Tutorato Aritmetica

Simone Cappellini & Diego Santoro
http://poisson.phc.dm.unipi.it/~cappellini
http://poisson.phc.dm.unipi.it/~santoro

18 giugno 2019

ATTENZIONE: i testi di alcuni esercizi (il 31 e il 33) avevano degli errori, che sono stati corretti. Vi preghiamo di farci notare eventuali altri.

Qui potete trovare alcuni esercizi da svolgere. Parte di questi sono stati, o saranno, svolti durante gli incontri. Può essere un ottimo allenamento provare ad esercitarsi e a scriverne per bene la soluzione. Chiunque voglia può consegnarci il proprio lavoro per avere un riscontro su quanto ha scritto.

Esercizio 1: Risolvere il seguente sistema di congruenze:

$$\begin{cases} 55x \equiv 1 & \pmod{87} \\ 20^{3x-2} \equiv 4 & \pmod{11}. \end{cases}$$

Esercizio 2: Risolvere il seguente sistema di congruenze:

$$\begin{cases} 3^x \equiv x^5 + 1 & \pmod{7} \\ x^2 \equiv 1 & \pmod{15}. \end{cases}$$

Esercizio 3: Discutere al variare di $a \in \mathbb{Z}$ la risolubilità del seguente sistema

$$\begin{cases} (6a-1)x \equiv 1 & \pmod{35} \\ x \equiv a & \pmod{21}. \end{cases}$$

Esercizio 4: Discutere la risolubilità del sistema al variare di $a \in \mathbb{Z}$ e quando possibile determinarne le soluzioni

$$\begin{cases} x^2 + x + 1 \equiv 0 & \pmod{13} \\ ax \equiv 27 & \pmod{78}. \end{cases}$$

Esercizio 5: Discutere la risolubilità del sistema al variare di $a \in \mathbb{Z}$ e quando possibile determinarne le soluzioni

$$\begin{cases} 7^x \equiv a & \pmod{8} \\ (x+a)^4 \equiv 0 & \pmod{200}. \end{cases}$$

Esercizio 6: Al variare di $a \in \mathbb{Z}$, determinare i valori interi di x per cui

$$\frac{1}{3}x^3 - \frac{8}{21}ax^2 + \frac{3}{7}x + \frac{1}{7}a$$

è intero.

Esercizio 7: Risolvere il seguente sistema di congruenze:

$$\begin{cases} 7^x \equiv 4 & (\text{mod } 9) \\ x^2 + 2x - 8 \equiv 0 & (\text{mod } 99). \end{cases}$$

Esercizio 8: Determinare in funzione dell'intero $a \in \mathbb{Z}$ il numero di soluzioni del sistema:

$$\begin{cases} 6x \equiv 4a & (\text{mod } 72) \\ 5x \equiv 2 & (\text{mod } 39). \end{cases}$$

Esercizio 9: Risolvere il seguente sistema di congruenze:

$$\begin{cases} x^{131} \equiv x & (\text{mod } 55) \\ x^6 + x \equiv 0 & (\text{mod } 125). \end{cases}$$

Esercizio 10: Determinare per quali valori dell'intero a il seguente sistema di congruenze è risolubile e determinarne le soluzioni:

$$\begin{cases} x^{27} \equiv x^2 & (\text{mod } 144) \\ 10x \equiv a & (\text{mod } 25) \\ 2^{x-1} \equiv 4 & (\text{mod } 11). \end{cases}$$

Esercizio 11: Sia G un gruppo e siano H e K due sottogruppi di G, con $H \subset K$. Dire quali delle seguenti affermazioni sono vere e trovare un controesempio per le false.

- Se $H \lhd K$, allora $H \lhd G$.
- Se $K \lhd G$, allora $H \lhd G$.
- Se $H \lhd K$ e $K \lhd G$, allora $H \lhd G$.

Esercizio 12: Mostrare che se H è un sottogruppo di G di indice 2, allora H è normale in G.

Esercizio 13: Sia $f : G \to G'$ un omomorfismo di gruppi. Dire quali delle seguenti affermazioni sono vere e trovare un controesempio per le false.

