COMPITO DI ALGEBRA 1

14 settembre 2021

Esercizio 1.
Siano p un numero primo, $A = \mathbb{Z}/p^3\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ e $\pi : A \to B$ un omomorfismo di gruppi surgettivo.

1. Dimostrare che B è abeliano.
2. Sia $B \cong \mathbb{Z}/p^{f_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{f_k}\mathbb{Z}$ con $f_i \geq 1$ per ogni $i = 1, \ldots, k$. Mostrare che $k \leq 3$.
3. Dimostrare che B **non** può essere isomorfo a $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$.

Soluzione.

1. Dato che π è surgettivo dal primo teorema di omomorfismo si ha $A/\ker\pi \cong B$, ed è noto che il quoziente di un gruppo abeliano è abeliano.
2. Consideriamo l'omomorfismo $\varphi : A \to B/pB$ dato dalla composizione dell'omomorfismo $\pi : A \to B$ e della proiezione canonica $B \to B/pB$. In quanto composizione di omomorfismi surgettivi, φ è surgettivo. Inoltre $\ker\varphi$ contiene pA, in quanto $\varphi(pa) = p\varphi(a) = 0$ per ogni $a \in A$. Dal primo teorema di omomorfismo otteniamo allora un omomorfismo surgettivo $A/pA \to B/pB$. Come visto a lezione (e come è facile da dimostrare), $A/pA \cong (\mathbb{Z}/p\mathbb{Z})^3$ e $B/pB \cong (\mathbb{Z}/p\mathbb{Z})^k$. L'esistenza di un omomorfismo surgettivo $(\mathbb{Z}/p\mathbb{Z})^3 \to (\mathbb{Z}/p\mathbb{Z})^k$ implica chiaramente $3 \geq k$.
3. Supponiamo per assurdo che esista un omomorfismo surgettivo $\pi : A \to B \cong \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$. Allora $pB = p\pi(A) = \pi(pA) = \pi(p\mathbb{Z}/p^3\mathbb{Z} \times \{0\} \times \{0\})$ sarebbe un gruppo ciclico, ma $pB \cong p\mathbb{Z}/p^2\mathbb{Z} \times p\mathbb{Z}/p^2\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ non è ciclico, assurdo.

Esercizio 2.

1. Sia $n > 4$ e sia H un sottogruppo di S_n. Dimostrare che se $[S_n : H] > 2$, allora $[S_n : H] \geq n$.
2. Determinare per quali interi positivi dispari d il gruppo S_6 ammette un sottogruppo di indice d.

Soluzione.

1. Sia $d = [S_n : H]$. Consideriamo l'azione di moltiplicazione a sinistra di S_n sull'insieme delle classi laterali S_n/H. Essa corrisponde ad un omomorfismo $\varphi : S_n \to S_{S_n/H} \cong S_d$. Il nucleo K di tale omomorfismo è un sottogruppo normale di S_n: dalla classificazione di tali sottogruppi normali (per $n > 4$) otteniamo allora che K è uno fra $\{\mathrm{id}\}$, A_n e S_n. Se $K = S_n$ o $K = A_n$, l'azione di S_n su S_n/H fattorizza tramite il gruppo S_n/K di ordine al massimo 2, e quindi l'orbita di ogni classe laterale ha cardinalità al massimo 2. Ma d'altro canto l'azione sulle classi laterali è transitiva (perché al variare di g la classe $g \cdot H = gH$ assume tutti i valori possibili), e quindi otteniamo che c'è un'unica orbita, di cardinalità al massimo 2. Questo significa $|S_n/H| \leq 2$, il che contraddice l'ipotesi. Ne segue che $K = \{\mathrm{id}\}$, e dunque S_n si immerge in S_d, da cui per ragioni di cardinalità $d \geq n$.

   Nota. La dimostrazione precedente è sostanzialmente quella del teorema di Poincaré. Applicando questo risultato si ottiene in effetti che se S_n ha un sottogruppo H di indice d con $2 < d < n$, allora ha anche un sottogruppo normale di indice k con $d \mid k \mid d!$, e quindi in particolare $k \neq 1, 2, n!$. Questo contraddice il fatto che gli unici sottogruppi normali di S_n sono $S_n, A_n, \{e\}$, di indici $1, 2, n!$.

