1 Campi di spezzamento

In ogni sezione viene dato un polinomio $P(X)$ a coefficienti interi e si discute il grado di un suo campo di spezzamento su $\mathbb{Q}$ e sui campi $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$.

1.1 $X^4 + X^2 + 1$

Trovare il grado di un campo di spezzamento di $P(X) = X^4 + X^2 + 1$ su $\mathbb{Q}$. Esaminando le fattorizzazioni di $P(X)$ in due fattori di grado 2 troviamo che

$$P(X) = (X^2 - X + 1)(X^2 + X + 1),$$

quindi i quattro zeri di $P(X)$ in $\mathbb{C}$ sono $\frac{1}{2}(\pm 1 \pm i\sqrt{3})$, cioè $e^{ki\pi/3} = (e^{i\pi/3})^k$ con $k = 1, 2, 4, 5$. Siccome gli zeri sono tutti potenze di $e^{i\pi/3}$, segue che il campo di spezzamento di $P(X)$ su $\mathbb{Q}$ contenuto in $\mathbb{C}$ è $\mathbb{Q}(e^{i\pi/3})$, ha grado 2. Infatti il polinomio minimo di $e^{i\pi/3}$ è il sesto polinomio ciclotomico, $X^2 - X + 1$.

- Sul campo $\mathbb{F}_2$ si ha $P(X) = (X^2 + X + 1)^2$ e $X^2 + X + 1$ è irriducibile quindi i campi di spezzamento di $P(X)$ hanno grado 2.
- Sul campo $\mathbb{F}_3$ si ha $P(X) = (X - 1)^2(X + 1)^2$ quindi $\mathbb{F}_3$, che ovviamente ha grado 1 su $\mathbb{F}_3$, è un campo di spezzamento di $P(X)$.
- Sul campo $\mathbb{F}_5$ si ha $P(X) = (X^2 + X + 1)(X^2 - X + 1)$ e i due fattori sono irriducibili perché hanno grado 2 e non hanno zeri in $\mathbb{F}_5$. I quattro zeri di $P(X)$ sono $\frac{1}{2}(\pm 1 \pm \alpha)$ dove α è tale che $\alpha^2 = 2$. Ne segue che $\mathbb{F}_5(\alpha) = \mathbb{F}_5[\alpha]$ è un campo di spezzamento per $P(X)$ su $\mathbb{F}_5$ e ha grado 2.

1.2 $X^3 + 2$

Trovare il grado di un campo di spezzamento di $P(X) = X^3 + 2$ su $\mathbb{Q}$. Siano $u = \sqrt[3]{2}$ e $\zeta = e^{i\pi/3}$. I tre zeri complessi di $P(X)$ sono $-u, \zeta u, \zeta^2 u$. Sia E il campo di spezzamento di $P(X)$ su $\mathbb{Q}$ contenuto in $\mathbb{C}$. Allora da $-u, \zeta u \in E$ segue $\zeta = -(\zeta u)/(-u) \in E$ per cui $E = \mathbb{Q}(u, \zeta)$. Ora u ha grado 3 su $\mathbb{Q}$ (il suo polinomio minimo è $X^3 - 2$, irriducibile per il criterio di Eisenstein) e ζ ha grado 2 su $\mathbb{Q}$ (il suo polinomio minimo è $X^2 - X + 1$, il sesto polinomio ciclotomico). Dalla formula dei gradi $[E : \mathbb{Q}] = [E : \mathbb{Q}(u)] \cdot [\mathbb{Q}(u) : \mathbb{Q}] = [E : \mathbb{Q}(u)] \cdot 3$ e $[E : \mathbb{Q}] = [E : \mathbb{Q}(\zeta)] \cdot [\mathbb{Q}(\zeta) : \mathbb{Q}] = [E : \mathbb{Q}(\zeta)] \cdot 2$, quindi $[E : \mathbb{Q}]$ è diviso da 2 e da 3, per cui è diviso da $2 \cdot 3 = 6$, essendo 2 e 3 coprimi. D'altra parte $[E : \mathbb{Q}] = [\mathbb{Q}(u, \zeta) : \mathbb{Q}] = [\mathbb{Q}(u)(\zeta) : \mathbb{Q}(u)] \cdot [\mathbb{Q}(u) : \mathbb{Q}] \leq 2 \cdot 3 = 6$ essendo il grado di ζ su $\mathbb{Q}(u)$ minore o uguale a 2, infatti ζ ha grado 2 su $\mathbb{Q}$. Segue che $[E : \mathbb{Q}] = 6$.