- Se H è un sottogruppo di G, allora $f(H)$ è un sottogruppo di G'.
- Se H' è un sottogruppo di G', allora $f^{-1}(H')$ è un sottogruppo di G.
- Se H è un sottogruppo normale di G, allora $f(H)$ è un sottogruppo normale di G'.
- Se H' è un sottogruppo normale di G', allora $f^{-1}(H')$ è un sottogruppo normale di G.
- Se f è surgettiva e H è un sottogruppo normale di G, allora $f(H)$ è un sottogruppo normale di G'.

Esercizio 14: Dato un gruppo G definiamo il *centro* di G come l'insieme $Z(G) = \{g \in G | gh = hg \ \forall h \in G\}$.

- Mostrare che $Z(G)$ è un sottogruppo di G.
- Mostrare che $Z(G)$ è un sottogruppo normale di G.

Esercizio 15: Dato un gruppo G definiamo $\mathrm{Aut}(G) = \{f : G \to G |\ f$ è un isomorfismo $\}$. Definiamo, inoltre, per ogni $g \in G$, la funzione $\varphi_g : G \to G$ definita da $\varphi_g(h) = ghg^{-1}\ \forall h \in G$.

- Mostrare che $\mathrm{Aut}(G)$ con l'operazione di composizione di funzioni è un gruppo.
- Mostrare che, per ogni $g \in G$, $\varphi_g \in \mathrm{Aut}(G)$.
- Indicato con $\mathrm{Int}(G)$ l'insieme $\mathrm{Int}(G) = \{\varphi \in \mathrm{Aut}(G) | \exists g \in G$ t.c. $\varphi = \varphi_g\}$, mostrare che $\mathrm{Int}(G)$ è un sottogruppo di $\mathrm{Aut}(G)$.
- Mostrare che $G/Z(G) \cong \mathrm{Int}(G)$.

Esercizio 16: Sia $f\colon G \longrightarrow G$ un omomorfismo da un gruppo G in sé tale che $f \circ f = f$. Mostrare che allora:

- $\mathrm{Ker}\, f \cap \mathrm{Im}\, f = \{e\}$;
- $G = \mathrm{Ker}\, f \cdot \mathrm{Im}\, f$.

Esercizio 17: Sia G un gruppo e sia $H < G$. Definiamo il centralizzatore di H in G come $Z(H) := \{g \in G \mid gh = hg\ \forall h \in H\}$. Dimostrare che:

- $Z(H)$ è un sottogruppo di G;
- Se $H \triangleleft G$ allora anche $Z(H) \triangleleft G$;
- Per ogni omomorfismo di gruppi $f\colon G \longrightarrow G'$ vale $f(Z(H)) \subseteq Z(f(H))$;
- Dare un esempio di un omomorfismo $f\colon G \longrightarrow G'$ e di un sottogruppo H di G tali che $Z(H) = G$ e $Z(f(H)) \neq G'$.

Esercizio 18: Fissato $n \geq 3$, sia $D_n := \left\{s^i r^j \;\middle|\; i, j \in \mathbb{Z},\ s^2 = r^n = e,\ srs = r^{-1}\right\}$, detto gruppo diedrale. Mostrare che:

- D_n è un gruppo finito non abeliano di cardinalità $2n$;
- Dimostra che $H = \left\{e, r^2\right\}$ è un sottogruppo normale di D_4;
- Trova i sottogruppi $Z(D_4)$ e $Z(H)$.

Esercizio 19: Contare il numero di elementi di ordine 4 e 12 in S_8.

Esercizio 20: Dimostrare i seguenti enunciati:

- Non esistono omomorfismi surgettivi da $\mathbb{Z}_6$ in S_3.
- Non esistono omomorfismi surgettivi da $\mathbb{Z}_3 \times \mathbb{Z}_4$ in S_3.
- Per ogni gruppo abeliano G e per ogni $n \geq 3$, non esistono omomorfismi surgettivi da G in S_n.

Esercizio 21: Dato $k \leq n$, il ciclo $\tau = (i_1, \ldots, i_k) \in S_n$ e la permutazione $\sigma \in S_n$ mostrare che vale:

$$\sigma\tau\sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_k)).$$

Dedurre che la struttura della decomposizione in cicli disgiunti viene conservata tramite il coniugio per elementi di S_n (ovvero che se $\sigma = c_1 \circ \cdots \circ c_k$ cicli disgiunti, con c_i un n_i-ciclo allora $\tau\sigma\tau^{-1} = \tilde{c}_1 \circ \cdots \circ \tilde{c}_k$ cicli disgiunti, dove $\tilde{c}_i$ è un n_i-ciclo per ogni $\tau \in S_n$).