2. L'indice di un sottogruppo divide la cardinalità del gruppo, quindi nel nostro caso d deve essere un divisore di $6! = 720 = 2^4 \cdot 3^2 \cdot 5$. Limitandosi ai divisori dispari dobbiamo quindi considerare $d \in \{1, 3, 9, 5, 15, 45\}$. Ovviamente S_6 ammette un sottogruppo di indice 1 (se stesso), e dal punto precedente sappiamo che non ci sono sottogruppi di indice 3 o 5. Sia P un 2-Sylow di S_6: allora $|P| = 16$ e quindi il suo indice è $720/16 = 45$. Un sottogruppo di indice 15 è ad esempio $S_4 \times S_2$, dove identifichiamo S_4 (rispettivamente S_2) al sottogruppo di S_6 che fissa gli elementi $\{5, 6\}$ (rispettivamente gli elementi $\{1, 2, 3, 4\}$). Resta solo da determinare se esista un sottogruppo di indice 9, o equivalentemente di cardinalità 80. Affermiamo che un tale sottogruppo H non esiste. Lo dimostriamo per assurdo: se H esistesse, dovrebbe contenere un elemento di ordine 5 (per Cauchy), ovvero un 5-ciclo, e un sottogruppo di ordine 16 (per i teoremi di Sylow). Un tale sottogruppo sarebbe anche un 2-Sylow di S_6, e quindi in particolare conterrebbe una trasposizione (si noti che la trasposizione $(1, 2)$ appartiene ad un 2-Sylow di S_6. Siccome tutti i 2-Sylow sono fra loro coniugati, ogni 2-Sylow di H, che è anche un 2-Sylow di S_6, contiene un coniugato di $(1, 2)$, che è ancora una trasposizione). A meno di coniugio (ovvero a meno di sostituire H con gHg^{-1}, che ha ancora cardinalità 80) possiamo supporre che il 5-ciclo sia $\sigma = (1, 2, 3, 4, 5)$. Sia poi $\tau = (a, b)$ una trasposizione contenuta in H.

   (a) Se $\{a, b\} \subseteq \{1, 2, 3, 4, 5\}$, e quindi sia σ che τ sono elementi di S_5 (considerato

come il sottogruppo di S_6 che fissa 6) allora per quanto visto nel corso σ e τ generano l'intero S_5, che ha $5! = 120 > 80$ elementi, assurdo;

(b) Se $a = 6$ o $b = 6$ (diciamo per simmetria $b = 6$), allora i coniugati $\sigma^i(a, 6)\sigma^{-i} = (\sigma^i(a), 6)$ di τ sono, al variare di i, tutte le trasposizioni della forma $(j, 6)$. Come noto, queste generano l'intero gruppo S_6, assurdo.

In conclusione, S_6 ammette un sottogruppo di indice d dispari per $d = 1, 15, 45$.

Esercizio 3. Sia K un campo e sia $S = \{f \in K[x] \mid f \text{ non ha radici in } K\}$.

1. Dimostrare che S è una parte moltiplicativa di $K[x]$.
2. Sia $A = S^{-1}K[x]$. Mostrare che gli ideali massimali di A sono tutti e soli quelli del tipo $S^{-1}(x - a)$ con $a \in K$.
3. Mostrare per ogni ideale massimale M di A si ha $A/M \cong K$.

SOLUZIONE.

1. Siano $f, g \in S$ e sia $h(x) = f(x)g(x)$. Se $h(x)$ avesse una radice $a \in K$ si avrebbe $0 = h(a) = f(a)g(a)$ e, dato che $f(a)$ e $g(a)$ appartengono al campo K, per il principio di annullamento del prodotto si avrebbe $f(a) = 0$ oppure $g(a) = 0$. Questo è assurdo dato che f e g appartengono a S, quindi $h \in S$ in quanto non ha radici in K. Inoltre $0 \in S$ e $1 \notin S$, quindi S è una parte moltiplicativa di $K[x]$.

2. Mostriamo per prima cosa che gli ideali massimali di A sono del tipo $S^{-1}(x - a)$ con $x - a \in K[x]$. Sia M un ideale massimale, in particolare M è un ideale primo quindi, per quanto visto a lezione, $M = S^{-1}P$ con P ideale primo di $K[x]$, con $P \neq \{0\}$ perché altrimenti non sarebbe massimale. Gli ideali di $K[x]$ sono principali e $P = (p(x))$ è un primo non nullo se e solo se $(p(x))$ è irriducibile. Se $p(x)$ non ha radici è invertibile in $A = S^{-1}K[x]$, quindi $S^{-1}(p(x)) = A$. Ne segue che se $S^{-1}(p(x))$ è massimale allora $p(x)$, che è irriducibile, deve avere una radice, quindi, a meno di moltiplicazione per una costante non nulla, possiamo scegliere $p(x) = x - a$ per un certo $a \in K$.

