Esercitazione Scritto Algebra I

(1) Dire per quali valori di $a \in \mathbb{Z}$ il seguente sistema di congruenze

$$\begin{cases} 5^{x^3-1} \equiv 2^a (\mathrm{mod}\, 13) \\ x^2 - 1 \equiv 0 \,(\mathrm{mod}\, 4) \end{cases}$$

è risolubile e risolverlo.

Soluzione: Osserviamo che 2 genera il gruppo moltiplicativo di $\mathbb{Z}/13\mathbb{Z}$, che è ciclico di ordine 12. Questo si può verificare considerando le prime sei potenze modulo 13 che sono $\{2, 4, 8, 16 \equiv 3, 6, 12 \equiv -1\}$. Quindi 2^a può assumere qualsiasi valore diverso da 0. Osserviamo inoltre che $5 \equiv -8 \equiv 2^9 (\mathrm{mod}\, 13)$. Quindi perché 2^a sia congruo a una potenza di 5 il valore di a deve essere un multiplo di 9 modulo 12. Le possibilità sono $\{9, 6, 3, 0\}$.

Dato che 5 ha ordine 4 nel gruppo moltiplicativo $\mathbb{Z}/13\mathbb{Z}^*$, dobbiamo guardare la classe di x^3-1 modulo 4. La seconda equazione impone $x = \pm 1 (\mathrm{mod}\, 4)$, quindi i valori possibili sono $x \equiv 1 (\mathrm{mod}\, 4), a \equiv 0 (\mathrm{mod}\, 12)$ e $x \equiv -1 (\mathrm{mod}\, 4), a \equiv 9^2 \equiv 6 (\mathrm{mod}\, 12)$.

(2) G è un gruppo di ordine 63, e P è un suo 7-Sylow.

- Mostrare che P è normale, e che G è prodotto semidiretto di P con un altro sottogruppo di G.
- Sia $f : G \to \mathrm{Aut}(P)$ l'omomorfismo che associa a ciascun elemento $g \in G$ il corrispondente automorfismo $P \ni x \mapsto gxg^{-1} \in P$. Mostrare che $\ker f$ contiene strettamente P.
- Mostrare che G non è isomorfo ad alcun sottogruppo del gruppo simmetrico S_9.

Soluzione:

- Il numero N_7 di 7-Sylow deve essere congruo 1 modulo 7 e dividere $63 = 7 \cdot 9$. L'unica possibilità è $N_7 = 1$, quindi P non ha coniugati oltre a se stesso, e conseguentmente è normale. Inoltre, dato un 3-Sylow Q di G, abbiamo che $P \cap Q = \{e\}$ perché gli ordini sono coprimi tra loro, e conseguentmente $PQ = G$. Questo implica immediatamente che $G = P \rtimes Q$.
- P ha ordine 7, quindi è ciclico. I suoi automorfismi di conseguenza sono uguali a $\mathbb{Z}/7\mathbb{Z}^* \simeq \mathbb{Z}/6\mathbb{Z}$. Dato che ogni elemento di G ha ordine dispari, l'immagine di $G \to \mathbb{Z}/6\mathbb{Z}$ deve essere contenuta in $\mathbb{Z}/3\mathbb{Z}$, il che implica che il kernel ha ordine almeno 21.
- Per il teorema di Cauchy il kernel di f contiene un elemento g di ordine 3. Un elemento sta nel kernel di f se e solo se commuta con un generatore di P. Consideriamo quindi un generatore h di P. L'ordine del prodotto di due elementi che commutano tra di loro è sempre il minimo comune multiplo degli ordini, quindi l'elemento hg ha ordine 21, ma S_9 non contiene nessun elemento di ordine 21, dato che un tale elemento dovrebbe contenere nella sua scrittura un 7-ciclo e un 3-ciclo disgiunti.

(3) Se $H < G$, allora $C(H) = \{g \in G \mid gh = hg \text{ per ogni } h \in H\}$ è il *centralizzatore* di H.

- Mostrare che $C(H)$ è un sottogruppo di G.
- Mostrare che se $H \lhd G$, allora $C(H) \lhd G$.

Soluzione:

- Chiaramente l'identità appartiene a $C(H)$. Se $a, b \in C(H)$ e $h \in H$, abbiamo $ab \cdot h = a \cdot h \cdot b = h \cdot ab$. rimane da dimostrare che se $a \in C(H)$ allora $a^{-1} \in C(H)$. Sappiamo che $a \cdot h = h \cdot a$. Moltiplicando a destra e sinistra per a^{-1}, otteniamo $h \cdot a^{-1} = a^{-1} \cdot h$.
- Siano $a \in C(H), h \in H, g \in G$. Allora $(gag^{-1})h(gag^{-1})^{-1} = ga(g^{-1}hg)a^{-1}g^{-1}$. Siccome H è normale, abbiamo $g^{-1}hg = h' \in H$. Quindi $(gag^{-1})h(gag^{-1})^{-1} = g(ah'a^{-1})g^{-1} = gh'g^{-1} = h$, il che dimostra che (gag^{-1}) commuta con h.

(4)
- Dimostrare che per ogni numero primo p e intero a, l'ideale $(p, x-a)$ è massimale in $\mathbb{Z}[x]$.
- Sia $f(x)$ un polinomio monico irriducibile in $\mathbb{Z}[x]$, di grado $n > 0$. Dimostrare che nessun polinomio nella forma $2 \cdot g(x) - 1$ appartiene all'ideale $(f(x))$.
- Sia $f(x)$ come sopra. Dimostrare che l'ideale $(f(x))$ non è mai massimale in $\mathbb{Z}[x]$.

