in un'opportuna estensione E di F. Essendo $f(x)$ irriducibile e monico, è il polinomio minimo di a e quindi come è noto dalla teoria $F[a]$ è un sovracampo di F di dimensione n su F da cui $|F[a]| = |F^n| = p^n$. Siccome $F[a]$ è un campo, $F[a] - \{0\}$ è un gruppo moltiplicativo di ordine $p^n - 1$ da cui $a^{p^n-1} = 1$. Moltiplicando entrambi i membri per a otteniamo $a^{p^n} = a$ cioè $a^{p^n} - a = 0$ da cui a è zero del polinomio $x^{p^n} - x$, o detto altrimenti il polinomio $x - a$ divide il polinomio $x^{p^n} - x$. Siccome a è zero anche di $f(x)$, $x - a$ divide anche $f(x)$ per cui il massimo comun divisore monico $P(x) := (f(x), x^{p^n} - x) \in F[x]$ è diverso da 1 (infatti ha a come zero). Ma allora $P(x)$ divide $f(x)$ e $P(x)$ è monico e diverso da 1, quindi siccome $f(x)$ è monico e irriducibile segue $P(x) = f(x)$. Dalla definizione di $P(x)$ segue allora che $f(x)$ divide $x^{p^n} - x$.

3. Si considerino le due permutazioni $a = (1, 2, 4, 6, 7)$, $b = (2, 6, 7, 4)$ e sia $G = \langle a, b\rangle$ il sottogruppo di S_7 generato da a e b.

   (a) Provare che $bab^{-1} \in \langle a\rangle$.

   (b) Determinare l'ordine di G.

   (c) Quanti sono i 2-sottogruppi di Sylow di G?

   (d) Quanti sono gli elementi di ordine 4 appartenenti a G?

   (e) E' vero che tutti gli elementi di G di ordine 4 sono coniugati?

   (f) Quante sono le classi di coniugio di G?

Svolgimento. (a)

$$bab^{-1} = (2, 6, 7, 4)(1, 2, 4, 6, 7)(2, 4, 7, 6) = (1, 6, 2, 7, 4) = a^3 \in \langle a\rangle.$$

(b) $A = \langle a\rangle$ e $B = \langle b\rangle$ hanno ordine coprimo (5 e 4 rispettivamente) quindi $A \cap B = \{1\}$. Siccome B normalizza A (per il punto 1) dalla teoria segue che $AB \leq G$ quindi $AB = \langle a, b\rangle = G$. Ne segue che $|G| = |AB| = |A||B|/|A \cap B| = |A||B| = 5 \cdot 4 = 20$.

(c) Siccome $aba^{-1} = (1, 2, 4, 6, 7)(2, 6, 7, 4)(1, 7, 6, 4, 2) = (1, 6, 4, 7)$ non è una potenza di b (muove 1), segue $aba^{-1} \notin B$ per cui B non è normale in G. D'altra parte è un 2-sottogruppo di Sylow di G e per il teorema di Sylow il numero di 2-sottogruppi di Sylow di G, che chiamerò n_2, divide $|G : B| = 5$ quindi è 1 oppure 5. Di nuovo per il teorema di Sylow siccome B non è normale in G, $n_2 \neq 1$ quindi $n_2 = 5$. Quindi G ha cinque 2-sottogruppi di Sylow.

(d) Siccome B è un 2-sottogruppo di Sylow ciclico di ordine 4, tutti i 2-sottogruppi di Sylow di G sono ciclici di ordine 4 (sono coniugati a B, in particolare sono isomorfi a B). Ogni 2-sottogruppo di Sylow contiene $\varphi(4) = 2$ elementi di ordine 4, e ogni elemento di ordine 4 è contenuto in un unico 2-sottogruppo di Sylow (quello che genera). Siccome $n_2 = 5$ segue che G ha $5 \cdot 2 = 10$ elementi di ordine 4.

(e) Contiamo i coniugati di b. Come è noto dalla teoria b ha esattamente $|G : C_G(b)|$ coniugati, dove $C_G(b) = \{g \in G \ : \ bg = gb\}$ è il centralizzante di b in G. Siamo ridotti a trovare tale centralizzante. Certamente $b \in C_G(b)$ (b commuta con se stesso) quindi $B \subseteq C_G(b)$. Siccome B ha ordine 4 e indice 5, se $C_G(b) \neq B$ allora $C_G(b) = G$, ma quest'ultima uguaglianza non è vera perché come visto nel punto (a), a e b non commutano (infatti $bab^{-1} = a^3 \neq a$) e quindi certamente $a \notin C_G(b)$. Ne segue che $C_G(b) = B$ ha ordine 4, quindi b ha $|G : C_G(b)| = |G|/|C_G(b)| = 20/4 = 5$ coniugati. Siccome G ha dieci elementi di ordine 4 (per il punto (d)), gli elementi di ordine 4 di G non sono tutti coniugati (altrimenti sarebbero tutti coniugati a b, assurdo dato che b ha solo cinque coniugati).