   Viceversa vediamo che ogni ideale di A generato da un polinomio del tipo $x - a$ è massimale. Infatti $S^{-1}(x - a)$ è un ideale proprio in quanto $1 \notin S^{-1}(x - a)$ perché l'equazione $1 = (x - a)\frac{r(x)}{s(x)}$ non ammette soluzioni con $r(x) \in K[x]$ e $s(x) \in S$ (altrimenti $s(x) = (x - a)r(x)$ mentre per ipotesi $s(x)$ non ha radici in K), quindi è contenuto in un ideale massimale, cioè $S^{-1}(x - a) \subseteq S^{-1}(x - b)$ per un certo $b \in K$. Questo vuol dire che $(x - a) = (x - b)\frac{r(x)}{s(x)}$ per certi $r(x) \in K[x]$ e $s(x) \in S$, quindi

$(x-a)s(x) = (x-b)r(x)$. Valutando l'ultima equazione in b si ha $(b-a)s(b) = 0$: dato che $s(x)$ non ha radici in K, si ha $a = b$ quindi l'ideale di A generato da $x - a$ è massimale.

3. Sia $\varphi_a \colon A \to K$ la mappa di valutazione in a, cioè la mappa definita da $r(x)/s(x) \to r(a)/s(a)$ per ogni $r(x) \in K[x]$ e $s(x) \in S$. Questa mappa è ben definita: infatti $s(a) \neq 0$ dato che $s(x) \in S$ quindi non ha radici in K; inoltre non dipende dal rappresentante che scegliamo per l'elemento di A, in quanto se $\frac{r(x)}{s(x)} = \frac{r_1(x)}{s_1(x)}$ con $r_1(x) \in K[x]$ e $s_1(x) \in S$, allora anche la loro valutazione in a coincide.

   Verifichiamo che la mappa φ_a è un omomorfismo di anelli: infatti

$$\begin{aligned}\varphi_a\left(\frac{r(x)}{s(x)} + \frac{r_1(x)}{s_1(x)}\right) &= \varphi_a\left(\frac{r(x)s_1(x) + r_1(x)s(x)}{s(x)s_1(x)}\right) = \frac{r(a)s_1(a) + r_1(a)s(a)}{s(a)s_1(a)} \\ &= \frac{r(a)}{s(a)} + \frac{r_1(a)}{s_1(a)} = \varphi_a\left(\frac{r(x)}{s(x)}\right) + \varphi_a\left(\frac{r_1(x)}{s_1(x)}\right)\end{aligned}$$

$$\begin{aligned}\varphi_a\left(\frac{r(x)}{s(x)} \cdot \frac{r_1(x)}{s_1(x)}\right) &= \varphi_a\left(\frac{r(x)r_1(x)}{s(x)s_1(x)}\right) = \frac{r(a)r_1(a))}{s(a)s_1(a)} \\ &= \frac{r(a)}{s(a)} \cdot \frac{r_1(a)}{s_1(a)} = \varphi_a\left(\frac{r(x)}{s(x)}\right) \cdot \varphi_a\left(\frac{r_1(x)}{s_1(x)}\right).\end{aligned}$$

   L'omomorfismo è surgettivo in quanto $\varphi_a(k) = k$ per ogni $k \in K$. Inoltre $\frac{r(x)}{s(x)} \in \ker(\varphi_a)$ se e solo se $\frac{r(a)}{s(a)} = 0$ cioè se $x - a \mid r(x)$. Questo dimostra che $\ker(\varphi_a) = (x-a) = I$ e dal primo teorema di omomorfismo si ha $A/I \cong K$.

Esercizio 4. Per ogni numero primo p sia K_p il campo di spezzamento su $\mathbb{Q}$ del polinomio $x^p - 2$.

1. Contare i sotto-campi di K_{11} di grado 2, 5 e 10 su $\mathbb{Q}$ e dimostrare che sono tutti contenuti in $\mathbb{Q}(\zeta_{11})$.

2. Dimostrare che K_7K_{11} è un'estensione di Galois di $\mathbb{Q}$ e che $\mathrm{Gal}(K_7K_{11}/\mathbb{Q}) \cong \mathrm{Gal}(K_7/\mathbb{Q}) \times \mathrm{Gal}(K_{11}/\mathbb{Q})$.