- Sul campo $\mathbb{F}_2$ si ha $P(X) = X^3$ quindi $\mathbb{F}_2$, che ovviamente ha grado 1 su $\mathbb{F}_2$, è un campo di spezzamento di $P(X)$.
- Sul campo $\mathbb{F}_3$ si ha $2^3 = 2$ quindi $X^3 + 2 = (X + 2)^3$ (ho applicato l'endomorfismo di Frobenius) quindi $\mathbb{F}_3$ è un campo di spezzamento di $P(X)$ e ha grado 1.

- Sul campo $\mathbb{F}_5$ si ha $P(2) = 0$ e applicando Ruffini otteniamo $P(X) = (X-2)(X^2+2X+4)$. Il polinomio X^2+2X+4 è irriducibile su $\mathbb{F}_5$, infatti ha grado 2 e non ha zeri in $\mathbb{F}_5$, quindi detto α un suo zero il campo $\mathbb{F}_5(\alpha) = \mathbb{F}_5[\alpha]$ è un campo di spezzamento per $P(X)$ su $\mathbb{F}_5$, e ha grado 2.

1.3 $X^6 + 1$

Trovare il grado di un campo di spezzamento di $P(X) = X^6+1$ su $\mathbb{Q}$. Ricordiamo che $X^3+1 = (X+1)(X^2-X+1)$. Sostituendo X con X^2 abbiamo allora $X^6+1 = (X^2+1)(X^4-X^2+1)$. Gli zeri complessi di questo polinomio sono $\pm i$ e $\pm e^{i\pi/6}$, $\pm e^{i5\pi/6}$, di cui gli ultimi quattro sono potenze di $\zeta = e^{i\pi/6} = \frac{1}{2}(\sqrt{3}+i)$. Ne segue che il campo di spezzamento E di $P(X)$ su $\mathbb{Q}$ contenuto in $\mathbb{C}$ è uguale a $\mathbb{Q}(i,\zeta) = \mathbb{Q}(\zeta,\sqrt{3})$. Si ha $\zeta - \zeta^5 = \frac{1}{2}(\sqrt{3}+i) - \frac{1}{2}(-\sqrt{3}+i) = \sqrt{3}$ quindi $\sqrt{3} \in \mathbb{Q}(\zeta)$ e segue che $E = \mathbb{Q}(\zeta)$ ha grado 4 su $\mathbb{Q}$.

- Sul campo $\mathbb{F}_2$ si ha $X^6+1 = (X^3+1)^2 = (X+1)^2(X^2+X+1)^2$ e X^2+X+1 è irriducibile, quindi ogni suo zero genera un campo di spezzamento per $P(X)$, che quindi ha grado 2.

- Sul campo $\mathbb{F}_3$ si ha $X^6+1 = (X^2+1)^3$ e X^2+1 è irriducibile, quindi ogni suo zero genera un campo di spezzamento per $P(X)$, che quindi ha grado 2.

- Sul campo $\mathbb{F}_5$ si ha $X^6+1 = (X^2+1)(X^4-X^2+1) = (X-2)(X-3)(X^4-X^2+1)$. Esaminando le fattorizzazioni di X^4-X^2+1 in due fattori di grado 2 troviamo $X^4-X^2+1 = (X^2+2X-1)(X^2-2X-1)$. Quindi i sei zeri di $P(X)$ sono 2, 3, $\pm 1 \pm \alpha$ dove α è un elemento che verifica $\alpha^2 = 2$. Quindi un campo di spezzamento di $P(X)$ su $\mathbb{F}_5$ è $\mathbb{F}_5(\alpha) = \mathbb{F}_5[\alpha]$, ha grado 2.