Esercizio 22: Date le permutazioni $\sigma = (123)(456) \in S_6$ e $\tau = (132)(465) \in S_6$ esibire $\eta \in S_6$ tale che $\eta\sigma\eta^{-1} = \tau$.

Esercizio 23: Mostrare che se σ e τ in S_n hanno la stessa struttura nella decomposizione in cicli disgiunti allora sono coniugate (ovvero che se $\sigma = c_1 \circ \cdots \circ c_k$ cicli disgiunti, con c_i un n_i-ciclo e $\tau\sigma\tau^{-1} = \tilde{c}_1 \circ \cdots \circ \tilde{c}_k$ cicli disgiunti, dove $\tilde{c}_i$ è un n_i-ciclo per ogni $\tau \in S_n$, allora esiste $\eta \in S_n$ tale che $\eta\sigma\eta^{-1} = \tau$).

Esercizio 24: Sia $\sigma \in S_n$. Considerare la funzione $\chi : S_n \to S_n$ definita da $\chi(\tau) = \tau\sigma\tau^{-1}$ e mostrare che $\frac{|S_n|}{|Z(\sigma)|} = |Cl(\sigma)|$, dove $Z(\sigma) = \{\tau \in S_n | \tau\sigma\tau^{-1} = \sigma\}$ è il centralizzatore di σ e $Cl(\sigma) = \{\tau\sigma\tau^{-1} | \tau \in S_n\}$ è la classe di coniugio di σ. (Hint: provare ad usare le idee del primo teorema di omomorfismo, facendo attenzione al fatto che χ non è un omomorfismo)

Esercizio 25: Siano date le permutazioni $\tau = (12)(345)$ e $\sigma = (567)$ in S_9.

- Calcolare $\tau\sigma$ e calcolare gli ordini di σ,τ e $\tau\sigma$.
- Descrivere i centralizzatori di σ, τ e $\tau\sigma$ e in particolare calcolarne la cardinalità.

Esercizio 26: Si consideri il gruppo $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

- Determinare il numero degli elementi di ordine 6 e il numero dei sottogruppi ciclici di ordine 6 di G.
- Determinare i possibili ordini dei sottogruppi ciclici di G.

Esercizio 27: Sia G il gruppo $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$.

- Contare il numero di elementi di G di ogni possibile ordine.
- Determinare gli omomorfismi da G in $\mathbb{Z}/10\mathbb{Z}$.

Esercizio 28: Dimostrare che il centro di S_n è banale per $n \geq 3$.

Esercizio 29: Sia $(A, +, \cdot)$ un anello commutativo con identità e sia I un suo ideale. Mostrare che $(A/I, \tilde{+}, \tilde{\cdot})$ è un anello commutativo con identità, dove per definizione $[a]\tilde{+}[b] = [a + b]$ e $[a]\tilde{\cdot}[b] = [a \cdot b]$. (Attenzione: va dimostrato anche che tali operazioni sono ben definite).

Esercizio 30: Sia A un anello commutativo con identità e sia I un suo ideale.

- Mostare che I è primo $\Leftrightarrow$ A/I è un dominio.
- Mostrare che I è massimale $\Leftrightarrow$ A/I è un campo.

Esercizio 31: Siano A e B due anelli, sia $f : A \to B$ un omomorfismo di anelli, e indichiamo con J un ideale di B.

- Mostrare che $f^{-1}(J)$ è un ideale di A.
- Mostrare che se J è primo, allora anche $f^{-1}(J)$ è primo.
- Mostrare che se f è surgettivo e I è un ideale di A, allora $f(I)$ è un ideale di B.
- Mostrare che se f è surgettivo e J è massimale, allora anche $f^{-1}(J)$ è massimale.
- Trovare un controesempio per le ultime due affermazioni nel caso in cui f non sia surgettivo.

Esercizio 32: Dato A un anello commutativo con identità e data una famiglia arbitraria I_j di suoi ideali, dimostrare che $\bigcap_j I_j = \{a \in A | a \in I_j \forall j\}$ è un ideale di A. Dedurne che dato un qualsiasi sottoinsieme non vuoto S di A è ben definito l'ideale generato da S, definito come il più piccolo ideale di A che contiene S e indicato con (S). Mostrare che $(S) = \{a_1 s_1 + \dots a_n s_n | a_i \in A\, s_i \in S\}$.

