Scritto di Algebra II

5 Settembre 2017

1) Dimostrare che

a) Ogni gruppo di ordine 45 è abeliano.
b) Ogni gruppo di ordine 135 è nilpotente.

Soluzione. Denotiamo con $n_p(S)$ il numero di p Sylow in un gruppo finito S per un dato p.

Sia G il nostro gruppo. Nel caso a) $|G| = 3^2 \times 5$. Nel caso b) $|G| = 3^3 \times 5$.

Sia nel caso a) che nel caso b), $n_5(G)$ divide 27 ed è congruo a 1 modulo 5. Inoltre $n_3(G)$ divide 5 ed è congruo a 1 modulo 3.

Dunque $n_5(G) = 1 = n_3(G)$. Sia l'unico 5 Sylow H che l'unico 3 Sylow K sono normali.

Ne segue che che $G = K \times H$. Dunque G essendo prodotto dei suoi Sylow è nilpotente. Inoltre nel caso caso a) $|K| = 9 = 3^2$. Dunque K è abelianio come lo è H che è ciclico. Ne segue che G, essendo prodotto di gruppi abeliani è abeliano.

2) Sia G un gruppo finito nilpotente. Sia G un gruppo finito nilpotente. Si supponga che ogni suo sottogruppo di Sylow sia ciclico. Dimostrare che G è ciclico. Lo stesso è vero per gruppi risolubili?

Soluzione. Se G è nilpotente esso è prodotto dei suoi Sylow. Dunque

$$G = H_1 \times H_2 \times \cdots \times H_r$$

con gli H_i gruppi ciclici di ordine e due a due coprimi. In particolare G è abeliano.

Se prendiamo per ogni $i = 1, \ldots, r$ un generatore x_i di H_i, l'elemento $x_1 x_2 \cdots x_r$ ha ordine uguale a $|H_1||H_2| \cdots |H_r| = |G|$ e G è ciclico.

Se prendiamo $G = S_3$, G ha ordine 6. I suoi Sylow hanno ordine 2 e 3 e sono dunque ciclici ma G non è abeliano e dunque non è ciclico.

3) Sia $K = \mathbb{F}_{p^n}$. Si consideri l'applicazione $s : K \to K$ definita da $s(a) = a^2$. Dimostrare che

i) Se $p = 2$, s è suriettiva.
ii) Se $p > 2$, $|Im(s)| = (p^n + 1)/2$.
iii) Ogni elemento di K è somma di due quadrati.

Soluzione. Chiaramente $0^2 = 0$ e s si restringe ad un omomorfismo di gruppi moltiplicativi

$$s' : K^* \to K^*.$$

Il nucleo si s' consiste degli elementi $a \in K^*$ tali che $a^2 = 1$, ovvero $a = \pm 1$

Sia ora $p = 2$. Allora $1 = -1$, il nucleo di s' ha un solo elemento e dunque s è iniettiva. Dato che K è finito s è anche suriettiva provando i).

Se $p > 2$ $1 \neq -1$. Il nucleo di s' ha due elementi e l'immagine ha $|K^*|/2 = (p^n - 1)/2$ elementi. $K^2 = Im(s) = \{0\} \cup Im(s')$ ha dunque $(p^n - 1)/2 + 1 = (p^n + 1)/2$ dimostrando ii).

Ora sia $a \in K$, $|a - K^2| = |K^2| = (p^n + 1)/2$. Dunque $|a - K^2| + |K^2| = p^n + 1 > p^n$. Ne segue che $(a - K^2) \cap K^2 \neq \emptyset$. Si prenda allora $z = b^2 \in (a - K^2) \cap K^2$. $b^2 = a - c^2$ ovvero $a = b^2 + c^2$ mostrando iii).

4) Sia $\mathbb{Q} \subset K \subset \mathbb{C}$ un campo di spezzamento di $f(x) = x^3 - 3$ su $\mathbb{Q}$.
a) Determinare i campi L contenuti in K.
b) Esibire $z \in \mathbb{C}$ tale che $K = \mathbb{Q}(z)$.

Soluzione. Sia $\sqrt[3]{3}$ la radice terza reale di 3. Le radici di $x^3 - 3$ sono $\sqrt[3]{3}$, $\sqrt[3]{3}\alpha$, $\sqrt[3]{3}\overline{\alpha}$ con

$$\alpha = \frac{-1 + i\sqrt{3}}{2}$$

una radice primitiva terza di 1. Ne seque che

$$K = \mathbb{Q}(\sqrt[3]{3}, \alpha).$$

$[K : \mathbb{Q}] = 6$ con gruppo di Galois $G = S_3$. Dato che S_3 a parte i due sottogruppi ovvi ha quattro sottogruppi, uno di ordine 3 e tre di ordine 2, in K ci sono 6 sottocampi.

$$K,\ \mathbb{Q},\ \mathbb{Q}(\sqrt[3]{3}),\ \mathbb{Q}(\sqrt[3]{3}\alpha),\ \mathbb{Q}(\sqrt[3]{3}\overline{\alpha}),\ \mathbb{Q}(\alpha) = \mathbb{Q}(i\sqrt{3}).$$

Per trovare un $\beta \in K$ tale che $K = \mathbb{Q}(\beta)$, basta prendere un elemento in K che non sia fissato da alcun elemento del gruppo di Galois G. Sappiamo che G è il gruppo delle permutazioni delle radici di $x^3 - 3$. Inoltre se $g \in G$ ha ordine divisibile per 3, $g(i\sqrt{3}) = i\sqrt{3}$. Se g ha ordine 2, $g(i\sqrt{3}) = -i\sqrt{3}$.

Prendiamo $\beta = \sqrt[3]{3} + i\sqrt{3}$.

Se $g \in G$ ha ordine divisibile per 3 e $g(\beta) = \beta$ anche $g(\sqrt[3]{3}) = \sqrt[3]{3}$ dunque g è l'identità.

Se g ha ordine 2 e $g(\sqrt[3]{3}) = \sqrt[3]{3}$ allora $g(\beta) = \overline{\beta}$. Se $g(\sqrt[3]{3}) = \sqrt[3]{3}\alpha$ o $g(\sqrt[3]{3}) = \sqrt[3]{3}\overline{\alpha}$, Allora la parte reale di $g(\beta)$ è $-\sqrt[3]{3}/2$ che è diversa dalla parte reale di β.