(f) Come visto nel punto (e) G ha due classi di elementi di ordine 4, ognuna di cardinalità 5. Siccome $bab^{-1} = a^3$, $b^k ab^{-k} = a^{3^k}$ da cui tutti gli elementi non identici di A sono coniugati ad a (le classi di $3^k \mod 5$ sono $1, 2, 3, 4$) quindi G ha una classe di elementi di ordine 5 che consiste dei 4 elementi a, a^2, a^3, a^4. C'è un unico elemento di ordine 2 in ogni 2-sottogruppo di Sylow (infatti un gruppo ciclico di ordine 4 ha un unico elemento di ordine 2) e siccome i 2-sottogruppi di Sylow sono coniugati anche gli elementi di ordine 2 risultano tutti coniugati. Riassumendo, G ha una classe di un elemento di ordine 1 (l'identità), 2 classi di cinque elementi ordine 4, una classe di quattro elementi di ordine 5 e una classe di cinque elementi di ordine 2.

4. Siano $\omega = \cos\left(\frac{2\pi}{n}\right)$ e $\epsilon = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$, radice primitiva ennesima dell'unità.

   (a) Qual è il grado di ϵ su $\mathbb{Q}$?

   (b) Provare che ω appartiene a $\mathbb{Q}[\epsilon]$.

   (c) Scrivere il polinomio minimo di ϵ su $\mathbb{Q}[\omega]$.

   (d) Determinare $[\mathbb{Q}[\omega] : \mathbb{Q}]$.

Svolgimento. (a) Sappiamo dalla teoria che ϵ ha grado $\varphi(n)$ su $\mathbb{Q}$, dove φ è la funzione di Eulero.

(b)

$$\begin{aligned} \omega &= \cos\left(\frac{2\pi}{n}\right) = \frac{1}{2}\left(\cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right) + \cos\left(\frac{2\pi}{n}\right) - i\sin\left(\frac{2\pi}{n}\right)\right) \\ &= \frac{1}{2}(\epsilon + \epsilon^{-1}) \in \mathbb{Q}[\epsilon]. \end{aligned}$$

(c) Per il punto (b) si ha $\omega = \frac{1}{2}(\epsilon + \epsilon^{-1})$ da cui moltiplicando per 2ϵ abbiamo $2\omega = \epsilon^2 + 1$, cioè ϵ è zero di $f(x) = x^2 - 2\omega + 1 \in \mathbb{Q}[\omega][x]$. Per mostrare che $f(x)$ è il polinomio minimo richiesto resta da mostrare che è irriducibile su $\mathbb{Q}[\omega]$. Se non lo fosse allora poiché ha grado 2 si avrebbe $\epsilon \in \mathbb{Q}[\omega]$ ma questo è falso perché $\epsilon \notin \mathbb{R}$ e $\mathbb{Q}[\omega] \subseteq \mathbb{R}$.

(d) Come visto in (c), $|\mathbb{Q}[\epsilon] : \mathbb{Q}[\omega]| = 2$ e come visto in (a) $|\mathbb{Q}[\epsilon] : \mathbb{Q}| = \varphi(n)$ da cui per la formula dei gradi $\varphi(n) = |\mathbb{Q}[\epsilon] : \mathbb{Q}| = |\mathbb{Q}[\epsilon] : \mathbb{Q}[\omega]| \cdot |\mathbb{Q}[\omega] : \mathbb{Q}| = 2|\mathbb{Q}[\omega] : \mathbb{Q}|$. Dividendo per 2 troviamo $|\mathbb{Q}[\omega] : \mathbb{Q}| = \varphi(n)/2$.

5. Sia $F = \mathbb{Z}/5\mathbb{Z}$ e sia $f(x) = x^{20} + x^{10} + 9 \in F[x]$.

   (a) Fattorizzare $f(x)$.

   (b) Determinare l'ordine di un campo di spezzamento di $f(x)$.

Svolgimento. (a) Ricordiamo che negli anelli di caratteristica p primo vale $(a + b)^p = a^p + b^p$ (endomorfismo di Frobenius) e $a^p \equiv a \mod p$ per ogni $a \in \mathbb{Z}$ (piccolo teorema di Fermat).

Ne segue che $f(x) = x^{20} + x^{10} + 9 = (x^4)^5 + (x^2)^5 + 9^5 = (x^4 + x^2 + 9)^5$. Siamo ridotti a fattorizzare $x^4 + x^2 + 9$, che non ha zeri in F (facile verifica). Un modo è esprimere tale polinomio come prodotto di due fattori di grado 2 e uguagliare i coefficienti. Un altro modo è scrivere $x^4 + x^2 + 9 = x^4 + 6x^2 + 9 = (x^2 + 3)^2$. Ne segue che $f(x) = (x^2 + 3)^{10}$. Il polinomio non può essere ulteriormente scomposto perché $x^2 + 3$ è irriducibile su F, infatti ha grado 2 e non ha zeri in F (facile verifica).