Esercizio 33: Dato un anello commutativo con identità A e dati due elementi x e y in A, diciamo che x divide y se esiste $z \in A$ tale che $zx = y$, e in tal caso indichiamo $x|y$. Diciamo inoltre che un elemento non invertibile $a \in A$ è primo se per ogni coppia di elementi $b, c \in A$, $a|bc$ implica $a|b$ oppure $a|c$. Diciamo invece che un elemento non invertibile $a \in A$ è irriducibile se per ogni coppia $b, c \in A$ $a = bc$ implica che b è invertibile o che c è invertibile.

- Mostrare che $a \in A$ è primo se e solo se (a) è un ideale primo di A.
- Mostrare che se A è un dominio e $a \neq 0$, allora a primo $\Rightarrow$ a irriducibile.
- Mostrare che se A è un dominio, allora a è irriducibile se e solo se (a) è massimale tra gli ideali principali.[1]
- Mostrare che se A è un PID e $a \neq 0$ allora a irriducibile $\Rightarrow$ a primo.

Esercizio 34: Sia $f : G \to G'$ un omomorfismo di gruppi e sia H un sottogruppo di G. Poniamo $S_H = \{g \in G | f(gh) = f(hg) \forall h \in H\}$.

- Dimostrare che S_H è un sottogruppo di G;
- Dimostrare che se H è un sottogruppo normale di G allora anche S_H lo è;
- Dare un esempio in cui S_H non sia normale in G.

Esercizio 35: Contare il numero di omomorfismi $S_3 \to \mathbb{Z}/6\mathbb{Z}$.

Esercizio 36: Mostrare che dato un gruppo G e due elementi $g, h \in G$ vale $Z(hgh^{-1}) = hZ(g)h^{-1}$, dove come al solito con $Z(x)$ indichiamo il centralizzatore in G dell'elemento x.

Esercizio 37:
Contare il numero di omomorfismi iniettivi $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \to S_6$.

[1] Ricordiamo che un ideale I è detto principale se esiste $x \in A$ tale che $I = (x)$. Quindi l'esercizio chiede di mostrare che se $(a) \subset I$ con I principale, allora $I = A$ o $I = (a)$.

ESERCIZIO 38: Risolvere il sistema di congruenze:

$$\begin{cases} 3^{x^2+2} \equiv 5^x & (\text{mod } 11) \\ 16x^2 \equiv 1 & (\text{mod } 21). \end{cases}$$

ESERCIZIO 39:

- Dimostrare che $[2]_{13}$ è un generatore di $(\mathbb{Z}/13\mathbb{Z})^*$.
- Determinare i valori dell'intero a per cui la seguente congruenza ha soluzione

$$2^{2x} \equiv a \pmod{13}.$$

- Risolvere $2^{2x} \equiv 3^x \pmod{13}$.

ESERCIZIO 40: Sia G un gruppo. Consideriamo la relazione su G: $x \sim y$ se esiste $g \in G$ tale che $gxg^{-1} = y$.

- Dimostrare che $\sim$ è una relazione di equivalenza su G.
- Sia C_x la classe di equivalenza di x. Dimostrare che $C_x = \{x\}$ se e solo se $x \in Z(G)$.
- Dimostrare che per ogni $f \in Aut(G)$ ed ogni $x \in G$ esiste $y \in G$ tale che $f(C_x) = C_y$.

ESERCIZIO 41: Sia G un gruppo finito e sia N un suo sottogruppo normale.

- Dimostrare che per ogni $g \in G$, si ha che $o_{G/N}(gN)$ divide $o_G(g)$.
- Sia H un sottogruppo di G e supponiamo che $MCD(|G/N|, |H|) = 1$. Dimostrare che $H \subset N$.
- E' vero che se $H \subset N$ allora $MCD(|G/N|, |H|) = 1$?

.

ESERCIZIO 42: Sia $(G, \cdot)$ un gruppo abeliano. Consideriamo l'applicazione

$$\varphi : G \to G \times G$$

$$g \mapsto (g^2, g^{-1})$$

e l'applicazione

$$\pi : G \times G \to G$$

$$(g_1, g_2) \mapsto g_1 g_2^2$$

Dimostrare che

- φ e π sono omomorfismi di gruppi.
- φ è iniettiva.
- π è surgettiva.
- $\ker\pi = \text{Im}\varphi$.

