SVOLGIMENTO DELL'APPELLO DI ALGEBRA 2 DEL 25/02/2014 (SECONDO APPELLO)

1 Esercizio 1

Sia H un sottogruppo di G. Provare che se $|G : H|$ è finito allora H contiene un sottogruppo normale di G di indice finito.

Svolgimento. Consideriamo l'azione di G sull'insieme $\Omega = \{Hx \ : \ x \in G\}$ dei laterali destri di H in G data dalla moltiplicazione a destra: $\Phi : \Omega \times G \to \Omega$, $(Hx, g) \mapsto Hxg$. Sia N il nucleo di questa azione. Allora dalla teoria generale sappiamo che c'è un omomorfismo $G \to \mathrm{Sym}(\Omega)$ con nucleo N, da cui, per il primo teorema di isomorfismo, deduciamo un omomorfismo iniettivo $G/N \to \mathrm{Sym}(\Omega)$. Ora $|\Omega| = |G : H| = n$ è finito per ipotesi, quindi $\mathrm{Sym}(\Omega)$ è isomorfo al gruppo finito S_n (il gruppo simmetrico di grado n). Ne segue che esiste un omomorfismo iniettivo $G/N \to S_n$, in particolare $|G : N| = |G/N| \leq |S_n| = n!$. Quindi $|G : N|$ è anch'esso finito. Inoltre $N \subseteq H$ infatti se $g \in N$ allora g fissa tutti i laterali destri di H, in particolare fissa $H \cdot 1 = H$, cioè $Hg = H$, in altre parole $g \in H$.

2 Esercizio 2

Siano E, F, K tre campi con $E \leq F \leq K$ e sia $u \in K$. Provare che se F è algebrico su E e u è algebrico su F, allora u è algebrico su E.

Svolgimento. Poiché u è algebrico su F esiste un polinomio non nullo $P(x) \in F[x]$ che ha u come zero, cioè $P(u) = 0$. Scriviamo $P(x) = \sum_{i=1}^{k} a_i x^i$ con $a_0, \ldots, a_k \in F$ (osserviamo qui che siccome F è algebrico su E, $a_0, \ldots, a_k$ sono algebrici su E). Segue che u è algebrico su $E(a_0, a_1, \ldots, a_k)$, cioè il grado $|E(a_0, a_1, \ldots, a_k)(u) : E(a_0, a_1, \ldots, a_k)|$ è finito. Dobbiamo mostrare che u è algebrico su E, cioè che $E(u)$ ha dimensione finita su E, cioè che il grado $|E(u) : E|$ è finito. Siccome $E(u)$ è un E-sottospazio vettoriale di $E(a_0, \ldots, a_k)(u) = E(a_0, \ldots, a_k, u)$, basta mostrare che $|E(a_0, \ldots, a_k, u) : E|$ è finito. Per la formula dei gradi questo accade se e solo se $|E(a_0, a_1, \ldots, a_k, u) : E(a_0, a_1, \ldots, a_k)|$, $|E(a_0, a_1, \ldots, a_k) : E|$ sono finiti e in questo caso

$$|E(a_0, a_1, \ldots, a_k)(u) : E| = |E(a_0, a_1, \ldots, a_k, u) : E|$$

$$= |E(a_0, a_1, \ldots, a_k, u) : E(a_0, a_1, \ldots, a_k)| \cdot |E(a_0, a_1, \ldots, a_k) : E|.$$

Siccome $|E(a_0, a_1, \ldots, a_k)(u) : E(a_0, a_1, \ldots, a_k)|$ è finito, siamo ridotti a mostrare che il grado $|E(a_0, a_1, \ldots, a_k) : E|$ è finito. Mostriamolo per induzione su k. Se $k = 0$ allora abbiamo $|E(a_0) : E|$, che è finito perché a_0 è algebrico su E (essendo F algebrico su E). Supponiamo ora che $k > 0$. Per la formula dei gradi