1.4 $X^6 + 3$

Trovare il grado di un campo di spezzamento di $P(X) = X^6+3$ su $\mathbb{Q}$. Sia $u := \sqrt[6]{3}$ e sia $\zeta = e^{i\pi/6} = \frac{1}{2}(\sqrt{3}+i)$. I sei zeri complessi di $P(X)$ sono $\pm\zeta u$, $\pm\zeta^3 u$, $\pm\zeta^5 u$. Sia E il campo di spezzamento di $P(X)$ su $\mathbb{Q}$ contenuto in $\mathbb{C}$. Allora si vede subito che $E = \mathbb{Q}(\zeta u, \zeta^2)$. Siccome $\zeta^2 = \frac{1}{2}(1+i\sqrt{3})$ si ha $E = \mathbb{Q}(\zeta u, i\sqrt{3})$. D'altra parte $i\sqrt{3} = (\zeta u)^3$ e quindi $E = \mathbb{Q}(\zeta u)$ ha grado 6 su $\mathbb{Q}$, essendo $P(X) = X^6+3$ il polinomio minimo di ζu su $\mathbb{Q}$ (irriducibile per il criterio di Eisenstein).

- Sul campo $\mathbb{F}_2$ si ha $X^6+3 = X^6+1$ e questo caso è stato discusso nell'esercizio precedente.

- Sul campo $\mathbb{F}_3$ si ha $X^6+3 = X^6$ quindi un campo di spezzamento di $P(X)$ su $\mathbb{F}_3$ è $\mathbb{F}_3$.

- Sul campo $\mathbb{F}_5$ si ha $3^3 = 2 = -3$ quindi X^2-3 divide X^6+3 (sto semplicemente dicendo che detto $T = X^2$, essendo $3^3+3 = 0$ per il teorema di Ruffini $T-3$ divide T^3+3) e applicando Ruffini troviamo $X^6+3=(X^2-3)(X^4+3X^2+4)$. Cercando le fattorizzazioni troviamo allora che $X^6+3=(X^2-3)(X^2+X+2)(X^2+4X+2)$. Detto α un elemento tale che $\alpha^2=3$ gli zeri di $P(X)$ sono $\pm\alpha$ e $\pm 3\pm 3\alpha$, quindi $\mathbb{F}_5(\alpha)=\mathbb{F}_5[\alpha]$ è un campo di spezzamento di $P(X)$ su $\mathbb{F}_5$ e ha grado 2.

1.5 X^4-2

Trovare il grado di un campo di spezzamento di X^4-2 su $\mathbb{Q}$. Sia $u=\sqrt[4]{2}$. I quattro zeri complessi di $P(X)=X^4-2$ sono $\pm u$, $\pm iu$. Sia E il campo di spezzamento di $P(X)$ su $\mathbb{Q}$ contenuto in $\mathbb{C}$, cioè $E=\mathbb{Q}(u,-u,iu,-iu)=\mathbb{Q}(u,iu)=\mathbb{Q}(u,i)$. Siccome $\mathbb{Q}(u)\subseteq\mathbb{R}$, $i\notin\mathbb{Q}(u)$ quindi siccome i ha grado 2 su $\mathbb{Q}$ (essendo zero di X^2+1), i ha grado 2 anche su $\mathbb{Q}(u)$ (tale grado è infatti al più 2 e non può essere 1 essendo $i\notin\mathbb{Q}(u)$). Dalla formula dei gradi

$$[E:\mathbb{Q}]=[\mathbb{Q}(u,i):\mathbb{Q}]=[\mathbb{Q}(u)(i):\mathbb{Q}(u)]\cdot[\mathbb{Q}(u):\mathbb{Q}]=2\cdot 4=8.$$

- Sul campo $\mathbb{F}_2$ si ha $P(X)=X^4$ quindi $\mathbb{F}_2$ è un suo campo di spezzamento, e ha grado 1.

