**2° COMPITINO DI ALGEBRA 1**

21 dicembre 2018

**Soluzioni**

**1.** Sia $A$ un *anello booleano*, ovvero un anello (commutativo unitario) con la proprietà per ogni $x \in A$ si abbia $x^2 = x$. Dimostrare che

(a) $x + x = 0$ per ogni $x \in A$.

(b) Ogni ideale finitamente generato di $A$ è principale.

SOLUZIONE:

(a) Osserviamo che

$$x + x = (x + x)^2 = (x + x)(x + x) = x^2 + x^2 + x^2 + x^2 = x + x + x + x,$$

da cui, sommando ad entrambi i lati l'opposto di $x + x$, si ottiene come voluto $0 = x + x$.

(b) Per induzione sul numero di generatori è sufficiente mostrare che ogni ideale generato da 2 elementi è principale. Cerchiamo allora di trovare un generatore per l'ideale $(x, y)$. Ci si può aspettare che il generatore sia del tipo $g = a_0 + a_1x + a_2y + a_3xy$, con $a_0, \dots, a_3 \in \mathbb{F}_2$ (in effetti ogni polinomio in $x, y$ è equivalente ad un'espressione di questo tipo, visto che $x^2 = x$ e $y^2 = y$ e che abbiamo dimostrato che $A$ è di caratteristica 2). Osserviamo ora che

$$gx = a_0x + a_1x^2 + a_2xy + a_3x^2y = (a_0 + a_1)x + (a_2 + a_3)xy$$

e

$$gy = a_0y + a_1xy + a_2y^2 + a_3xy^2 = (a_0 + a_2)y + (a_1 + a_3)xy;$$

per avere $gx = x$ è quindi sufficiente che $a_0 + a_1 = 1$ e $a_2 + a_3 = 0$, e similmente per avere $gy = y$ basta che $a_0 + a_2 = 1$ e $a_1 + a_3 = 0$. Risolvendo il sistema

$$\begin{cases} a_0 + a_1 = 1 \\ a_2 + a_3 = 0 \\ a_0 + a_2 = 1 \\ a_1 + a_3 = 0 \end{cases}$$

si trova $a_1 = a_2 = a_3$ e $a_0 = 1 - a_1$, il che lascia due possibilità: o $g = 1$ (ma allora $(g) = A$, da escludere) o $g = x + y + xy$. In questo secondo caso quanto visto sopra mostra $x \in (g)$ e $y \in (g)$, e d'altro canto è chiaro che $g \in (x, y)$, dunque $(x, y) = (g)$.

**2.** Consideriamo l'anello $A = \mathbb{Q}[x, y]$ e il suo ideale $I = (x - y, x^3 + y^3 - x)$. Descrivere due campi $K_1, K_2$ ed un isomorfismo $A/I \cong K_1 \times K_2$.

SOLUZIONE: Mostriamo innanzitutto che l'ideale $I$ coincide con l'ideale $J = (x - y, 2x^3 - x)$. In effetti si ha $2x^3 - x = (x^3 + y^3 - x) + (x^3 - y^3) = (x^3 + y^3 - x) + (x - y)(x^2 + xy + y^2)$, quindi $2x^3 - x$ appartiene ad $I$, e viceversa $x^3 + y^3 - x = 2x^3 - x - (x - y)(x^2 + xy + y^2)$, quindi $x^3 + y^3 - x$ appartiene a $J$. Siccome $x - y$ appartiene sia ad $I$ che a $J$, ne segue come voluto che $I = J$. Il terzo teorema di isomorfismo per anelli fornisce

$$\frac{A}{I} \cong \frac{A/(x-y)}{I/(x-y)} \cong \frac{\mathbb{Q}[x]}{(2x^3 - x)},$$

dove l'isomorfismo $A/(x - y) \to \mathbb{Q}[x]$ è dato da $p(x, y) \mapsto p(x, x)$ (si osservi che valutando il polinomio $x^3 + y^3 - x$ in $y = x$ si ottiene proprio $2x^3 - x$). Siccome la fattorizzazione in irriducibili di $2x^3 - x$ in $\mathbb{Q}[x]$ è $x(2x^2 - 1)$ (e in particolare $x$ e $2x^2 - 1$ sono coprimi), il teorema cinese dei resti mostra che

$$A/I \cong \frac{\mathbb{Q}[x]}{(x)} \times \frac{\mathbb{Q}[x]}{(2x^2 - 1)} \cong \mathbb{Q} \times \mathbb{Q}(\sqrt{2}),$$

dove il secondo isomorfismo segue dal fatto che $2x^2 - 1 = 2(x^2 - \frac{1}{2})$, dove $x^2 - \frac{1}{2}$ è il polinomio minimo di $1/\sqrt{2}$, e dall'ovvio isomorfismo $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(1/\sqrt{2})$.

