

## COMPITO DI ALGEBRA 1

18 giugno 2019

- Sia  $G$  un gruppo di ordine  $8 \cdot 11 \cdot 19$ . Dimostrare che  $G$  contiene un sottogruppo normale di ordine  $11 \cdot 19$ .
  - Determinare il minimo intero  $n$  per cui  $\mathcal{S}_n$  contiene un sottogruppo di ordine  $8 \cdot 11 \cdot 19$ .

SOLUZIONE: (a) Sia  $G$  un gruppo di ordine  $8 \cdot 11 \cdot 19$ . Per i teoremi di Sylow, i sottogruppi di Sylow  $P_{11}$  e  $P_{19}$  relativi ai primi 11 e 19 sono normali: infatti il numero di 11-sottogruppi di Sylow è un divisore di  $8 \cdot 19$  congruo a 1 modulo 11, ed è facile verificare che 1 è l'unico tale divisore. Allo stesso modo, il numero di 19-sottogruppi di Sylow è un divisore di  $8 \cdot 11$  congruo ad 1 modulo 19, e nuovamente 1 è l'unico divisore con questa proprietà. Ne segue che  $H = P_{11}P_{19}$  è un prodotto di sottogruppi normali di  $G$  e dunque è esso stesso un sottogruppo normale di  $G$  dell'ordine voluto (si ha  $|P_{11}P_{19}| = |P_{11}| \cdot |P_{19}|$  in quanto gli ordini di questi sottogruppi sono relativamente primi fra loro, per cui l'intersezione  $P_{11} \cap P_{19}$  è banale).

(b) Il gruppo  $H$  costruito al punto precedente è anche ciclico, poiché  $11 \nmid 19 - 1$ . Il più piccolo intero  $n$  per cui  $\mathcal{S}_n$  contiene un sottogruppo di ordine  $11 \cdot 19$  è  $n = 11 + 19 = 30$ , poiché in  $\mathcal{S}_n$  ci devono essere elementi di ordine 11 e 19 che commutano fra loro. Supponiamo allora che  $G < \mathcal{S}_{30}$  contenga il sottogruppo  $H$  generato da due cicli disgiunti di ordine 11 e 19. Allora, visto che  $H \triangleleft G$ ,  $G$  deve essere contenuto nel normalizzatore  $N(H)$  di  $H$  in  $\mathcal{S}_{30}$ . Ma  $N(H)$  ha ordine  $11 \cdot 19 \cdot 10 \cdot 18$ , che non è divisibile per 8, quindi questo è assurdo. Considerando  $\mathcal{S}_{31}$  e nuovamente  $H$  il sottogruppo generato da due cicli disgiunti di ordine 11 e 19, si ottiene che la cardinalità del normalizzatore di  $H$  in  $\mathcal{S}_{31}$  è uguale alla precedente, quindi nemmeno  $\mathcal{S}_{31}$  contiene un gruppo  $G$  dell'ordine cercato.

Osserviamo comunque che il normalizzatore di  $H$  in  $\mathcal{S}_{30}$ , contiene un sottogruppo  $K$  di ordine  $4 \cdot 8 \cdot 19$  e cioè il sottogruppo generato da  $H$  e dalle due permutazioni

$$\begin{aligned} & (1, 11)(2, 10)(3, 9)(4, 8)(5, 7) \quad , \\ & (12, 30)(13, 29)(14, 28)(15, 27)(16, 26)(17, 25)(18, 24)(19, 23)(20, 22) \quad . \end{aligned}$$

Ne segue che  $\mathcal{S}_{32}$  contiene il sottogruppo  $G = K \times \langle (31, 32) \rangle$ , che ha ordine  $8 \cdot 11 \cdot 19$ , e quindi  $n = 32$  è il numero minimo cercato.

- Consideriamo il gruppo  $G = \text{GL}_2(\mathbb{F}_5)$ , ovvero il gruppo delle matrici  $2 \times 2$  con coefficienti in  $\mathbb{F}_5$  e determinante diverso da 0. Sia  $T$  il sottogruppo delle matrici triangolari superiori.

- (a) Dimostrare che  $T \cong \mathbb{Z}/5\mathbb{Z} \rtimes (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})$ .  
 (b) Determinare il numero di 5-Sylow di  $G$ .

