SOLUZIONI DEL COMPITO DI ALGEBRA 1

16 gennaio 2015

Esercizio 1.

Per ogni $n \geq 3$, determinare il più piccolo sottogruppo normale di $\mathcal{S}_n$ che contiene un n-ciclo.

Soluzione esercizio 1 Siano σ un n-ciclo e H il sottogruppo cercato; allora $H \cap \mathcal{A}_n \triangleleft \mathcal{A}_n$. Se $n \geq 5$ sappiamo che $\mathcal{A}_n$ è un gruppo semplice, quindi, poichè $H \cap \mathcal{A}_n$ contiene l'elemento $\sigma^2 \neq id$, si ha che $H \cap \mathcal{A}_n = \mathcal{A}_n$. Ne segue che, per $n \geq 5$, il sottogruppo H deve contenere sia σ che $\mathcal{A}_n$, quindi se n è dispari ($\sigma \in \mathcal{A}_n$) $H = \mathcal{A}_n$ Se invece n è pari $\sigma \notin \mathcal{A}_n$ quindi $\mathcal{A}_n \subsetneq H$ e di conseguenza $H = \mathcal{S}_n$.

Per $n = 3$ è chiaro che $H = \mathcal{A}_3$. Per $n = 4$ il sottogruppo H cercato deve contenere tutti i 4 cicli e i loro prodotti, ad esempio $(a, b, c, d)(a, c, b, d) = (a, d, b)$ che implica $\mathcal{A}_4 \subsetneq H$ e quindi $H = \mathcal{S}_4$.

Esercizio 2.

Sia G un gruppo di ordine $5^2 \cdot 7 \cdot 17$. Mostrare che:
a) G ha un 5-Sylow S normale;
b) $S \subseteq Z(G)$;
c) G è abeliano.

Soluzione esercizio

(a) L'indice di un 5-Sylow S è congruo ad $1 \mod 5$, ma $7, 17, 7 \cdot 17$ non sono $\equiv 1 \mod 5$. Ne segue che l'indice S è 1 e dunque S è normale.

(b) La cardinalità di S è il quadrato di un primo, dunque S è abeliano. La cardinalità di $\mathrm{Aut}(S)$ è 20 (se $S = \mathbb{Z}/25\mathbb{Z}$) oppure $(5^2 - 1)(5^2 - 5) = 480$ (se $S = (\mathbb{Z}/5\mathbb{Z})^2$) ed in entrambi i casi $7 \nmid |\mathrm{Aut}(S)|$ e $17 \nmid |\mathrm{Aut}(S)|$, dunque S è centralizzato da tutti i Sylow. Dunque S è nel centro.

(c) Un gruppo di ordine $7 \cdot 17$ è abeliano in quanto $7 \nmid (17 - 1)$ e dunque è ciclico perchè la sua cardinalità è libera da quadrati. Poichè $S \subset Z(G)$ si ha che $G/Z(G)$ è isomorfo ad un quoziente di G/S che ha ordine $7 \cdot 17$ ed è quindi ciclico. Segue che G è abeliano perchè se il quozionte di un gruppo rispetto al centro è ciclico, allora il gruppo è abeliano.

Esercizio 3.

Sia p un numero primo e sia

$$A = \{(a_1, a_2, a_3, \dots) \mid a_i \in \mathbb{Z}/p^i\mathbb{Z},\ a_{i+1} \equiv a_i \pmod{p^i}\ \forall i \geq 1\}.$$

L'insieme A munito delle operazioni componente per componente è un anello commutativo con identità.
a) Quali sono gli elementi di A^*?
b) Mostrare che A possiede un unico ideale massimale M e che questo è principale.
c) Mostrare che ogni ideale non nullo di A è del tipo M^k per un certo $k \geq 0$.