(b) Come visto $f(x) = (x^2 + 3)^{10}$ e $x^2 + 3$ è irriducibile, quindi detto α uno zero di $x^2 + 3$ in un'opportuna estensione di F, $F[\alpha]$ è un campo di spezzamento per $f(x)$ e ha grado 2 su F quindi ha ordine $|F^2| = |F|^2 = 5^2 = 25$.

6. Si consideri l'insieme I degli elementi $a + ib \in \mathbb{Z}[i]$ che soddisfano la proprietà che 6 divide sia $a + b$ che $a - b$.

   (a) Provare che I è un ideale di $\mathbb{Z}[i]$.

   (b) E' vero che I è un ideale massimale di $\mathbb{Z}[i]$?

   (c) Provare che se $a + ib$ è un elemento non nullo di I allora $a^2 + b^2 \geq 18$.

   (d) Quanti elementi ha l'anello $\mathbb{Z}[i]/I$?

   (e) Determinare $z = a + ib$ tale che $I = (z)$ (*suggerimento: ricordarsi che in un dominio euclideo un ideale non nullo è generato da un elemento non nullo di norma minima).*

Svolgimento. (a) È chiaro che $0 \in I$ dato che 6 divide 0. Se $a + ib, c + id \in I$ allora $a+ib+c+id = (a+c)+i(b+d)$ e $(a+c)+(b+d) = (a+b)+(c+d)$ è divisibile per 6 (infatti $a + b$ e $c + d$ lo sono quindi lo è la loro somma) e $(a + c) - (b + d) = (a - b) + (c - d)$ anche (infatti $a - b$ e $c - d$ lo sono quindi lo è la loro somma). Resta da mostrare che se $a + ib \in I$ e $c + id \in \mathbb{Z}[i]$ allora $(a + ib)(c + id) \in I$. Si ha $(a + ib)(c + id) = (ac - bd) + i(ad + bc)$ e $(ac - bd) + (ad + bc) = c(a + b) + d(a - b)$, $(ac - bd) - (ad + bc) = c(a - b) - d(a + b)$ sono divisibili per 6 perché $a + b$, $a - b$ lo sono.

(b) No, perché I è contenuto propriamente nell'insieme dei $a + ib \in \mathbb{Z}[i]$ tali che $a + b$ e $a - b$ sono divisibili per 3, e tale insieme è un ideale proprio di $\mathbb{Z}[i]$ (questo si dimostra analogamente al punto (a)).

(c) Scriviamo $a + b = 6h$ e $a - b = 6k$ con h, k interi. Allora $a - 6k = b = 6h - a$ da cui $a = 3(k + h)$ e $6h - b = a = 6k + b$ da cui $b = 3(h - k)$. Abbiamo allora $a^2 + b^2 = (3(k+h))^2 + (3(h-k))^2 = 18((k+h)^2 + (h-k)^2)$. Per mostrare che questo numero è maggiore o uguale di 18 basta mostrare che $(k + h)^2 + (h - k)^2 > 0$ (infatti questo equivale a dire che $(k+h)^2 + (h-k)^2 \geq 1$, essendo i numeri coinvolti interi), e siccome il membro sinistro di questa disuguaglianza è una somma di due quadrati, in particolare di due numeri non negativi, per concludere basta mostrare che almeno uno tra $h + k$ e $h - k$ è non nullo. Se per assurdo fosse $h + k = 0 = h - k$ allora segue facilmente $h = k = 0$ da cui $a + b = 0 = a - b$ da cui $a = b = 0$, e questo contraddice il fatto che $a + ib$ è non nullo.

(d) Osserviamo che I contiene l'ideale $J := \{a+ib \ : \ 6 \text{ divide } a, b\}$, e quozientare con J equivale a ridurre a, b modulo 6. Quindi $|\mathbb{Z}[i]/J| = 36$ e dato che I contiene J possiamo vedere $\mathbb{Z}[i]/I$ come quoziente di $\mathbb{Z}[i]/J$. Per determinare $|\mathbb{Z}[i]/I|$ basta quindi determinare $|I/J|$ (infatti $|\mathbb{Z}[i]/I| = |(\mathbb{Z}[i]/J)/(I/J)| = 36/|I/J|$), cioè basta contare le coppie (a, b) di interi modulo 6 tali che 6 divide sia $a+b$ che $a-b$. Ma questo equivale a dire che $a \equiv \pm b \mod 6$, in particolare $b \equiv -b \mod 6$ cioè 3 divide b. Ma allora ci sono solo due possibilità per $b \mod 6$, cioè 0 e 3, a cui corrispondono i valori $a = 0$ e $a = 3$ (modulo 6) rispettivamente per a. Ne segue che gli unici possibili valori di (a, b) modulo 6 sono $(0, 0)$ e $(3, 3)$. Abbiamo ottenuto che $|I/J| = 2$ e quindi $|\mathbb{Z}[i]/I| = |(\mathbb{Z}[i]/J)/(I/J)| = 36/|I/J| = 36/2 = 18$.

(e) Per il punto (c) ogni elemento di I ha norma maggiore o uguale di 18. In virtù del suggerimento basta quindi trovare un elemento di I di norma 18. Basta prendere $z = 3 + 3i$.