SVOLGIMENTO DELL'APPELLO DI ALGEBRA 2 DEL 05/02/2014 (PRIMO APPELLO)

1 Esercizio 1

Supponiamo che un gruppo G agisca su un insieme Ω. Provare che se $\omega \in \Omega$, allora la cardinalità dell'orbita di ω tramite G coincide con l'indice dello stabilizzatore di ω in G.

Svolgimento.

L'orbita di ω è per definizione $O := \{g\omega \ : \ g \in G\}$. L'indice dello stabilizzatore di ω in G è per definizione la cardinalità dell'insieme $L := \{gH \ : \ g \in G\}$ dove $H = \mathrm{Stab}_G(\omega) = \{g \in G \ : \ g\omega = \omega\}$. Per concludere basta trovare una biiezione $L \to O$. Definiamo

$$f : L \to O, \qquad gH \mapsto g\omega.$$

Dobbiamo mostrare che f è una funzione ben definita, e che è biiettiva.

- *Buona definizione*. Dobbiamo mostrare che se $x, y \in G$ sono tali che $xH = yH$ allora $x\omega = y\omega$. $xH = yH$ significa che $y^{-1}x \in H = \mathrm{Stab}_G(\omega)$, cioè $y^{-1}x\omega = \omega$. Ne segue che $y\omega = y(y^{-1}x\omega) = x\omega$.
- *Iniettività*. Mostriamo che f è iniettiva. Siano quindi $x, y \in G$ con $f(xH) = f(yH)$, cioè $x\omega = y\omega$, e mostriamo che $xH = yH$. Da $x\omega = y\omega$, moltiplicando a sinistra per y^{-1}, troviamo $y^{-1}x\omega = \omega$, cioè $y^{-1}x \in \mathrm{Stab}_G(\omega) = H$, cioè $xH = yH$.
- *Suriettività*. f è suriettiva perché se $x\omega \in O$ allora $f(xH) = x\omega$.

2 Esercizio 2

Siano F ed E due campi, con $F \leq E$, e sia $u \in E$.

1. Si provi che u è algebrico su F se e solo se il grado $|F[u] : F|$ è finito.
2. Si provi che se $|F[u] : F| = n$ allora ogni elemento di $F[u]$ si scrive in uno e un solo modo nella forma $a_0 + a_1u + \ldots + a_{n-1}u^{n-1}$ con $a_0, \ldots, a_{n-1} \in F$.

Svolgimento.

Punto 1. Supponiamo che u sia algebrico su F, cioè che esista un polinomio $P(x) \in F[x]$ di grado $m > 0$ con $P(u) = 0$. Dobbiamo mostrare che $|F[u] : F|$ è finito, cioè che $F[u]$ ha dimensione finita su F. Un generico elemento di $F[u]$ è del tipo $A(u)$ dove $A(x) \in F[x]$. Effettuando la divisione con resto di $A(x)$ per $P(x)$

troviamo due polinomi $Q(x)$, $R(x)$ (quoziente e resto) con $R(x)$ nullo oppure di grado strettamente minore di m, tali che $A(x) = P(x)Q(x)+R(x)$. Sostituendo $x = u$ e ricordando che $P(u) = 0$ troviamo allora $A(u) = P(u)Q(u) + R(u) = R(u)$. In altre parole, ogni elemento di $F[u]$ è del tipo $R(u)$ dove $R(x)$ è un polinomio di $F[x]$ che è nullo oppure di grado strettamente minore di m. Siccome ogni polinomio di grado minore di m è del tipo $a_0+a_1x+\ldots+a_{n-1}x^{m-1}$, segue che $F[u]$ è generato su F da $1, u, u^2, \ldots, u^{m-1}$ e quindi ha dimensione finita su F.

Ora supponiamo che $|F[u] : F|$ sia finito, cioè che $F[u]$ abbia dimensione finita su F, sia essa n. Allora gli $n+1$ elementi $1, u, u^2, \ldots, u^n$ sono linearmente dipendenti (essendo più di n), cioè esistono $a_0, \ldots, a_n \in F$ non tutti nulli con $a_0+a_1u+\ldots+a_nu^n = 0$. Quindi $P(x) := a_0+a_1x+\ldots+a_nx^n$ è un polinomio non nullo che ha u come zero. Ne segue che u è algebrico su F.