SOLUZIONE:

- (a) Una matrice in  $T$  è della forma  $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$  con  $a, b, c \in \mathbb{F}_5$ . Il determinante di una tale matrice è  $ac$ , dunque è non nullo se e soltanto se  $a \neq 0, c \neq 0$ . Ne segue che ci sono  $4 = \#\mathbb{F}_5^*$  scelte per  $a$ , 4 scelte per  $c$ , e 5 scelte per  $b$ , dunque  $\#T = 80$ . L'insieme  $P_5$  formato dalle matrici  $\left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F}_5 \right\}$  è un sottogruppo di  $T$ . Questo è immediato da verificare direttamente: dal momento che siamo in un gruppo finito, è sufficiente verificare che il prodotto di due matrici in  $P_5$  sia ancora in  $P_5$ , e questo è ovvio:

$$\begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b_1 + b_2 \\ 0 & 1 \end{pmatrix} \in P_5.$$

Osserviamo che  $P_5$  è un sottogruppo di Sylow di  $T$ , perché è dell'ordine giusto; inoltre,  $P_5$  è l'unico 5-Sylow di  $T$ . Questo si può dimostrare o per verifica diretta, facendo vedere che  $P_5$  è normale in  $T$ , oppure con il seguente ragionamento: una matrice  $M$  di ordine 5 rispetta  $M^5 = \text{Id}$ , dunque i suoi autovalori sono radici del polinomio  $t^5 - 1 = (t - 1)^5$  in  $\mathbb{F}_5$ . Ne segue che gli autovalori di  $M$  sono entrambi uguali ad 1, e siccome  $M$  è triangolare per ipotesi deve essere della forma  $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ , ovvero deve stare in  $P_5$ . Siccome  $P_5$  contiene tutti gli elementi di ordine 5, esso è l'unico 5-Sylow di  $T$  e dunque è normale.

Infine, osserviamo che  $T$  contiene il sottogruppo  $D$  delle matrici diagonali, che è chiaramente isomorfo a  $\mathbb{F}_5^* \times \mathbb{F}_5^*$  tramite l'isomorfismo

$$\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \mapsto (a, c).$$

A sua volta,  $\mathbb{F}_5^* \times \mathbb{F}_5^*$  è isomorfo a  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ . Abbiamo ora tutti gli ingredienti necessari a concludere che  $T$  è un prodotto semidiretto:  $P_5$  è normale in  $T$ ,  $D$  è un sottogruppo di  $T$ , l'intersezione fra  $P_5$  e  $D$  è banale per motivi di cardinalità, e  $|P_5| \cdot |D| = 5 \cdot 4^2 = 80 = \#T$ . Questo ci dice che  $T \cong P_5 \rtimes D \cong \mathbb{Z}/5\mathbb{Z} \rtimes (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})$ .

- (b) Mostriamo che  $G$  possiede esattamente 6 sottogruppi di Sylow relativi al primo 5. Come noto dalla teoria, l'ordine di  $G$  è  $(5^2 - 1)(5^2 - 5) = 24 \cdot 20 = 2^5 \cdot 3 \cdot 5$ . Un 5-Sylow di  $G$  ha dunque ordine 5, e quindi in particolare il sottogruppo  $P_5$  identificato al punto precedente è un 5-Sylow di  $G$ . Abbiamo già stabilito

che  $P_5$  è normale in  $T$ , quindi il normalizzatore di  $P_5$  in  $G$ , chiamiamolo  $N$ , contiene  $T$ . Dal momento che il numero  $n_5$  di 5-Sylow di  $G$  è uguale a  $[G : N]$  per il secondo teorema di Sylow, e visto che  $T$  è contenuto in  $N$ , abbiamo che  $n_5 = [G : N] \mid [G : T] = 6$ . Per il terzo teorema di Sylow,  $n_5$  può allora essere soltanto 1 oppure 6 (questi sono gli unici divisori di 6 congrui ad 1 modulo 5). Basta ora escludere il caso  $n_5 = 1$ , e per far questo è sufficiente osservare che un altro sottogruppo di  $G$  di ordine 5 è dato da  $P'_5 = \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} : b \in \mathbb{F}_5 \right\}$ . Visto che  $G$  possiede almeno due 5-Sylow diversi, per quanto visto prima ne deve possedere esattamente 6.