$|E(a_0, a_1, \ldots, a_k) : E|$ è finito se e solo se $|E(a_0, a_1, \ldots, a_k) : E(a_0, \ldots, a_{k-1})|$ e $|E(a_0, a_1, \ldots, a_{k-1}) : E|$ sono finiti e in questo caso

$$|E(a_0, a_1, \ldots, a_k) : E| =$$

$$= |E(a_0, a_1, \ldots, a_k) : E(a_0, \ldots, a_{k-1})| \cdot |E(a_0, a_1, \ldots, a_{k-1}) : E|.$$

Siccome $|E(a_0, a_1, \ldots, a_{k-1}) : E|$ è finito per ipotesi induttiva siamo ridotti a mostrare che $|E(a_0, a_1, \ldots, a_k) : E(a_0, \ldots, a_{k-1})| = |E(a_0, a_1, \ldots, a_{k-1})(a_k) : E(a_0, \ldots, a_{k-1})|$ è finito, cioè che a_k è algebrico su $E(a_0, a_1, \ldots, a_{k-1})$. Ma per ipotesi F è algebrico su E, per cui a_k è algebrico su E, cioè esiste un polinomio $Q(x) \in E[x]$ non nullo con $Q(a_k) = 0$. Ma ovviamente è anche vero che $Q(x) \in E(a_0, \ldots, a_{k-1})[x]$ e quindi a_k è algebrico anche su $E(a_0, \ldots, a_{k-1})$.

3 Esercizio 3

Siano h e k i seguenti elementi del gruppo simmetrico S_8 : $h = (12345678)$, $k = (24)(37)(68)$.

1. Si calcoli khk^{-1} e si dica se il sottogruppo $\langle h \rangle$ è normale in $G = \langle h, k \rangle$.
2. È vero che $G = \langle h \rangle \langle k \rangle$?
3. Si determini il centro di G.

Svolgimento.

Punto 1. k ha ordine 2 quindi $k^{-1} = k$. Componendo le permutazioni (al solito, da destra a sinistra) abbiamo quindi

$$khk^{-1} = (24)(37)(68)(12345678)(24)(37)(68) = (14725836) = h^3.$$

Ne segue che se $n \in \mathbb{Z}$ allora $kh^n k^{-1} = (khk^{-1})^n = h^{3n}$, quindi $k\langle h \rangle k^{-1} = \langle h \rangle$. In altre parole k appartiene al normalizzante $N_{S_8}(\langle h \rangle)$. Siccome $h \in \langle h \rangle$, anche h appartiene al normalizzante $N_{S_8}(\langle h \rangle)$, quindi, siccome tale normalizzante è un sottogruppo di S_8, deduciamo che $G = \langle h, k \rangle$ è contenuto nel normalizzante $N_{S_8}(\langle h \rangle)$, cioè $\langle h \rangle$ è normale in G.

Punto 2. Sia $H = \langle h \rangle \langle k \rangle$. Ovviamente $H \subseteq G$ e H contiene h e k. Siccome G è generato da h e k, per concludere che $H = G$ basta mostrare che H è un sottogruppo di G. Che sia $1 \in H$ segue dal fatto che $1 \in \langle h \rangle$, $1 \in \langle k \rangle$ e $1 = 1 \cdot 1$. Siano $a, c \in \langle h \rangle$ e $b, d \in \langle k \rangle$. Chiusura dell'inverso: abbiamo $(ab)^{-1} = b^{-1}a^{-1}bb^{-1} \in \langle h \rangle \langle k \rangle = H$ essendo $b^{-1}a^{-1}b \in \langle h \rangle$ in quanto $a^{-1} \in \langle h \rangle$ e $\langle h \rangle \trianglelefteq G$. Chiusura del prodotto: $(ab)(cd) = abcd = abcb^{-1} \cdot bd \in \langle h \rangle \langle k \rangle$ essendo $bcb^{-1} \in \langle h \rangle$ in quanto $c \in \langle h \rangle \trianglelefteq G$.