Soluzione:
- Consideriamo la mappa $\psi : \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}$ data da $\psi(f) = [f(a)]$, la classe di $f(a)$ modulo p. È un morfismo di anelli perché è la composizione di $f \mapsto f(a) \in \mathbb{Z}$ e $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Chiaramente l'ideale $(p, x-a)$ è contenuto nel kernel di ψ. In generale, dato un polinomio $f \in \mathbb{Z}[x]$, usando l'algoritmo di Euclide otteniamo $f(x) = q(x)(x-a) + f(a)$. Questo dimostra che la classe di $f(a)$ è zero modulo p se e solo se $f(x) \in (p, x-a)$, quindi $(p, x-a) = \mathrm{Ker}(\psi)$. Dato che la mappa è suriettiva e $\mathbb{Z}/p\mathbb{Z}$ è un campo, $(p, x-a) = \mathrm{Ker}(\psi)$ è massimale.
- Assumiamo per assurdo che $2g(x) - 1 = f(x)h(x)$. Questo è equivalente a dire che $f(x)h(x) \equiv 1 \pmod 2$. Ma $\mathbb{F}_2[x]$ è un anello euclideo, quindi gli elementi invertibili hanno tutti grado zero, mentre $f(x)$ essendo monico ha grado positivo, assurdo.
  Dimostrazione alternativa: Assumiamo per assurdo che esistano $g(x)$ e $h(x)$ come sopra. Scriviamo $f(x) = a_0x^n + \ldots + a_n$, $h(x) = b_0x^m + \ldots + b_m$. Dato che $f(x)$ è monico, b_0 deve essere divisibile per due. Chiamiamo b_r il primo coefficiente non divisibile per due, che deve esistere in quanto il termine di grado 0 di $f(x)h(x)$ è dispari. Consideriamo il termine di grado $r+n$ di $f(x)h(x)$. Deve essere pari perché $r+n > 0$. È nella forma $a_0b_r + a_1b_{r-1} + \ldots + a_rb_0 = b_r + 2(\ldots)$, che è dispari, assurdo.
- Sia $\psi : \mathbb{Z}[x] \to \mathbb{Z}[x]/(f(x))$ la proiezione. Se l'ideale $(f(x))$ fosse massimale allora $\mathbb{Z}[x]/(f(x))$ sarebbe un campo, quindi l'immagine di 2 in $\mathbb{Z}[x]/(f(x))$ sarebbe 0 o invertibile. Se l'immagine di 2 è invertibile, scegliamo una controimmangine $g(x)$ del suo inverso. Allora $2g(x) - 1 \in \mathrm{Ker}(\psi) = (f(x))$ che è impossibile per il punto precedente. Inoltre chiaramente 2 non appartiene all'ideale $(f(x))$ perché tutti gli elementi dell'ideale hanno grado strettamente maggiore di 0. Quindi possiamo concludere che $\mathbb{Z}[x]/(f(x))$ non è un campo e conseguentemente $(f(x))$ non è un ideale massimale.

(5) Siano $\pm\alpha, \pm\beta \in \mathbb{C}$ le quattro radici distinte di $f(x) = (x^2-7)^2 + 15 \in \mathbb{Q}[x]$.
- Calcolare $\alpha\beta$; quanto vale $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]$?
- Calcolare $[\mathbb{Q}(\alpha+\beta) : \mathbb{Q}]$, $[\mathbb{Q}(\alpha-\beta) : \mathbb{Q}]$.
- Usando i punti precedenti, dimostrare che $f(x)$ è irriducibile su $\mathbb{Q}$.
- Determinare, utilizzando la corrispondenza di Galois, tutte le estensioni intermedie $\mathbb{Q} \subset L \subset \mathbb{Q}(\alpha)$ tali che $[L : \mathbb{Q}] = 2$.

Soluzione:
- Osserviamo che $\alpha = \sqrt{7 + \sqrt{-15}}$, $\beta = \sqrt{7 - \sqrt{-15}}$. Abbiamo $\alpha\beta = \sqrt{7^2 + 15} = 8$. Quindi $\beta = 8\alpha^{-1}$ e conseguentemente $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 1$.
- Consideriamo i quadrati $(\alpha+\beta)^2$, $(\alpha-\beta)^2$. Abbiamo $(\alpha+\beta)^2 = 7 + 7 + 2 \cdot 8 = 30$ e $(\alpha-\beta)^2 = 7 + 7 - 16 = -2$, quindi $\alpha + \beta = \pm\sqrt{30}$, $\alpha - \beta = \pm\sqrt{-2}$. In particolare $[\mathbb{Q}(\alpha+\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha-\beta) : \mathbb{Q}] = 2$.

- Dato che $\beta \in \mathbb{Q}(\alpha)$ abbiamo che $\alpha + \beta$ e $\alpha - \beta$ sono contenuti in $\mathbb{Q}(\alpha)$ che conseguentemente deve essere un'estensione di $\mathbb{Q}$ di grado almeno 4. Dato che $f(x)$ ha α come radice deve essere il suo polinomio minimo e quindi deve essere irriducibile.
- Dai punti precedenti possiamo concludere che $\mathbb{Q}(\alpha)$ è uguale a $\mathbb{Q}(\sqrt{-2}, \sqrt{30})$. Quindi il suo gruppo di Galois è $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, che ha esattamente 3 sottogruppi di indice 2. Conseguentemente $\mathbb{Q}(\alpha)$ ha esattamente 3 sottoestensioni distinte di grado 2. L'abbiamo già calcolate: sono $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-15})$ e $\mathbb{Q}(\sqrt{30})$.