esame scritto di algebra II – 20 giugno 2016
soluzioni

Esercizio 1. *Sia G un gruppo con $|G| = 154$.*

(1) Si provi G ha un sottogruppo normale N di indice 2;
(2) si provi che il sottogruppo N del punto (1) è abeliano.

SOLUZIONE. Come al solito, se p è un divisore di $|G|$ (in questo caso, $p \in \{2, 7, 11\}$) denotiamo con $n_p(G)$ il numero di p-sottogruppi di Sylow di G.

(1) Dal Teorema di Sylow si ha

$$n_{11}(G) \equiv 1 \pmod{11} \qquad \text{e} \qquad n_{11}(G) \Big| |G|/11 = 14$$

da cui $n_{11} = 1$, e dunque esiste un unico 11-sottogruppo di Sylow K di G; pertanto $K \trianglelefteq G$. Consideriamo il gruppo quoziente $\overline{G} = G/K$; poiché $|\overline{G}| = |G|/|K| = 14$, si ha

$$n_7(\overline{G}) \equiv 1 \pmod{7} \qquad \text{e} \qquad n_7(\overline{G}) \Big| 14/7 = 2;$$

quindi $\overline{G}$ ha un unico 7-sottogruppo di Sylow, che, per il Teorema di Corrispondenza si scrive come $\overline{N} = N/K$. Inoltre $N/K \trianglelefteq G/K$ e dunque, sempre per il Teorema di Corrispondenza, $N \trianglelefteq G$. Infine

$$|N| = |N/K||K| = 7 \cdot 11 = 77$$

e N è il sottogruppo cercato.

(2) Sappiamo già che $K \trianglelefteq N$, $|K| = 11$. Ancora per il Teorema di Sylow

$$n_7(N) \equiv 1 \pmod{7} \qquad \text{e} \qquad n_7(N) \Big| |N|/7 = 11$$

e ancora deduciamo che N ha un unico 7-sottogruppo di Sylow T, e $T \trianglelefteq N$. Poiché T e K hanno ordine coprimo $T \cap K = 1$ e quindi $|TK| = |T||K| = 77$, da cui $TK = N$. Siccome T e K sono entrambi normali in N, si conclude che $N \simeq T \times K$. Infine, T e K sono abeliani (in quanto ciclici, dato che hanno ordine primo), e dunque anche N è abeliano.

Esercizio 2. *Sia $E|F$ un'estensione di Galois, e sia $\mathcal{G} = Gal(E|F)$. Per ogni $\sigma \in \mathcal{G}$ e $0 \neq a \in E$, si consideri l'applicazione $\pi_{(a,\sigma)} : E \to E$ definita ponendo, per ogni $x \in E$, $\pi_{(a,\sigma)}(x) = a\sigma(x)$. Sia*

$$W = \{\pi_{(a,\sigma)} | 0 \neq a \in E,\ \sigma \in \mathcal{G}\}.$$

(1) Si provi che W è un sottogruppo di $Aut((E, +))$.
(2) Si determini un omomorfismo suriettivo $W \to \mathcal{G}$.
(3) Si determini il centro $Z(W)$.

SOLUZIONE. Innanzi tutto occorre provare che, per ogni $\sigma \in \mathcal{G}$ e $0 \neq a \in E$, l'applicazione $\pi_{(a,\sigma)}$ è un automorfismo di $(E, +)$. Siano $x, y \in E$, allora

$$\pi_{(a,\sigma)}(x+y) = a\sigma(x+y) = a(\sigma(x)+\sigma(y)) = a\sigma(x)+a\sigma(y) = \pi_{(a,\sigma)}(x)+\pi_{(a,\sigma)}(y)$$

il che dimostra $\pi_{(a,\sigma)} \in Aut(E, +)$.

(1) Per provare che $W = \{\pi_{(a,\sigma)} | 0 \neq a \in E,\ \sigma \in \mathcal{G}\}$ è un sottogruppo di $Aut(E,+)$ conviene trovare la regola di composizione; siano quindi $\alpha, \beta \in W$ con $\alpha = \pi_{(a,\sigma)}$, $\beta = \pi_{(b,\rho)}$ $(a, b \in E^*,\ \sigma, \rho \in \mathcal{G})$. Per $x \in E$ si ha

$$(\alpha \circ \beta)(x) = \alpha(b\rho(x)) = a\sigma(b\rho(x)) = a\sigma(b)\sigma(\rho(x)) = a\sigma(b)(\sigma\rho(x)),$$

da cui deduciamo la regola di moltiplicazione:

$$\pi_{(a,\sigma)} \circ \pi_{(b,\rho)} = \pi_{(a\sigma(b),\sigma\rho)}.$$

In particolare, osservando che $\iota_E = \pi_{(1,1)}$, si ricava la formula per l'inversa:

$$\pi_{(a,\sigma)}^{-1} = \pi_{(\sigma^{-1}(a^{-1}),\sigma^{-1})}.$$

A questo punto (dato che $W \neq \emptyset$), siamo pronti per applicare il criterio per sottogruppi; siano $\pi_{(a,\sigma)}, \pi_{(b,\rho)}$ elementi di W, allora

$$\pi_{(a,\sigma)}^{-1} \circ \pi_{(b,\rho)} = \pi_{(\sigma^{-1}(a^{-1}),\sigma^{-1})} \circ \pi_{(b,\rho)} = \pi_{(\sigma^{-1}(a^{-1})\sigma^{-1}(b),\sigma^{-1}\rho)} = \pi_{\sigma^{-1}(a^{-1}b),\sigma^{-1}\rho)}$$

cha appartiene a W. Dunque $W \leq Aut(E,+)$.

(2) Osserviamo preventivamente che, per ogni $a, b \in E^*$ e $\sigma, \rho \in \mathcal{G}$, risulta $\pi_{(a,\sigma)} = \pi_{(b,\rho)}$ se e solo se $(a,\sigma) = (b,\rho)$. Infatti, se $\pi_{(a,\sigma)} = \pi_{(b,\rho)}$, allora

$$a = \pi_{(a,\sigma)}(1) = \pi_{(b,\rho)}(1) = b$$

e quindi, per ogni $x \in E$,

$$\sigma(x) = a^{-1}\pi_{(a,\sigma)}(x) = b^{-1}\pi_{(b,\rho)}(x) = \rho(x)$$

da cui $\sigma = \rho$.
Possiamo ora definire $\Phi : W \to \mathcal{G}$, ponendo per ogni $\pi_{(a,\sigma)} \in W$

$$\Phi(\pi_{(a,\sigma)}) = \sigma.$$

La regola di moltiplicazione provata in precedenza ci dà:

$$\Phi(\pi_{(a,\sigma)} \circ \pi_{(b,\rho)}) = \Phi(\pi_{(a\sigma(b),\sigma\rho)}) = \sigma\rho = \Phi(\pi_{(a,\sigma)})\Phi(\pi_{(b,\rho)})$$

per ogni $\pi_{(a,\sigma)}, \pi_{(b,\rho)} \in W$. Dunque, Φ è un omomorfismo. Che sia suriettivo è chiaro.

(3) Sia $\pi_{(a,\sigma)} \in Z(W)$; allora per ogni $\pi_{(b,\rho)} \in W$ (cioè, per ogni $b \in E^*$ ed ogni $\rho \in \mathcal{G}$), utilizzando la formula per la moltiplicazione

$$\pi_{(a\sigma(b),\sigma\rho)} = \pi_{(a,\sigma)} \circ \pi_{(b,\rho)} = \pi_{(b,\rho)} \circ \pi_{(a,\sigma)} = \pi_{(b\rho(a),\rho\sigma)}.$$

da cui, per quanto visto prima, $(a\sigma(b), \sigma\rho) = (b\rho(a), \rho\sigma)$. In particolare, questo deve valere per $b = 1$ e $\rho \in \mathcal{G}$, ovvero

$$a = a \cdot 1 = a \cdot \sigma(1) = 1 \cdot \rho(a)$$

quindi $\rho(a) = a$ per ogni $\rho \in \mathcal{G}$, cioè $a \in Inv(\mathcal{G}) = Inv(Gal(E|F)) = F$ (poich $E|F$ è un'estensione di Galois). Di conseguenza, per ogni $b \in E$,

$$\sigma(b) = a^{-1}a\sigma(b) = a^{-1}b\rho(a) = a^{-1}ba = a^{-1}ab = b$$

dunque $\sigma = 1$ (automorfismo identico). In conclusione

$$Z(W) = \{\pi_{(a,1)} \mid a \in F^*\}.$$

Esercizio 3. *Sia E il campo di spezzamento sul campo $\mathbb{F}$ del polinomio*

$$f = x^3 - 3 \in \mathbb{F}[x].$$

Si determini il grado $[E : \mathbb{F}]$ nei casi seguenti: $\mathbb{F} = \mathbb{Q}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$.