Punto 3. Il centro di G è dato da quegli elementi $h^n k^m$ che commutano con ogni elemento di G, dove $n, m \in \mathbb{Z}$. Osserviamo che siccome h ha ordine 8 e k ha ordine 2, possiamo assumere che sia $n \in \{0, \dots, 7\}$ e $m \in \{0, 1\}$. Consideriamo il caso $m = 1$. Gli elementi $h^n k$ non stanno nel centro, infatti non commutano con h: $h \cdot h^n k = h^{n+1} k$ mentre $h^n kh = h^n khk^{-1} k = h^n h^3 k = h^{n+3} k$, e $h^{n+3} k \neq h^{n+1} k$ infatti se fosse $h^{n+3} k = h^{n+1} k$ allora moltiplicando a sinistra per h^{-n-1} e a destra per k^{-1} avremmo $h^2 = 1$, assurdo dato che h ha ordine 8. Quindi gli elementi del centro $Z(G)$ hanno tutti la forma h^n. Andiamo ora a vedere quali sono gli elementi della forma h^n che stanno nel centro di G. Tali elementi devono commutare con k, cioè dev'essere $h^n k = kh^n$, cioè, moltiplicando a destra per k^{-1}, $h^n = kh^n k^{-1} = (khk^{-1})^n = h^{3n}$, da cui, moltiplicando tutto per h^{-n}, $h^{2n} = 1$. Siccome h ha ordine 8, $h^{2n} = 1$ significa che 8 divide $2n$, cioè 4 divide n, cioè $h^n = 1$ oppure $h^n = h^4$ (ricordiamo infatti che $h^8 = 1$).

Per concludere che $Z(G) = \{1, h^4\}$ bisogna mostrare che effettivamente $h^4 \in Z(G)$. Ripercorrendo gli argomenti usati vediamo che h^n commuta con k se e solo se $h^{2n} = 1$, e questo è vero per $n = 4$ poiché h ha ordine 8. Siccome ovviamente h^4 commuta anche con h, essendo una sua potenza, il centralizzante di h^4 in G contiene $\langle k, h \rangle = G$ e quindi $h^4 \in Z(G)$.

4 Esercizio 4

Sia G un gruppo di ordine 253, non abeliano.

1. Provare che $Z(G) = 1$.
2. Sia $g \in G$ di ordine 11: quanti sono i coniugati di $g \in G$?
3. Quante sono le classi di coniugio di G e quanti elementi contiene ognuna di queste classi di coniugio?

Svolgimento. $253 = 11 \cdot 23$.

Punto 1. Se il centro $Z(G)$ non fosse $\{1\}$ allora, siccome G è non abeliano e $|G|$ è il prodotto di due primi, per il teorema di Lagrange $|Z(G)|$ è uguale a 11 oppure 23. Ma allora $G/Z(G)$ ha ordine 11 oppure 23, quindi è ciclico, e sappiamo che se $G/Z(G)$ è ciclico allora $G = Z(G)$, cioè G è abeliano, cosa esclusa per ipotesi.

Segue la dimostrazione che se $G/Z(G)$ è ciclico allora G è abeliano. Detto $x \in G$ tale che xZ genera G/Z, dove $Z = Z(G)$, siccome G/Z è ciclico ogni laterale di Z è del tipo $x^n Z$ con $n \in \mathbb{Z}$. Ne segue che ogni elemento di G si scrive $x^n z$ con $n \in \mathbb{Z}$ e $z \in Z$. Per mostrare che $G = Z$, cioè che G è abeliano, bisogna quindi mostrare che per ogni $n, m \in \mathbb{Z}$ e $z, w \in Z$ si ha $x^n z x^m w = x^m w x^n z$. Siccome $z, w \in Z$ e due potenze di x commutano tra loro, si ha

$$x^n z x^m w = x^n x^m zw = x^m x^n wz = x^m w x^n z.$$

Punto 2. Sappiamo dalla teoria generale che il numero di coniugati di g è uguale all'indice del centralizzante $C_G(g)$. Ovviamente g commuta con g e quindi $g \in C_G(g)$, da cui anche $\langle g \rangle \subseteq C_G(g)$. D'altra parte $C_G(g) \neq G$, altrimenti $g \in Z(G)$ e questo contraddice il punto 1. Siccome $\langle g \rangle \leq C_G(g)$, 11 divide $|C_G(g)|$, che divide $11 \cdot 23 = |G|$, e siccome 23 è primo e $C_G(g) \neq G$, troviamo $|C_G(g)| = 11$, cioè $C_G(g) = \langle g \rangle$, per cui g ha $|G : C_G(g)| = 23$ coniugati in G.