- Sul campo $\mathbb{F}_3$ si ha $P(X)=X^4+1=(X^2+X+2)(X^2-X+2)$ (fattorizzazione ottenuta andando a cercare i fattori ma anche osservando che $P(X)=(X^2+2)^2-X^2$ e applicando il prodotto notevole) quindi gli zeri di $P(X)$ sono $2(\pm 1\pm\alpha)$ dove α è un elemento tale che $\alpha^2=2$. Segue che $\mathbb{F}_3(\alpha)=\mathbb{F}_3[\alpha]$ è un campo di spezzamento di $P(X)$ su $\mathbb{F}_3$ e ha grado 2.

- Sul campo $\mathbb{F}_5$ si ha che $P(X)=X^4-2$ è irriducibile (lo si dimostra cercando le fattorizzazioni a mano). Sia u un suo zero. Allora $P(X)=X^4-2=(X^2-u^2)(X^2+u^2)=(X+u)(X-u)(X^2-4u^2)=(X+u)(X-u)(X+2u)(X-2u)$. Quindi $\mathbb{F}_5(u)=\mathbb{F}_5[u]$ è un campo di spezzamento di $P(X)$ su $\mathbb{F}_5$ e ha grado 4.

Ricordo che quanto accade con $\mathbb{F}_5$ è generale: se F è un campo finito e $f(X)\in F[X]$ è un polinomio irriducibile con uno zero α in un'estensione di F allora $F(\alpha)$ è un campo di spezzamento di $f(X)$ su F.

1.6 X^4+2

Trovare il grado di un campo di spezzamento di $P(X)=X^4+2$ su $\mathbb{Q}$. Siano

$$\zeta=e^{i\pi/4}=\frac{\sqrt{2}}{2}(1+i),\qquad u=\sqrt[4]{2}.$$

I quattro zeri complessi di $P(X)$ sono ζu, $\zeta^3 u$, $\zeta^5 u=-\zeta u$ e $\zeta^7 u=-\zeta^3 u$. Sia $E\subseteq\mathbb{C}$ il campo di spezzamento di $P(X)$ su $\mathbb{Q}$, cioè $E=\mathbb{Q}(\zeta u,\zeta^3 u,\zeta^5 u,\zeta^7 u)$. Allora siccome E è un campo $E\ni(\zeta u)(\zeta^7 u)=\zeta^8 u^2=u^2$, $E\ni(\zeta u)^2=\zeta^2 u^2$ per cui anche $E\ni(\zeta^2 u^2)/u^2=\zeta^2=\frac{1}{2}(1+i)^2=i$. Ma allora essendo $\sqrt{2}=u^2$

si ha $\zeta = \frac{\sqrt{2}}{2}(1+i) = u^2(1+i)/2 \in E$ essendo $u, i \in E$. Ne segue che anche $E \ni (\zeta u)/\zeta = u$ e quindi

$$E = \mathbb{Q}(\zeta u, \zeta^3 u, \zeta^5 u, \zeta^7 u) = \mathbb{Q}(u, \zeta) = \mathbb{Q}(u, i).$$

Il grado di $\mathbb{Q}(u, i) = E$ su $\mathbb{Q}$ è 8, infatti $\mathbb{Q}(u)$ ha grado 4 su $\mathbb{Q}$ (perché il polinomio minimo di u su $\mathbb{Q}$ è $X^4 - 2$, irriducibile per il criterio di Eisenstein) i ha grado ≤ 2 su $\mathbb{Q}(u)$ (essendo i zero di $X^2 + 1$) e $i \notin \mathbb{Q}(u)$ essendo $\mathbb{Q}(u) \subseteq \mathbb{R} \not\ni i$ per cui i ha grado 2 su $\mathbb{Q}(u)$, quindi per la formula dei gradi

$$[E : \mathbb{Q}] = [\mathbb{Q}(u)(i) : \mathbb{Q}(u)] \cdot [\mathbb{Q}(u) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

