Algebra 1

Esercizio 1. Dire per quali valori dei parametri interi α e β il sistema

$$\begin{cases} \alpha x \equiv 8 \mod 14 \\ x \equiv 2\beta \mod 6 \end{cases}$$

ha soluzioni. IL sistema ha soluzione se entrambe le equazioni hanno soluzione. Partiamo dalla seconda.

Per il Teorema Cinese del Resto l'equazione $x \equiv 2\beta \mod 6$ equivale a

$$\begin{cases} x \equiv 0 \mod 2 \\ x \equiv -\beta \mod 3 \end{cases}$$

essa ha soluzione per ogni valore di β e la soluzione $x = 2y$ è pari. Sostituendo nella prima equazione e dividendo per 2, otteniamo $\alpha y \equiv 4 \mod 7$ che ha soluzione se e solo se α è coprimo con 7.

Esercizio 2. Sia $q = p^h$ con p primo. Dire qualè l'ordine di un p-sottogruppo di Sylow del gruppo $GL_3(F_q)$ delle matrici 3×3 invertibili a coefficienti in F_q. Esibire un p-sottogruppo di Sylow $P < GL_3(F_q)$ espicito.

L'ordine di $GL_3(F_q)$ è il numero di basi ordinate di F_q^3. Queste possono contarsi nel modo seguente: il primo vettore può essere un qualsiasi vettore non nullo, quindi ci sono $q^3 - 1$ scelte, il secondo ogni vettore non nella retta generata dal precendete, quindi ci sono $q^3 - 3$ scelte, il terzo ogni vettore non nel piano generato dai primi due. Dunque si hanno in totale $(q^3 - 1)(q^3 - q)(q^3 - q^2)$ elementi e la massima potenza di p che divide tale numero è p^{3h}. Un esempio di tale gruppo è fornito dalle matrici triangolari superiori con 1 sulla diagonale.

Esercizio 3. Sia G un gruppo di ordine 196. Dimostrare che G ha un quoziente abeliano.

Risulta $196 = 2^2 7^2$. Dai teoremi di Sylow, esiste un unico 7-Sylow N, che è quindi normale. Il quoziente G/N ha ordine 4, ed è quindi ciclico o di Klein. In ogni caso è abeliano.

Esercizio 4. Siano A e B due anelli commutativi con unità. $f : A \to B$ un omomorfismo $\mathfrak{p} \subset B$ un ideale primo. Dimostrare che $f^{-1}(\mathfrak{p}) \subset A$ è un ideale primo. È vero in generale che se $\mathfrak{p}$ è massimale anche $f^{-1}(\mathfrak{p})$ lo è?

Sia $\mathfrak{q} = f^{-1}(\mathfrak{p})$; se $xy \in \mathfrak{q}$, allora $f(xy) \in \mathfrak{p}$, ma f è un omomorfismo, quindi $f(x)f(y) \in \mathfrak{p}$ e poiché $\mathfrak{p}$ è un ideale primo $f(x) \in \mathfrak{p}$ o $f(y) \in \mathfrak{p}$, ovvero $x \in \mathfrak{q}$, $y \in \mathfrak{q}$, come si voleva. L'asserzione analoga per gli ideali massimali è falsa; sia $i(n) = n/1$ l'immersione di $\mathbb{Z}$ in $\mathbb{Q}$. L'ideale (0) è massimale in $\mathbb{Q}$ (infatti $\mathbb{Q}/(0)$ è un campo) mentre $(0) = i^{-1}((0))$ non è evidentemente massimale in $\mathbb{Z}$.

Esercizio 5. Si consideri il polinomio $f(x) = x^4 + 6x^3 - 4x^2 + 10x - 6 \in F[x]$, con $F = \{\mathbb{Q}, \mathbb{F}_3, \mathbb{F}_5\}$. Si determini la cardinalità di $F[x]/(f(x))$ e quando tale anello è un campo.

$F[x]/(f(x))$ è in biezione con $F^{\deg f(x)}$ ed è un campo se e solo se $f(x)$ è irriducibile su F; questo è il caso se $F = \mathbb{Q}$ (si può usare il criterio di Eisenstein con $p = 2$); negli altri due casi il polinomio ha le radici $\overline{0}$ se $F = \mathbb{F}_3$ e $\overline{-1}$ se $F = \mathbb{F}_5$. Nel primo caso $\mathbb{Q}[x]/(f(x))$ è in biezione con $\mathbb{Q}^4$ ed è pertanto numerabile. Negli altri due casi la cardinalità è $3^4, 5^4$ rispettivamente.

Esercizio 6. Si consideri il polinomio $x^6 - 3 \in \mathbb{Q}[x]$ Sia $K \supset Q$ è il suo campo di spezzamento. Si determini il numero di campi $\mathbb{Q} \subset L \subset K$ con $[L : \mathbb{Q}] = 3$

Le radici di $x^6 - 3$ sono $\sqrt[6]{3}\omega^i$, $i = 0..,5$ ove ω è una radice primitiva sesta dell'unità. Si può prendere $\omega = 1/2 + i\sqrt{3}/2$, pertanto $K = \mathbb{Q}(\sqrt[6]{3}, \omega)$ è un'estensione Galoisiana di $\mathbb{Q}$ di grado 12. Il corrispondente gruppo di Galois è isomorfo al gruppo diedrale D_6, ed è generato dai $\mathbb{Q}$-automorfismi ϕ, ψ definiti da

$$\phi(\omega) = \omega^{-1},\ \phi(\sqrt[6]{3}) = \sqrt[6]{3}, \quad \psi(\omega) = \omega,\ \psi(\sqrt[6]{3}) = \omega\sqrt[6]{3}$$

Dal teorema di corrispondenza, il numero dei campi $\mathbb{Q} \subset L \subset K$ con $[L : \mathbb{Q}] = 3$ eguaglia il numero dei sottogruppi di ordine 4 di D_6. Ci sono tre tali sottogruppi

$$G_i = \{Id, \psi^3, \psi^i\phi, \psi^{i+3}\phi\}, \quad i = 0, 1, 2$$

Compito per l'esame da 9 crediti: esercizi, 1, 4, 5, 6 (solo il campo di spezzamento) e il seguente esercizio in due ore e mezzo

Esercizio 7. Sia G in gruppo finito e siano H, K sottogruppi normali di G di indice primo p tali che $H \cap K = \{1\}$. Dimostrare che G è un gruppo abeliano non ciclico di ordine p^2.

Dal teorema di corrispondenza segue che H, K, avendo indice primo, sono sottogruppi massimali di G (ovvero $H \leq S \leq G \implies H = S$ o $S = G$). Siccome HK è un sottogruppo di G contenente propriamente K, risulta $G = HK$ (in effetti $G = H \times K$) e

$$p = |G/H| = |HK/H| = |K/H \cap K| = |K|.$$

Similmente $|H| = p$. Allora G ha ordine p^2, dunque è abeliano, e non è ciclico perchè ha due sottogruppi dello stesso ordine.