3. Sia  $A$  un anello commutativo con identità, e sia  $\mathcal{P} = \{P_i\}_{i \in I}$  l'insieme dei suoi ideali primi. Supponiamo che per ogni  $i \neq j$  si abbia  $P_i \cap P_j = \{0\}$ . Dimostrare che:
- (a)  $A$  è un anello locale oppure è isomorfo ad un prodotto diretto di campi;
  - (b)  $\mathcal{P}$  contiene al massimo due elementi.

SOLUZIONE: (a) Per il lemma di Zorn,  $\mathcal{P}$  contiene almeno un elemento.

Supponiamo dapprima che  $\mathcal{P} = \{P\}$  abbia un solo elemento. Allora  $P$  è l'unico ideale massimale di  $A$ , quindi  $A$  è un anello locale (questo caso include quello in cui  $A$  è un campo).

Supponiamo ora che  $\mathcal{P}$  abbia almeno due elementi, e siano  $P \neq Q$  due elementi distinti di  $\mathcal{P} = \{P\}$ . Se uno dei due è contenuto nell'altro, allora  $P \cap Q = \{0\}$  implica che uno dei due sia uguale a  $\{0\}$  e l'altro sia l'unico ideale massimale, quindi  $A$  è un anello locale.

Se invece non ci sono contenimenti, allora  $P$  e  $Q$  sono ideali massimali distinti, per cui  $P + Q = A$ . Per il teorema cinese per anelli si ha

$$A \cong A/P \cap Q \cong A/P \times A/Q$$

e quindi  $A$  è isomorfo al prodotto diretto di due campi.

(b) Se  $P$  e  $Q$  sono ideali primi diversi da zero, la condizione  $P \cap Q = \{0\}$  implica che  $P$  e  $Q$  non sono contenuti uno nell'altro. Quindi ogni ideale primo diverso da zero è massimale.

Se ci sono due ideali primi diversi da zero, allora la soluzione del punto (a) dice che  $A$  è isomorfo ad un prodotto diretto di due campi, quindi  $\{0\}$  non è un ideale primo.

Supponiamo allora, per assurdo, che  $A$  contenga tre ideali primi distinti diversi da zero,  $P$ ,  $Q$  ed  $R$ . Allora  $\{0\} = P \cap Q \subseteq R$ . Dimostriamo che  $P \subseteq R$  oppure  $Q \subseteq R$ , contraddicendo la massimalità di  $P$  o di  $Q$ . Se così non fosse, ci sarebbe un elemento  $x \in P \setminus R$  ed un elemento  $y \in Q \setminus R$ . Ma allora avremmo che  $xy \in (P \cap Q) \setminus R$ , contraddizione.

4. Sia  $p(x) = 1 - x^2 + x^4 - x^6 + x^8 - x^{10} + x^{12}$  e sia  $K$  il suo campo di spezzamento su  $\mathbb{Q}$ .

- (a) Determinare il gruppo di Galois di  $K$  su  $\mathbb{Q}$ .
- (b) Per ognuno dei campi  $L$  con  $\mathbb{Q} \subseteq L \subseteq K$  e  $[L : \mathbb{Q}] = 2$ , descrivere  $L$  nella forma  $\mathbb{Q}(\sqrt{d})$  con  $d$  intero.
- (c) Quanti sono i campi  $F$  con  $\mathbb{Q} \subseteq F \subseteq K \cap \mathbb{R}$ ?

SOLUZIONE:

Osserviamo innanzitutto che  $p(x) = \sum_{j=0}^6 (-x^2)^j = \frac{1 - (-x^2)^7}{1 - (-x^2)} = \frac{1 + x^{14}}{1 + x^2}$ , che possiamo ulteriormente riscrivere nella forma

$$p(x) = \frac{(1 + x^{14})(1 - x^{14})}{(1 + x^2)(1 - x^{14})} = \frac{x^{28-1}}{(x^2 + 1)(x^{14} - 1)}.$$

Le radici di  $x^{28} - 1$  sono le radici 28-esime dell'unità (ognuna di queste è una radice semplice:  $x^{28} - 1$  non ha radici doppie), mentre le radici di  $x^2 + 1$  (risp. di  $x^{14} - 1$ ) sono le radici quarte (risp. 14-esime) dell'unità. Ne segue che il rapporto scritto sopra, e dunque anche  $p(x)$ , ha come radici precisamente le radici 28-esime dell'unità che non sono né radici quarte, né radici 14 di 1, ovvero proprio le radici *primitive* 28-esime dell'unità. Osserviamo che, come noto, ci sono  $\varphi(28) = 12$  tali radici, che è in effetti proprio il grado di  $p(x)$ .