Esercizio 43: Dato un anello commutativo $(A, +, \cdot)$ indichiamo con $\mathcal{D}$ l'insieme dei suoi divisori di zero e con A^* l'insieme dei suoi elementi invertibili. Inoltre diciamo che $a \in A$ è nilpotente se esiste un $n \in \mathbb{N}$ tale che $a^n = 0$, e indichiamo con $\mathcal{N}$ l'insieme degli elementi nilpotenti di A.

- Mostrare che l'insieme $(A^*, \cdot)$ è un gruppo abeliano.
- Mostrare che $\mathcal{N}$ è un ideale, e che $\mathcal{N} \subset \mathcal{D}$.
- Mostrare che se A è finito allora $A = \mathcal{D} \sqcup A^*$, dove il simbolo $\sqcup$ indica l'unione disgiunta. Dedurne che se A un dominio di integrità finito allora A è un campo.

Esercizio 44: Dati due anelli commutativi con identità A e A' diciamo che un omomorfismo di anelli $f : A \to A'$ è unitario se $f(1_A) = 1_{A'}$. Mostrare che se A' è un dominio allora ogni omomorfismo di anelli non nullo $f : A \to A'$ è unitario.[2]

Esercizio 45: Sia $\mathbb{K}$ un campo, sia $f(x)$ un polinomio non nullo in $\mathbb{K}[x]$ e si consideri $I = (f(x)) \in \mathbb{K}[x]$. Mostrare che $\mathbb{K}[x]/I$ è un campo se e soltanto se $f(x)$ è irriducibile in $\mathbb{K}[x]$. Altrimenti, se $f(x)$ è riducibile, $\mathbb{K}[x]/I$ ha zero divisori.

Esercizio 46: Sia $\mathbb{F} \subset \mathbb{K}$ una estensione di campi. Dato $\alpha \in \mathbb{K}$ diciamo che α è algebrico se esiste un polinomio f in $\mathbb{F}[x]$ tale che $f(\alpha) = 0$; diciamo che è trascendente altrimenti. Si consideri l'omomorfismo di anelli $v_\alpha : \mathbb{F}[x] \to \mathbb{K}$ definito da $v_\alpha(g) = g(\alpha)$.

- dimostrare che α è algebrico se e solo se il nucleo di v_α è diverso dall'ideale nullo.
- se α è algebrico chiamiamo *polinomio minimo di α su $\mathbb{F}$* il generatore monico di Ker v_α. Sia ora $p(x) \in \mathbb{F}[x]$ un polinomio che si annulla in α. Mostrare che $p(x)$ è il polinomio minimo di α su $\mathbb{F}$ se e solo se $p(x)$ è monico e irriducibile su $\mathbb{F}$.

Esercizio 47: Sia $K \subset L$ una estensione di campi. Sia $\alpha \in L$ un elemento algebrico su K di grado dispari. Dimostrare che $K(\alpha^2) = K(\alpha)$.

Esercizio 48: Sia $f : \mathbb{K} \to \mathbb{K}$ un omomorfismo di campi non nullo. Mostrare che $Fix_f = \{x \in \mathbb{K} | f(x) = x\}$ è un sottocampo di $\mathbb{K}$.

Esercizio 49: Trovare un campo $\mathbb{K}$, un naturale $n \geq 3$ e un polinomio $f \in \mathbb{K}[x]$ di grado n tale che il grado del campo di spezzamento di f su $\mathbb{K}$ sia $n!$.

Esercizio 50: Mostrare che se G è un gruppo infinito e H un suo sottogruppo di indice finito, allora H ha intersezione non banale con ogni sottogruppo infinito di G.
E' ancora vero se H è un sottogruppo non banale di G di indice infinito?

Esercizio 51: Dato G un gruppo e H un suo sottogruppo diciamo che H è un sottogruppo **caratteristico** di G se per ogni automorfismo φ di G vale $\varphi(H) = H$[3]. Diciamo che un sottogruppo proprio H è **massimale** se non esiste nessun sottogruppo proprio di G che lo contiene strettamente.

[2] Il docente del corso nella definizione di omomorfismo di anelli ha richiesto che fosse unitario. Questo esercizio mostra che in una varietà di casi abbastanza ampia questa richiesta non è particolarmente stringente.