Punto 2. Si tratta di dimostrare che $\{1, u, u^2, \ldots, u^{n-1}\}$ è una base di $F[u]$ su F. Siccome sono proprio n, quant'è la dimensione di $F[u]$ su F, basta mostrare che sono un insieme di generatori di $F[u]$ su F. Come visto nel punto precedente gli $n + 1$ elementi $1, u, u^2, \ldots, u^n$ sono linearmente dipendenti (essendo più di n), cioè esistono $a_0, \ldots, a_n \in F$ non tutti nulli con $a_0 + a_1u + \ldots + a_nu^n = 0$. Sia $P(x) := a_0 + a_1x + \ldots + a_nx^n$. Un generico elemento di $F[u]$ è del tipo $A(u)$ con $A(x) \in F[x]$. Effettuando la divisione con resto di $A(x)$ per $P(x)$ troviamo due polinomi $Q(x)$, $R(x)$ (quoziente e resto) con $R(x)$ nullo oppure di grado strettamente minore di n, tali che $A(x) = P(x)Q(x) + R(x)$. Sostituendo $x = u$ e ricordando che $P(u) = 0$ troviamo allora $A(u) = P(u)Q(u) + R(u) = R(u)$. In altre parole, ogni elemento di $F[u]$ è del tipo $R(u)$ dove $R(x)$ è un polinomio di $F[x]$ che è nullo oppure di grado strettamente minore di n. Siccome ogni polinomio di grado minore di n è del tipo $a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$, segue che $F[u]$ è generato su F da $1, u, u^2, \ldots, u^{n-1}$.

3 Esercizio 3

Sia $F = \mathbb{Z}/7\mathbb{Z}$ il campo di ordine 7. Su $G = F \times F^*$ si definisca un'operazione ponendo, per ogni $(a, x), (b, y) \in G$, $(a, x)(b, y) = (a + xb, xy)$.

1. Si provi che con tale operazione G è un gruppo.
2. Si provi che ponendo, per ogni $u \in F$ e ogni $(a, x) \in G$, $(a, x) \cdot u := xu - a$ si definisce un'azione di G sull'insieme F.
3. Si provi che il nucleo di questa azione è il sottogruppo identico, concludendo che G è isomorfo ad un sottogruppo di S_7.
4. Si provi che G contiene un 7-sottogruppo di Sylow di S_7.
5. Si determini $n_7(S_7)$, il numero di 7-sottogruppi di Sylow di S_7.

6. Denotato con P un 7-sottogruppo di Sylow di S_7, si dimostri che $N_{S_7}(P) \cong G$.

Svolgimento.

Punto 1. Mostriamo che l'operazione data è associativa. Siano quindi $(a, x), (b, y), (c, z) \in G$. Abbiamo

$$((a, x)(b, y))(c, z) = (a + xb, xy)(c, z) = a + xb + xyc, xyz),$$

$$(a, x)((b, y)(c, z)) = (a, x)(b + yc, yz) = (a + x(b + yc), xyz).$$

Siccome $a + xy + xyc = a + x(b + yc)$ segue che l'operazione è associativa. L'elemento neutro è $(0, 1)$, infatti $(a, x)(0, 1) = (a + x \cdot 0, x \cdot 1) = (a, 1)$ per ogni $(a, x) \in G$. L'inverso di $(a, x) \in G$ è un elemento $(b, y) \in G$ tale che $(a, x)(b, y) = (0, 1)$, cioè $(a + xb, xy) = (0, 1)$, cioè $b = -ax^{-1}$, $y = x^{-1}$ (notiamo che questo ha senso perché $x \in F^*$). Ne segue che $(a, x)^{-1} = (-ax^{-1}, x^{-1})$.

Punto 2. Sia $u \in F$. Osserviamo che $(0, 1) \cdot u = 1 \cdot u - 0 = u$, cioè l'elemento neutro agisce fissando tutto. Per concludere che la legge data è un'azione di G su F dobbiamo mostrare che se $(a, x), (b, y) \in G$ e $u \in F$ allora $(a, x)((b, y) \cdot u) = ((a, x)(b, y)) \cdot u$. Abbiamo

$$(a, x)((b, y) \cdot u) = (a, x) \cdot (yu - b) = x(yu - b) - a,$$

$$((a, x)(b, y)) \cdot u = (a + xb, xy) \cdot u = xyu - (a + xb).$$

Il risultato segue dal fatto che $x(yu - b) - a = xyu - (a + xb)$.

