Corso di Algebra 2 - a.a. 2019-2020

Prova scritta del 14/07/2020

1. Siano A un dominio, M un A-modulo e M' un sottomodulo di M.
   (a) Dimostrare che, se M' e M/M' sono senza torsione, allora anche M è senza torsione.
   (b) Dimostrare che, se M' e M/M' sono di torsione, allora anche M è di torsione.
   (c) Dimostrare che, se A è a ideali principali, P_1 e P_2 sono due ideali massimali distinti di A, M' è di P_1-torsione e M/M' è di P_2-torsione, allora $M \cong M' \oplus M/M'$.

2. In ciascuno dei seguenti casi stabilire se esite un gruppo di ordine n che non contenga nessun sottogruppo di Sylow normale.
   (a) $24 < n < 30$.
   (b) $n = 80$.
   (c) $n = 180$.

3. Sia $f := (X^3 - X + 1)(X^2 + 1)$.
   (a) Determinare $\mathrm{G}_{\mathbb{F}_3}(f)$.
   (b) Dimostrare che $\mathrm{G}_{\mathbb{Q}(i)}(f) \cong S_3$.
   (c) Trovare un'estensione di campi $\mathbb{Q} \subseteq K$ tale che $\mathrm{G}_K(f) \cong \mathrm{G}_{\mathbb{F}_3}(f)$.

1. (a) Sia $x \in M$ di torsione, cioè tale che $ax = 0$ per qualche $a \in A \setminus \{0\}$. Si ha $M' = ax + M' = a(x + M')$, da cui segue $x + M' = M'$ (perché M/M' è senza torsione), cioè $x \in M'$. Poiché anche M' è senza torsione, da $ax = 0$ si ottiene allora $x = 0$, il che dimostra che M è senza torsione.

   (b) Per ogni $x \in M$ l'elemento $x + M' \in M/M'$ è di torsione, per cui esiste $a \in A \setminus \{0\}$ tale che $M' = a(x + M') = ax + M'$, e dunque $ax \in M'$. Per ipotesi anche ax è quindi di torsione, cioè esiste $b \in A \setminus \{0\}$ tale che $0 = b(ax) = (ba)x$. Poiché $ba \neq 0$ (essendo A un dominio), ciò dimostra che x è di torsione.

   (c) Notiamo intanto che, grazie al punto precedente, M è di torsione perché lo sono M' e M/M'. Si ha allora $M = \bigoplus_{P \in \mathrm{Max}(A)} \mathrm{T}_P(M)$. Dato che $M' \subseteq \mathrm{T}_{P_1}(M)$, se ne deduce che

$$M/M' \cong \mathrm{T}_{P_1}(M)/M' \bigoplus_{P \in \mathrm{Max}(A) \setminus \{P_1\}} \mathrm{T}_P(M).$$

   Poiché $\mathrm{T}_{P_1}(M/M') = \{0\}$ (visto che $M/M' = \mathrm{T}_{P_2}(M/M')$ e $P_2 \neq P_1$), il modulo $\mathrm{T}_{P_1}(M)/M'$ (che è chiaramente di P_1-torsione ed è isomorfo a un sottomodulo di M/M') deve essere nullo, cioè $M' = \mathrm{T}_{P_1}(M)$. Da questo segue che M' è un addendo diretto di M (con complementare $\bigoplus_{P \in \mathrm{Max}(A) \setminus \{P_1\}} \mathrm{T}_P(M)$), e dunque $M \cong M' \oplus M/M'$ (con $M/M' \cong \bigoplus_{P \in \mathrm{Max}(A) \setminus \{P_1\}} \mathrm{T}_P(M) = \mathrm{T}_{P_2}(M)$).

2. (a) Non esiste. Sia infatti G un gruppo di ordine n. Se $n = 25 = 5^2$ o $n = 27 = 3^3$ o $n = 29$, allora n è una potenza di un numero primo, e quindi G coincide con l'unico suo sottogruppo di Sylow, che è evidentemente normale. Se $n = 26 = 2 \cdot 13$, il 13-Sylow è normale perché di indice 2. Se $n = 28 = 2^2 \cdot 7$, il 7-Sylow è normale perché il numero s_7 di 7-Sylow soddisfa $s_7 \equiv 1 \mod 7$ e $s_7 \mid 4$, e quindi $s_7 = 1$.