**3.** Siano $\alpha, \beta$ due elementi algebrici su $\mathbb{Q}$ di grado 3; siano poi, rispettivamente, $f(X)$ e $g(X)$ i polinomi minimi di $\alpha$ e $\beta$ su $\mathbb{Q}$ e $F$, $K$ i loro campi di spezzamento. Supponiamo che $[F : \mathbb{Q}] = 6$.

(a) Dimostrare che, se $\beta \notin F$, allora $[F(\beta) : F] = 3$.

(b) Determinare i possibili gradi di $FK$ su $\mathbb{Q}$.

(c) Determinare quante possono essere le sottoestensioni di $FK$ di grado 2 su $\mathbb{Q}$.

SOLUZIONE:

(a) Si ha $[F(\beta) : F] \leq [\mathbb{Q}(\beta) : \mathbb{Q}] = 3$ e $[F(\beta) : F] \geq 2$ dal momento che $\beta \notin F$. Ne segue che $[F(\beta) : F]$ è uguale a 2 o 3, e dobbiamo escludere il primo caso. Supponiamo che $[F(\beta) : F] = 2$: allora il polinomio $g(x)$, che è irriducibile in $\mathbb{Q}$, avrebbe una radice in $F$; ma siccome $F/\mathbb{Q}$ è un'estensione normale, questo implicherebbe che $g(x)$ avrebbe tutte le radici in $F$, e in particolare $\beta$ apparterrebbe ad $F$, assurdo.

Osserviamo che la medesima dimostrazione prova anche che se $\alpha \notin K$, allora $[K(\alpha) : K] = 3$.

(b) In quanto composto di due estensioni normali, $FK$ è un'estensione normale di $\mathbb{Q}$, con gruppo di Galois isomorfo a un sottogruppo di $\mathrm{Gal}(F/\mathbb{Q}) \times \mathrm{Gal}(K/\mathbb{Q})$. Dal momento che i due fattori separatamente sono sottogruppi di $S_3$, si ottiene che $\mathrm{Gal}(FK/\mathbb{Q})$ ha cardinalità che divide $(\#S_3)^2 = 36$. D'altro canto $FK$ contiene $F$, che ha grado 6 su $\mathbb{Q}$, quindi $6 \mid [FK : \mathbb{Q}] = \#\,\mathrm{Gal}(FK/\mathbb{Q})$. Le possibilità per $[FK : \mathbb{Q}]$ sono dunque a priori $6, 12, 18, 36$. Mostriamo che $6, 18, 36$ sono possibili, ma 12 no.