Punto 3. Un elemento (a, x) di G sta nel nucleo dell'azione se e solo se $(a, x) \cdot u = u$ per ogni $u \in F$, in altre parole $xu - a = u$ per ogni $u \in F$. Scegliendo $u = 0$ troviamo $a = 0$, per cui $xu = u$ per ogni $u \in F$. Ora scegliendo $u = 1$ troviamo $x = 1$. Ne segue che $(a, x) = (0, 1)$, e quindi il nucleo dell'azione è banale. Siccome G agisce fedelmente (cioè con nucleo banale) su F, che ha sette elementi, segue dalla teoria generale che c'è un omomorfismo iniettivo canonico $G \to S_7$, quindi G è isomorfo alla sua immagine in S_7.

Punto 4. D'ora in poi identifichiamo G con la sua immagine in S_7. Siccome $|S_7| = 7! = 7 \cdot 6!$ e 7 non divide $6!$ i 7-sottogruppi di Sylow di S_7 hanno ordine 7. Siccome $|G| = |F \times F^*| = |F||F^*| = 7 \cdot 6$, per il teorema di Cauchy G ha un elemento x di ordine 7, quindi il sottogruppo $\langle x \rangle$ ha ordine 7, e quindi è un 7-sottogruppo di Sylow di S_7.

Punto 5. Contiamo i 7-sottogruppi di Sylow di S_7. Ognuno di essi ha ordine 7, quindi, siccome 7 è primo, essi sono ciclici generati da elementi di ordine 7. Gli elementi di S_7 di ordine 7 sono i 7-cicli, e quindi ogni 7-sottogruppo di Sylow contiene l'identità e sei 7-cicli. Il numero di 7-cicli in S_7 è $6!$ (fisso un elemento da cui far partire il ciclo e gli altri sono liberi) e quindi, siccome ogni 7-sottogruppo di Sylow contiene sei 7-cicli, $n_7(S_7) = 6!/6 = 5!$.

Punto 6. Sia Q un 7-sottogruppo di Sylow di S_7 contenuto in G (esiste per il punto 4). Per il teorema di Sylow esiste $g \in S_7$ tale che $gQg^{-1} = P$. Mostriamo che si ha $gN_{S_7}(Q)g^{-1} = N_{S_7}(gQg^{-1})$.

- ($\subseteq$). Sia $x \in N_{S_7}(Q)$. Mostriamo che $gxg^{-1} \in N_{S_7}(gQg^{-1})$, cioè che $(gxg^{-1})(gQg^{-1})(gxg^{-1})^{-1} = gQg^{-1}$. Si ha $(gxg^{-1})(gQg^{-1})(gxg^{-1})^{-1} = gxg^{-1}gQg^{-1}gx^{-1}g^{-1} = gxQx^{-1}g^{-1} = gQg^{-1}$, dove l'ultima uguaglianza segue dal fatto che $x \in N_{S_7}(Q)$.
- ($\supseteq$). Sia $y \in N_{S_7}(gQg^{-1})$. Mostriamo che $y \in gN_{S_7}(Q)g^{-1}$, cioè che $g^{-1}yg \in N_{S_7}(Q)$. Siccome $y \in N_{S_7}(gQg^{-1})$ si ha $g^{-1}ygQ(g^{-1}yg)^{-1} = g^{-1}ygQg^{-1}y^{-1}g = g^{-1}gQg^{-1}g = Q$.

Siccome il coniugio tramite g è un isomorfismo di gruppi e $gQg^{-1} = P$, segue che $N_{S_7}(Q)$ è isomorfo a $N_{S_7}(P)$. Quindi per concludere basta mostrare che $N_{S_7}(Q) = G$. Cominciamo col mostrare che $N_{S_7}(Q)$ e G hanno lo stesso ordine. Dal punto precedente $5! = n_7(S_7) = |S_7 : N_{S_7}(P)| = 7!/|N_{S_7}(P)|$ per cui $|N_{S_7}(P)| = 7!/5! = 7 \cdot 6 = |G|$. Ne segue che per mostrare che $G = N_{S_7}(Q)$ basta mostrare che $G \subseteq N_{S_7}(Q)$ (infatti tali due insiemi sono finiti della stessa cardinalità), cioè che G normalizza Q. Questo segue dal fatto che $Q \trianglelefteq G$, infatti $|G| = 6 \cdot 7$ quindi per il teorema di Sylow $n_7(G) = 1$.