- Sul campo $\mathbb{F}_2$ si ha $P(X) = X^4 + 2 = X^4$ quindi $\mathbb{F}_2$ è un campo di spezzamento per $P(X)$ su $\mathbb{F}_2$, e ha grado 1.
- Sul campo $\mathbb{F}_3$ si ha $P(X) = X^4 - 1 = (X^2 - 1)(X^2 + 1) = (X - 1)(X + 1)(X^2 + 1)$ quindi detto α uno zero di $X^2 + 1$, che è irriducibile, un campo di spezzamento è $\mathbb{F}_3(\alpha)$, ha grado 2.
- Sul campo $\mathbb{F}_5$ si vede che $P(X)$ è irriducibile studiando le fattorizzazioni e quindi, per la nota nell'esercizio precedente, un campo di spezzamento è $\mathbb{F}_5(\alpha)$ dove α è una qualsiasi radice di $P(X)$ in una qualche estensione di $\mathbb{F}_5$. Si può fare anche a mano, come per l'esercizio precedente, ottenendo $P(X) = X^4 - 3 = (X^2 - \alpha^2)(X^2 + \alpha^2) = (X - \alpha)(X + \alpha)(X - 2\alpha)(X + 2\alpha)$.

1.7 $X^4 + 4$

Trovare il grado di un campo di spezzamento di $P(X) = X^4 + 4$ su $\mathbb{Q}$. Risolvendo l'equazione biquadratica troviamo $X^2 = \pm 2i$ da cui i quattro zeri complessi di $P(X)$ sono $\pm(1 \pm i)$, quindi un campo di spezzamento per $P(X)$ è $\mathbb{Q}(i)$, e ha grado 2 su $\mathbb{Q}$.

- Sul campo $\mathbb{F}_2$ si ha $P(X) = X^4$ quindi $\mathbb{F}_2$ è un campo di spezzamento per $P(X)$ su $\mathbb{F}_2$, e ha grado 1.
- Sul campo $\mathbb{F}_3$ si ha $P(X) = X^4 + 1$ e questo caso è stato discusso nell'esercizio riguardante il polinomio $X^4 - 2$.
- Sul campo $\mathbb{F}_5$ si ha $P(X) = X^4 - 1 = (X^2 - 1)(X^2 + 1) = (X - 1)(X + 1)(X - 2)(X + 2)$ quindi $\mathbb{F}_5$ è un campo di spezzamento per $P(X)$ su $\mathbb{F}_5$, e ha grado 1.

1.8 $X^4 + 2X^2 + 9$

Trovare il grado di un campo di spezzamento di $P(X) = X^4 + 2X^2 + 9$ su $\mathbb{Q}$. Risolvendo l'equazione biquadratica otteniamo che gli zeri u di $P(X)$ verificano $u^2 = -1 \pm 2i\sqrt{2}$. Ora si ha $-1 \pm 2i\sqrt{2} = (1 \pm i\sqrt{2})^2$ per cui i quattro zeri complessi di $P(X)$ sono $\pm(1 \pm i\sqrt{2})$. Segue che $\mathbb{Q}(i\sqrt{2})$ è un campo di spezzamento per $P(X)$ su $\mathbb{Q}$ e ha grado 2.

- Sul campo $\mathbb{F}_2$ si ha $P(X) = X^4 + 1 = (X+1)^4$ quindi $\mathbb{F}_2$ è un campo di spezzamento per $P(X)$ su $\mathbb{F}_2$, e ha grado 1.
- Sul campo $\mathbb{F}_3$ si ha $P(X) = X^4 + 2X^2 = X^2(X^2-1) = X^2(X-1)(X+1)$ quindi $\mathbb{F}_3$ è un campo di spezzamento per $P(X)$ su $\mathbb{F}_3$, e ha grado 1.
- Sul campo $\mathbb{F}_5$ si ha $P(X) = X^4 + 2X^2 + 4$ e studiando le fattorizzazioni abbiamo $P(X) = (X^2 + 2X + 3)(X^2 - 2X + 3)$. Le radici di $P(X)$ sono quindi $\pm 1 \pm \alpha$ dove α è un elemento tale che $\alpha^2 = 3$. Segue che $\mathbb{F}_5(\alpha)$ è un campo di spezzamento di $P(X)$ su $\mathbb{F}_5$, ha grado 2.