Soluzione. Sia $\mathbb{F} = \mathbb{Q}$. In questo caso f è irriducibile, e $[E : \mathbb{Q}]\big|3! = 6$. Ora $E = \mathbb{Q}(\sqrt[3]{3}, \omega)$, dove $\omega = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$ è radice terza dell'unità. Siccome $\omega \notin \mathbb{Q}(\sqrt[3]{3})$ si ha anche $[E : \mathbb{Q}] > [Q(\sqrt[3]{3}) : \mathbb{Q}] = 3$. Quindi $[E : \mathbb{Q}] = 6$.

Sia $\mathbb{F} = \mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \bar{4}\}$. Mediante un calcolo diretto si trova che $\{a^3 \mid a \in \mathbb{F}\} = \mathbb{F}$, quindi $f = x^3 - 3$ ha una sola radice, $\bar{2}$, in $\mathbb{F}$. Dunque (dopo aver diviso)

$$f = (x - \bar{2})(x^2 + 2x - 1)$$

con $g = x^2 + 2x - 1$ irriducibile in $\mathbb{F}[x]$ (perché non ha radici in $\mathbb{F}$). Poiché, allora, E coincide con il campo di spezzamento di g si conclude $[E : \mathbb{F}] = 2$.

Sia $\mathbb{F} = \mathbb{Z}/7\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \bar{6}\}$. Ancora con un calcolo diretto si trova che $f = x^3 - 3$ non ha radici nel campo $\mathbb{F}$; dunque (poiché ha grado 3) f è irriducbile si $\mathbb{F}$. Sia $b \in E$ radice di f; allora f è il polinomio minimo di b e dunque $[\mathbb{F}[b] : \mathbb{F}] = 3$. Ma ogni estensione tra campi finiti è normale. Quindi $E = \mathbb{F}[b]$ e $[E : \mathbb{F}] = 3$.

Esercizio 4. *Sia E il campo di spezzamento su $\mathbb{Q}$ del polinomio*

$$f = x^5 + 3x^3 - 2x^2 - 6;$$

(1) Si determini il grado $[E : \mathbb{Q}]$;
(2) si determini (a meno di isomorfismo) il gruppo di Galois $Gal(E|\mathbb{Q})$;
(3) si dica quante sono le estensioni intermedie $\mathbb{Q} \subseteq L \subseteq E$ tali che $[E : L] = 2$, e si dica quanti di questi campi L sono normali su $\mathbb{Q}$

Soluzione. (1) Cominciamo con l'osservare che, in $\mathbb{Q}[x]$,

$$f = x^5 + 3x^3 - 2x^2 - 6 = (x^2 + 3)(x^3 - 2).$$

Le radici complesse di $x^2 + 3$ sono $\pm i\sqrt{3}$; mentre le radici di $x^3 - 2$ sono $\sqrt[3]{2}$, $\omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$, dove $\omega = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$. In particolare, abbiamo $\omega \in \mathbb{Q}[i\sqrt{3}]$. Dunque

$$E = \mathbb{Q}[\sqrt[3]{2}, \omega, i\sqrt{3}] = \mathbb{Q}[\sqrt[3]{2}, i\sqrt{3}].$$

Ora $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$, dato che $x^3 - 2$ è irriducibile in $\mathbb{Q}[x]$ (dunque è il polinomio minimo di $\sqrt[3]{2}$). Inoltre $i\sqrt{3} \notin \mathbb{Q}[\sqrt[3]{2}]$ (dato che $\mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{R}$). Quindi

$$[E : \mathbb{Q}][E : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

(2) Sia $G = Gal(E|\mathbb{Q})$. Allora $|G| = [E : \mathbb{Q}] = 6$. Inoltre G non è abeliano, perché, se lo fosse, ogni suo sottogruppo sarebbe normale e dunque, per il Teorema di Corrispondenza di Galois, ogni campo intermedio tra $\mathbb{Q}$ ed E sarebbe un'estensione normale di $\mathbb{Q}$, e questo non è vero dato che, ad esempio $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ non è normale. Quindi, G non è abeliano e pertanto $G \simeq S_3$.

(3) Per il teorema di Corrispondenza di Galois, $\mathbb{Q} \subseteq L \subseteq E$ è tale che $[E : L] = 2$ se e solo se $L = Inv_E(H)$ dove $H \leq G = Gal(E|\mathbb{Q})$ con $|H| = 2$. Poiché G è isomorfo a S_3, G ha esattamente 3 sottogruppi di ordine 2 (che sono quelli generati dalle tre trasposizioni), nessuno dei quali è normale in G. Pertanto, esistono esattamente 3 campi intermedi $\mathbb{Q} \subseteq L \subseteq E$ con $[E : L] = 2$ e nessuno di essi è un'estensione normale du $\mathbb{Q}$.