Prova scritta di Algebra 2 - 8/9/2022

Esercizio 1.

(1) Classificare i gruppi abeliani di ordine 20.
(2) Calcolare la cardinalità dell'anello degli endomorfismi di ciascuno dei gruppi trovati.

(1) Dal teorema di classificazione, visto che $20 = 2^2 \cdot 5$ si ottiene subito ci sono solo due gruppi abeliani di ordine 20:

$$A_1 = (\mathbb{Z}/2)^2 \oplus \mathbb{Z}/5, \qquad A_2 = \mathbb{Z}/4 \oplus \mathbb{Z}/5.$$

(2) Se $f \in \operatorname{End} A_1$, allora f manda la 2-torsione in sé stessa e lo stesso per la 5-torsione. Dunque $f((\mathbb{Z}/2)^2) \subset (\mathbb{Z}/2)^2$ e $f(\mathbb{Z}/5) \subset \mathbb{Z}/5$. Dunque $\operatorname{End} A_1 = \operatorname{End}((\mathbb{Z}/2)^2) \oplus \operatorname{End}(\mathbb{Z}/5)$. Gli endomorfismi di $(\mathbb{Z}/2)^2$ come gruppo abeliano coincidono con i suoi endomorfismi come spazio vettoriale sul campo $\mathbb{Z}/2$. Dunque $\operatorname{End}((\mathbb{Z}/2)^2)$ coincide con l'anello delle matrici 2×2. Invece $\operatorname{End} \mathbb{Z}/5 = \mathbb{Z}/5$. Dunque la cardinalità di $\operatorname{End} A_1$ è $2^4 \cdot 5 = 80$.
Per A_2 invece si ha

$$\begin{aligned}
\operatorname{End} A_2 &= \operatorname{Hom}(\mathbb{Z}/4 \oplus \mathbb{Z}/5, \mathbb{Z}/4 \oplus \mathbb{Z}/5) = \\
&= \operatorname{Hom}(\mathbb{Z}/4, \mathbb{Z}/4) \oplus \operatorname{Hom}(\mathbb{Z}/4, \mathbb{Z}/5) \oplus \\
&\oplus \operatorname{Hom}(\mathbb{Z}/5, \mathbb{Z}/4) \oplus \operatorname{Hom}(\mathbb{Z}/5, \mathbb{Z}/5) = \\
&= \operatorname{Hom}(\mathbb{Z}/4, \mathbb{Z}/4) \oplus \operatorname{Hom}(\mathbb{Z}/5, \mathbb{Z}/5) = \\
&= \mathbb{Z}/4 \oplus \mathbb{Z}/5.
\end{aligned}$$

Quindi $|\operatorname{End} A_2| = 20$.

Esercizio 2.
Sia G un gruppo di ordine $1265 = 5 \cdot 11 \cdot 23$.

(1) Dimostrare che G possiede un sottogruppo normale.

Supponiamo ora che esista un morfismo non banale $f : G \to \mathbb{Z}/46$.

(2) Dimostrare che esiste un sottogruppo normale di G di ordine 55.
(3) Dimostrare che esiste un sottogruppo normale di G di ordine 11.

(1) $n_{23} = 1 + 23k \leq 5 \cdot 11$, dunque $k = 0, 1, 2$, ma solo per $k = 0$ otteniamo un divisore di 55. Dunque $n_{23} = 1$, $P_{23} \lhd G$.

(2) $\operatorname{Im} f$ è un sottogruppo di $\mathbb{Z}/46 = \mathbb{Z}/2 \times \mathbb{Z}/23$. Dunque $o(\operatorname{Im} f)$ deve essere uguale a $1, 2, 23$, o a 46. Siccome f non è banale, $o(\operatorname{Im} f) \neq 1$. Inoltre $\operatorname{Im} f = G/\ker f$, dunque $o(\operatorname{Im} f)$ divide $o(G)$. L'unica possibilità è che $o(\operatorname{Im} f) = 23$. Dunque $o(\ker f) = 55$ e $N := \ker f$ è il sottogruppo normale cercato.