4 Esercizio 4

Si considerino i seguenti due polinomi in $\mathbb{Q}[x]$: $f_1(x) = x^3 - 2$ e $f_2(x) = x^4 - 3$. Siano E_1 ed E_2 i rispettivi campi di spezzamento.

1. Provare che $f_1(x)$ ed $f_2(x)$ sono irriducibili in $\mathbb{Q}[x]$.
2. Determinare $|E_1 : \mathbb{Q}|$.
3. Determinare $|E_2 : \mathbb{Q}|$.
4. Provare che $i\sqrt{3} \in E_1 \cap E_2$.
5. Determinare $|E_1 \cap E_2 : \mathbb{Q}|$.
6. Sia E il campo di spezzamento di $f_1(x)f_2(x)$. Determinare $|E : \mathbb{Q}|$.

Svolgimento.

Punto 1. L'irriducibilità segue dal criterio di Eisenstein, applicata a 2 per $f_1(x)$ e a 3 per $f_2(x)$.

Punto 2. Si ha $E_1 = \mathbb{Q}(u, \zeta u, \zeta^2 u)$ dove $u = \sqrt[3]{2}$ e $\zeta = e^{i2\pi/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Quindi E_1 contiene $\zeta u/u = \zeta$ e quindi $E_1 = \mathbb{Q}(u, i\sqrt{3})$. Siccome $u \in \mathbb{R}$, $\mathbb{Q}(u) \subseteq \mathbb{R}$ quindi $i\sqrt{3} \notin \mathbb{Q}(u)$ per cui, essendo $i\sqrt{3}$ zero di x^2+3, si ha $|E_1 : \mathbb{Q}(u)| = |\mathbb{Q}(u)(i\sqrt{3}) : \mathbb{Q}(u)| = 2$, per cui dalla formula dei gradi $|E_1 : \mathbb{Q}| = |E_1 : \mathbb{Q}(u)| \cdot |\mathbb{Q}(u) : \mathbb{Q}| = 3 \cdot 2 = 6$.

Punto 3. Si ha $E_2 = \mathbb{Q}(v, i)$ dove $v = \sqrt[4]{3}$, infatti i quattro zeri complessi di $x^4 - 3$ sono $v, -v, iv, -iv$. Ora v ha grado 4 e $i \notin \mathbb{Q}(v)$ essendo $\mathbb{Q}(v) \subseteq \mathbb{R}$, per cui $|\mathbb{Q}(v)(i) : \mathbb{Q}(v)| = 2$ e dalla formula dei gradi $|E_2 : \mathbb{Q}| = |\mathbb{Q}(v)(i) : \mathbb{Q}(v)| \cdot |\mathbb{Q}(v) : \mathbb{Q}| = 2 \cdot 4 = 8$.

Punto 4. Abbiamo $E_1 = \mathbb{Q}(u, i\sqrt{3})$ e $E_2 = \mathbb{Q}(v, i)$. Allora $E_2 \ni iv^2 = i\sqrt{3}$ e quindi $i\sqrt{3} \in E_1 \cap E_2$.

Punto 5. Per la formula dei gradi per $i = 1, 2$ abbiamo $|E_i : \mathbb{Q}| = |E_i : E_1 \cap E_2| \cdot |E_1 \cap E_2 : \mathbb{Q}|$, quindi il grado $|E_1 \cap E_2 : \mathbb{Q}|$ divide $|E_1 : \mathbb{Q}| = 6$ e $|E_2 : \mathbb{Q}| = 8$, quindi divide il massimo comun divisore $MCD(6, 8) = 2$. D'altra parte $E_1 \cap E_2$ contiene $i\sqrt{3}$ quindi ha grado almeno 2 su $\mathbb{Q}$. Questo dimostra che tale grado è proprio uguale a 2.