   (b) Non esiste. Sia infatti G un gruppo di ordine $80 = 2^4 \cdot 5$. Si ha $s_5 \equiv 1 \mod 5$ e $s_5 \mid 16$, da cui $s_5 = 1$ o $s_5 = 16$. Se $s_5 = 1$, allora il 5-Sylow è normale. Se invece $s_5 = 16$, poiché ogni 5-Sylow ha ordine 5 (che è un numero primo), ogni 5-Sylow contiene $5 - 1 = 4$ elementi di ordine 5 e due 5-Sylow distinti si interescano solo nell'elemento neutro. Ne segue che l'insieme T degli elementi di G di ordine 5 ha cardinalià $16 \cdot 4 = 64$. Dato che ogni 2-Sylow di G (di ordine 16) è chiaramente contenuto in $G \setminus T$ e $\#(G \setminus T) = 80 - 64 = 16$, necessariamente $G \setminus T$ è l'unico 2-Sylow di G, ed è pertanto normale.

(c) Esiste: per esempio $G := A_5 \times C_3$. Infatti, essendo semplice, A_5 non ha sottogruppi di Sylow normali. Perciò per ogni primo p che divide $\#A_5 = 60$ ($p = 2, 3, 5$) esistono due p-Sylow distinti H e K di A_5. È chiaro che, se $p = 2$ o $p = 5$, allora $H \times \{1\}$ e $K \times \{1\}$ sono due p-Sylow distinti di G; analogamente, se $p = 3$, allora $H \times C_3$ e $K \times C_3$ sono due p-Sylow distinti di G. Questo dimostra che, per ogni primo p che divide $180 = 2^2 \cdot 3^2 \cdot 5$, G non ha un p-Sylow normale.

3. (a) $g := X^3 - X + 1$ e $h := X^2 + 1$ sono irriducibili in $\mathbb{F}_3[X]$ perché di grado 3 e 2 e senza radici in $\mathbb{F}_3$, come è immediato verificare. Allora un campo di spezzamento di $f = gh$ su $\mathbb{F}_3$ è $\mathbb{F}_3^d$ con $d = \mathrm{mcm}(\deg(g), \deg(h)) = 6$ e $\mathrm{G}_{\mathbb{F}_3}(f) \cong C_d = C_6$.

(b) $h = (X - i)(X + i)$ si spezza su $\mathbb{Q}(i)$, dunque $\mathrm{G}_{\mathbb{Q}(i)}(f) = \mathrm{G}_{\mathbb{Q}(i)}(g)$. Come si è visto nel punto precedente g è irriducibile in $\mathbb{F}_3[X]$, e quindi lo è anche in $\mathbb{Q}[X]$. Allora g non ha radici in $\mathbb{Q}(i)$ (se $\alpha \in \mathbb{Q}(i)$ fosse radice di g, si avrebbe $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [\mathbb{Q}(i) : \mathbb{Q}] = 2$, ma $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(\mathrm{m}_{\alpha,\mathbb{Q}}) = \deg(g) = 3$), e pertanto g è irriducibile anche in $\mathbb{Q}(i)[X]$ (avendo grado 3). Per concludere che $\mathrm{G}_{\mathbb{Q}(i)}(g) \cong S_3$ basta poi osservare che il discriminante $\Delta(g) = -4(-1)^3 - 27 \cdot 1^2 = -23$ non è un quadrato in $\mathbb{Q}(i)$ (se lo fosse si avrebbe $\sqrt{23}i \in \mathbb{Q}(i)$, e quindi $\sqrt{23} \in \mathbb{Q}(i) \cap \mathbb{R} = \mathbb{Q}$).

(c) Si può prendere $K = \mathbb{Q}(\delta)$ con $\delta := \sqrt{23}i$ tale che $\delta^2 = \Delta(g)$. Infatti, indicando con α una radice (complessa) di g, un campo di spezzamento di g (rispettivamente h) su K è $K(\alpha)$ (rispettivamente $K(i)$), e dunque un campo di spezzamento di f su K è $L := K(\alpha, i)$. Si ha $[K(\alpha) : K] = \deg(\mathrm{m}_{\alpha,K}) = \deg(g) = 3$ (g è irriducibile in $K[X]$, come si può vedere analogamente al punto precedente, usando il fatto che $[K : \mathbb{Q}] = 2$) e $[K(i) : K] = \deg(\mathrm{m}_{i,\mathbb{Q}}) = \deg(h) = 2$ (h è irriducibile in $K[X]$ perché $i \notin K$). Poiché $\mathrm{mcd}(3, 2) = 1$, si ottiene $[L : K] = 3 \cdot 2 = 6$, per cui $G := \mathrm{G}_K(f) = \mathrm{G}_K(L)$ ha ordine 6. Dato che $K \subseteq K(\alpha)$ è un'estensione normale (perché campo di spezzamento di g) di grado 3, per il teorema fondamentale della teoria di Galois $\mathrm{G}_{K(\alpha)}(L)$ è un sottogruppo normale di indice 3 di G. Dalla classificazione dei gruppi di ordine 6 si conclude che $G \cong C_6 \cong \mathrm{G}_{\mathbb{F}_3}(f)$.