Soluzione esercizio 3 (a) La prima osservazione è che l'unità dell'anello A è l'elemento $\underline{1} = (1, 1, 1, \dots)$ che evidentemente appartiene ad A ed è l'elemento neutro per il prodotto perché le operazioni si fanno componente per componente. Un elemento $\alpha = (a_i)_{i\geq 1} \in A$ è invertibile se e solo se esiste $\beta = (b_i)_{i\geq 1} \in A$ tale che $\alpha\beta = (a_ib_i)_{i\geq 1} = \underline{1}$. Mostriamo che gli α invertibili sono esattamente quelli con $a_1 \not\equiv 0$. Infatti, se $(a_i)_{i\geq 1}$è invertibile, allora $a_1b_1 \equiv 1 \pmod{p}$ ha soluzione, cioè a_1 è invertibile in $\mathbb{Z}/p\mathbb{Z}$ e quindi diverso da 0. D'altra parte, sia $a_1 \not\equiv 0$: allora, poichè per ogni $i \geq 1$ si ha $a_i \equiv a_1 \not\equiv 0 \pmod p$ si ha che a_i è invertibile in $\mathbb{Z}/p^i\mathbb{Z}$ e quindi $(a_i^{-1}) \in A$ in quanto $a_{i+1} \equiv a_i \pmod{p^i}$ implica $a_{i+1}^{-1} \equiv a_i^{-1} \pmod{p^i}$

(b) Un anello possiede un unico ideale massimale se e solo se $M = A \setminus A^*$ è un ideale (infatti se M è un ideale è chiaramente l'unico ideale massimale e d'altra parte se A ha un unico ideale massimale questo deve contenere tutti gli elementi non invertibili, ma non può contenere gli invertibili). Si ha $M = \{(a_i) \in A \mid a_1 = 0\}$ ed è immediato verificare che tale insieme è chiuso rispetto alla somma interna ed al prodotto per elementi di A. Sia $\pi = (0, p, p, p \dots)$, $\pi \in A$; vediamo che $M = (\pi)$. Chiaramente $(\pi) \subseteq M$ perché $\pi \in M$. D'altra parte sia $(a_i)_{i\geq 1} \in M$, allora $a_1 = 0$, $a_i = pb_i$ per ogni $i \geq 2$ e $a_{i+1} \equiv a_i \pmod{p^i}$, quindi $b_{i+1} \equiv b_i \pmod{p^{i-1}}$. Si può mostare per induzione che per ogni i è possibile scegliere $\tilde{b}_i$ tale che $\tilde{b}_i \equiv b_i \pmod{p^{i-1}}$ e $\tilde{b}_{i=1} \equiv \tilde{b}_i \pmod{p^i}$. Ne segue che $(\tilde{b}_2, \tilde{b}_2, \tilde{b}_3, \tilde{b}_4 \dots) \in A$ e $(a_i)_{i\geq 1} = \pi(\tilde{b}_2, \tilde{b}_2, \tilde{b}_3, \tilde{b}_4 \dots) \in (\pi)$.

(c) Sia I un ideale non nullo di A. Se $I = A$ la tesi vale con $k = 0$. Se $I \subsetneq A$ allora $I \subseteq M$; sia $k \geq 1$ il massimo esponente tale che $I \subseteq M^k = (\pi^k)$: poichè $I \not\subset M^{k+1}$ esiste un elemento $(a_i)_{i\geq 1} \in I$ tale che $a_i \equiv 0 \pmod{p^i}$ per $i \leq k$ e $a_{k+i} = p^k b_{k+i}$ per $i \geq 1$, dove $b_{k+i+1} \equiv b_{k+i} \pmod{p^i}$ e $b_{k+1} \not\equiv 0 \pmod p$. Ne segue che, scegliendo come nel punto precedente $\tilde{b}_{k+i+1} \equiv b_{k+i} \pmod{p^i}$ e $\tilde{b}_{k+i+1} \equiv \tilde{b}_{k+i} \pmod{p^{k+i}}$, e ponendo $\tilde{b}_i = \tilde{b}_{k+1}$ per $i \leq k$, si ha $(\tilde{b}_i)_{i\geq 1} \in A$ e $\pi^k = (a_i)_{i\geq 1}(\tilde{b}_i)_{i\geq 1} \in I$ da cui $I = M^k$.

Esercizio 4.
Sia $T = X^3 + X^{-3}$, consideriamo l'estensione di campi $\mathbb{C}(X) \supset \mathbb{C}(T)$.
a) Determinare il grado dell'estensione.
b) Mostrare che l'estensione è di Galois e determinare il gruppo di Galois.
c) Determinare le sottoestensioni e per ciascuna calcolare un elemento primitivo.