Punto 6. E non è altro che il sottocampo di $\mathbb{C}$ generato da E_1 ed E_2, cioè $E = \langle E_1, E_2 \rangle = \mathbb{Q}(u, \zeta, v, i) = \mathbb{Q}(u, v, i)$ (notiamo infatti che $\zeta = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = -\frac{1}{2} + \frac{iv^2}{2}$). Quindi il grado $|E : \mathbb{Q}|$, per la formula dei gradi, è diviso da $|E_1 : \mathbb{Q}| = 6$ e da $|E_2 : \mathbb{Q}| = 8$, quindi è diviso dal minimo comune multiplo $mcm(6, 8) = 24$. D'altra parte per la formula dei gradi

$$|E : \mathbb{Q}| = |\mathbb{Q}(u, v, i) : \mathbb{Q}(u, v)| \cdot |\mathbb{Q}(u, v) : \mathbb{Q}(v)| \cdot |\mathbb{Q}(v) : \mathbb{Q}| \qquad (*)$$

e siccome i, u, v hanno gradi su $\mathbb{Q}$ rispettivamente 2, 3 e 4, abbiamo $|\mathbb{Q}(u, v, i) : \mathbb{Q}(u, v)| \leq 2$, $|\mathbb{Q}(u, v) : \mathbb{Q}(v)| \leq 3$ e $|\mathbb{Q}(v) : \mathbb{Q}| = 4$, quindi da $(*)$ segue $|E : \mathbb{Q}| \leq 2 \cdot 3 \cdot 4 = 24$. Siccome 24 divide $|E : \mathbb{Q}|$ concludiamo che $|E : \mathbb{Q}| = 24$.

5 Esercizio 5

Sia $f(x) = x^3 + 6x^2 + x + 1 \in F[x]$ con $F = \mathbb{Z}/7\mathbb{Z}$ e sia $A = F[X]/(f(x))$.

1. Fattorizzare $f(x)$ in $F[x]$.
2. Determinare l'ordine di E, un suo campo di spezzamento.
3. Quanti sono gli ideali massimali dell'anello A?
4. Quanti sono gli elementi invertibili dell'anello A?

Svolgimento.

Punto 1. Si ha $f(2) = 0$ quindi applicando il teorema di Ruffini $f(x) = (x-2)(x^2+x+3)$ e il polinomio $g(x) = x^2+x+3$ è irriducibile in quanto ha grado 2 e non ha zeri in F (infatti $g(0) = 3$, $g(1) = 5$, $g(2) = 2$, $g(3) = 1$, $g(4) = 2$, $g(5) = 5$, $g(6) = 3$).

Punto 2. Sia α uno zero di $g(x) = x^2 + x + 3$ in un'opportuna estensione. Applicando il teorema di Ruffini troviamo $g(x) = (x-\alpha)(x+1+\alpha)$, quindi $E = F(\alpha)$ è un campo di spezzamento per $f(x)$ su F. Siccome α ha grado 2 su F, come F-spazio vettoriale E è isomorfo a F^2 quindi $|E| = |F^2| = |F|^2 = 7^2$.

Punto 3. Siccome $A = F[x]/(f(x))$ per il teorema di corrispondenza gli ideali massimali di A sono tanti quanti gli ideali massimali di $F[x]$ contenenti $f(x)$. Siccome $F[x]$ è un PID, gli ideali massimali di $F[x]$ contenenti $f(x)$ sono esattamente gli ideali della forma $(P(x))$ con $P(x)$ polinomio che divide $f(x)$. Quelli massimali sono esattamente quelli per cui $P(x)$ è irriducibile. In conclusione, gli ideali massimali di A sono tanti quanti i fattori irriducibili di $f(x)$, cioè due.

Punto 4. Siccome $x-2$ e x^2+x+3 sono coprimi (essendo irriducibili e non associati, in quanto di grado diverso), per il teorema cinese del resto si ha

$$\begin{aligned} A &= F[x]/(f(x)) = F[x]/((x-2)(x^2+x+3)) \\ &\cong F[x]/(x-2) \times F[x]/(x^2+x+3) \cong F \times K \end{aligned}$$

dove $K = F[x]/(x^2+x+3)$ è un campo. L'operazione di prodotto in $F \times K$ è per componenti, quindi i suoi elementi invertibili sono esattamente gli elementi di $F^* \times K^*$, quindi sono $(|F|-1)(|K|-1) = (7-1)(7^2-1) = 6 \cdot 48 = 288$.