Soluzione. Il campo K_p è il composto di $\mathbb{Q}(\sqrt[p]{2})$ (di grado p su $\mathbb{Q}$, perché $x^p - 2$ è irriducibile per i lemmi di Gauss e Eisenstein) e $\mathbb{Q}(\zeta_p)$ (di grado $\varphi(p) = p - 1$). Siccome p e $p-1$ sono coprimi si ha quindi $\#\,\mathrm{Gal}(K_p/\mathbb{Q}) = [K_p : \mathbb{Q}] = p(p-1)$. In particolare, il gruppo di Galois di $K_p/\mathbb{Q}$ ha un unico p-Sylow, perché l'unico divisore di $p(p-1)$ congruo

ad 1 modulo p è 1. Per corrispondenza di Galois, K_p ha dunque un unico sotto-campo di grado $p-1$ su $\mathbb{Q}$ (corrispondente all'unico p-Sylow): questo sotto-campo è $\mathbb{Q}(\zeta_p)$, in quanto in effetti $[\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1$.

1. Sia $G_{11} = \mathrm{Gal}(K_{11}/\mathbb{Q})$. Un sotto-campo L come voluto corrisponde ad un sotto-gruppo H di G_{11} con $[G_{11}:H] = 2, 5, 10$. In particolare, $|H| = 55, 22$ o 11, e quindi H contiene un 11-Sylow (dunque l'unico 11-Sylow) P_{11} di G_{11}. Per corrispondenza di Galois, $L = K_{11}^H$ è contenuto nel campo fisso $K_{11}^{P_{11}}$, che come osservato sopra è $\mathbb{Q}(\zeta_{11})$. Si tratta quindi di contare i sotto-campi di $\mathbb{Q}(\zeta_{11})$ di grado $2, 5$ o 10 su $\mathbb{Q}$. Questi corrispondono ai sottogruppi di $\mathrm{Gal}(\mathbb{Q}(\zeta_{11})/\mathbb{Q}) \cong (\mathbb{Z}/11\mathbb{Z})^\times \cong \mathbb{Z}/10\mathbb{Z}$ di indice $2, 5, 10$: siccome $\mathbb{Z}/10\mathbb{Z}$ è un gruppo ciclico, per ogni $d = 2, 5, 10$ esiste un unico sottogruppo di indice d, e quindi un unico sotto-campo di K_{11} di grado d su $\mathbb{Q}$.

2. Un composto di estensioni di Galois è di Galois. Per quanto noto dalla teoria, per dimostrare che $\mathrm{Gal}(K_7K_{11}/\mathbb{Q}) \cong \mathrm{Gal}(K_7/\mathbb{Q}) \times \mathrm{Gal}(K_{11}/\mathbb{Q})$ basta far vedere che $K_7 \cap K_{11} = \mathbb{Q}$. Tale intersezione ha grado su $\mathbb{Q}$ che è un divisore di $([K_7:\mathbb{Q}], [K_{11}:\mathbb{Q}]) = (42, 110) = 2$. Se $L := K_7 \cap K_{11}$ non coincide con $\mathbb{Q}$, deve allora avere grado 2 su $\mathbb{Q}$ e quindi essere uno dei campi considerati al punto 1. In particolare, $L \subseteq \mathbb{Q}(\zeta_{11})$. Con un ragionamento identico otteniamo anche $L \subseteq \mathbb{Q}(\zeta_7)$. È noto dalla teoria che $\mathbb{Q}(\zeta_7, \zeta_{11}) = \mathbb{Q}(\zeta_{77})$ ha grado su $\mathbb{Q}$ uguale a $\varphi(77) = \varphi(7)\varphi(11) = [\mathbb{Q}(\zeta_7):\mathbb{Q}][\mathbb{Q}(\zeta_{11}):\mathbb{Q}]$. Siccome

$$\varphi(77) = [\mathbb{Q}(\zeta_7, \zeta_{11}):\mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_7):\mathbb{Q}] \cdot [\mathbb{Q}(\zeta_{11}):\mathbb{Q}]}{[\mathbb{Q}(\zeta_7) \cap \mathbb{Q}(\zeta_{11}):\mathbb{Q}]} = \frac{\varphi(77)}{[\mathbb{Q}(\zeta_7) \cap \mathbb{Q}(\zeta_{11}):\mathbb{Q}]},$$

dove si è usato il fatto che le estensioni $\mathbb{Q}(\zeta_7)/\mathbb{Q}$ e $\mathbb{Q}(\zeta_{11})/\mathbb{Q}$ sono di Galois, otteniamo $\mathbb{Q}(\zeta_7) \cap \mathbb{Q}(\zeta_{11}) = \mathbb{Q}$ come voluto.