- Grado 6: sappiamo che esistono polinomi irriducibili a coefficienti razionali di grado 3 con campo di spezzamento di grado 6 (per esempio $x^3 - 2$). Basta prendere come $\alpha = \beta$ una radice di tali polinomi irriducibili per avere $FK = F = K$ di grado 6 su $\mathbb{Q}$.
- Grado 12. Supponiamo per assurdo che $[FK : \mathbb{Q}] = 12$. Se si avesse $\beta \in F$, allora il polinomio irriducibile $g(x)$ avrebbe una radice in $F$, e siccome $F/\mathbb{Q}$ è normale $g(x)$ si spezzerebbe completamente in $K$. Ma allora $K$ sarebbe contenuto in $F$, quindi $FK$ sarebbe uguale a $F$, e quindi sarebbe di grado al più 6, contraddizione. Ne segue che $g(x)$ non può avere radici in $F$, e quindi la parte (a) implica $[F(\beta) : F] = 3$, da cui $[FK : \mathbb{Q}]$ sarebbe divisibile per $[F(\beta) : \mathbb{Q}] = [F(\beta) : F][F : \mathbb{Q}] = 18$, assurdo.
- Grado 18. Consideriamo $\alpha = \sqrt[3]{2} \cdot \zeta_3$ e $\beta = \zeta_7 + \zeta_7^{-1}$. Allora il campo di spezzamento di $f(x)$ è di grado 6, mentre quello di $g(x)$ è di grado 3. Mostriamo che $[FK : \mathbb{Q}] = 18$. Certamente $6 \mid [FK : \mathbb{Q}]$, perché $[F : \mathbb{Q}] = 6$, quindi $[FK : \mathbb{Q}]$ può essere solo 6 o 18. Osserviamo poi che $FK$ contiene $K(\alpha)$, e in virtù della parte (a) il grado $[K(\alpha) : \mathbb{Q}] = [K(\alpha) : K][K : \mathbb{Q}] = 3[K(\alpha) : K]$ è uguale a 9 se $\alpha \notin K$. D'altro canto $K$ è contenuto in $\mathbb{R}$, mentre $\alpha$ per definizione non lo è, quindi $\alpha$ non può appartenere a $K$, e dalla discussione precedente si ha che $[K(\alpha) : \mathbb{Q}] = 9$. Ma questo grado divide $[FK : \mathbb{Q}]$, e quindi $[FK : \mathbb{Q}] = 18$.
- Grado 36. Consideriamo i polinomi $f(x) = x^3 - 2$ e $g(x) = x^3 - 2x - 2$, entrambi irriducibili per il criterio di Eisenstein, e siano $\alpha$ una radice del primo e $\beta$ una radice del secondo. I discriminanti dei due polinomi sono $-27(-2)^2 = -2^2 3^3$ e $-4(-2)^3 - 27(-2)^2 = -2^2 \cdot 19$, quindi $K$ contiene $\mathbb{Q}(\sqrt{-3})$ e $F$ contiene $\mathbb{Q}(\sqrt{-19})$. Dal momento che il rapporto fra $-19$ e $-3$ non è un quadrato in $\mathbb{Q}$, le estensioni $\mathbb{Q}(\sqrt{-19})$ e $\mathbb{Q}(\sqrt{-3})$ sono distinte, e quindi $FK$ contiene l'estensione di grado quattro $\mathbb{Q}(\sqrt{-19}, \sqrt{-3})$. Si ottiene allora che il grado di $FK$ su $\mathbb{Q}$ è divisibile per 4, quindi $[FK : \mathbb{Q}]$ è o 12 o 36. La prima possibilità è già stata esclusa, quindi $[FK : \mathbb{Q}] = 36$ come voluto.

(c) Siano $L_1, \ldots, L_r$ le sottoestensioni quadratiche di $FK$. Osserviamo che $F$ (e quindi a maggior ragione $FK$) contiene la sottoestensione quadratica che corrisponde per teoria di Galois al sottogruppo $A_3$ di $S_3 \cong \mathrm{Gal}(F/\mathbb{Q})$, ovvero

la sottoestensione $\mathbb{Q}(\sqrt{\Delta})$, dove $\Delta$ è il discriminante di $f(x)$. Ne segue che $r$ è almeno 1. Ricordiamo che il composito $L := L_1 \cdots L_r$ è un'estensione normale di $\mathbb{Q}$ di grado una potenza di 2, e più precisamente il suo gruppo di Galois è $(\mathbb{Z}/2\mathbb{Z})^t$ per qualche $t$ (maggiore o uguale a 1 per quanto visto prima). Inoltre $L$ è contenuto in $FK$, quindi $[L : \mathbb{Q}]$ divide $[FK : \mathbb{Q}]$, che a sua volta divide 36, quindi $[L : \mathbb{Q}] = 2^t$ può valere solo 2 o 4, quindi il gruppo di Galois $\mathrm{Gal}(L/\mathbb{Q})$ è isomorfo a $\mathbb{Z}/2\mathbb{Z}$ o a $(\mathbb{Z}/2\mathbb{Z})^2$. Nei due casi rispettivamente, $FK$ contiene esattamente una sottoestensione quadratica ($L$ stesso) o ne contiene 3 (corrispondenti ai tre sottogruppi di indice 2 di $(\mathbb{Z}/2\mathbb{Z})^2$). Come visto al punto precedente, entrambe le possibilità possono essere realizzate.