Punto 3. Osserviamo che un generico elemento di G deve avere ordine un divisore di G, cioè 1, 11, 23 oppure $11 \cdot 23 = |G|$. D'altra parte siccome G non è abeliano, non è ciclico e quindi G non contiene elementi di ordine $|G| = 11 \cdot 23$. Segue che ogni elemento non identico di G ha ordine 11 oppure 23.

Ogni elemento di ordine 11 genera un unico 11-Sylow, e siccome gli 11-Sylow hanno ordine 11 l'intersezione di due di essi è $\{1\}$ (per il teorema di Lagrange). Ne segue che il numero di elementi di ordine 11 è uguale al numero di 11-Sylow moltiplicato per il numero di elementi di ordine 11 in un 11-Sylow, cioè 10. Per il teorema di Sylow il numero di 11-Sylow è 1 oppure 23. Se fosse 1 allora G avrebbe solo 10 elementi di ordine 11, e questo contraddice il punto 2 (ogni elemento di ordine 11 ha 23 coniugati, e questi hanno tutti ordine 11). Quindi G ha 23 11-Sylow e quindi ha $23 \cdot 10 = 230$ elementi di ordine 11. Siccome ogni classe di coniugio di elementi di ordine 11 consiste di 23 elementi (punto 2) segue che il numero di classi di coniugio di elementi di ordine 11 è 10.

Rimangono da studiare gli elementi di ordine 23. Sia x un elemento di ordine 23. Analogamente a quanto detto nel punto 2, siccome $x \in C_G(x)$ e $Z(G) = \{1\}$ si ha $C_G(x) = \langle x \rangle$ e quindi x ha $|G : C_G(x)| = 11$ coniugati. Per il teorema di Sylow G ha un unico 23-Sylow (il numero di 23-Sylow deve dividere 11 ed essere congruo a 1 modulo 23), quindi siccome i 23-Sylow hanno ordine 23, ogni elemento di G di ordine 23 genera il 23-Sylow di G. Siccome $23 = 2 \cdot 11 + 1$ e ogni elemento di ordine 23 ha 11 coniugati, segue che ci sono due classi di coniugio di elementi di ordine 23, ognuna con 11 elementi.

Riassumendo, G contiene una classe di elementi di ordine 1, che consiste di un solo elemento (l'identità), dieci classi di elementi di ordine 11, che consistono di 23 elementi, e due classi di elementi di ordine 23, che consistono di 11 elementi. In totale G ha $1 + 10 + 2 = 13$ classi di coniugio.

5 Esercizio 5

Si scelgano in $\mathbb{Z}[i]$ gli elementi $a = 8 + 9i$ e $b = 5$.

1. Fattorizzare a e b.
2. Determinare un generatore per l'ideale $I = (a) + (b)$ e per l'ideale $J = (a) \cap (b)$.
3. È vero che $Z[i]/I$ è un campo?

4. Qual è l'ordine di $Z[i]/I$?

Svolgimento.