2 Esercizi sul Lemma di Zorn

Nei seguenti esercizi è data una famiglia *non vuota* $\mathfrak{X}$ ordinata per inclusione e si richiede di mostrare che $\mathfrak{X}$ ha elementi massimali. La strategia è sempre la stessa: si applica il Lemma di Zorn. Si considera quindi una catena C in $\mathfrak{X}$, cioè un sottoinsieme totalmente ordinato di $\mathfrak{X}$, e si mostra che ammette un maggiorante in $\mathfrak{X}$, cioè che esiste un elemento $x \in \mathfrak{X}$ tale che $c \subseteq x$ per ogni $c \in C$. Per il Lemma di Zorn segue allora che $\mathfrak{X}$ ha elementi massimali.

1. Sia G un gruppo e siano $a \neq 1$ un suo elemento, S un suo sottoinsieme, con $1 \notin S$. Allora le seguenti famiglie $\mathfrak{X}$ di sottogruppi di G, ordinate per inclusione, sono non vuote e hanno elementi massimali: la famiglia dei sottogruppi di G che non contengono a, la famiglia dei sottogruppi di G disgiunti da S, e, quando S è finito, la famiglia dei sottogruppi di G che non contengono S.

2. Sia A anello commutativo unitario e siano S un sottoinsieme di A che non contiene 0, x un elemento non nilpotente di A (cioè $x^n \neq 0$ per ogni n intero positivo). Allora la famiglia $\mathfrak{X}$ degli ideali di A disgiunti da S, ordinata per inclusione, è non vuota e ha elementi massimali. Ora sia S l'insieme delle potenze di un elemento x di A non nilpotente, cioè $S = \{x^n \ : \ n \in \mathbb{N}_{>0}\}$ (S non contiene 0 essendo $0^1 = 0$). Mostrare che allora gli elementi massimali di $\mathfrak{X}$ sono ideali primi di A e dedurre che un elemento di A è nilpotente se e solo se appartiene a tutti gli ideali primi di A.

Esercizio 1. Osserviamo che in tutti e tre i casi $\{1\} \in \mathfrak{X}$, quindi $\mathfrak{X} \neq \emptyset$. Sia $C = \{H_\lambda\}_{\lambda \in \Lambda}$ una catena in $\mathfrak{X}$, e sia $H := \bigcup_{\lambda \in \Lambda} H_\lambda$. Certamente H è un maggiorante per C, essendo $H_\lambda \subseteq H$ per ogni $\lambda \in \Lambda$ (per definizione di unione). Rimane da dimostrare che $H \in \mathfrak{X}$, e per questo è necessario che H sia un sottogruppo di G.

- L'elemento neutro 1 di G appartiene ad H essendo $1 \in H_\lambda$ per ogni $\lambda \in \Lambda$ e quindi anche $1 \in H$.

- Sia $x \in H$ e mostriamo che $x^{-1} \in H$. Siccome $x \in H = \bigcup_{\lambda\in\Lambda} H_\lambda$ per definizione di unione esiste $\lambda \in \Lambda$ con $x \in H_\lambda$ per cui anche $x^{-1} \in H_\lambda$ (essendo H_λ un sottogruppo) quindi $x^{-1} \in H$ (per definizione di unione).
- Siano $x, y \in H$ e mostriamo che $xy \in H$. Siccome $H = \bigcup_{\lambda\in\Lambda} H_\lambda$ per definizione di unione esistono $\lambda, \mu \in \Lambda$ tali che $x \in H_\lambda$ e $y \in H_\mu$. Siccome l'inclusione induce in C un ordine totale (perché C è una catena) si ha $H_\lambda \subseteq H_\mu$ oppure $H_\mu \subseteq H_\lambda$. Nel primo caso $x \in H_\lambda \subseteq H_\mu \ni y$ quindi siccome H_μ è un sottogruppo di G, $xy \in H_\mu \subseteq H$ e quindi $xy \in H$. Nel secondo caso $y \in H_\mu \subseteq H_\lambda \ni x$ quindi siccome H_λ è un sottogruppo di G, $xy \in H_\lambda \subseteq H$ quindi $xy \in H$.