[3] Questa uguaglianza è un'uguaglianza insiemistica, quindi non si richiede che tutti gli elementi di H siano tenuti fissi da φ.

- Mostrare che H caratteristico $\Rightarrow$ H normale.
- Mostrare che $Z(G)$ è caratteristico.
- Mostrare che l'intersezione di tutti i sottogruppi massimali di G è caratteristico.
- Mostrare un esempio in cui H è normale ma H non è caratteristico.

ESERCIZIO 52: Determinare, in funzione del parametro intero a, le soluzioni del sistema di congruenze

$$\begin{cases} 39x \equiv 2a & (\text{mod } 57) \\ x^2 \equiv 1 & (\text{mod } 12). \end{cases}$$

ESERCIZIO 53: Determinare, per un modulo opportuno, il numero di soluzioni del sistema di congruenze

$$\begin{cases} 5^{x^3} \equiv 8 & (\text{mod } 13) \\ x^{27} \equiv x^3 & (\text{mod } 13). \end{cases}$$

ESERCIZIO 54: Sia A un anello con la seguente proprietà: per ogni $x \in A$ esiste un $n \geq 2$, dipendente da x, tale che $x^n = x$. Mostrare che un ideale di A è primo se e solo se è massimale.

ESERCIZIO 55: Sia $K = \mathbb{Q}(i, \sqrt[3]{2})$.

- Calcolare il grado di K su $\mathbb{Q}$.
- Dimostrare che $K = \mathbb{Q}(i\sqrt[3]{2})$
- Calcolare il polinomio minimo f di $i\sqrt[3]{2}$ su $\mathbb{Q}$.
- K è il campo di spezzamento di f su $\mathbb{Q}$.

ESERCIZIO 56: Sia $\alpha \in \mathbb{C}$ una radice di $x^4 + 1$. Qual è la dimensione di $\mathbb{Q}(\alpha)$ su $\mathbb{Q}$? E' vero che $x^4 + 1$ si fattorizza come prodotto di fattori di grado 1 in $\mathbb{Q}(\alpha)$?

ESERCIZIO 57: Sia $\mathbb{K} = \mathbb{Q}[\sqrt{2}]$.

- Caratterizzare gli interi a per cui $\mathbb{Q}[a] = \mathbb{K}$.
- Al variare di a in $\mathbb{Z}$ calcolare il grado del campo di spezzamento del polinomio $x^2 - a$ su $\mathbb{K}$.

ESERCIZIO 58: Sia G un gruppo e sia $(H, +)$ un gruppo abeliano.

- Dimostrare che l'insieme $Hom(G, H)$ con l'operazione $\tilde{+}$ definita da $f\tilde{+}g(x) = f(x) + g(x)$ è un gruppo abeliano.
- Fissati $f, g \in Hom(G, H)$ mostrare che l'insieme $K = \{x \in G | f(x) = g(x)\}$ è un sottogruppo normale di G.
- Descrivere $(Hom(G, \mathbb{Z}), \tilde{+})$ con G gruppo finito.
- Descrivere $(Hom(\mathbb{Z}, \mathbb{Z}), \tilde{+})$.

ESERCIZIO 59: Risolvere il seguente sistema di congruenze.

$$\begin{cases} 2^{x^2} \equiv 8^{x-2} & (\text{mod } 11) \\ 5x \equiv 4 & (\text{mod } 22). \end{cases}$$

ESERCIZIO 60: Sia p un numero primo e sia $G = \{z \in \mathbb{C} | \exists n \in \mathbb{N} \text{ tale che } z^{p^n} = 1\}$.

- Dimostrare che G è un gruppo rispetto alla moltiplicazione.
- Dimostrare che un sottogruppo H di G è proprio se e solo se esiste un intero m tale che $z^{p^m} = 1$ per ogni $z \in H$.
- Dimostrare che ogni sottogruppo proprio di G è finito e ciclico.

ESERCIZIO 61: Sia $\alpha = \sqrt{5} + i \in \mathbb{C}$.

- Calcolare il polinomio minimo $f(x)$ di α su $\mathbb{Q}$.
- Calcolare il grado del campo di spezzamento del polinomio $f(x)$ su $\mathbb{Q}$ e su $\mathbb{F}_7$.