Punto 1. Si ha $5 = 1^2 + 2^2 = (1+2i)(1-2i)$ e $1+2i$, $1-2i$ sono irriducibili avendo norma 5, un numero primo. Ora fattorizziamo a. Per farlo calcoliamone la norma:

$$\begin{aligned} N(a) &= (8+9i)(8-9i) = 64+81 = 145 = 5 \cdot 29 \\ &= (1^2+2^2)(5^2+2^2) = (1+2i)(1-2i)(5+2i)(5-2i). \end{aligned}$$

Ora si procede selezionando un fattore per ogni coppia di fattori coniugati: $(1+2i)(5+2i) = 1+11i$ non funziona ma $(1+2i)(5-2i) = 9+8i$ funziona, infatti $a = 8+9i$ è il coniugato di $-i(9+8i)$ quindi

$$a = \overline{-i(9+8i)} = \overline{-i(1+2i)(5-2i)} = i(1-2i)(5+2i) = (2+i)(5+2i).$$

Questa è una fattorizzazione di a in irriducibili in quanto $N(2+i) = 5$ e $N(5+2i) = 29$ sono numeri primi, e gli elementi di norma un numero primo sono irriducibili.

Punto 2. Siccome $\mathbb{Z}[i]$ è un dominio euclideo, per l'algoritmo di Euclide $I = (a) + (b) = (a, b)$ è generato da un qualsiasi massimo comun divisore di a e b, che si trova semplicemente guardando le fattorizzazioni di a e b in irriducibili. Siccome $a = (2+i)(5+2i)$ e $5 = (1+2i)(1-2i)$, e $1-2i = -i(2+i)$, segue che $I = (1-2i)$. Un elemento di $J = (a) \cap (b)$ non è altro che un multiplo sia di a che di b, quindi J è generato da un qualsiasi minimo comune multiplo di a e b. Guardando le fattorizzazioni in irriducibili troviamo che $J = ((1+2i)(1-2i)(5+2i)) = (5(5+2i))$.

Punto 3. $\mathbb{Z}[i]/I$ è un campo perché I è un ideale massimale, infatti $\mathbb{Z}[i]$ è un PID e $I = (1-2i)$ è generato da un elemento irriducibile, perché di norma 5, un numero primo.

Punto 4. Il coniugio $a + ib \mapsto a - ib$ induce un isomorfismo di anelli $A = \mathbb{Z}[i]/(1+2i) \cong B = \mathbb{Z}[i]/(1-2i)$. Inoltre $1+2i$ e $1-2i$ sono coprimi, in quanto irriducibili e non associati. Il fatto che non siano associati si vede osservando che il prodotto di $1+2i$ per un invertibile (cioè per 1, -1, i o $-i$) non è mai uguale a $1-2i$ (infatti $1 \cdot (1+2i) = 1+2i$, $-1 \cdot (1+2i) = -1-2i$, $i \cdot (1+2i) = -2+i$ e $-i \cdot (1+2i) = 2-i$). Per il teorema cinese del resto

$$\mathbb{Z}[i]/(5) = \mathbb{Z}[i]/((1+2i)(1-2i)) \cong \mathbb{Z}[i]/(1+2i) \times \mathbb{Z}[i]/(1-2i) = A \times B,$$

da cui $|\mathbb{Z}[i]/(5)| = |A \times B| = |A|^2$, dove l'ultima uguaglianza segue dal fatto che $A \cong B$. Siamo ridotti a calcolare $|\mathbb{Z}[i]/(5)|$. Un generico elemento di $\mathbb{Z}[i]/(5)$ è del tipo $a+ib+(5)$, dove $a, b \in \mathbb{Z}$. Effettuando la divisione con resto di a e b per

5 troviamo che $a+ib+(5) = r+is+(5)$ con $r,s \in \{0,1,2,3,4\}$. Tale scrittura di un elemento di $\mathbb{Z}[i]/(5)$ è unica, infatti se $r,s,t,u \in \{0,1,2,3,4\}$ sono tali che $r+is+(5) = t+iu+(5)$ allora esistono $\alpha, \beta \in \mathbb{Z}$ con $r-t+i(s-u) = 5(\alpha+i\beta)$, quindi 5 divide le differenze $r-t$ e $s-u$ in $\mathbb{Z}$, da cui, essendo $r,s,t,u \in \{0,1,2,3,4\}$, segue $r=t$ e $s=u$. Quindi un generico elemento $a+ib+(5)$ è determinato da cinque possibili scelte per a e altrettante per b. In conclusione $|\mathbb{Z}[i]/(5)| = 5^2$ e quindi $|A|^2 = 5^2$ da cui $|A| = 5$.