Per mostrare che $H \in \mathfrak{X}$ ci rimane da verificare una condizione, che è diversa nei tre casi.

- Caso 1. $\mathfrak{X} = \{K \leq G \ : \ a \notin K\}$. Dobbiamo quindi mostrare che $a \notin H$. Se fosse $a \in H$ allora per definizione di unione siccome $H = \bigcup_{\lambda\in\Lambda} H_\lambda$ esiste $\lambda \in \Lambda$ tale che $a \in H_\lambda$, e questo contraddice il fatto che $H_\lambda \in \mathfrak{X}$.
- Caso 2. $\mathfrak{X} = \{K \leq G \ : \ S \cap K = \emptyset\}$. Dobbiamo quindi mostrare che $S \cap H = \emptyset$. Se fosse $S \cap H \neq \emptyset$ allora esisterebbe $a \in S$ con $a \in H = \bigcup_{\lambda\in\Lambda} H_\lambda$, quindi per definizione di unione esiste $\lambda \in \Lambda$ tale che $a \in H_\lambda$ e siccome $a \in S$ questo contraddice il fatto che $H_\lambda \in \mathfrak{X}$.
- Caso 3. S è finito e $\mathfrak{X} = \{K \leq G \ : \ S \not\subseteq K\}$. Dobbiamo quindi mostrare che $S \not\subseteq H$. Scriviamo $S = \{a_1, \ldots, a_k\}$ e supponiamo per assurdo che sia $S \subseteq H$. Allora $a_i \in H$ per ogni $i = 1, \ldots, k$ quindi per definizione di unione siccome $H = \bigcup_{\lambda\in\Lambda} H_\lambda$ esistono $\lambda_1, \ldots, \lambda_k \in \Lambda$ tali che $a_i \in H_{\lambda_i}$ per ogni $i = 1, \ldots, k$. Siccome l'ordine in C indotto dall'inclusione è totale, esiste $j \in \{1, \ldots, k\}$ tale che $H_{\lambda_i} \subseteq H_{\lambda_j}$ per ogni $i = 1, \ldots, k$ (in un insieme totalmente ordinato i sottoinsiemi finiti hanno un unico minimo e un unico massimo), quindi $a_i \in H_{\lambda_j}$ per ogni $i = 1, \ldots, k$ cioè $S \subseteq H_{\lambda_j}$ e questo contraddice il fatto che $H_{\lambda_j} \in \mathfrak{X}$.

Esercizio 2. Osserviamo che $\{0\} \in \mathfrak{X}$, quindi $\mathfrak{X} \neq \emptyset$. Sia $C = \{I_\lambda\}_{\lambda\in\Lambda}$ una catena in $\mathfrak{X}$, e sia $I := \bigcup_{\lambda\in\Lambda} I_\lambda$. Certamente I è un maggiorante per C, essendo $I_\lambda \subseteq I$ per ogni $\lambda \in \Lambda$ (per definizione di unione). Rimane da dimostrare che $I \in \mathfrak{X}$, e per questo è necessario che I sia un ideale di A.

- 0 appartiene ad I essendo $0 \in I_\lambda$ per ogni $\lambda \in \Lambda$ e quindi anche $0 \in I$.
- Sia $x \in I$ e sia $a \in A$, mostriamo che $ax \in I$. Per definizione di unione siccome $I = \bigcup_\lambda I_\lambda$ esiste $\lambda \in \Lambda$ tale che $x \in I_\lambda$ per cui $ax \in I_\lambda$ essendo I_λ un ideale, quindi anche $ax \in I$ per definizione di unione. In particolare quando $a = -1$ otteniamo che $-x \in I$, cioè I contiene gli inversi additivi dei suoi elementi.