Soluzione esercizio 4 Chiamiamo $K := \mathbb{C}(X)$, $F := \mathbb{C}(T)$. Notiamo che $\alpha : X \mapsto 1/X$ e $\beta : X \mapsto \zeta_3 X$ sono due automorfismi di K che fissano F.

(a) Prima soluzione Siano $U = X + X^{-1}$ e $V = X^3$, $\mathbb{C}(U)$ e $\mathbb{C}(V)$ sono due sottocampi propri di K (non è necessario dimostrarlo, ma sono rispettivamente i sottocampi invarianti di α e β), che contengono F (per vedere che $\mathbb{C}(U)$ contiene F possiamo notare che $U^3 - 3U = T$). Il campo K è un'estensione di $\mathbb{C}(U)$ di grado 2 (basta vedere che il polinomio $x^2 - Ux + 1$ si annulla su X ed è irriducibile in $\mathbb{C}(U)$ perchè Δ non è un quadrato). Inoltre K è un'estensione di $\mathbb{C}(V)$ di grado 3 (il polinomio $x^3 - V$ si annulla su X ed è irriducibile in $\mathbb{C}(V)$ perchè nessuna delle radici è in $\mathbb{C}(V)$). Ne segue che K è un'estensione di F di grado multiplo di $2 \cdot 3$ e poichè $x^6 - Tx^3 + 1$ è un polinomo a coefficienti in F che si annulla in X, ne segue che il grado di K su F è esattamente 6 e $p(x) = x^6 - Tx^3 + 1$ è il polinomio minimo di X su F.

(a) Seconda soluzione Chiaramente X annulla il polinomio $x^6 - Tx^3 + 1 \in F[x]$; vediamo che tale polinomio è irriducibile. Vediamo che è irriducibile in $\mathbb{C}[T, x]$ e l'irriducibilità in $F[x]$ seguirà dal lemma di Gauss. Supponiamo $p(T, x) = x^6 - Tx^3 + 1 = a(T, x)b(T, x)$, poichè $p(T, x)$ ha grado 1 in T necessariamente uno tra $a(T, x)$ e $b(T, x)$ ha grado 0 in T, diciamo $a(T, x) = a(x)$. Questo però non è possibile perchè $p(t, x)$ è primitivo come polinomio in T. Ne segue che il polinomio $p(T, x)$ è irriducibile e qundi è il polinomio minimo di X su F, da cui poiché $K = F(X)$, $[K : F] = 6$.

(b) Le radici di $p(x)$ sono $X, \zeta_3 X, \zeta_3^2 X, X^{-1}, \zeta_3 X^{-1}, \zeta_3^2 X^{-1}$ che stanno tutte in K. Segue che K è il campo di spezzamento di $p(x)$ ed è dunque un'estensione di Galois. Gli elementi del gruppo di Galois sono determinati dall'immagine che associano a X ed è evidente che qualsiasi radice di $p(x)$ può essere ottenuta tramite opportune combinazioni di α e β. Dunque $G := \mathrm{Gal}(K/F) = \langle \alpha, \beta \rangle$. Si vede che α ha ordine 2 e β ha ordine 3. Inoltre $\alpha\beta\alpha = \beta^2$, dunque G è isomorfo a S_3.

(c) La sottoestensione invariante dispetto a $\langle \beta \rangle$ è $\mathbb{C}(V)$, infatti è β-invariante ed è un'estensione normale di F di grado 2. Le sottoestensioni $\mathbb{C}(U) = F(U), \mathbb{C}(X + \zeta_3 X^{-1}) = F(X + \zeta_3 X^{-1})$ e $\mathbb{C}(X +$

$\zeta_3^{-1}X^{-1}) = F(X + \zeta_3^{-1}X^{-1})$ sono tre estensioni di F di grado 3 invarianti rispettivamente per $\langle\alpha\rangle, \langle\alpha\beta\rangle$ e $\langle\alpha\beta^2\rangle$ e quindi sono i relativi campi fissi.