(3) Consideriamo gli 11-Sylow di N: il loro numero è della forma $n_{11} = 1 + 11k$ e $n_{11} | o(N) = 5$. Dunque $n_{11} = 1$. Pertanto N contiene un solo 11-Sylow P_{11}. Questo pertanto è un sottogruppo caratteristico. Ma se P_{11} è caratteristico in N ed N è normale in G, allora P_{11} è normale in G.

Esercizio 3.
Sia E/F una estensione di campi e siano $\alpha, \alpha' \in E$.

(1) Per $f(X) \in F[X]$ e $\beta \in F(\alpha)$ definiamo un prodotto
$$f(X) \cdot \beta := f(\alpha)\beta$$
dove il prodotto a destra è quello di E. Verificare che con questo prodotto $F(\alpha)$ è un $F[X]$-modulo e calcolare il suo annullatore.

(2) Nello stesso modo definiamo una struttura di $F[X]$-modulo su $F(\alpha')$:
$$f(X) \cdot \beta' := f(\alpha')\beta', \qquad f(X) \in F[X], \beta' \in F(\alpha').$$
Dimostrare che se esiste un isomorfismo di campi $\eta : F(\alpha) \to F(\alpha')$ che è F-lineare e che soddisfa $\eta(\alpha) = \alpha'$, allora $F(\alpha)$ ed $F(\alpha')$ sono isomorfi come $F[X]$-moduli.

(3) Supponiamo che E sia il campo di spezzamento di un polinomio monico $f(X) \in F[X]$, che $\mathrm{Gal}(E/F)$ agisca transitivamente sulle radici di f. Dimostrare che allora $f(X) = p(X)^m$ dove $p(X)$ è un polinomio irriducibile.

(1)
$$\begin{gathered} f(X) \cdot (\beta + \beta') = f(\alpha)(\beta + \beta') = \\ = f(\alpha)\beta + f(\alpha)\beta' = f(X) \cdot \beta + f(X) \cdot \beta'. \end{gathered}$$
ecc.

Osserviamo che come modulo $F(\alpha) = F[X] \cdot 1$. Dunque

$$\begin{aligned}\operatorname{Ann} F(\alpha) &= \operatorname{Ann}(1) = \{f(X) \in F[X] : f(X) \cdot 1 = f(\alpha) = 0\} = \\ &= (m_{\alpha,F}).\end{aligned}$$

(2) Infatti η è anche un isomorfismo di $F[X]$-moduli:

$$\eta(f(X) \cdot \beta) = \eta(f(\alpha)\beta) = \eta(f(\alpha))\eta(\beta)$$

perché η è un morfismo di anelli. Inoltre $\eta(f(\alpha)) = f(\eta(\alpha)) = f(\alpha')$ perché η è F-lineare e $\eta(\alpha) = \alpha'$. Dunque

$$\eta(f(X) \cdot \beta) = f(\alpha')\eta(\beta) = f(X) \cdot \eta(\beta).$$

Questo dimostra che η è un morfismo di $F[X]$-moduli. Lo stesso ragionamento vale per η^{-1}, per cui η è un isomorfismo.

(3) Poiché f è monico, sarà un prodotto di fattori irriducibili monici. Basta dimostrare che questi sono tutti uguali. Siano dunque p e q due fattori irriducibili monici di f. Anche p e q si spezzano in E, dunque esisteranno una radice α di p ed una radice α' di q. Siccome α e α' sono anche radici di f esiste $\eta \in \operatorname{Gal}(E/F)$ tale che $\eta(\alpha) = \alpha'$. Ma allora η dà un isomorfismo $F(\alpha) \cong F(\alpha')$ sia come campi che come moduli per il punto (2). Dunque i due moduli hanno lo stesso annullatore. Dunque $m_{\alpha,F} = m_{\alpha',F}$. Ma essendo p e q irriducibili $m_{\alpha,F} = p$ e $m_{\alpha',F} = q$. Pertanto $p = q$.