- Siano $x, y \in I$, mostriamo che $x+y \in I$. Siccome $I = \bigcup_{\lambda \in \Lambda} I_\lambda$ per definizione di unione esistono $\lambda, \mu \in \Lambda$ tali che $x \in I_\lambda$ e $y \in I_\mu$. Siccome l'inclusione induce in C un ordine totale (perché C è una catena) si ha $I_\lambda \subseteq I_\mu$ oppure $I_\mu \subseteq I_\lambda$. Nel primo caso $x \in I_\lambda \subseteq I_\mu \ni y$ quindi siccome I_μ è un ideale di A, $x+y \in I_\mu \subseteq I$ e quindi $x+y \in I$. Nel secondo caso $y \in I_\mu \subseteq I_\lambda \ni x$ quindi siccome I_λ è un ideale di A, $x+y \in I_\lambda \subseteq I$ quindi $x+y \in I$.

Per mostrare che $I \in \mathfrak{X}$ ci rimane da verificare che $S \cap I = \emptyset$. Se fosse $S \cap I \neq \emptyset$ allora esisterebbe $a \in S$ con $a \in I = \bigcup_{\lambda \in \Lambda} I_\lambda$, quindi per definizione di unione esiste $\lambda \in \Lambda$ tale che $a \in I_\lambda$ e siccome $a \in S$ questo contraddice il fatto che $I_\lambda \in \mathfrak{X}$.

Consideriamo ora il caso in cui $S = \{x^n \ : \ n \in \mathbb{N}_{>0}\}$ dove x è un elemento non nilpotente di A, cioè $x^n \neq 0$ per ogni $n \in \mathbb{N}_{>0}$. Sia P un elemento massimale di $\mathfrak{X}$ (abbiamo appena dimostrato che esiste). Mostriamo che è un ideale primo. Dobbiamo cioè mostrare che se $\alpha, \beta \in A$ con $\alpha\beta \in P$ allora almeno uno tra α e β appartiene a P. Supponiamo quindi per assurdo che sia $\alpha\beta \in P$ con $\alpha \notin P$ e $\beta \notin P$. Allora gli ideali $P + (\alpha)$ e $P + (\beta)$ contengono P propriamente, infatti α e β non appartengono a P. Siccome P è un elemento massimale di $\mathfrak{X}$ segue che $P + (\alpha), P + (\beta) \notin \mathfrak{X}$. In altre parole esistono n, m interi positivi con $x^n \in P + (\alpha)$ e $x^m \in P + (\beta)$, cioè esistono $a, c \in P$ e $b, d \in A$ con $x^n = a + \alpha b$, $x^m = c + \beta d$. Allora abbiamo

$$x^{n+m} = x^n x^m = (a + \alpha b)(c + \beta d) = ac + a\beta d + \alpha bc + \alpha\beta bd$$

e questo elemento appartiene a P, infatti $a, c \in P$, $\alpha\beta \in P$ e P è un ideale. Deduciamo che $x^{n+m} \in P$ e questo contraddice il fatto che $P \in \mathfrak{X}$. In conclusione, P è un ideale primo di A.

Sia ora $\mathcal{N}$ l'insieme degli elementi nilpotenti di A. Mostriamo che $\mathcal{N}$ è uguale all'intersezione degli ideali primi di A.

- ($\subseteq$). Se $x \in \mathcal{N}$ e I è un ideale primo di A allora esiste un intero positivo n con $x^n = 0 \in I$ e quindi, siccome I è un ideale primo, da $x \cdot x^{n-1} = x^n \in I$ segue $x \in I$ oppure $x^{n-1} \in I$, e per induzione concludiamo che $x \in I$. Quindi x appartiene a tutti gli ideali primi di A, quindi appartiene alla loro intersezione.

- ($\supseteq$). Sia x un elemento di A che appartiene a tutti gli ideali primi di A, e mostriamo che $x \in \mathcal{N}$. Se fosse $x \notin \mathcal{N}$ allora per quanto dimostrato sopra la famiglia $\mathfrak{X} = \{J \trianglelefteq A \ : \ x^n \notin J \ \forall n \in \mathbb{N}_{>0}\}$ ha un elemento massimale P, che come visto è un ideale primo di A. Siccome $P \in \mathfrak{X}$ si ha $x = x^1 \notin P$ e questo contraddice il fatto che x appartiene a tutti gli ideali primi di A.