6 Esercizio 6

Sia $\epsilon \in \mathbb{C}$ una radice primitiva nona di 1 e sia $u = \epsilon + \epsilon^{-1}$.

1. Determinare il polinomio minimo di ϵ su $\mathbb{Q}$.
2. Provare che $u^3 - 3u = -1$.
3. Determinare il polinomio minimo $f(x)$ di u su $\mathbb{Q}$.
4. Provare che se $\alpha \in \mathbb{C}$ una radice di $f(x)$, allora anche $\alpha^2 - 2$ lo è.
5. Determinare il campo di spezzamento di $f(x)$ su $\mathbb{Q}$.

Svolgimento.

Punto 1. Il polinomio minimo di ϵ su $\mathbb{Q}$ è il nono polinomio ciclotomico (che sappiamo essere irriducibile dalla teoria), $\Phi_9(x)$. Sappiamo dalla teoria che $x^9-1 = \Phi_1(x)\Phi_3(x)\Phi_9(x) = (x^3-1)\Phi_9(x)$, per cui $\Phi_9(x) = (x^9-1)/(x^3-1) = x^6+x^3+1$.

Punto 2. Si ha

$$u^3-3u = (\epsilon+\epsilon^{-1})^3-3(\epsilon+\epsilon^{-1}) = \epsilon^3+(1/\epsilon)^3+3\epsilon+3\epsilon^{-1}-3(\epsilon+\epsilon^{-1}) = \epsilon^3+1/\epsilon^3.$$

Ma poiché $\Phi_9(\epsilon) = \epsilon^6+\epsilon^3+1 = 0$, si ha $\epsilon^3(\epsilon^3+1) = -1$ da cui $1/\epsilon^3 = -1-\epsilon^3$, per cui $u^3-3u = \epsilon^3+1/\epsilon^3 = \epsilon^3+(-1-\epsilon^3) = -1$.

Punto 3. Per il punto 2, $u^3-3u = -1$, quindi u è zero di $f(x) = x^3-3x+1$. Tale polinomio è irriducibile in $\mathbb{Q}[x]$ per il lemma di Gauss, infatti è irriducibile in $\mathbb{Z}[x]$ essendo di grado 3 e senza zeri interi (gli eventuali zeri devono dividere il termine noto 1 e quindi sono 1 oppure -1, ma $f(1) = -1$ e $f(-1) = 3$). Siccome $f(x)$ è monico irriducibile con u come zero, $f(x)$ è il polinomio minimo di u su $\mathbb{Q}$.

Punto 4. Ricordando che $f(\alpha) = \alpha^3 - 3\alpha + 1 = 0$, cioè $\alpha^3 = 3\alpha - 1$, calcoliamo

$$\begin{aligned} f(\alpha^2 - 2) &= (\alpha^2 - 2)^3 - 3(\alpha^2 - 2) + 1 \\ &= \alpha^6 - 6\alpha^4 + 12\alpha^2 - 8 - 3\alpha^2 + 6 + 1 \\ &= (3\alpha - 1)^2 - 6\alpha(3\alpha - 1) + 9\alpha^2 - 1 \\ &= 9\alpha^2 - 6\alpha + 1 - 18\alpha^2 + 6\alpha + 9\alpha^2 - 1 = 0. \end{aligned}$$

Punto 5. Siccome due zeri di $f(x)$ sono α e $\alpha^2 - 2$, e sono distinti, infatti se fosse $\alpha = \alpha^2 - 2$ allora α avrebbe grado al più due su $\mathbb{Q}$, mentre sappiamo che ha grado 3, applicando il teorema di Ruffini si trova che il terzo zero è $-\alpha^2 - \alpha + 2$. Ne segue che il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è $\mathbb{Q}(\alpha)$.