- (a) Per quanto osservato sopra, il campo di spezzamento di  $p(x) = \Phi_{28}(x)$  è  $\mathbb{Q}(\zeta_{28})$ . Segue dalla teoria generale che il suo gruppo di Galois su  $\mathbb{Q}$  è  $(\mathbb{Z}/28\mathbb{Z})^* \cong (\mathbb{Z}/7\mathbb{Z})^* \times (\mathbb{Z}/4\mathbb{Z})^* \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .
- (b) Dal teorema di corrispondenza di Galois sappiamo che il numero di campi  $L$  come nel testo è uguale al numero di sottogruppi di  $G := \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  di indice 2. Un sottogruppo  $H$  di  $G$  di indice 2 contiene sicuramente  $2G = 2\mathbb{Z}/6\mathbb{Z} \times 2\mathbb{Z}/2\mathbb{Z}$ . Siccome la corrispondenza fra sottogruppi di  $G$  contenenti  $2G$  e sottogruppi di  $G/2G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  preserva l'indice, è sufficiente contare i sottogruppi di  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  di indice 2, che sono chiaramente tre. Dobbiamo quindi trovare tre campi quadratici contenuti in  $K$ . Osserviamo che  $K = \mathbb{Q}(\zeta_{28}) = \mathbb{Q}(\zeta_4, \zeta_7) = \mathbb{Q}(i, \zeta_7)$ , dunque un sotto-campo quadratico di  $K$  è evidente ed è dato da  $\mathbb{Q}(i)$ . Dalla teoria sappiamo inoltre che  $\mathbb{Q}(\zeta_7)$  contiene un unico sotto-campo quadratico, dato da  $\mathbb{Q}(\sqrt{-7})$  (il segno  $-$  è dovuto al fatto che  $7 \equiv 3 \pmod{4}$ ). Ne segue quindi che  $K$  contiene  $i$  e  $\sqrt{-7}$ , e dunque  $K$  contiene anche  $\sqrt{7}$ . Dal momento che i campi  $\mathbb{Q}(i)$ ,  $\mathbb{Q}(\sqrt{7})$  e  $\mathbb{Q}(\sqrt{-7})$  sono tutti diversi (questo è vero in quanto nessuno dei rapporti  $7/(-7)$ ,  $7/(-1)$ ,  $(-7)/(-1)$  è un quadrato in  $\mathbb{Q}$ ), abbiamo trovato i tre campi richiesti.

- (c) L'intersezione  $K \cap \mathbb{R}$  coincide con il sotto-campo di  $K$  fissato dal coniugio complesso. Sappiamo che  $\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/28\mathbb{Z})^\times$ , e tramite questo isomorfismo il coniugio complesso corrisponde a  $-1 \in (\mathbb{Z}/28\mathbb{Z})^\times$ . Dalla teoria di Galois sappiamo allora che  $\text{Gal}(K \cap \mathbb{R}/\mathbb{Q}) \cong (\mathbb{Z}/28\mathbb{Z})^\times / \{\pm 1\}$ ; osserviamo che  $K \cap \mathbb{R}$  è un'estensione di Galois di  $\mathbb{Q}$  in quanto il sottogruppo corrispondente, ovvero  $\{\pm 1\}$ , è normale in  $G$  (come ogni altro sottogruppo, visto che  $G$  è abeliano). Il gruppo  $(\mathbb{Z}/28\mathbb{Z})^\times / \{\pm 1\}$  è chiaramente abeliano (in quanto quoziente di un gruppo abeliano) e di cardinalità

$$\frac{\#(\mathbb{Z}/28\mathbb{Z})^\times}{\#\{\pm 1\}} = \frac{\varphi(28)}{2} = 6.$$

Come ben noto, esiste un unico gruppo abeliano di cardinalità 6, ovvero il gruppo ciclico di quest'ordine. Per corrispondenza di Galois, i sotto-campi di  $K \cap \mathbb{R}$  sono allora in bigezione con i sottogruppi di  $\mathbb{Z}/6\mathbb{Z}$ ; a loro volta, questi sono in bigezione con i divisori di 6, quindi i campi cercati sono 4 (di gradi 1, 2, 3, 6 su  $\mathbb{Q}$ ).